A comparison between risk and vulnerability methods

- applied to a Flue Gas Desulphurisation Facility (FGD) at a coal power plant in Germany

Svante Einarsson

Department of Fire Safety Engineering and Systems Safety
Lund University, Sweden

Brandteknik och Riskhantering
Lunds tekniska högskola
Lunds universitet

Report 5252, Lund 2008-04-15

A comparison between risk and vulnerability methods

- applied to a Flue Gas Desulphurisation Facility (FGD) at a coal power plant in Germany

Svante Einarsson
Lund 2008

Title
A comparison between risk and vulnerability methods - applied to a Flue Gas Desulphurisation Facility (FGD) at a coal power plant in Germany

By
Svante Einarsson

Report 5252
ISSN: 1402-3504
ISRN: LUTVDG/TVBB--5252—SE

Number of pages: 83
Illustrations: Svante Einarsson

Key words
Risk analysis, Vulnerability analysis, Flue Gas Desulphurisation (FGD), Preliminary analysis Event tree, An Approach to Vulnerability Analysis, mitigation

Abstract
This report describes the differences between a risk analysis and a vulnerability analysis, when applied to a Flue Gas Desulphurisation (FGD) facility. A Preliminary risk analysis complemented by an Event Tree analysis is compared with *An App-roach to Vulnerability Analysis of Complex Industrial Systems* by Einarsson and Rausand (1998). The focus of this report is to demonstrate the different steps of the different analyses, therefore comprehensively discuss major associated dangers for an FGD, but not to give a complete and detailed risk picture. The report points out advantages and disadvantages with the different analyses and is thus of helpful assistance when considering the option of choosing a risk- or a vulnerability analysis for an industrial system.

Department of Fire Safety Engineering and Systems Safety
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
http://www.brand.lth.se/english

Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

Brandteknik och Riskhantering

Lunds Universitet
Box 118
221 00 Lund

brand@brand.lth.se
http://www.brand.lth.se

Telefon: 046-222 73 60
Telefax: 046-222 46 12

Foreword

This thesis has been conducted to meet the requirements for a Master of Science degree in Risk Management and Safety Engineering and a Bachelor of Science degree in Fire Protection Engineering at the Department of Fire Safety Engineering and Systems Safety, Lund University, Sweden.

It is with highest gratitude that I like to thank the involved people for their support and guidance throughout the development of this thesis. Without them my work would have been in vain.

With that said I wish you all an enjoying and interesting time reading this thesis.
Svante Einarsson
Köln, April 2008

Sammanfattning

Utvecklingen och intresset för risk- och sårbarhetsanalyser växer för närvarande på bred front. Intresset är idag mest fokuserat mot ett samhällsperspektiv. Metoderna för analyser är av stort intresse för alla områden i samhället, även för industrin. Det är bakgrunden till målet med detta examensarbete, vilket jämför och visar på fördelarna och nackdelarna med de olika metoderna. För att uppnå detta har de två nämnda analysmetoderna applicerats på en rökgasreningsanläggning (FGD) vid ett kolkraftverk i Tyskland.

Den tekniska definitionen av risk presenteras vanligtvis som svaret på tre frågor:

- Vad kan hända? (dvs. Vad kan gå fel?)
- Hur troligt är det att det kommer att hända?
- Om det händer, vad är konsekvenserna?

Definitionen av sårbarhet är mer komplicerad och har i motsatt till risk ingen vedertagen accepterad definition. Sårbarhet kan dock enkelt förstås som motsatsen till robusthet och motståndskraft. Någonting som är robust har tolerans mot skada emot sig själv medan sårbarhet saknar denna kvalitet.

Båda termerna är använda i risk- och krishantering. Risk är oftare förknippat med riskhantering och sårbarhet med krishantering, men det är inte ovanligt att de blandas. En enkel förståelse av de två begreppen är att riskhantering handlar om att förebygga förluster medan krishantering handlar om att minimera förluster när en olycka redan har inträffat.

International Electrotechnical Commission (IEC) har givit definitionen av riskanalys som någonting som till stor del liknar den ovannämnda definitionen av risk. Möjliga hot är identifierade av faroidentifieringen, sannolikheten är bedömd med hjälp av frekvensanalys och konsekvensen är beräknad med hjälp av konsekvensanalys. Det finns en lång lista med olika riskanalyser med olika detaljeringsgrad. De kvalitativa analyserna är de mest generella och minst tidskrävande och de kvantitativa analyserna syftar till att ge en så precis riskbedömning som möjligt förknippad med så lite osäkerhet som möjligt.

Sårbarhetsanalyser varierar med de områden som de appliceras på. Detta examensarbete är koncentrerat på det ”öppna systemets” utgångsläge. Med ett öppet system fokuserar analysen sina ansträngningar mot att identifiera och värdera både de interna och externa hoten i ett system. Hot som tekniska fel och sabotage ska båda vara inkluderade i analysen.

Objektet som har legat till grund för utvärderingen av fördelar och nackdelar med risk- och sårbarhetsanalyser är en anläggning för att rena utsläppsgaserna från svavel hos ett kolkraftverk. Anläggningen består av ett antal stora metallrör och rum inklädda i gummi och plast. Gummit och plasten fungerar som ett rostskyddslager mot den starkt korrosiva gipsblandningen som används för reningsprocessen.

Den utförda faroidentifieringen för båda analyserna reflekterar skillnaderna i den öppna systemansatsen för sårbarhetsanalysen och den stängda systemansatsen för riskanalysen. Det högst signifikanta hotet identifierat av riskanalysen är en brand som börjar i gummit. Sårbarhetsanalysen framhäver i sin tur den mänskliga faktorn som det högst signifikanta hotet.

Djupstudien av brandrisken har gjorts med hjälp av ett händelseträd. Sannolikhetsuppskattningen för de olika ingående parametrarna har estimeras med sannolikhetsfördelningar och konsekvensen har antagits bli en totalförlust av FGD:n eller en mycket liten påverkan om branden blir släkt. Resultatet visar att medelvärdet för den årliga brandskadan är 1,78 millioner Euro. Resultatet är dock osäkert och varierar från den 5:e till den 95:e percentilen med 0,37 till 3,79 millioner Euros.

Djupstudien av den mänskliga faktorn presenterar fem olika scenarion som har värderats enligt Einarsson och Rausand (1998) och deras två-stegs sårbarhetsanalys. Resultatet visar att de förväntade skadorna är täckta till största del av företagets försäkring, med undantag av potentiella förluster i trovärde/anseende.

Slutsatser, som har varit tydliga i fråga om för- och nackdelar med de olika metoderna, är som följer:

- Den längre traditionen med riskanalyser, jämfört med sårbarhetsanalyser, har visat sig ha en positivare inverkan vid utförandet av analyserna på alla steg av riskanalysen.
- Ett av händelseträdets fördelar är möjligheten att kombinera många riskscenarion i ett och samma riskscenario.
- Händelseträdet presenterar en enkel och lättförstålig överblick hur man kan förstå en risk, som bör vara lätt för oinvigda läsare att förstå.
- Potentialen hos händelseträdet är väldigt stor när det gäller beräkning av exakta värden. Detta medför dessvärre problem med osäkerhet desto mer exakt analysen syftar till att vara.
- Det har visat sig att den mänskliga faktorn och externa hot till viss del är utelämnat i en traditionell riskanalys. Man kan emellertid inkludera även dessa aspekter i en riskanalys.
- Ansatserna inför sårbarhetsanalyser är mycket vid. Det bör i de flesta fall anses positivt att vidga hotspektrat. Det är dock problematiskt att hantera irrelevanta hot och att fatta beslut om vilka av dem som är relevanta respektive irrelevanta.
- De ursprungliga orsakerna till mänskliga fel, såsom organisatoriska fel, är adresserade i sårbarhetsanalysen men negligerade i IEC standarden för riskanalyser.
- Tidsspannet för de olika analyserna, har i tidigare studier uppgetts variera betydligt. Det har dock i denna studie visats att variationen inte behöver vara så stor eftersom de förmildrande interna omständigheterna kan bli inkluderade i ett händelseträd så väl som i en sårbarhetsanalys.
- Det största problemet med sårbarhetsansatsen är hur man presenterar resultatet. Informationen är bristande med avseende på tillvägagångssättet och resultatet är svårt att tolka. Målet med analysen är dock inte att ge en exakt värdering utan istället att ställa upp en rangordning mellan de olika scenarionas kritiska nivå.

Summary

The development and interest in risk and vulnerability analyses are presently growing on a broad front. The interest has perhaps recently been mostly directed towards the societal arena for the concept of risk and vulnerability analyses, but the methods are nevertheless of high concern for all parts of the society, including the industry. With that background, it is the aim of this thesis to compare and demonstrate the advantages and disadvantages for the methods. By doing so, the two different analyses methods have been applied to a Flue Gas Desulphurisation (FGD) facility at a coal power plant in Germany.

The technical definition of risk is commonly presented as a set of three questions and their answers.

- *What can happen? (i.e., What can go wrong?)*
- *How likely is it that that will happen?*
- *If it does happen, what are the consequences?*

The definition of vulnerability is more complex and has, contrary to risk, no commonly accepted definition. Vulnerability can, however, simply be understood as the opposite to robustness and resilience. Something that is robust has a tolerance of damage against itself, while vulnerability is lacking that quality.

Both terms are used in risk- and crisis management. Risk is more often connected with risk management and vulnerability with crisis management, but it is not unusual that they are mixed. A simple understanding of the two managements is that risk management deals with loss prevention, while crisis management deals with minimisation of losses when an accident already has occurred.

The International Electrotechnical Commission (IEC) has given the definition of risk analyses as something very similar to the above definition of risk. Possible threats are identified by hazard identification, probability is assessed by frequency analysis and consequences are evaluated by consequence analysis. There is a long list of different risk analyses with different detail levels. The qualitative analyses are the most general and least time consuming, and the quantitative analyses aim to give precise risk estimations with as little uncertainty linked to them as possible.

Vulnerability analyses vary with the field the analysis is applied to. This thesis has concentrated on the “open system” as starting point. With an open system, the analysis focuses its efforts towards identifying and assessing both internal and external threats to the system. Threats such as technical failures and sabotages should both be included in the analysis.

The object that has been used to extract the advantages and disadvantages with risk and vulnerability analyses is a facility that cleans sulphur from the discharge of a coal power plant. The facility consists of a number of large metal pipes and rooms clothed in rubber and plastic. The rubber and plastic function as a corrosive protection layer from the highly corrosive gypsum slurry that is the result from the cleaning process.

The performed hazard identifications for both analyses reflect the differences in the open system approach for the vulnerability analysis and the closed system approach for the risk

analysis. The most significant threat identified by the risk analysis is a fire that starts in the rubber. The vulnerability analysis emphasises the human factor as its most significant threat.

The in-depth study of the fire risk was performed with the help of an event tree. The probability parameters were estimated with distributions and the consequence was assumed to be either a total destruction of the FGD or a very small impact if the fire was extinguished. The result showed that a mean value for yearly fire damage is 1.78 million Euros. The result is, however, unsure and varies from the 5^{th} to the 95^{th} percentile of 0.37 to 3.79 million Euros.

The in-depth study of the human factors presents five different scenarios that are evaluated according to Einarsson and Rausand (1998) and their two step vulnerability analysis. The results show that the possible damages are covered to the most part by the company's insurance, with the exception of potential losses of credibility/reputation.

The conclusions that have been evident about the pros and cons with the different analyses methods are as follows:

- The longer tradition of the risk analysis compared to vulnerability analysis has proven to make a positive difference in conducting the analysis on all steps of the method.
- One of the event tree analysis advantages is the possibility of combining many risk scenarios into one.
- The event tree presents a straightforward and easily overviewed way of understanding a risk, which should be easy for unfamiliar readers to understand.
- The potential for the event tree analysis is very large in calculating an exact risk value. This unfortunately creates a problem with uncertainty the more exact the analysis aims to be.
- It has been shown that human errors and external threats are somewhat neglected in a traditional risk analysis. That does not necessarily mean that one cannot include these aspects in a risk analysis.
- The scope of vulnerability analyses is very wide. This should, for the most part, be regarded as positive when widening the spectrum of threats. The problem is, however, how to handle irrelevant threats and decide which are relevant and which are not.
- Root causes to human errors, such as organisational errors, are addressed in vulnerability analyses, but neglected in the IEC standard for risk analyses.
- The time period over how long the different analyses stretch are said to differ considerably, according to previous studies. This study has proven that this difference is not very large since internal mitigation aspects can be included in an event tree as well as in a vulnerability analysis.
- The most severe problem with the vulnerability approach is the manner of presenting the result. The information given by Einarsson and Rausand (1998) seems to be incomplete, thus risking faulty interpretations, concerning the procedure, furthermore the result is hard to interpret. The aim of the analysis is, however, not to give an exact estimate but rather establish a ranking of the scenarios according to their criticality.

Index

1 INTRODUCTION 1

1.1 BACKGROUND 1
1.2 AIM 1
1.3 METHOD 1
1.4 DISPOSITION 2
1.5 RESTRICTIONS 2
1.6 COMMENTS 2

2 DEFINITIONS OF RISK, VULNERABILITY, ETC. 3

2.1 RISK 3
2.2 CRISIS 4
2.3 EMERGENCY 4
2.4 VULNERABILITY 5

3 RISK- AND CRISIS MANAGEMENT 6

3.1 RISK MANAGEMENT 6
3.2 CRISIS MANAGEMENT 7
3.2.1 FEMA 7
3.2.2 CCMD 8
3.3 SIMILARITIES AND DIFFERENCES 9

4 RISK AND VULNERABILITY ANALYSES 11

4.1 RISK ANALYSES 11
4.1.1 Qualitative methods 11
4.1.2 Semi-Quantitative methods 12
4.1.3 Quantitative methods 12
4.2 VULNERABILITY ANALYSES 13
4.2.1 Fundamental start points 13
4.2.2 Proposal of content in a vulnerability analysis 15
4.3 VULNERABILITY ANALYSIS VERSUS RISK ANALYSIS 16
4.3.1 Mutual problems 17

5 THE COMPANY, THE POWER PLANT AND THE FGD 20

5.1 THE POWER PLANT 20
5.1.1 Flue Gas Cleaning Processes 21
5.1.2 Flue Gas Desulphurisation (FGD) Process 21
5.1.3 Description of the FGD at the power plant 22

6 SELECTION OF ANALYSES 23

6.1 BACKGROUND THEORY 23
6.1.1 Plant specific answers 23
6.2 CHOICE OF VULNERABILITY ANALYSIS METHOD 24
6.3 CHOICE OF RISK ANALYSIS METHODS 25

7 HAZARD OR THREAT IDENTIFICATION 27

7.1 HAZARD IDENTIFICATION FOR THE RISK ANALYSIS 27
7.1.1 Choice of the specific checklist 27
7.2 HAZARD IDENTIFICATION FOR THE VULNERABILITY ANALYSIS 27
7.2.1 Internal risk factors 28
7.2.2 External risk factors 30

8 RESULTS FROM ANALYSES 32

8.1 RISK ANALYSIS 32
8.1.1 Overview of hazard identification 32
8.1.2 In-depth study of fire risks 37
8.2 VULNERABILITY ANALYSIS 46

8.2.1 Overview of the internal and eternal risk factors *46*
8.2.2 In-depth study of human errors *50*

9 RISK EVALUATION **58**

9.1 SAFETY ATTITUDE AT THE COMPANY AND THE POWER PLANT 58
9.2 SUGGESTIONS OF OPTIONS FOR RISK SCENARIOS 58
9.3 SUGGESTIONS OF OPTIONS FOR VULNERABILITY SCENARIOS 59

10 RISK REDUCTION/CONTROL **61**

10.1 DECISION MAKING 61
10.2 IMPLEMENTATION AND MONITORING 61

11 CONCLUSIONS **63**

11.1 RISK ANALYSIS 63
11.2 VULNERABILITY ANALYSIS 64
11.3 CONCLUDING REMARKS 65
11.3.1 Joining the two methods into one *65*

APPENDIX 1 USED CHECKLIST **73**

APPENDIX 2 RISK CHART OF EXTERNAL NATURAL THREATS **74**

APPENDIX 3 QUESTIONS FOR THE VULNERABILITY HAZARD IDENTIFICATION **75**

APPENDIX 4 IGNITION CHECK CHART **77**

APPENDIX 5 FIRE PLUME CALCULATION **78**

APPENDIX 6 FIRE GROWTH OF RUBBER ACCORDING TO AT^3-CURVES **79**

APPENDIX 7 REGRESSION ANALYSIS **80**

APPENDIX 8 HUMAN ERROR, VIOLATION AND LATENT FAILURE RELATED SCENARIOS FOR THE FGD **81**

APPENDIX 9 QUANTITATIVE ANALYSIS OF VULNERABILITY SCENARIOS A AND B **82**

1 Introduction

1.1 Background

Risk management and crisis management are today looked upon as very important issues for a variety of different organisations. The common way is to see crises management as something separate from risk management. This view may simply be described as crises management deals with already occurred accidents and disasters while risk management deals with the prevention of those events. There are however scholars who have the opinion that risk management is almost the same as crises management and vice versa.

The aim for both managements is to reduce the effects of accidents as much as possible with regards to what is economical and reasonable for the organisation. Both managements consist of a line of steps, which have their similarities and differences. The first step in risk management is the risk analysis; to identify the areas of potential danger and what losses that may cause. The first step in crises management is many times referred to as vulnerability analysis which is quite similar to the risk analysis but has its start point in what is vulnerable and what can get hurt and then identifying what may cause those negative effects. In other words, both methods address the same thing but have different initial starting positions.

1.2 Aim

With the background of today's development and interactions in the area of risk and crises management, will the thesis discuss the differences of vulnerability and a risk analyses. The two different analysis methods will be applied to a real example, a Flue Gas Desulphurisation Facility (FGD) of a coal power plant in the Ruhr region of Germany. The result of the two analyses will then be used as the first input into the risk management process that will be applied to the FGD facility. The aim is then to compare the two analyses with each other and draw some interesting conclusions.

1.3 Method

There are almost countless of different risk analyses methods and vulnerability methods on the market today (Nystedt 2000). An extensive investigation and study of relevant literature associated with risk- and vulnerability analyses methods are therefore necessary. From the literature three suitable methods will be chosen and applied to the FUG. Further more; the gathered information will then be used in the theoretical part of this paper.

Three weeks of practical information gathering at the plant have been used to describe the FGD and its hazards. Different studies have been done on site, such as interviews of employed personal, different tours around the facility by different key personal, studies of documentation, etc. The focus of the work at the site is to identify the risks associated with the FGD. This is accomplished with a preliminary risk analysis, a checklist, and with the help of Einarsson and Rausand's (1998) risk factors. The gathered information from the plant will then be used as input to one risk analysis method and one vulnerability method. Out from the result of the analyses, the main threats/hazards are chosen and are the objects for a more in-depth analysis. The last two steps in the risk management process are based on what will be extracted from the risk- and vulnerability methods. Finally, the results from the analysis are

compared and conclusions are drawn out of what advantages and disadvantage the different risk- and vulnerability methods possesses.

1.4 Disposition

This paper consists of two major parts, first the background theory part and then the practical part.

It is necessary to start with the definitions of some of the key elements. Therefore definitions of risk and vulnerability, emergency and hazard, will be given in chapter 2. These are key elements in chapter 3, where risk- and crisis management are discussed. To fully understand risk- and vulnerability methods and their differences, one has to know in what context they are used. Risk- and crisis management is the normal arenas for the methods, which leads us to chapter 4 where the methods are explained. In this chapter categorising, description and comparison of the methods are executed.

The practical part starts out with a description of the power plant and the object (FGD), in chapter 5. The next chapter deals with the specific selection of which methods are to be used for the object. Some background information is also given to support the selection. The common initial step in both analyses is hazard or threat identification. This topic is discussed in chapter 7. The results of the analyses are presented in chapter 8, together with explanations of how they have been achieved. In chapter 9 and 10 are then the two last parts of the risk management process executed, which suggests different alternatives of risk/vulnerability reducing and theory about how to choose the best one.

The thesis ends with a discussion of what is observed to be positive and negative with vulnerability and risk analyses in an industrial setting.

1.5 Restrictions

There is a long list of different risk analysis and vulnerability analysis methods, other than the ones included in this thesis (Nystedt 2000). Due to time limits, only one risk analyses and one vulnerability analysis is carried out. The quantification of the risks and vulnerabilities is limited for the same reason. Conclusions drawn from this thesis are limited to apply only to the specific FGD facility. Since the comparison between the analyses is only based on one occasion and not to a number of objects, the results cannot be used as proof for new theories about the differences between the methods.

1.6 Comments

The author of this paper is not to be confused with the frequently referenced scholar Stefan Einarsson, even though their names are similar.

2 Definitions of Risk, Vulnerability, etc.

To get an understanding of what risk- and crises-management is all about we will have to define some of the key terms in this field.

2.1 Risk

There is no unified consensus amongst the scientific world today concerning the term risk. Risk is explained from two different camps, the natural science and the social science. The natural science camp defines risk from the technical "objectivistic" view point (Abrahamsson and Magnusson 2003). The objectivistic view point it is here assumed that risk is something that can be measured and is absolute. The problem is, though, that the methods available today are not adequate enough to give us an exact measurement, but can only provide us with a good estimation with little or extensive uncertainty attached to it. The social science camp claims that it is absurd to think that risk should be looked upon in an objectivistic way. People have their own backgrounds and experiences and will therefore intentionally or unintentionally affect their risk estimation (Renn 1998).

Due to the nature of the topic for this thesis, a social science view point is not feasible because there would be no comprehensive results to compare and draw conclusions from. Therefore the social science view point is taken under little consideration if any.

The International Electrotechnical Commission (IEC 1995) gives a generally accepted definition, by the natural science camp:

"*Risk* - a combination of frequency, or probability, of occurrence and the consequence of a specified hazardous event. *Note - The concept of risk always has two elements: the frequency or probability with which a hazardous event occurs and the consequences of the hazardous event*."

Another well spread definition includes the answer to three questions (Kaplan and Garrick 1981):

- *What can happen? (i.e., What can go wrong?)*
- *How likely is it that that will happen?*
- *If it does happen, what are the consequences?*

The two definitions are very similar and give us an understanding that between the 14 years, when the two definitions were defined, no larger development has taken place. Abrahamsson and Magnusson (2003) use the same definition as Kaplan and Garrick (1981) when they describe what risk analysis and vulnerability analysis are. They do, however, mark the fact that the definition is relatively uncomplicated and gives us no answer to certain social criticisms like why certain events are considered as more undesired than others and why people have a different risk perception than others.

As far as the general public is concerned, risk is associated with something negative (Enander 2005). In this paper, risk is to be understood as mainly something negative that has the potential to hurt people, the environment and property. There are, however, two sides of the coin and one can argue that without risk there is no profit. This is true to all companies, they

have to take risks and invest in affairs that are dangerous in some way; risks do not have to be associated only with nuclear power plants or air planes, falling down the stairs is also a risk. There are also non-economical positive aspects of risk. A higher awareness of risk may lead to an increase in safety preventive actions and increased ability to cope with upcoming situations (Nystedt 2000).

2.2 Crisis

Risk is, as seen above, not the easiest to define, but compared to crises it is a lot easier. There are countless definitions for crises; this paper will only present a few of them. One definition that is given for "national crisis" by Sundelius (1997) is:

"National crises have the meaning to us that the central actors understand the situation as:

1. *large values is at stake*
2. *limited time is available*
3. *the circumstances is under considerable uncertainty"*

This definition can easily be translated into a smaller scale, like a company where the central actors, the board of the company, would have the understanding of the situation as points 1 to 3 above listed.

The Canadian Centre for Management Development (CCMD 2001) gives another definition:

"A 'crisis' is a situation that somehow challenges the public's sense of appropriateness, tradition, values, safety, security or the integrity of the government."

Here is the public in the center and we are also given a broader sense of the first point in Sundelius (1997) definition. Appropriateness, tradition, safety, security and integrity can all be seen as containing a value. Value is not only meant as economical value, but there is also value in safety and security, etc. For a company, however, the most relevant value is the economical aspect and some might argue that all values come done to money in the end anyway.

In Fredholm's (2003) definition, we are clearly instructed to view a crisis as something with a possible *negative* outcome. His definition reads as follow:

"a sudden situation that one or several people may get there life situation considerable changed in a negative direction"

In contrast to risk, a crisis can hardly ever be considered to be something positive; unless regarded from the point of view of enemies or competitive companies.

2.3 Emergency

The words crisis and emergencies are many times used as the same thing. The Canadian Centre for Management Development (CCMD 2003) gives us the definition as:

"An 'emergency' is an abnormal situation that requires prompt action, beyond normal procedures, in order to limit damage to persons, property or the environment."

They have the opinion that even though crisis and emergency have much in common, they are two separate things. The clearest difference is that an emergency may get out of hand and turn into a crisis where the decision-makers lose the control of the situation, while the emergency is stretching the organisation, but it is still under control of the decision makers.

2.4 Vulnerability

Like crisis, vulnerability is not an easy thing to define. Many different definitions are available and the word is used in a wide variety of areas (Abrahamsson and Magnusson 2003). The Oxford English Dictionary gives us a useful starting point in our search for a good definition. The word vulnerable is the Latin word *vulnerabilis* and originates from *vulnerare* "*to wound*" (Compact Oxford English Dictionary 2007). Vulnerability is defined as:

"The quality or state of being vulnerable, in various senses" (Oxford English Dictionary 2004)

To make the field of vulnerability a bit easier to overview, it can be divided into three major groups: the vulnerability linked to natural catastrophes, social vulnerability and vulnerability linked to technical systems – planned and unplanned threats (Abrahamsson and Magnusson 2003). This paper aims to only discuss the vulnerability liked with technical systems. Einarsson and Rausand (1998) have defined the "technical" vulnerability to:

"The properties of an industrial system; its premises, facilities, and production equipment, including its human resources, human organisation and all its software, hardware, and net-ware, that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside the system boundaries."

A fairly easy way to understand the definition is to look at vulnerability as something opposite of robustness and resilience (Einarsson and Rausand 1998; Hallin et al 2004). Something that is robust has a tolerance of damage against itself, while vulnerability is lacking that quality.

The definition can be turned back and forward but will still end up with a relationship between what is vulnerable and what the cause of that is – the hazard. Something cannot be generally vulnerable without any specific threat against it (Hallin et al 2004), just like a risk cannot expose a threat if there is no object that is the target of that threat. Philip Bukle (1998) points out that people are not vulnerable because of what state they are in (e.g. handicapped or old); the real reason is that they lack the resources that they need to deal with the threats that lie upon them. The same applies to companies; they are not vulnerable because they are dealing with hazards; they are vulnerable because they are *not* dealing with their hazards.

3 Risk- and Crisis management

Many times the concepts of risk management, risk assessment and crisis management are mixed and defined differently by different users. In this chapter the different definitions are clarified, according to present standards.

3.1 Risk management

The International Electrotechnical Commission (IEC 1995) has introduced an international standard for what risk management is. The definition they suggest is illustrated in figure 1, below. It consists of three major parts: risk analysis, risk evaluation and risk reduction/control, with their subsequent categories.

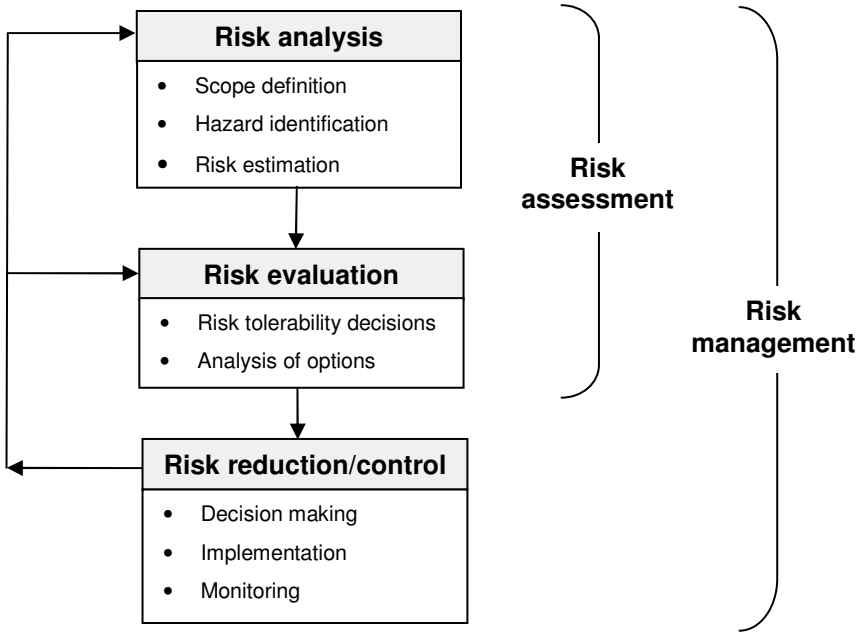


Figure 1 Risk management process according to International Electrotechnical Commission (IEC 1995)

Risk management is described as a process with its first phase called risk analysis. It is here that the topic of what is to be analysed is determined; in other words the process of fixating the goals of the study. The next step is to identify the different hazards that may occur. This step can look very different from one risk analysis method to another. Some methods are more general and fast, while some are very thorough and time consuming (this will be discussed further in chapter 4). The same differences apply to the risk estimation step, where the different risk analysis methods can be divided into three groups - qualitative, semi-quantitative and qualitative, the last of which being the most detailed.

The second phase of the process deals first with what is tolerable for each one of the separate risks. The ones that are not considered to be tolerable are then the object of the option analysis. Different risk-reducing alternatives are here compared with each other. After the completion of the two first steps, the so-called risk assessment has been executed and stands for how the organisation views the identified risks, if they can be accepted and what alternatives there are to be considered.

The last phase is the risk reduction/control phase, starting with deciding upon which of the risk-reducing alternatives one should choose, based on the analysis performed in the previous step. Then follows the implementation and monitoring steps, where the winning risk-reducing alternative is put into action and then followed up and checked.

The thought is that this process will go on and on; it is not supposed to stop just after one round of the above described phases and steps. After the new risk reducing measures have been put into action, the cycle starts again from the top with a new risk analysis.

3.2 Crisis management

Crisis does not have, as mentioned previously, a uniform definition, and that is true for crisis management as well. Crisis management, though, can be explained very briefly as the process that is supposed to identify, minimise and deal with upcoming hazards and, after the crisis is over, also bring back the situation to normal conditions. The intent of this paper is not to bring out all the different variations of the definition, but to discuss two well-respected ones. The definitions are similar and consist of four identical major parts: Mitigation, Preparedness, Response and Recovery.

3.2.1 FEMA

The definition was developed by the United States Federal Emergency Management Agency (FEMA), which works for the strengthening in the resilience and improvement of general crisis management in the US (FEMA 1997).

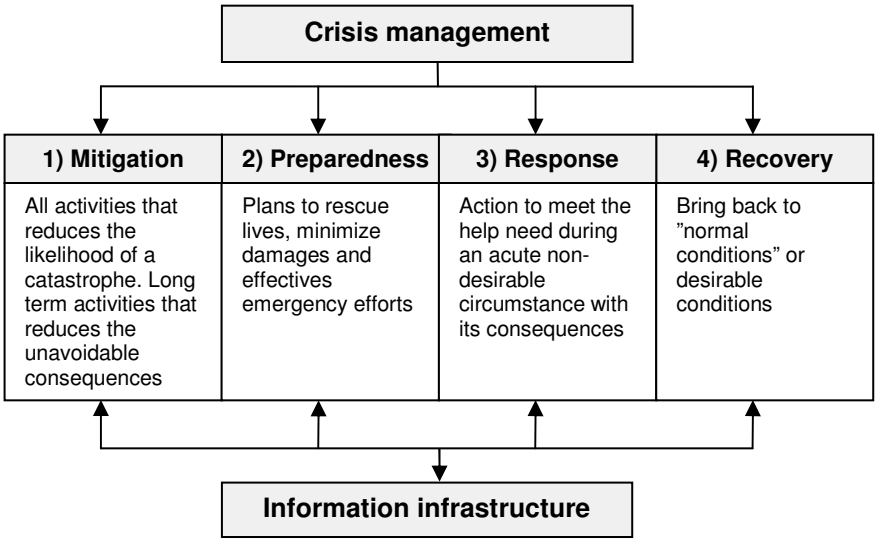


Figure 2 Crisis managements different part according to US Federal Emergency Management Agency (FEMA 1997)

The mitigation part is very similar to what we usually think of as risk management. In FEMA’s definition both likelihood and consequences are mentioned and aimed to be reduced. In this way is risk analysis a useful tool to find out where the mitigation is needed the most – also known as risk evaluation. Different mitigation measures are then taken, this also known as the risk reduction/control phase in IEC’s risk management process. An example of mitigation measures can be sprinkler systems against fires, an extra power source for control

rooms, changing materials to less ignitable ones, well regulated breaks for personnel so that they stay alert, management and personal that posses a high safety culture, inspections and revisions of the safety, etc.

The preparedness phase is directed to deal with planning and rehearsing for what should be done when a crisis occurs. From Perrow's (1984) view is the preparedness phase of absolute most importance, since an accident will occur to all complex and high couple systems sooner or later. The development of operational plans and communication plans, are together with assigning the different individual's task and performance duties in case of an accident, of essence in this step. The different plans that are constructed should not be too complicated or detailed, but be made with the aim to be efficient and useful in case of an accident (Andersen, 2003; Perry, 2004).

The part that many people associate with crisis management is the response phase. This is where it is possible to see if the mitigation and the preparedness phases have been well executed or not. Actions are taken to meet the help need from the different crisis situations and activation of the beforehand developed emergency plans are to be executed. The actions performed might as well include those that have taken place shortly before the accident, since these are hopefully results of actions due to early warning systems. In several cases of crisis situations in Sweden (such as when the collapse of a sulphur acid tank in Helsingborg 2005 and during the snow chaos in Gävle 1998, etc), "luck" has been a big part of the response phase, when somehow the plans are not well enough developed and unexpected, external resources have also been of absolute necessity. This shows how important a large and well functioning network with other organisations and individuals is when the unexpected occurs.

The last step is the recovery phase, which has its focus on bringing the situation back to its original position. The recovery phase should be aimed towards both immediate activation, of such as vital support systems, and towards more long term problems, such as resetting the infrastructure to its initial stage (Abrahamsson and Magnusson 2003). The recovery phase might be very long and hard for the employees that worked close to the scene of the accident when it occurred. It is therefore important to put aside recourses to the affected before the accident as well as afterwards. After the crisis is over, it is also important to extract information about how the organisation can improve for the next accident.

Below the four major parts is the "information infrastructure" square, which is pointing out the importance of information exchange. An important factor is here early warning system, for example fire detectors and surveillance cameras. Others are information flow and feedback between the different major steps (Abrahamsson and Magnusson 2003).

3.2.2 CCMD

The second description of crisis management was developed by the Canadian Centre for Management Development (CCMD 2003). The two definitions are similar in how they are built up and the different parts that are included. There is one larger difference however, which is the mitigation step. In CCMD is the emphasis upon reducing the consequences of accidents, while FEMA wants to direct recourses to also reduce the likelihood of those accidents. In other words, the CCMD's first step is not as extensive as FEMA's. Abrahamsson and Magnusson (2003) write that CCMD's crisis management definition can be looked upon as a complement to the FEMA's. What follows below is the description and what can be noticed is how they define which phase is executed when – before, during and after.

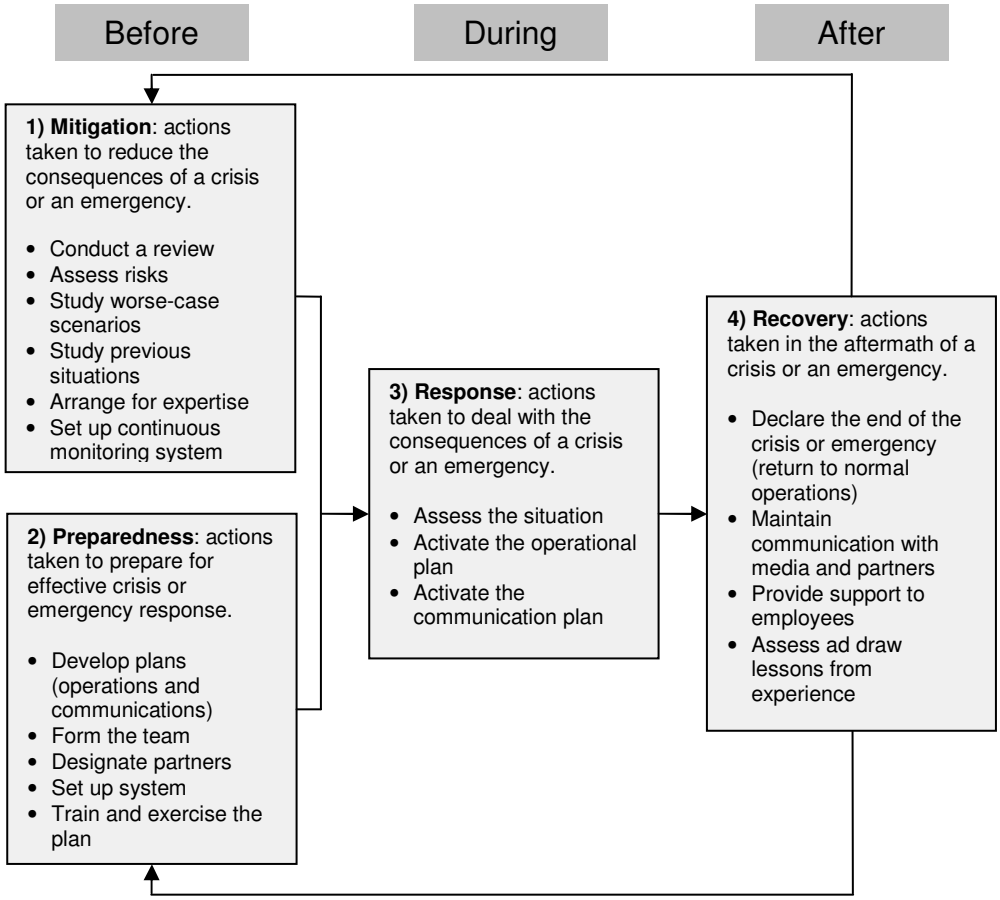


Figure 3 Crisis management processes according to CCMD (Canadian Centre for Management Development)

Worth mentioning is that traditionally crisis management has been concentrated towards phases 2-4 (see Figure 2 and 3), while phase 1 has been the subject of risk- and vulnerability analyses and just played a minor roll. It is just within the last decade that we have put the whole process together (Abrahamsson and Magnusson 2003).

To just rely on a risk analysis for the dimensioning of the crisis management might create the problem of not being prepared for a surprise. Even though vulnerability analysis is based on specific scenarios which do not represent a comprehensive risk picture, it might possess an advantage in this case. For instance, after analyzing the specific scenarios there could be a discovery of short- comings that are of a more general agenda, such as communication problems. Therefore it is likely to believe that these shortcomings can influence the analysis ability to handle other undefined non-desirable events (Hallin et al 2004).

3.3 Similarities and Differences

The obvious common reason for initiating the risk- and/or crisis management processes is to reduce losses, of some kind (i.e. lives, property and money) in the future. To reduce all losses so that there is no risk of accidents or future crisis is the same thing as shutting down the organisation. To manage your risks and crisis is to handle them at the level you prefer, also called *risk appetite,* in the risk society (COSO 2003).

A simple way of dividing the two processes is to say that risk management deals with prevention of losses, while crisis management deals with minimisation of losses when an accident already has occurred. It is not effective to only look at what is risky or vulnerable, it is vital to assess both likelihood and consequences to reduce losses of value. Risk management, has though traditionally focused its resources to reduce the likelihood of an accident while crisis management has focused its resources on reducing the consequences of an accident (Abrahamsson and Magnusson 2003).

However well performed and effective an organisation makes their risk- and/or crisis management process, there is no way to foresee all that might go wrong (Andersen 2003). The paradox is that if potential hazards are not foreseen in vast magnitude, there is a big risk of making yourself vulnerable. One of the largest problems with the two processes is that they are built up on the foundation of imagination and historic events; to make up accident scenarios. Andersen (2003) is also pointing out that even if someone has identified a potential threat, he might be dismissed due to such an event being seen as completely unrealistic (e.g. The 11th of September catastrophe).

4 Risk and Vulnerability analyses

This chapter deals with the theoretical background of the two methods.

4.1 Risk analyses

Risk analysis is the foundation and first phase in the risk management process, described in chapter 3. IEC (1995) describes its contents as trying to answer three elementary questions:

- *What can go wrong (by hazard identification)?*
- *How likely is this to happen (by frequency analysis)?*
- *What are the consequences (by consequence analysis)?*

The questions are, if one looks closer, developed from Kaplan and Garrick's (1981) definition of "risk". There is, in practice, only one difference and that is that IEC has delegated different analyses methods to answer each question.

Another way to describe risk analysis is to define what parts are included in the process (SS-EN 1050, 1996):

- *Define goals and restrictions.*
- *Make an inventory and identify risks.*
- *Analyse risks, including estimation of probability and consequence.*

Conducting the steps described above and answering the elementary questions from IEC is the fundamental way of performing a good risk analysis. There is, however, a long list of different methods and approaches to do this, which can be designated to belong to different groups: qualitative, semi-quantitative and quantitative methods. Below, in figure 4, are different common risk analyses methods divided into different levels of qualitative and quantitative elements. Two of the analyses will be used later in this paper for the examination of the relevant FGD, but the remaining will be not further discussed.

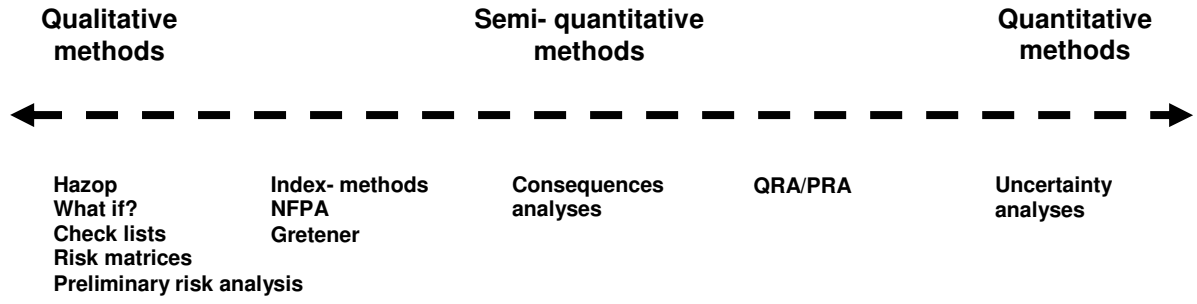


Figure 4 The spectrum of the different risk analyses methods with respect to the level of qualitative and quantitative elements (Olsson 1999; Nilsson 2003).

4.1.1 Qualitative methods

The most common use for qualitative methods is to identify risks. They are therefore most useful in the first phase of the risk analysis (Nilsson 2003). The name reveals that it is not numbers that one is dealing with when determining the hazards risk level. Instead terms like small, big and catastrophic are used to describe the potential consequences of a hazard; and

terms like unlikely, likely and very likely to describe the probability of a hazard. In this way these analyses can be used for comparing risk with each other, with a risk matrix for example (see also chapter 4.2). By not having to deal with fixed numbers and as much details these methods demand usually lighter work load, than what the quantitative methods does. This is not to say that the results are less useful and that the analysis is simpler to conduct than quantitative methods (Malmsten and Harrysson 2004). These kinds of analyses are many times adopted for special types of activities (e.g. chemical process industry (Nystedt 2000)) and are based on experiences conducted by expert groups (Davidsson 2003).

4.1.2 Semi-Quantitative methods

The most common use for semi-quantitative methods is to rank risks between each other. With the approach of giving each risk a more detailed ranking, these methods are very useful as a help in choosing between different activities associated with risk. The ranking system of the risks is many times given numbers, but it doesn't mean that it has to be exact; a gap between two numbers is sufficient. One way to exemplify this is with a risk matrix with numeric elements, as seen below.

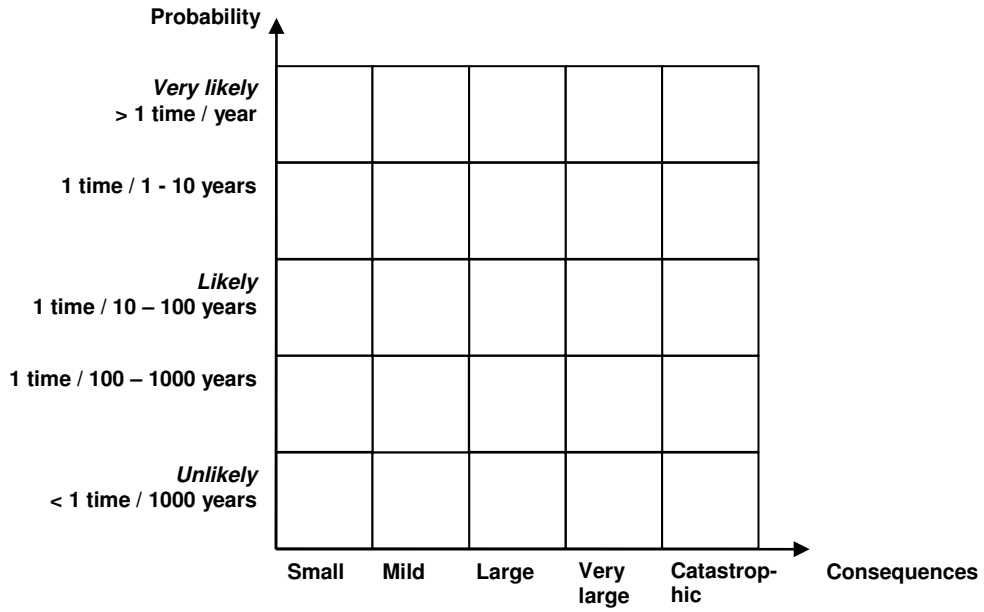


Figure 5 Example of a semi- quantitative risk matrix (Rosenberg 1989).

4.1.3 Quantitative methods

The most extensive methods of them all are the quantitative methods, which are totally numerical in theirs estimation of the risk level (Nilsson 2003). It is quite a demanding work to perform a quantitative risk analysis (QRA), which is the collective name for these kinds of risk analyses. There are many different ways to perform a QRA and the different methods vary from each other. There is, however, one thing that is common for them and that is that they are associated with uncertainty. In the effort to make these methods numerical and exact, they are dependent on statistics, expert opinions, calculation models, etc., which are, in one way or another, unsure facts. Statistics are unreliable because they are reports of the past and not hard facts of what will happen in the future. Experts' opinions are made by humans who have there own "favourite risk" and therefore influence the analyses. Calculation models are only models with their own restrictions and simplifications of the reality.

There are two ways to deal with this problem: either choose a deterministic or a probabilistic QRA. The deterministic one uses representative values in the data, for example the 80 or 95 % percentile and generates in the end a point estimation of the risk that is assumed to be conservative, i.e. on the safe side. The other way is to let the complete distribution propagate through the whole process to the end result. Through this approach is the end result presented as a distribution function of the risk (Nilsson 2003).

4.2 Vulnerability analyses

These types of analyses have been used for around 20 years by now and were initially dealt with computer and information technology (Einarsson 1999a). By now the arena for vulnerability analyses has spread and includes everything from company to societal vulnerabilities.

4.2.1 Fundamental start points

It is important to know from what field the applied analysis comes from when examining a system's vulnerability. There is a long line of different methods that aims to deal with their own specific part of vulnerability. From these different analyses are there important fundamental start points to be familiar with. If one has a solid background understanding of the start points, the right vulnerability analysis can be chosen for each task. Even aspects from not chosen analyses can be useful to have in mind when performing the selected analysis.

4.2.1.1 Everyone is vulnerable

Philip Buckle, Graham Marsh and Sydney Smale (2001) have society in mind when writing about vulnerability. They are of the opinion that there are characteristics of a system that are impossible to alter; for example the age of citizens in a community, or that a limestone-gypsum FGD operates under an extremely corrosive environment. Even though we cannot alter these characteristics, we can introduce assessments that can reduce their vulnerable side, also called barriers. Then there are also sides that are changeable; for example the location of the old people in the community, or what material a FGD consists of.

There are therefore two different aspects a vulnerability analysis should address. The first one is to identify and evaluate the different aspects that are not possible to alter within the system and suggest measures to decrease the vulnerability. The second aspect is to identify and evaluate sides of the system that are possible to alter and suggest measure so decrease that vulnerability.

4.2.1.2 "given a specific strain"

The start point that Johansson and Jönsson (2007) use focuses on the fact that vulnerability analyses differ from risk analyses in the initial three questions that each analyses should answer. They have adapted Kaplan and Gerrick's (1981) three questions that define risk and introduced three very similar questions to define vulnerability.

- *What can happen, given a specific strain?*
- *How likely is it to happen, given a specific strain?*
- *What are the consequences?*

The only difference is the words “given a specific strain,” which tells us that vulnerability analyses should only deal with a system that is under abnormal conditions while a risk analysis deals with problems when the system is operating normally.

Some definitions of vulnerability analyses, like this one, are very similar to the definition of risk analyses. Even so, there is a common denominator amongst vulnerability analyses that upholds the question of what is of value to protect in the system (Hallin et al 2004). The perspective is the opposite to risk analyses which try to answer questions like: what can threaten, what is valuable within the system, what are the points of attack and what is the capacity to manage and handle this strain?

4.2.1.3 Open system borders

Generally speaking, a vulnerability analysis is focused towards an “open system” (Einarsson 1999a). The system that is of concern is as well viewed in the light of its surrounding, and not only of its internal problems. For example, a computer network is chosen to be analysed, external aspects such as sabotage threats are then under consideration, as well as internal aspects as technical features. See also Figure 6 below for an illustration.

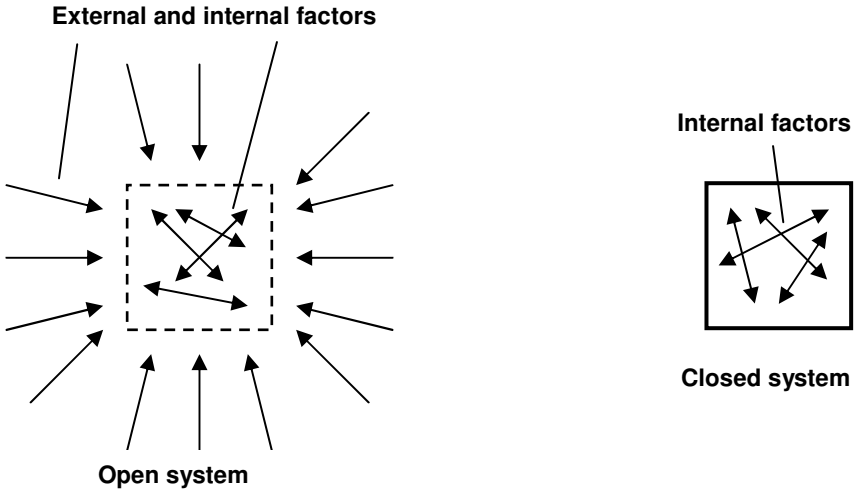


Figure 6 Illustrating the difference of a closed and an open system.

According to Einarsson (1999a) the vulnerability analysis has its main focus on the external factors and views a system out from the open system standpoint. He is also of the opinion that a vulnerability analysis aims to detect all the threats of a system and make the system resilient or robust to the consequences of that threat.

Another aspect linked to this viewpoint is that vulnerability analyses handle a “soft” paradigm to a system (Rosness 1993). The soft paradigm includes views such as that people are considered to be an interactive and not static part of the system (the human factor), acceptance of uncertainty and reduced data demands, archived by greater integration of hard and soft data with social judgements (Rosenhead 1989). This way of looking at a system is highly philosophical according to Einarsson (1999), but nevertheless to some degree applied into his and Rausand’s vulnerability analysis (Einarsson and Rausand 1998).

Vulnerability analyses are, in general, not focused on determining the probability of the different accident/hazard scenarios but are more focused on the description of the scenarios

and their possible consequences (Johansson and Jönssons 2007). When less focus is put into determining probabilities, a greater acceptance from the community can be obtained (Einarsson 1999a). A useful example to demonstrate this is to see it in the light of the "low probability – high consequence" debate with nuclear power plants. The public often has little understanding or faith in risk analysis that assesses the probability figures of a core melt of 10^{-11} and would therefore prefer a vulnerability analysis and its more qualitative approach.

4.2.2 Proposal of content in a vulnerability analysis

A proposal of what a vulnerability analysis should consist of is presented by Hallin et al (2004). Their proposal is not meant to be followed strictly but can work as a fundamental base for further discussions.

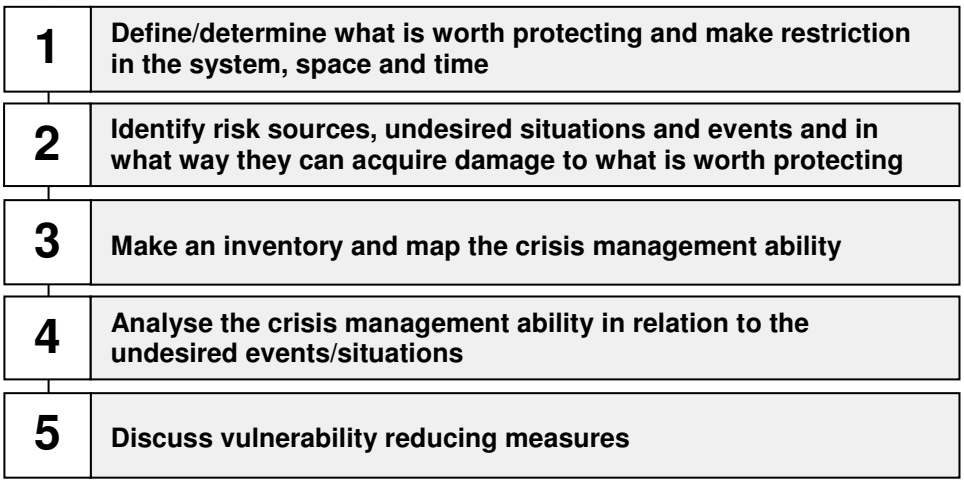


Figure 7 Elements in a vulnerability analysis (Hallin et al 2004).

There is a long line of aspects to be taken under consideration when initiating a vulnerability analysis. The first task is to determine what is of value to be protected. Depending on where the line is drawn for what is to be protected, the analysis will differ. The same goes for the second important task – what are the hazards, what can threaten the system we want to protect? The significance of classifying the system borders is important to stress, or else might relevant hazards be excluded and irrelevant hazards included.

The second step is to identify risk sources/hazards. This step is based on the foundation of how the system is defined, in step one. A crucial point for the whole analysis is that it is not practically possible to identify all scenarios of potential danger, but consideration and standpoints have to be made out of a partly subjective viewpoint. This problem is not addressed adequately in many vulnerability analyses according to Johansson and Jönsson (2007). They point out that one might get the wrong understanding that each strain on the system can only produce one risk scenario.

The task that follows after that is to describe and analyse the crisis management of the system. What are the resources that can be realised in an event of an accident, in form of knowledge, organisational leadership, communication and cooperation etc? Also, reasons for why the crisis management might have a difficult task should be identified, such as people of high age or decreased mobility, etc.

There are many ways to analyse the crisis management ability in relation to the undesired event. Some methods identify a number of hypothetical consequences that are the result of an initiating event and ask the question of how the consequence is handled (e.g. Einarsson and Rausand 1998).

The last step of a vulnerability analysis should discuss and suggest vulnerability reducing measures based on the previous last four steps. Included in this step is also monitoring and making sure that suggested measures are enforced. Even so, there is a possible goal of not directly producing just paperwork for the decision maker but also, by performing the analysis, vulnerability is raised on the everyday agenda and the network of the different actors and their awareness of this vulnerability is enforced. In this the analysis is a vulnerability reducer by itself.

4.3 Vulnerability analysis versus Risk analysis

Depending on which vulnerability analysis and which risk analysis that one chooses to conduct, the result from the analyses will differ significantly. It is therefore of great importance to remember this when discussing similarities and differences between the two groups of methods.

An aspect that seems to be the same for many vulnerability analyses is that they focus on trying to produce a measurement of how vulnerable a system is. This is done through an estimation of how big the consequences are following a triggered risk, and they are then compared with how the system manages the occurred event. It is common also to quantify the result in terms of loss of damage. When this is combined with a probability estimation, it is questionable if there is any difference between vulnerability analyses and risk analyses (Hallin et al 2004).

The fundamental differences between the two methods are that a risk analysis strives to quantify the risk while a vulnerability analysis is visualising weak points to a higher degree in the defence and management capability.

A common issue, as mentioned before, is how both methods have a problem with identifying all possible events. There are always more scenarios that could be subject for estimation. To only rely on prevention of undesired events, as the risk analysis, is therefore not definitive, an unexpected event could occur. To also focus the resources towards mitigation resilience of undesired events, as the vulnerability analysis focuses on can for that reason give a higher efficiency level.

A general picture (Figure 8) comparing risk analysis with vulnerability analysis is presented below. A clear difference in the method can be concluded from the picture, simply being that vulnerability analysis has a wider scope than risk analysis. Vulnerability analysis extends the scope and involves the mitigation, restoration and the final result. On the other hand, risk analysis is more focused on the accident origins than the vulnerability analysis. The difference is somewhat the same as that between risk management and crisis management.

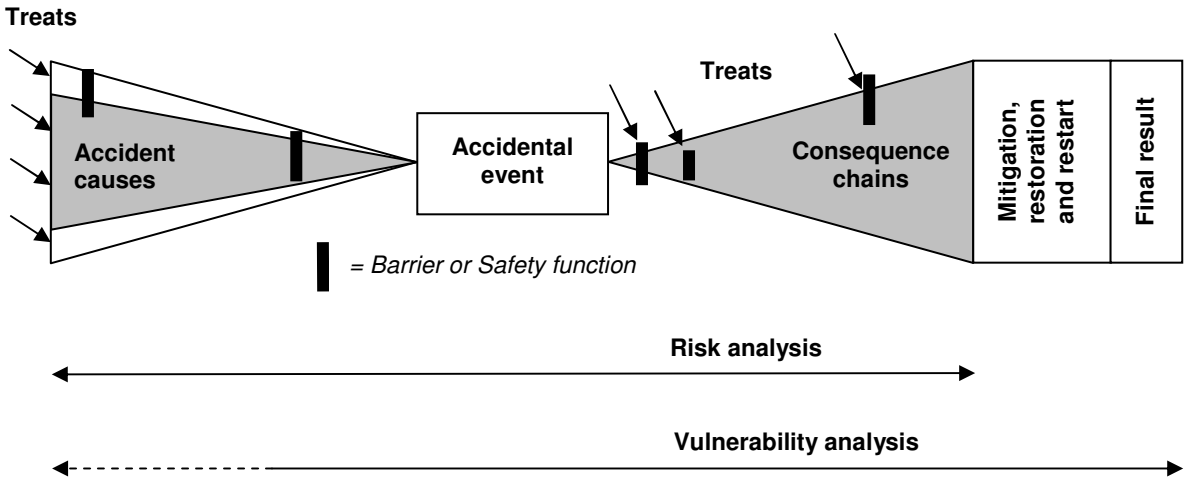


Figure 8 Difference in scope between vulnerability analysis and risk analysis (Einarsson and Rausand 1998; Einarsson 1999a). The shaded triangles demonstrate the scope of the risk analysis.
Note: The picture is a combination of the different versions that are presented in the two sources.

4.3.1 Mutual problems

The human factor or human errors exerts a fundamental dilemma for both methods. Humans are unreliable and cannot be trusted to perform the same quality of work over a period of time. That is why they are not able to work in all environments, especially environments that cannot tolerate variability in managing it. There are however both vulnerability analyses and risk analyses that focus on this problem, but their shortcoming consists of the lack of potential to take into account limits to human performance at all levels of the organisation (Einarsson 1999a).

The way that people perceive risk varies a lot in today's society and to estimate the probability in scenarios for risk and vulnerability analyses many times relies upon people's different perceptions. This is true for both the normal citizens and the experts. Citizens tend to overestimate risks with high consequence and low probability, as showed below in figure 9.

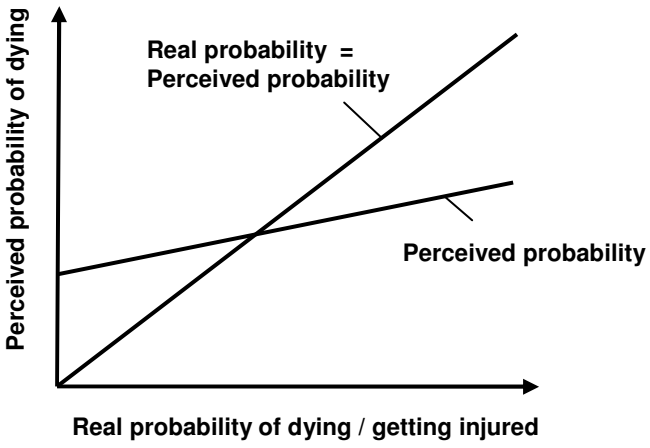


Figure 9 Risk perception (adapted by Einarsson 1999 from Mattson 1990).

This topic is highly controversial and has been debated amongst many scholars for a long time, such as Lennart Sjöberg (2001) and Ortwin Renn (1998). In their opinion, there is no one, including the risk experts, who can make risk estimations without having their own risk perception as a bias in the process. In that sense is it difficult to talk about "real probability" since it is more or less impossible to estimate in advance, and can only be said to be a utopia that we strive towards when we perform risk estimations.

Subjective estimations and evaluations are also a part of the entire risk analysis everyday, performed by expert risk firms (Lauridsen et al 2002). In the *Assurance project* seven different risk management firms (called partners) were involved and their task was to perform a QRA of the same chemical facility, an ammonia storage. The partners got the same background information and even some necessary assumptions were made together before the QRA could begin. There were different QRA methods used and each partner followed his own process and used his own tools and knowledge. As shown in the diagram below, the result was quite different and both the probability and the consequence assessment proved to give large differences in their results.

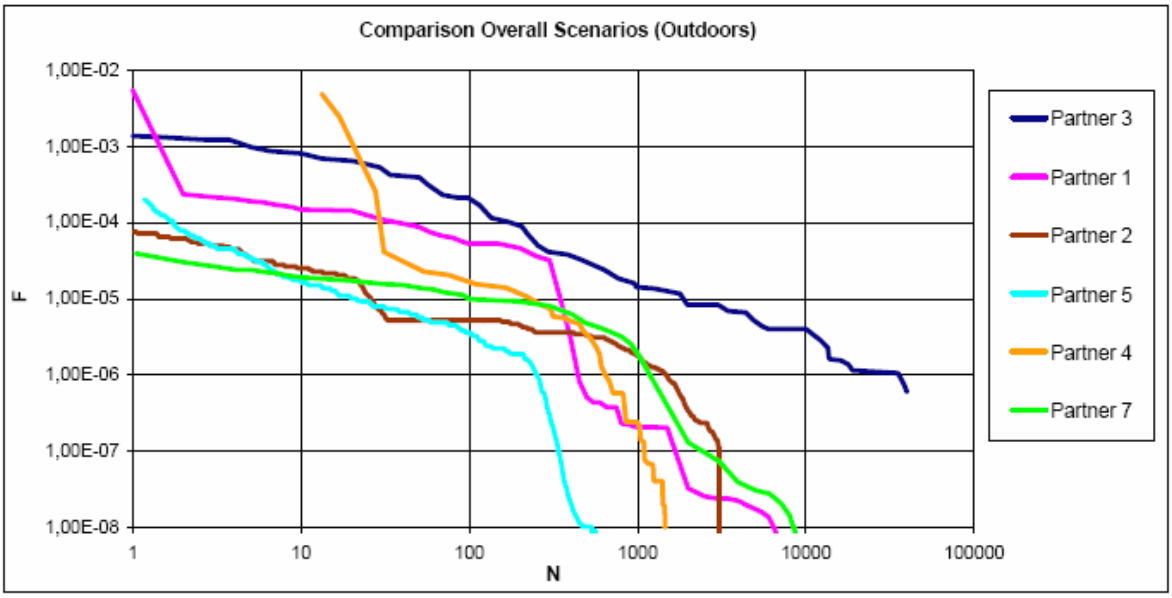


Figure 10 Discrepancy in societal risk calculations based on fictitious population data (Lauridsen et al 2002). The Y-axis represents frequency (or probability) and the X-axis represents number of fatalities.

This problem of different know-how, methods, perception etc. is not a problem just for risk analysis and QRA, but it applies also for vulnerability analyses. Analyses, like these, are performed by people and will therefore have a great dependence on who performs them.

According to Johansson and Jönsson (2007), there are six different main problems with risk and vulnerability analyses. Probability estimations are one of these problems. They are of the opinion that it is often hard to find information about previous accidents and events when assessing the probability for complex socio-technical systems. The same can be said about analyses of a less complex technical system. Many times the analyst must refer to expert opinions and logical models (such as event trees).

The first problem that one encounters is, however, not the probability estimation problem but instead the system definition problem. It is necessary to be precise right from the beginning of the analysis and define the system and what will be analysed. If this is not done properly, it

might lead to difficulties in discerning if other problems have been handled in the right way, such as the degree of risk covering.

The degree of risk covering highlights the problem that an analysis must cover all possible future events with a risk scenario. If the analysis does not, then there will be a problem with knowing how useful the analysis is since it just covers parts of the system's possible risks or vulnerabilities, called the problem of handling uncertainties in the analysis (Johansson and Jönsson 2007).

The problem with including too many risk scenarios, in the effort to minimise the above problems, is that the more scenarios you have the longer time and more money will the analyses demand. A way to decrease the time and money consumption is to reduce the detail level of the analyses. This is, however, the fifth problem according to Johansson and Jönsson (2007). When you reduce the detail level of the analyses, the question will be if the results of the analyses will be useful or not in the end.

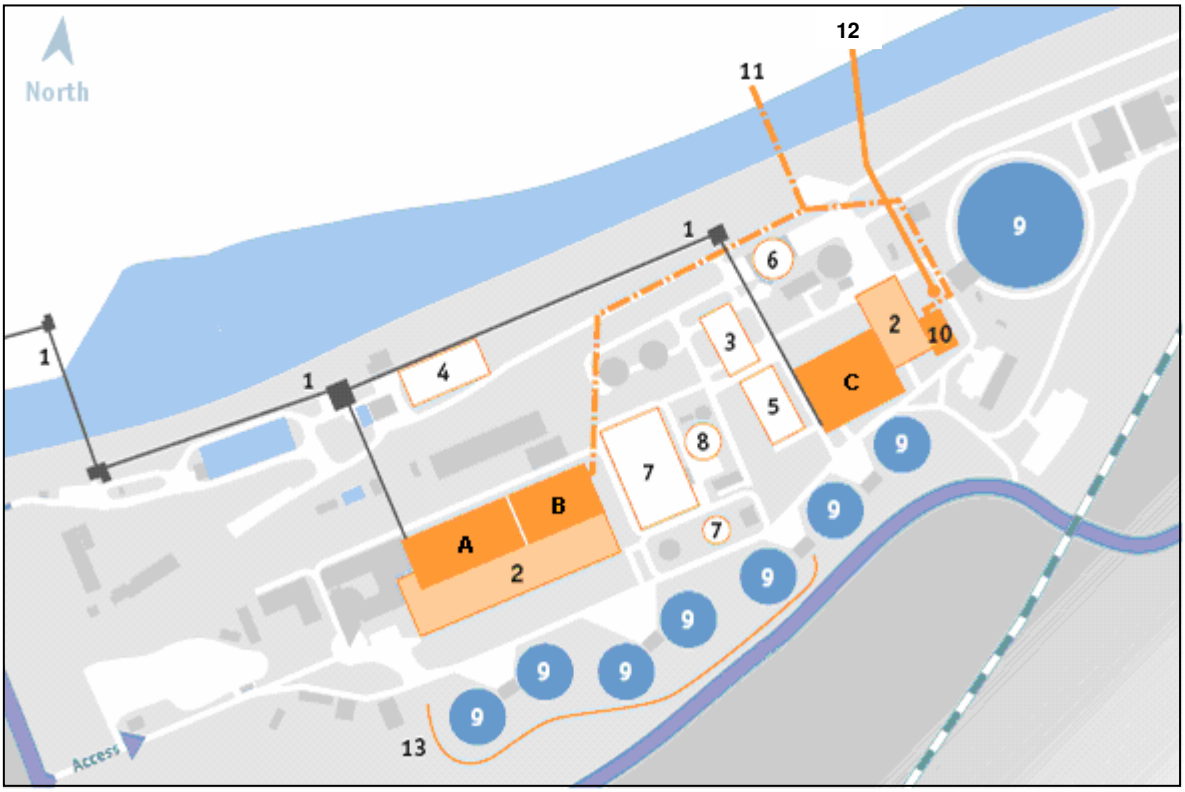
The last problem is concerning if the analyses in the end are representing the reality in an accurate way or not. This problem is common when assessing the consequences of the risk; in other words it can be hard to know exactly what the possible outcome will be of a scenario.

5 The company, the power plant and the FGD

The company is one of Germany's largest power companies and operates today in different parts of the world. It consists of two main parts: the first entails of five hard coal power plants situated in the heavy industrial Rhine/Ruhr region in Germany. The second part is financing, construction and operating of power plants worldwide. The company supplies not only energy to the general public but owns also two power plants in partnership with industrial companies. In 2005 they employed around 5000 employees and the turn-over was just below 5 billion Euros, with a profit after tax of 282 million Euros.

5.1 The power plant

The power plant is situated in the middle of the Ruhr region. It consists of three different units with a total capacity of 950 MW and produces 4.5 billion kWh each year, which supplies energy sufficient for 1.33 million households in its surroundings. District heating is also produced (0.8 billion kWh each year) which is fed into the Ruhr region's interconnected district heating system. The plant uses around 1.9 million tons of coal for its production each year. On the north side of the plant flows a canal, which is used for coal transportation and for the required water supply. Below follows a site map of the plant.



A-C	**Boiler house/"Unit" (steam generator)**
1	**Coal conveyor belts**
2	**Turbine house (turbine and generator)**
3	**DENOX system (SCR)**
4	**Ammonia tank**
5	**Electrostatic precipitator**
6	**Filter ash silo**
7	**Flue gas desulphurisation**
8	**Stack**
9	**Cooling towers**
10	**District heating building**
11	**Ruhr area interconnected district heating system**
12	**Power lines**
13	**Sound-absorbing wall**

Figure 11 Site plan of the power plant.

5.1.1 Flue Gas Cleaning Processes

The desire to decrease dangerous substances in outlets from combustion of organic substances (also known as Flue Gas) has been an important factor for the western world industry since quite some time. Germany introduced stronger emission limits for SO_2 in the beginning of the eighties, and it is since then that Flue Gas Desulphurisation (FGD) has been an important business (Lentjes 2007). The Selective Catalytic Reduction (SCR) process is also an important part of the cleaning process where the NO_x gases are removed. The pollutants that are cleaned away with these processes are major contributors to acid deposition, which can be a danger to a number of ecological systems. When let out, they also contribute to the corrosion of building materials and when entering the atmosphere they can create ground level ozone, which adversely affects human health (Goddard 2007). The third part of the cleaning process consists of the Electro Filter which cleans away up to 99.8 % of the ash from the flue gas.

5.1.2 Flue Gas Desulphurisation (FGD) Process

There are a number of different FGD processes on the market today. The British Department of Trade and Industry (2001) has described and divided up some of the major ones into the following list:

- *Wet Processes:*
  - limestone gypsum
  - sea-water washing
  - ammonia scrubbing
  - Wellman-Lord.

- *Semi-dry Processes:*
  - circulating fluidised bed
  - spray dry
  - duct spray dry.

- *Dry Processes*
  - furnace sorbent injection
  - sodium bicarbonate injection.

The FGD used in the power plant is the Wet Limestone Gypsum process, which is the most common, with a history of over 30 years of development. With this FGD plant over, 95 % of the SO_2 and almost 100 % of any hydrogen chloride (HCl) is removed from the flue gas (Department of Trade and Industry 2001). The cleaning process can be explained, very simply, as the passing of the flue gas through a system of showers that spray the gases with a limestone slurry that then cleans out the SO_2 and HCl. The final product is then high quality gypsum (calcium sulphate dihydrate), that can be sold to e.g. construction firms.

There are a number of different manufactures of this sort of facility and they are also able to produce different versions of the Wet Limestone Gypsum process facility, according to the client's demands. The chemical reaction between sulphur and the limestone slurry is however the same and reads as follows:

$$CaCO_3\,(s) + SO_2\,(g) + \tfrac{1}{2}\,O_2\,(g) + 2\,H_2O\,(l) \rightarrow CaSO_4 \times 2\,H_2O\,(s) + CO_2\,(g)$$

5.1.3 Description of the FGD at the power plant

The plant has two different FGD plants: one for units A and B and one for unit C. The two FGDs are very similar and are considered, out of a risk management perspective, to contain the same problems and hazards. That is the reason for this paper to settle with only describing and illustrating the FGD for unit C (exception in chapter 6.1.1). In the effort to make the paper easier to understand the two FGDs are considered as one unit in the rest of this paper. The FGD is the last step in the row of the three different flue gas cleaning processes. The flue gas has been purified of almost all its ash in the Electro filter and is pushed forward by a Fan (see no. 1 in Figure 12) into the Heat exchanger (2). Here the warm gas is cooled before entering the Absorber (3), where the so-called scrubbing process takes place. It is within the absorber that the limestone slurry reacts with sulphur and creates gypsum. After that the flue gas leaves the absorber and enters the heat exchanger again. Before the gas exit into the flue gas tower (4) the heat exchanger raises the temperature of the gas. From the absorber gypsum slurry is transported through the Gypsum configuration, where the slurry is made into gypsum and ends up in the Gypsum silos (5). The temperature of the flue gas within the FGD varies between 40 and 115 ^{o}C.

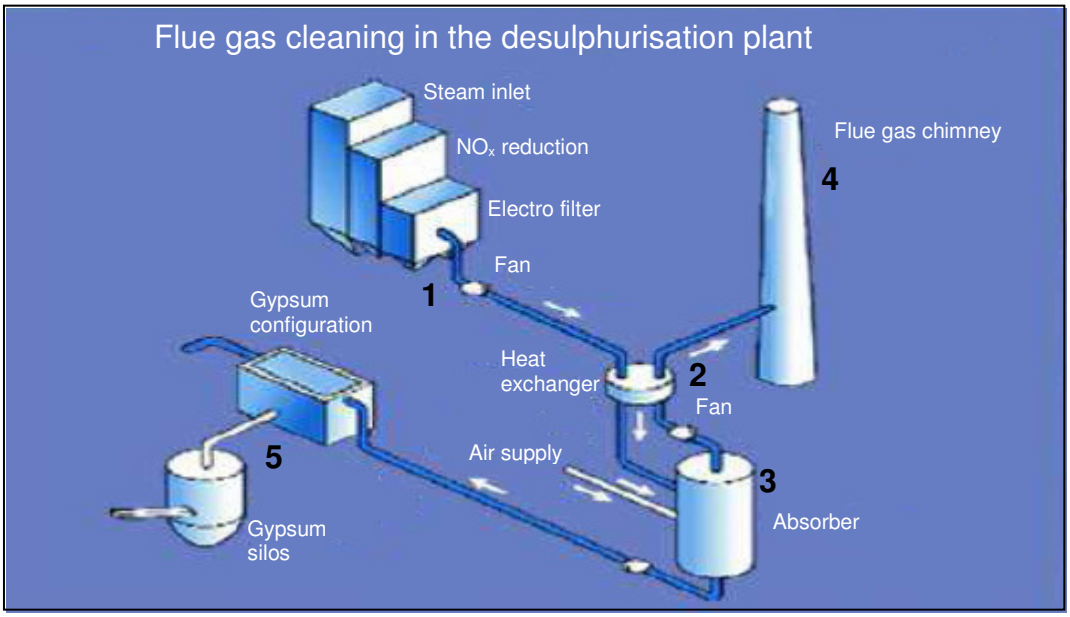


Figure 12 Schematic of the FGD process.

It is important that the plant holds a sour pH level in the absorber for the complete cleaning of the flue gas. The amount of flue gas that is, every hour, passing through the unit C's plant measures up to 1.6 million cubic meters. The consumption of lime-hydrate is 4.5 tons per hour and the production of gypsum weighs up to around 14 tons per hour. The electrical demand is 7 Mega Watts and the cylinder shaped absorber is 22 by 48 meters. The absorber consists of a metal steel layer to the outside, onto which rubber and coating materials/solvents are glued so that the limestone slurry does not corrode the absorber. The absorber is a complete sealed tank, which no one can access while the unit is in operation.

6 Selection of analyses

This chapter aims to give some background theory in how the best analysis can be chosen and as well to give plant specific answers as a help to choose the right analyses. Then follows chapter 6.2 and 6.3 which describe the chosen analyses and why they were chosen.

6.1 Background theory

There are a large number of different risk analyses available on the market today, as mentioned before. The options are many and it might seem hard to select the right one. Very rarely are there resources for more than one analysis to be performed at each occasion and system. The methods are also quite different (as described in chapter 4) and it is therefore important to make the right choice from the beginning. Below are some points as a help in the selection process, developed from Davidsson (2003) and Schlyter and Selvén (2004):

1. In which phase is the activity/object situated?
2. What is the purpose of the analysis – what is the result going to be used for?
3. What law requirements is the organisation demanded to follow?
4. What resources (time, money, information, etc.) are available?
5. What is the desired detail level of the risk analysis?

6.1.1 Plant specific answers

In the following chapter answers to the five questions given above are made for the specific FGD in the investigated power plant.

Question 1
The erection of the specific FUG facilities was in the 80s. Units A and B have been running since the 60s and were fitted with a FGD in the 80s, while unit C has been equipped with a FGD from the start. In other words, there are already running facilities that are of interest and therefore are risk reducing measures desirable to deal with risks that are already built into the system. For further understanding of the reason to call the two FGDs for “the FGD”, please see chapter 5.1.3.

Question 2
The overall aim for the risk analysis is to identify risk reducing measures for the new FGD facility that is going to be attached to the unit D, which will commence its production of energy in 2011.

Question 3
The overall deciding institution of the law in this field is the German Federal Authority of Environment, which gives instructions and regulations to the different states authorities of environment. They are the ones who decide how the law is used in practice (Davidsson et al 1997).

Einarsson (1999a) and Davidsson et al (1997) are pointing out that safety risk analysis is supposed to take a deterministic approach in Germany and that a QRA is not in general, considered acceptable for preparing statements about total risk from an industrial activity. With a deterministic approach a dimensioning accident scenario is used to decide the facilities risks. The purpose of the deterministic approach is to increase the technological demands and

routines for the facility so that the worst case scenarios will not occur, in a way that the consequences of the dimensioning accident are acceptable for the society.

Question 4
The time for the risk analyses and the vulnerability analyses that are to be performed is limited, as several analyses have to be executed. The amount of available information is estimated to be sufficient. Expertise and people with understanding of the FUG are considered to be sufficient.

Question 5
As the aim for this thesis is to compare a vulnerability analysis with a risk analysis, it is desirable that they have an equal or at least similar detail level. It is, however, desired to be as detailed as possible, since the aim is also to extract the best risk reducing measures compared to their costs.

6.2 Choice of vulnerability analysis method

Many alternatives are still available after the five questions been answered, but since it lies in the scope of this paper to compare a risk analysis with a vulnerability analysis, Stefan Einarsson's work on vulnerability- and risk analyses is of high interest. Einarsson presented, together with Marvin Rausand (1998) "*An Approach to Vulnerability Analysis of Complex Industrial Systems",* an article in the respected *Risk Analyses* magazine in 1998. Einarsson and Sigbjörnsson have also written *"Vulnerability of a hydroelectric power system: A case study*" in 1999, where they used the method presented by Einarsson and Raustrand (1998). The method in Einarsson's articles is developed for an industrial system, like a FGD. The articles and especially the case study give as well a detailed picture of how to conduct the analysis.

Another choice could be to use the first phase of the crisis managements, developed by FEMA (1997) or CCMD (2003) described in chapter 3.2.1 and 3.2.2, as vulnerability methods. They are, however, focused towards the society and not as desirable here for an industrial system. The information of how to conduct the analyses is as well less complete than the previously mentioned articles. The choice falls with that background upon Einarsson and Rausand's vulnerability method.

Einarsson and Rausand's vulnerability analysis is divided into two parts – Identification of Scenarios and Assessment of Scenarios. The purpose of the first step is to discover whether resources are available to mitigate the consequences of the scenario. The main objective of the second step is to establish a ranking of the scenarios according to their criticality. It is important to carefully consider all the potential threats; and in order to simplify this process Einarsson and Rausand (1998) have divided the threats into different risk factors. Even though all potential threats are under consideration, only the ones that are evaluated to be critical are object for further investigation. A HAZOP analysis with modified parameters and guidewords, or something similar, can be used to identify potential hazards together with knowledge of past events and data bases. After the first step is conducted, a decision of whether the quantitative second step is necessary or not is made.

6.3 Choice of risk analysis methods

A very common initial approach when encountering a new object is to perform a so-called preliminary risk analysis. This type of analysis is used to identify hazards, but aims not to describe them in detail (Nystedt 2000). The method can be used to identify hazards in an object that is on the design stage, or one that has already been running for some time. This analysis is many times combined with a more detailed one that assesses and evaluates the severe risks that have been identified. The analysis is based on letting people with experience of the object intuitively rank the different hazards probabilities and consequences, in this way an evaluation from available experience is made (Davidsson 2003). A preliminary risk analysis is therefore chosen as the foundation to get an overview of the risk in the specific FGD. The preliminary risk analysis is also used as the evaluation and prioritising tool for the more detailed risk analysis.

The likeness to Einarsson and Rausand's first step in their method is striking. It is however not as detailed as the second step and therefore another risk analysis with a higher detail level (like a QRA) is desirable to be used as well for comparison reasons. This contradicts the general German practice of not quantifying risks (Davidsson, et al 1997) and will therefore be extra difficult to execute. The focus of the QRA for this specific FGD will therefore not lay on trying to be as exact as possible with its quantitative estimations, but rather show the structure form and the advantages and disadvantages of the approach.

The second step is performed with the help of an event tree analysis. This is a popular form of a QRA and one of its strongest advantages is its graphical way of presenting the risk. In Figure 13 is an example of how an event tree can look like. The basic structure is to start with an initial event (below called "fire starts") and then give different logical options for the outcome to develop into. As the tree is expanding more information is given, e.g. the answer to the question if there are people present or fire extinguishers. There are usually two outcomes and answers to the questions, yes or no. Each answer is assigned a probability of outcome and as the tree expands the probabilities are multiplied with each other. At the endpoint of the tree (here called Outcome X) the different end outcomes are given a consequence if occurred.

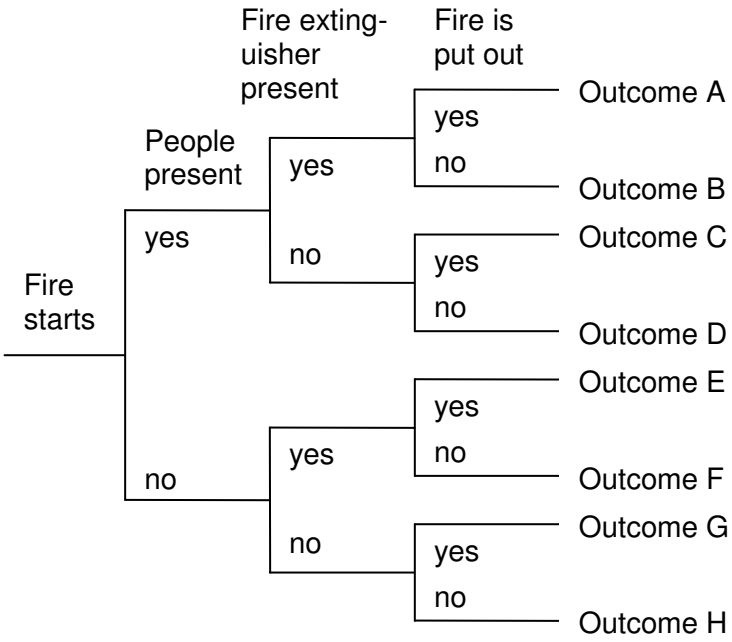


Figure 13 Example of an event tree (Frantzich 1998). Outcome A – F is presented to the right and consists of its individual consequence multiplied with its generated probability.

With an event tree it is easy to get an understanding what significance each specific action has for the overall tree. The end result is a combined estimation of Outcome A – F and a total estimation of the risk is given (in our case if a fire starts).

The event tree analysis can be made in a very high detail level but here it is used to show its potentials and usefulness as a QRA tool, since the detail level of the vulnerability analysis is not so high.

7 Hazard or threat identification

A large part of the result from a risk or vulnerability analysis depends on which hazards or threats have been identified. The identification is then dependent on the system borders and restrictions. Depending on where the lines are drawn for the system, different hazards and threats will be included in the analysis. As mentioned before a vulnerability analysis has a broad view of a system, also called “an open system approach”, while a risk analysis has a more narrow view, also called “a closed system approach”. The selected and described methods below will reflect that in a prominent way.

7.1 Hazard identification for the risk analysis

There are three categories of risk identification methods according to the International Electrotechnical Commission (IEC 1995) - The *Comparative methods*, includes methods as checklists, hazard indices and reviews of historical data. *Fundamental methods* are for example Hazard and Operability (HAZOP) studies, and Fault Modes and Effect Analysis (FMEA). The last group is Event tree and Fault tree methods which are of *Inductive reasoning techniques.*

The different time consumption and difficult level attached to this categorisation are also reflected, with Comparative methods, offering the least amount of effort and the Inductive reasoning techniques the greatest. In the light of only limited time a comparative approach was used in this paper, for the hazard identification.

With the support of a suitable developed checklist, hazard identification can be achieved as the first step in a preliminary risk analysis (Kemikontoret 2001). Such a checklist can also be based on suitable parts of the organisations own general checklist. Checklists are however normally made up of previous experiences and are used to identify already known hazards and to ensure that set standard procedures are followed (Nystedt 2000; Kemikontoret 2001). A well made checklist is dependent on good knowledge and long experience of the process of the facility in question. Checklists, though, can look very different from each other and there is a large diversity in detail levels between them. Checklists are also easy to use and offer a fast and cost efficient way to identify hazards.

7.1.1 Choice of the specific checklist

The checklist that was chosen for the specific FGD is based on Kemikontoret’s (2001) checklist, Appendix 1, which is also presented in this paper’s Appendix 1. A selection of questions has been chosen and attempts to reflect the whole spectra of Kemikontoret’s questions, looking at aspects from process development/construction, erection/montage, start-up and during operation. Questions concerning demolition have been neglected in this paper. Before the work with the development of the checklist, a discussion was conducted with the safety, health and environmental department of the company to understand where the greatest problems were and to focus the checklist towards their risk perception.

7.2 Hazard identification for the vulnerability analysis

In the method of Einarsson and Rausand (1998) follows an identification step that divides hazards (or risks as they call it) into two major categories - internal and external risk factors,

illustrated in Figure 14. Their attempt to identify relevant risk factors is not to be thought of as a complete description of all possible risk factors but to highlight the important ones. They claim that the list of possible risk factors never can be complete, but that their classification is a useful tool that may aid to identify vulnerability problems.

Presented in Appendix 3 is the set of questions, which are developed from the risk factors. They are used to identify and get a deeper understanding of some of the problems that can be relevant for the power plants risk factors.

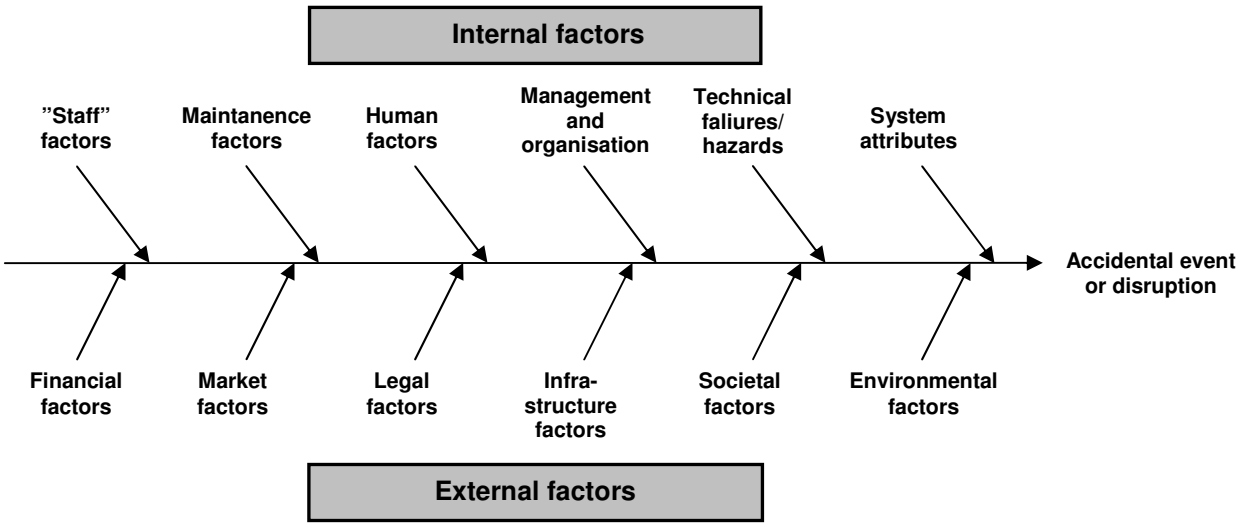


Figure 14 Cause-effect diagram illustrating the various categories of risk factors influencing an accidental event or disruption in a technical system (Einarsson and Rausand (1998).

7.2.1 Internal risk factors

7.2.1.1 System attributes

As the technology is advancing and systems are getting more complex, there are those (like Perrow 1984) that claim that accidents are inevitable. He has classified systems upon two variables:

- System interaction (linear vs. complex)
- System couplings (loose vs. tight)

A linear system is easily overlooked, just as how the different components of the system interact and are dependent on one another. In a complex system, the situation is the opposite. It is hard to predict why accidents occur and also hard to say why an accident occurred because the action-effect relation is not obvious. With an aging system the system also tends to be more complex, since as time goes by more and more extra functions or temporary replacements are added to the original version.

The "just in time" principle that is used a lot in the western world today is an example of tight couplings in a system. The advantages of a system with tight couplings are its efficiency, flexibility, and above all its reduction of costs. The downsides are however that the system is more vulnerable since it gives little or no buffer space for malfunctioning components (Einarsson and Rausand 1998).

Scott D. Sagan (2004) is pointing out that Perrow's theories are to be used as what "*confounds even smart and dedicated organisational efforts to produce perfect safety*". System interactions and couplings have the potential to work in the opposite way against redundant systems (safety systems). Sagan presents three ways that redundant systems can work against an increase in safety. The first problem is that more redundant features also increase the complexity of the entire system. Secondly, humans have the problem of being less observant when their responsibility decreases. The more people are surveying the same system the less each individual tends to feel responsible. Thirdly organisation leaders have the tendency to increase production pressure when safety functions are enlarged, leading to the benefits of the safety functions are lost. For example the increase in safety that down hill skiers may obtain when wearing helmets are many times lost due to increased speed (Sagan 2004).

7.2.1.2 Technical Failures and Technical Hazards factors

The malfunctioning of components in a system is maybe the first and only risk an untrained person might think of. The technical failures and hazards naturally have a significant influence on the total systems vulnerability. Expensive equipment does not usually have access to a back-up system or even spare parts, and might therefore lead to large economical losses, in case of failure. Less expensive equipment might contain great value and a malfunction could lead to great economical losses, e.g. a CD containing valuable information gets damaged. Even though a technical failure with a component usually only creates limited consequences, it might cause extensive "second effect" damages, e.g. a longer and very expensive shut down of a system (Einarsson and Rausand 1998).

7.2.1.3 Human factors

For quite some time now human factors have been considered to be associated with the highest number of accidents; over 80% of the total number of accidents is associated with human errors (Einarsson and Rausand 1998). In the human error field, it is also common to discuss *active* and *latent failures* as reasons for accidents. The active errors are the starting point of the accident chain; they are committed by the operator and can also be called unsafe acts. The latent failures can also be called "resting failures," and they need a trigging factor in order to develop into an accident. Latent failures are the result of poorly designed systems or fallible decisions by the management. Latent failures are hard to identify and are the reason for many major accidents, e.g. the Chernobyl accident or the M/S Herald of free enterprise accident (Reason 1990).

7.2.1.4 Management and organisation factors

The leadership and the management of an organisation are closely linked to human factors as described above. If the management does not bring risks and accidents up on its agenda then the entire organisation will suffer in the end. The board needs to demonstrate how important it is to keep accidents at a minimum or the employees might become careless. Appropriate tools for the management are: assigning a group(s) within the organisation to carry out their decision, developing standards, controlling the employees and carrying out safety analyses.

7.2.1.5 Maintenance factors

Maintenances are a large factor in causing major accidents, either during the process or just by being inadequate or incorrectly performed. An estimations of 35-40% of all serious accidents are in some way linked to maintenance, given for the process industry in the Nederland's (Hale et al 1993), and 30% in the chemical industry by the British Health and Safety Executives. The two main reasons for maintenance related accidents are usually considered to be human errors and inadequate organisation (Einarsson and Rausand 1998).

7.2.1.6 Staff factors

There are many aspects that are included in staff factors. For example:

a. Strikes and other labour conflicts
b. Loss of key personnel
c. Recruitment of new staff, availability of skilled personnel
d. Safety culture – job dedication
e. Unfaithful servants, embezzlement, sabotage, etc.)
f. Liability/damages claim from staff members (e.g., asbestos)

7.2.2 External risk factors

7.2.2.1 Environmental factors

It is easy to be confused today when talking about environmental factors and risks, thinking it involves global warming. This is not the case and to prevent this confusion perhaps environmental factors should be renamed as natural threats and hazards, since it deals with (Einarsson and Rausand 1998):

a. Geological threats (earthquakes, landslides etc.)
b. Meteorological threats (storms, floods, draughts, frost, lightning, etc.)
c. Biological hazard (epidemics viruses, bacteria etc.)
d. Extraterrestrial hazards (meteorites, cosmic radiation etc.)
e. Technological hazards (pollution, nuclear radiation, etc.)

7.2.2.2 Societal factors

In the societal factors the cultural and the political aspects are brought into the system. The political climate has a direct influence into the amount of sabotage and terrorist attacks that are directed towards the organisation. Different cultures have also different views on safety (Einarsson and Rausand 1998). The armed forces of USA and the Soviet Republic are a good example of this. The Soviet philosophy was to create military equipment that worked well during hard conditions, especially in war. The American philosophy relied on that their equipment was served and trimmed up at all times for the maximum performance and prevention of malfunction.

7.2.2.3 Infrastructural factors

Einarsson and Rausand (1998) are pointing out the increasing use of computer software as a potential risk factor. Computer software is still becoming more important and even though it brings advantages with the development, it also brings more vulnerability to the system. A

rough estimation is that 20% of all companies that suffer a major computer disaster never recover (Einarsson and Rausand 1998). There are several ways for this to happen, such as hackers, fires, deliberate sabotage, etc.

Other aspects can regard transportation of necessary equipment and raw materials to the process. If the supply company does not deliver the goods, then a crisis can occur like for Ericsson in the beginning of this millennium, due to a fire at a supplier's factory in Mexico.

7.2.2.4 Legal and regulatory factors

With increased demands of laws and regulations from the government, a company might be heavily impacted and vulnerable to sudden decisions. A certain law might be changed and may, for instance, demand that a company let out less pollution gases than before, and the consequences in economical terms can be massive. The Seveso directive was altered after the Sandoz fire in Basel, Switzerland and the Bhopal accident in India is an example of this (Seveso II Directive 2007).

7.2.2.5 Market factors

There is a long row of potential market factors that may influence a system's vulnerability. The market for selling products can decline or the market for buying raw material might rise, to the extent that the benefit of selling a product turns out to be negative. Perhaps the potential of the largest losses lies within lost market shares due to an accident? The accident itself might not cause those large economical losses, but while the production is down other companies come and take their market shares (Einarsson and Rausand 1998). Another reason for lost market shares due to an accident might be that the company gains a bad reputation.

7.2.2.6 Financial factors

Companies are often in the position where risky decisions have to be made, and if the decision turns out to be wrong can it in extreme cases lead to bankruptcy of the company. The state of a company's economy does not just affect the company itself, but also other dynamics like the employees. With a bad economical result, the stress levels amongst the employees might increase, which might lead to a decrease in safety measures and safety culture. A bit of stress might, however, be beneficial to the company as it boosts the employees' work performance (Einarsson and Rausand 1998).

The company's economy might also impact the risk and safety prevention performance, due to less money being available for new safety features. If a company is under economical pressure for a long period, it might even influence the risk policy and the safety goal.

8 Results from analyses

The result from the analyses is presented in two different main parts for each method. The first part is qualitative and aims to answer the questions from the hazard identification phase (Chapter 7 and Appendix 1 and 3). The second part is of a more quantitative nature which selects the main hazard and carries out an in-depth study of those hazards.

8.1 Risk analysis

This part presents first an overview of the hazard identification. Secondly, an event tree analysis is carried out on the risks that were identified to withhold the largest threat. In combination with that, a sensitivity analysis evaluating the uncertainties of the assumptions taken in the event trees analysis is executed.

8.1.1 Overview of hazard identification

The hazard identification of the analysis is based on the checklist questions presented in Appendix 1. The best way of presenting the result is thought to be in a deliberative way, as it is considered to be less confusing as the answers are, in some extent, overlapping. The questions will be answered according to the five different themes (the same as in the checklist in Appendix 1). In the end, a discussion about representative risk scenarios is found, which will be background information for the event tree analysis that follows.

8.1.1.1 Substances

The substances used in the construction of the FGD are polyethylene (plastic), rubber, toluene (glue), stone wool (insulation) and steel. The stone wool consists of stone and aluminium and is used for insulation of the FGD and does not contain any carcinogenic substances, e.g. asbestos.

Polyethylene is a thermoplastic and consists of only carbon and hydrogen (KEMI 2007). As most plastics, polyethylene burns well and can, even in granular form mixed with air, cause a dust explosion. The melting point of the substance is 85-140 °C, the flash point is 341 ^{o}C and the auto ignition temperature is 330-410 °C. The interval depends on the manufacturer's ability to add additives, which considerably alter the melting point of the substance. The material is however hard to ignite. Suitable fire extinguishing substances are powder, water spray, foam and carbon dioxide (ICSC 2007).

The rubber material in the FGD is called "Isobutyl rubber" and consists of 99 % isobutylene and 1 % isoprene. Butyl rubber has a flash point ("*the lowest temperature at which a flammable vapour/air mixture exists at the surface*", Drysdale 2002) of 250 ^{o}C (ExxonMobil 2002). There are many different variations of this substance, in common is that they all refer to it as highly flammable characteristics. Isobutyl rubber consists of isobutylene which is classified as extremely flammable with an auto ignition temperature of 465 ^{o}C. The other substance that Isobutyl rubber consists of, Isoprene, is also classified as extremely flammable with an auto ignition temperature of 220 ^{o}C (European Commission 2000a), or 427 ^{o}C (NLM 2007). When rubber is burning it produces very large amounts of black smoke. The rubber material is elastic and works as a corrosive protection layer between the steel and the

limestone slurry. An appropriate fire extinguishing substance is water spray (ExxonMobil 2002).

Toluene is the largest single substance in normal gasoline, but is also used in other products. In the FGD glue based on toluene is used to stick the rubber to the steel. When attaching new rubber to the steel, the rubber is prepared with glue outside the FGD for maximum fresh air supply. Meanwhile is also pure toluene present for the production of the glue. Inside the FGD instruments are placed that measure the concentration level of toluene in the surrounding air, these give a warning signal at half the concentration of the lower explosion limit (0.6%). Toluene is both highly flammable and explosive between the concentration limits of 1.2 – 8 % (v/v). The effect on humans is not very severe; the glue has an oral and dermal LC_{50} value of > 2000 mg/kg and an inhaling value of > 5 mg/l, which is generally regarded as not lethal. Toluene has low acute toxicity, and humans experimentally exposed to toluene experienced headache, dizziness, feeling of intoxication, irritation and sleepiness due to concentrations of 75 ppm (281 mg/m_3). Its flash point is 4 ^{o}C and its auto ignition temperature is 535 ^{o}C. Toluene ought to be and is extinguished in the plant by ABC-powder, water and alcoholic proofed foam (Aug. Hedinger GmbH & Co 2003; ESIS 2007; European Commission 2003).

The substances in the FGD during operation are flue gases, a water and limestone mix called limestone slurry and the by product - gypsum. Limestone is handled with appropriate gloves and glasses for the protection against mechanical irritation of the skin and eyes. Limestone dust is usually regarded as a low hazard for usual industrial handling. Gypsum has the same low hazardous effects as limestone. The limestone slurry is highly corrosive and can cause burns to the skin and eyes. The slurry is sprinkled over the flue gases with high pressure. As the facility is closed during operation and only restricted access is possible for workers due to minor repair work, the contamination risk of workers is evaluated to be low.

8.1.1.2 Construction/Design

The FGD is partly divided into different fire cells. Since the flue gases need to flow freely in large channels (diameter of around 3-6 meters), desirable fire walls are impossible to implement and divide the facility into small fire cells. There are fire walls between the gypsum configuration hall and the absorber. Therefore, if a fire starts in the absorber, or in the heat exchanger, the fire has the potential to spread into the other part. In case of a fire, movable water screens, which are placed around the working place during repair works, are manually turned on. The best position for the water screens is in the pipe between the heat exchanger and the absorber; in this way could a fire be (in best case) prevented from spreading between the two different parts.

The rubber used in the FGD melts at the temperature of 95 ^{o}C and could, together with hot flue gases start flowing down the walls of the FGD. There is, however, only one place in the FGD, inside the heat exchanger, that operates with flue gases that have that high temperature. Fortunately, the heat exchanger is only clothed with rubber where the temperature is around 65 ^{o}C. If the flue gases would be too warm despite this, due to some malfunctioning in the system, there is an automatic system that would shut down the FGD immediately.

8.1.1.3 Montage/Repair work

Most of the repair work that is conducted on the power plant is done by different contractors. These contractors have to follow the written regulations of how to perform safe maintenance

work, issued by the power plant company. Each contract worker receives a copy of the regulations the same time as a safety information meeting is held the first day workers arrive at the plant. Each and every contract worker, responsible person for the contractor and plant site management have to sign that they will follow the regulations. In other words, all workers have the responsibility to comply with these regulations. Fire prevention responsibilities must be defined clearly before repair works starts, according to the fire preventing procedure of the company. The contractor is responsible for only using the right tools (special lamps, electric apparatus etc.) and the company is responsible for the fire protection.

The German law regulating work safety (ArbSchG 1996) is based on the European directive 89/391/EEG (Swedish name) or 89/391/EWG (German name) which is similar to the Swedish law (Arbetsmiljölagen 1977:1160). Both laws are based on the same directive and can hold the single worker, the contractor and/or the company responsible if they break the law.

Contactors come often from other countries than Germany; commonly from east Europe and have gathered their skill there. According to an expert at VGB - PowerTech there could be a problem arising out of the fact in such countries the safety culture is not always comparable with that of Western Europe. However a thorough investigation of the contractors is made prior to employment, so that the company becomes aware of its safety performance.

During repair work, a safety engineer is making at least two rounds a day to inspect that the work is performed according to the written regulations. Aspects such as no smoking, use of the appropriate safety equipment, making sure the plant is in order and keeping it clean, etc., are checked.

8.1.1.4 During operation

The operation of the FGD is observed from the control room of the whole power unit. The operators there are following set written routines. An operator has to go through a long line of education. After a practical focused high school, they will have to do an apprenticeship school for three years for power plant workers. An additional school time of three years is demanded for them to become shift foremen. Routine training/education once a year is mandatory for all workers and for workers with special dangers associated with their work the training is twice a year.

The outgoing shift changes information of the present situation by passing forward it from the foreman of the shift to the next foreman. For that purpose written protocols is signed and works as additional information to the new shift workers. There are however no records of previous accidents or “near misses” since, according to the company, there was never anything to be reported.

8.1.1.5 Emergency response

When the FGD is under repair work and the facility is not in operation, there is an educated nurse in the plant’s emergency room, located on the ground floor of the building attached to the turbine house of unit A and B. The nurse is, together with the power plant’s own fire department, the first on the scene when an accident occurs. After 10-15 minutes the local town’s fire department and ambulances will as well come to aid.

The company has also trained 40 of its workers as regular firemen (according to German standard) and during repair work such a worker is given the task of being a fire watch. There are a minimum of 7 firemen on duty at the same time in the plant. The fire watch's overall objective is to monitor the work areas, especially during breaks and after work is finished. There are also mobile smoke detectors as an aid for discovering fires, see photo below.

Figure 15 A stand with a smoke detector at approximately one meter above the ground inside the absorber.

The fire watch is to be on duty from the moment of the opening of hatches and/or manholes until they are closed again. Before the repair work commences, the fire watch has the responsibility to set up the fire extinguishing equipment and test proper functioning. The workers and the fire watches are supposed to use this equipment for initial fire fighting, first from within the FGD and then, if the fire is not suppressed, from the outside through hatches. If the fire would continue to spread there are three different staircases to make use of as emergency escape routes.

There is, furthermore, an internal alert plan for the workers in case of an emergency. The worker that discovers the event reports it to the unit watch in the control room, and they report further to the shift foreman who alarms the internal and public fire department, the emergency nurse, the catastrophe protection and the responsible engineer. The engineer notifies the appropriate people according to the alarm plan.

Safety equipment is to be placed according to the fire prevention procedure issued by the company. The procedure describes how pressurised fire hoses, ABC – powder extinguishers, water screens, and optical smoke detectors are to be used and placed. Safety equipment is regularly checked according to a plan with the responsibility of the fire protection chef. Every 2^{nd} year the fire extinguisher is checked, and four times a year the detector and alarm bottoms are checked. The public fire department comes every 5^{th} year for their controls of the plant and the insurance company have their checks every 2^{nd} - 3^{rd} year and, in addition, they perform random tests when they know that repair work is in progress.

A risk analysis has been conducted concerning external events such as earthquakes, volcanoes, tsunamis, tornadoes, hail and lightning. The risk is presented in a list which has been assigned a simple risk scale from 1-4, 1 being equal to no risk and 4 being equal to high risk (see Appendix 2 for further information).

8.1.1.6 Risk scenarios

The largest threat for the FGD is regarded to be a fire starting in the rubber. Initiating factors are for example welding, cutting, lamps and radiant heaters, which are used during maintenance work. This treat is mainly due to carelessness, lack of feeling responsible, plain disobedience and lack of motivation of the workers. The instructions and information on how to perform safe work are plentiful and adequate. A rather frequent carelessness or disobedience seems to be smoking amongst contract workers. During safety checks by safety engineers, workers are reminded of the rules but the problem is nevertheless not completely eliminated. The risk is due to inadequate safety culture amongst the contract workers and not due to the company's safety information.

It is more likely that a fire will start in the rubber than in the polyethylene. If the rubber is ignited then the glue is as well. In Appendix 4, a chart is presented based on VGB – PowerTech's (1998) handbook for fire safety in power plants. Together with the help of the company, an expert at VGB - PowerTech and people from the insurance company, a preliminary risk evaluation is presented as well for the different ignition reasons in Appendix 4.

Since fires in the rubber are so likely to develop with an extremely fast rate it is of highest essence that prevention measures are working to the fullest and immediately. The obvious risks here are - that fire detectors, water screens and fire hoses malfunction, or that they are set up in a faulty way. Another risk is if they are placed in a wrong way and are therefore not effective. Problems with the fire watch can be that he/she can not be everywhere at the same time. When repair work is conducted, many workers can perform fire causing exercises (e.g. welding and cutting) on several places simultaneously. Likewise welding or cutting can cause a fire far away from the source: sparks can fall or jump long distances to initiate a fire. Fire hoses, detectors and screens have usually a very low faulty frequency, especially when they are regularly checked. The largest potential danger is more likely to be the placement of the equipment in a right and effective way. Figure 15 shows a stand with a fire detector, approximately one meter above the ground. This equipment was set there to detect if a falling spark from above, due to cutting, would ignite the rubber on the floor right below. A stand with a fire detector is likely not to identify an uprising fire, as the smoke gases are likely to pass on the side of the detector on its way to the top of the room. A more effective placement would be if the detector is placed in the ceiling of the room.

In short form; the first risk scenario is a fire uprising during maintenance work, initiated by welding, cutting, etc. by workers, due to their carelessness, lack of feeling responsible, plain disobedience and/or lack of motivation. The fire is then spreading to involve both the absorber and heat-exchanger, since they are connected without firewalls. The extremely fast fire growth is making it very hard for fire suppression, if not immediately initiated.

The second risk scenario involves the toluene. Leakage of a toluene container can generate a dangerous concentration in the air for the workers. Since the concentration of toluene is supervised and the handling time is minimised, the risk of workers being injured is regarded as small.

The third risk scenario concerns the limestone slurry. The corrosive limestone slurry is handled with care and workers are protected with gloves and glasses. An unfortunately event could, however, cause a worker to get contaminated during cleaning of the limestone slurry

tanks. The consequence in such an event should be limited and the worker should only obtain a light injury.

External risks as presented in Appendix 2 can be regarded as the fourth risk scenario. It should be mentioned that the (in Appendix 2) discussed risk are considered to have less effect on the FGD than the power plant as a whole.

The fifth risk scenario is also the only identified risk during operation. According to the company and VGB – PowerTech (1998) the only real risk is combined with repair work and maintenance in an FGD. The operation of the FGD is controlled by an automatic computer system, which is surveyed by employees. There is more or less no other human interface with the FGD during operation. The statement that there is no real risk associated with the FGD during operation is therefore likely, however to some regards unfortunate. To regard the FGD during operation as flawless in combination with no reporting system for "near misses" or accidents is a risk in itself.

8.1.2 In-depth study of fire risks

The in-depth study will first give a description of the scenarios, followed by the estimation of the risk and finally a presentation of the result.

8.1.2.1 Description of scenarios and method

Two fire scenarios are chosen to represent the fire threat of the FGD. There are naturally many more possible scenarios but will here have to be restricted due to time limitations.

1. A fire that starts in the rubber, caused by welding or cutting, in the immediate surrounding of the working personal.
2. A fire that starts in the rubber, caused by welding or cutting, not in the immediate surrounding of the working personal.

In case 1 the detection of the fire is almost immediate as there are always more then one person present during welding or cutting. Problems with putting out the fire should be small since the trained fire watch and other personnel are always around with plenty of water and extinguishing equipment. Calculation supporting this idea can be found in the next chapter, where the fire growth is compared with the water extinguishing capacity of the fire hoses and nozzles that are used at the site.

In case 2 the problem is quite different. Here the detection time is dependent on the patrolling fire watch and smoke detectors. The problem might be that the distance to the fire for the fire watch is too long and he/she does not reach the fire before it has expanded beyond controllable. A comparison between the fire growth and the water extinguishing capacity at the site is used to determine how likely it is that the fire is suppressed. The scenario is described in Figure 16 and in chapter 8.1.2.2 the assigned probability values are addressed that concern the scenario, while additional information can be obtained in Appendix 5 and 6.

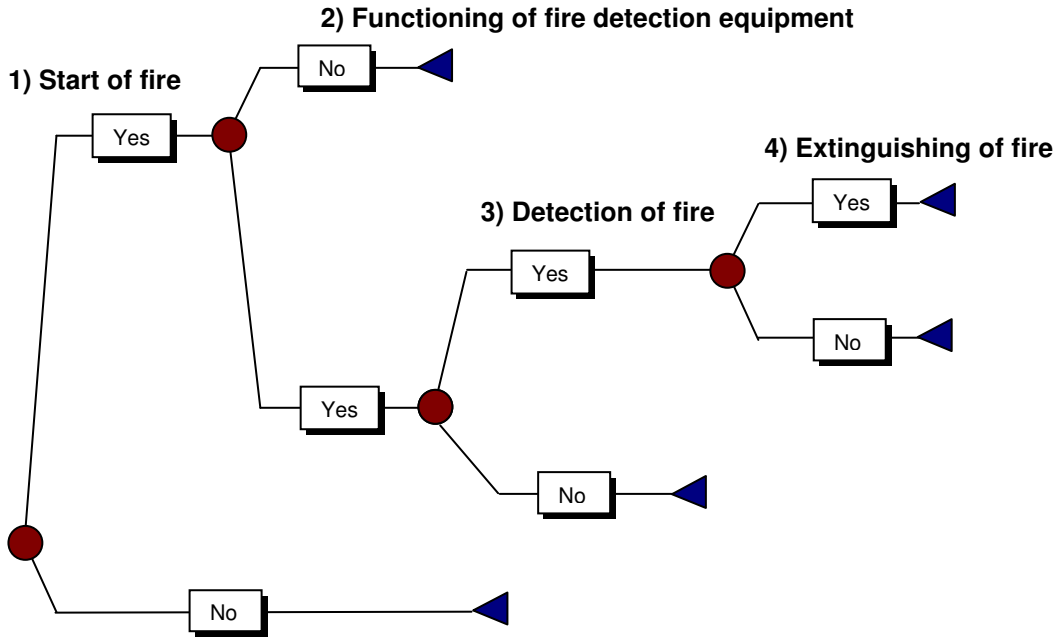


Figure 16 Event tree analysis of fire scenario 2.

8.1.2.2 Estimation of probability values for event tree analysis

1) Start of fire

The event tree (Figure 16) starts with what is called a "change nod", indicated with a red dot, concerning the start of a fire or not. The probability for a fire to start caused by welding is roughly estimated in the preliminary risk analysis and given a value of 1/10 - 1/1000 times per year (see also Appendix 4). A triangle distribution with the maximum value of 1/10, a middle value of 1/100 and a minimum value of 1/1000 fires per year is therefore used.

2) Functioning of fire detection equipment

There is always a possibility that the optical smoke detector and/or the fire alarm system will malfunction. The company checks the detectors and the fire alarm four times a year. The probability for malfunctioning decreases with increasing test runs. A smoke detector that is tested every third year has a probability of 0.13 (Levinson and Yeater 1983; Guymer and Parry, date unknown) to not be operational, while a smoke detector that is tested every year has a probability of 0.0242 (Kluge 1985) to malfunction. The fire alarm system is also dependent on check-ups, making it important that the service of the system be done by an authorised firm according to a set appropriate standard. A service done by such a firm will result in an expected malfunctioning of the fire system of 0.03, an authorized firm conducting a check-up not according to standard will generate a probability of 0.076 and a check-up by a non-authorised firm 0.147 (Moore 1993).

Since the company checks the whole system with an authorised firm according to standard the 0.03 value is appropriate to use. When including the information of decrease in malfunctioning due to more frequent check-ups a value of less then 0.242 is more appropriate. A triangle distribution for the malfunctioning of detectors and fire alarm is set to contain a maximum value of 0.03, a mean value of 0.02 and a minimum value of 0.01.

3) Detection of fire
There are two ways to discover the fire, first by the smoke detectors and secondly by the personnel and especially the fire watch.

As shown in Figure 15, the smoke detectors are, in some cases, put only about one meter above the ground. The reason for this placement is due to the assumption that a fire will only start directly under the detector. This assumption is proven to be risky since the radius of a fire plume on one meter elevation is estimated to be around 18 centimetres (calculations can be found in Appendix 5). It is much more likely to believe that the fire will start on a place further away from the detector than a distance of 36 centimetres (see figure 17).

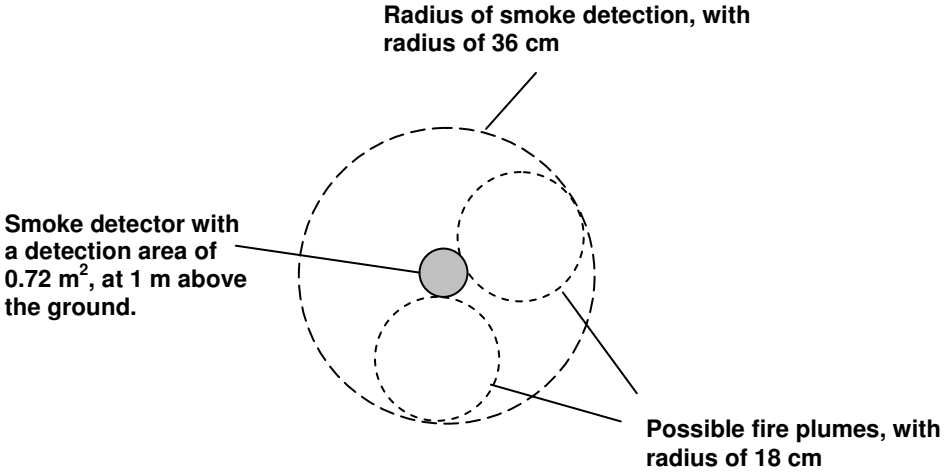


Figure 17 Demonstrating the detection area of the smoke detector.

The plume radius is dependent on the height above the surface and varies some as seen in Appendix 5 and as well the model for the plume estimation is based on a few simplified assumptions. The numbers in figure 17 are therefore to be taken as an estimate.

Even if the smoke detector is (more by luck than skill) placed in a way that the fire starts directly under it, it is difficult to predict if the fire is likely to be discovered in time for fire fighting. The probability estimation of detection is hard to generate. How unlikely the smoke detectors may detect the fire is hard to predict with only knowing the fire plume radius. Detection is as well dependent on employees taking fire watch rounds etc. The event tree analysis should include an additional branch for the case in which the fire detection system is out of operation and the fire is detected anyway, if the tree is made properly. The influence of the result is, however, very small and problems in generating the likelihood for such an event exceeds the benefits. There are, anyhow, a large number of such estimations and the analysis is not thought to benefit from any more uncertainties. The aim is not to be as precise in the result of the analysis as possible, but rather to demonstrate the procedure of a risk analysis.

The probability of detection is only a rough estimate and includes both the likelihood of a functioning detector and the likelihood of an employee to detect the fire. The uncertainty here is great for the probability estimation and therefore a uniform distribution with a large spread is chosen, with a maximum value of 0.4 and a minimum value of 0.01 for the smoke detection of the fire.

4) Extinguishing of fire
The estimation of the probability for the fire to be extinguished is based on the initial fire growth compared to the extinguishing capacity on site.

The fire growth is estimated to follow a αt^3- curve, similar to other fire tests with plastic materials. In the tests, presented in Initial Fires (Särdqvist 1993) the plastic materials are covered onto the walls and the ceiling of the fire rooms. In this fire scenario the rubber covers the floor of the fire room as well. In accordance with the tests, it is assumed that the initiation of the fire is made in the corner of the room and that the initiating effect is around 100 kW. These are both conservative assumptions, since a fire could also easily be initiated in the middle of the room, something more similar to a pool fire, with a much slower initial horizontal fire spread. The difference in materials, between the plastic and rubber, causes an uncertainty problem and therefore several curves are illustrated below. There are five different fire growths presented and two of them Söderblom and Sundström, are taken from Initial Fires. The other curves are faster, slower and a mean value of Söderblom and Sundström's curves.

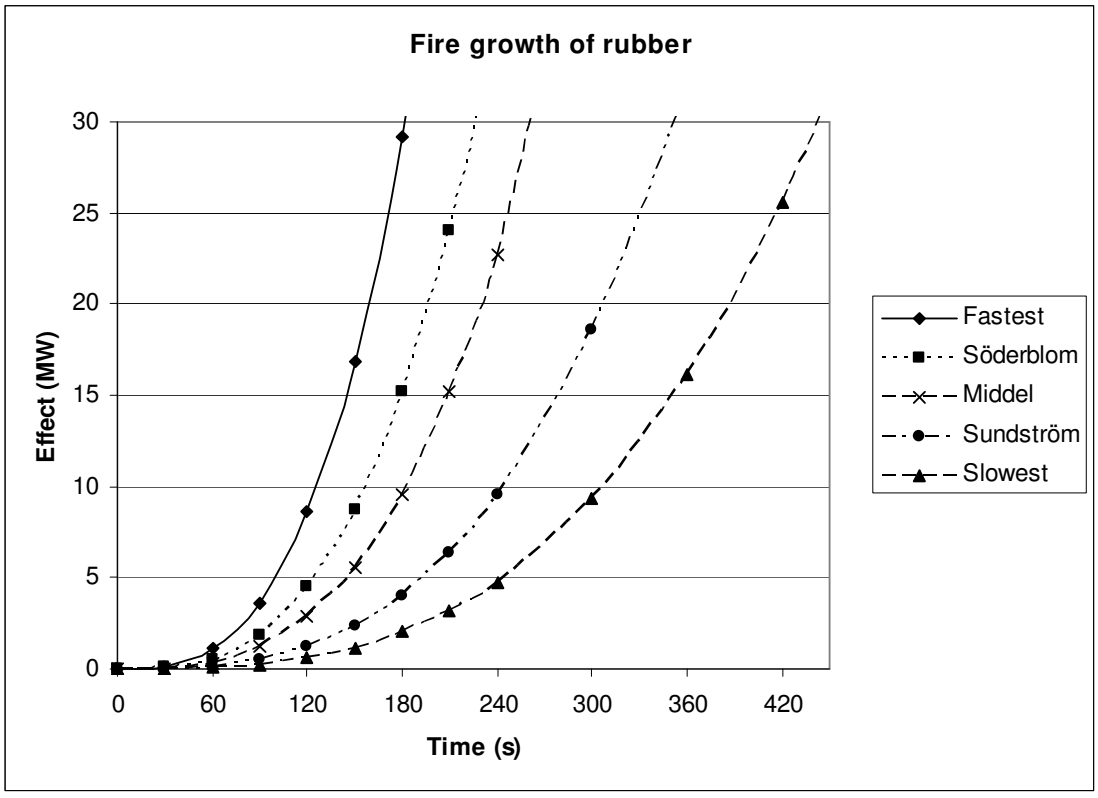


Figure 18 Fire growth of rubber.

The variety of fire growth is large but is nevertheless useful for the estimation of the fire fighting success.

The second variable is the extinguishing of the fire with the help of water. Water has an enormous fire extinguishing potential if applied in the right way. By adding water, the heat of the fire is transported to the water which turns into vapour. The heat of the fire is in that way consumed and loses its potential to keep burning. The extinguishing capacity of water is highly dependent on the size of the water droplets, with variations of REMP-value of 2 - 40 (Särdqvist 2006).

The company uses two different methods for putting out the fire with fire hoses, if the water screen that has its main function to prevent the spre6ading of fires is disregarded.

1. The fire watch and personnel in the immediate surrounding are to initiate exterior fire fighting, if possible, before the power plant's own fire department shows up. The available equipment includes fire hoses and fire extinguishers. Outside all openings of the FGD are fire hoses with standard nozzles placed. The fire hoses are for the most part pressurised during working hours. With these nozzles and with an exterior fire fighting tactic, the water droplets become so large (over 2-3 mm) that they pass through the flames nearly unaffected (Särdqvist 1996).

2. The second approach is the power plant's own fire department. Their time demand for initiating suppression is 3-5 min. They are equipped with additional equipments of air tubes and better nozzles (Fog fighters). They can apply water with droplets of less than 1 mm. This way, the droplets are combusted in the flames and a much higher extinguishing effectiveness of the water is possible. A factor of three can be added on the extinguishing capacity due to only 30 - 35 % of the energy being enough to put out a fire consisting of diffusion flames, compared to standard nozzles (Särdqvist 1996).

Calculating the potential heat absorption capacity of water is done in the following way:

Water is first heated from its initial temperature (assumed to be 10°C) to 100°C,
$(100 - 10)°C \cdot 0.00418$ MJ/kg°C = 0.38 MJ/kg.
Vaporisation of water at 100°C needs 2.26 MJ/kg.
To continue heating the water vapour is proportional to the following equation,
$(T - 100) \cdot 0.00201$ [MJ/kg], where T [°C] is the actual vapour temperature.

A fire fighting tactic as in method one (1) above has a lower heat absorption capacity than the second tactic. In method one, the water can have a maximum heat absorption of 0.38 + 2.26 = 2.64 MJ/kg, while method two has $2.64 + (T - 100) \cdot 0.00201$ MJ/kg (Särdqvist 1996).

In practice, water is not applied in this perfect way as the equations above suggest. Much of the water that is put on the fire is not vaporised. This is applicable on both methods and gives a maximum heat absorption of 0.38 MJ/kg. Many tests have been executed to determine the efficacy factor of how much of the water is applied with a maximum outcome. The results show that 0.2 – 0.4 are good estimates of this. This is, however, a very unsure estimation that depends on several factors, such as skill of the operation man, fire fighting tactic and equipment.

In Särdqvist (1996) some suitable values have been assigned to fire fighting as in the power plants tactics. For interior fire fighting with fog nozzles (as in case 2), an efficiency factor of 0.2 was used. For long-range fire fighting with well placed nozzles (as in case 1), an efficiency factor of 0.3 was used. These same numbers will be used in this paper.

For the calculations with the Fog fighter (fog nozzle) the assumption is that the actual vapour temperature is 600°C, since it is commonly used as a flashover temperature.

Equipment	Maximum heat absorption [MJ/kg]	Water flow rate (l/min)	Efficiency factor [-]	Heat absorption capacity [MW]
Standard nozzle (4 mm)	2.64	50	0.4	0.9
Standard nozzle (9 mm)	2.64	100	0.4	1.8
Standard nozzle (16 mm)	2.64	400	0.3	5.3
Fog nozzle	3·3.64	130	0.2	4.7
Fog nozzle	3·3.64	150	0.2	5.5
Fog nozzle	3·3.64	800	0.2	29.1

Figure 19 Chart of rough estimation of fire fighting ability on site.

With the help of the fire growth curve (figure 18) compared with the fire extinguishing capacities of the available nozzles on site (figure 19), the following conclusions can be made:

- With the 4 mm standard nozzle all model fires can be extinguished until approximately 60 seconds after ignition. The middle curve implies a slightly longer time of around 80 s and the slowest fire growth curve suggests that extinguishing is possible until 140 s after ignition.
- With the 9 mm standard nozzle all model fires can be extinguished until approximately 70 s after ignition. The middle curve implies a slightly longer time of around 100 s and the slowest fire growth curve suggests that extinguishing is possible until 180 s after ignition.
- With the 16 mm standard nozzle all model fires can be extinguished until approximately 100 s after ignition. The middle curve implies a slightly longer time of around 150 s and the slowest fire growth curve suggests that extinguishing is possible until 250 s after ignition.
- A BA team with a fog nozzle and a water flow of 130-150 l/min has almost the same potential fire extinguishing capacity as the 16 mm nozzle.
- A BA team with a fog nozzle and a water flow of 800 l/min has a significantly larger capacity and all model fires can be extinguished until approximately 180 seconds after ignition. The middle curve implies a slightly longer time of around 260 s and the slowest fire growth curve suggests that extinguishing is possible until 440 s after ignition.

Equipment	Time (s)		
	Slowest	Middle	Fastest
Standard nozzle (4 mm)	140	80	60
Standard nozzle (9 mm)	180	100	70
Standard nozzle (16 mm)	250	150	100
Fog nozzle (800 l/min)	440	260	180

Figure 20 Chart over the different times to reach fires that are not possible to be extinguished in regard of different nozzles and fire growth rates.

To simplify the fire scenario, it is assumed that the time for the detection of the fire is the same as the ignition time. There are extensive materials available from among others Drysdale (2002) on both detection time models and ignition time models, but which fall outside of the scope of this paper. By doing this simplification, one can compare the times in Figure 20 with the stated fire department response time and what is likely that the fire watch has for response time. The meaning of response time is here the time it

takes for the fire department/watch to be ready to suppress the fire after they are informed of the fire.

If the fire is developing according to the slowest fire growth (440 s) and the fire department is responding with the shortest response time (180 s), the fire is likely to be extinguished. It is, however, much more likely that the fire is developing faster and that the response time is longer. For the 180 s response time with the fire department, everything has to work perfectly and, even if it does, the likelihood that they can start suppressing the fire is slim after only 180 s.

It is assumed here that the fire watch needs at least 120 s to get to the right place, pulling forward the fire hoses and initiating the fire suppression after the fire alarm has been triggered. According to Figure 20, the 16 mm nozzle is, in principal, able to extinguish the fire regardless of which fire growth one chooses to follow. The other nozzles are, on other hand, ineffective in principal if one neglects the slowest fire growth curve.

With the above reasoning, one might draw the conclusion that the fire suppression equipment is sufficient. This is, however, only partly true. It presupposes a number of non-conservative assumptions. The suppression is here assumed to be able to reach inside all corners of the fire room. Since the opening hatch is only around 2 m^2, this assumption is highly critical. The distribution of water becomes a problem when applying larger volumes (Särdqvist 1996). The efficiency factor of the fire extinguishing can be regarded as representing an upper limit and can easily decrease. The fire growth curve is very un-precise and is likely to follow one of the faster fire growth curves due to the rubber's extremely flammable nature. The response time for the fire watch and the fire department is also highly questionable and the times that are presented here are likely to be carried out under perfect conditions.

With this many unsure factors, it is impossible to assign one value for the probability to extinguish the fire. A uniform distribution with the maximum probability of 0.4 and the minimum probability of 0.01 for the extinguishing of the fire is therefore chosen.

8.1.2.3 Estimation of consequence values for event tree analysis

In 1995 in Scholven, Germany, a 500 W lamp in contact with the rubber in the absorber caused a total destruction of the FGD, the cost being around 85 million Deutsche Mark (approximately 42 million Euros). From a discussion with the insurance firm has a value of 50 million Euros been estimated as the cost for a replacement of the FGD. If the fire instead is extinguished, it might cause much less damage, 1 million Euros is here used for this estimation.

8.1.2.4 Presentation of event tree with assigned probability distributions and consequence values

The same event tree as in chapter 8.1.2.1 is presented here. The difference is that here the different distributions for the probability estimations and the assumed consequence are inserted into the tree with black numbers and % quotes (see Figure 21). It needs to be stressed that here only the mean value of the probability distributions is shown, for example in the left up hand corner it says 3,7%, which is in reality the triangle distribution of [0.001;0.01;0.1] (minimum value, most likely, maximum).

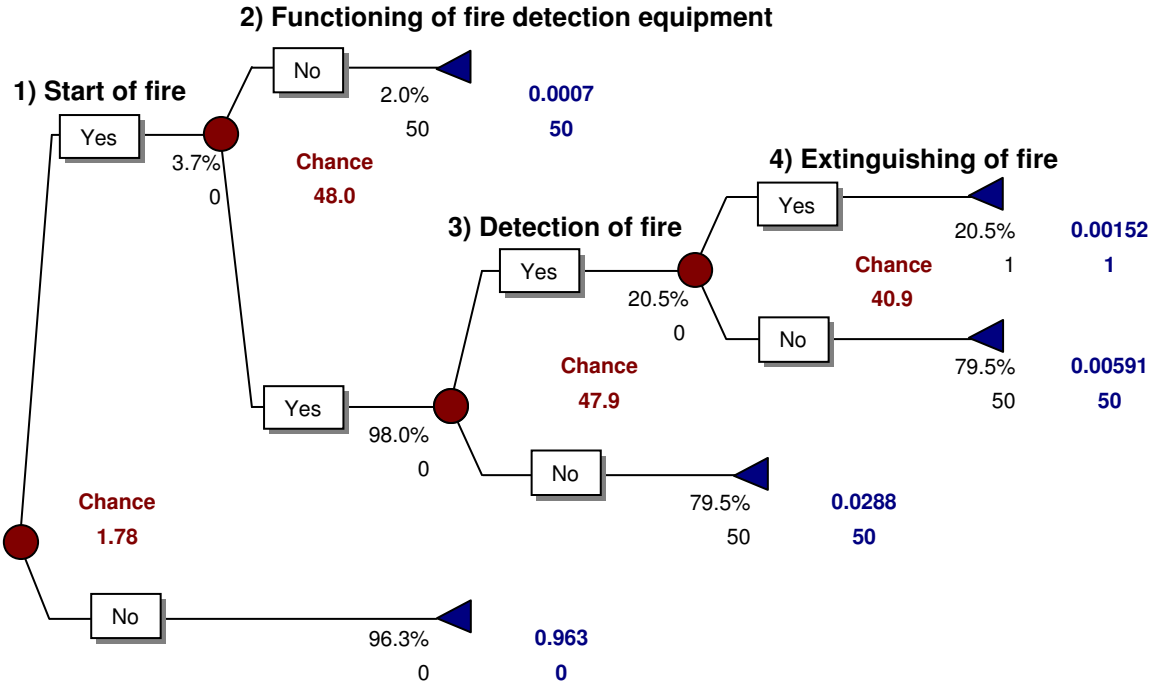


Figure 21 The event tree for fire scenario 2, with related consequences values and probability values, which are expressed as the mean of the distributions.

The blue values are calculated values by the program (PrecisionTree) which states the sum of the accumulated probability values for each branch of the tree. The red set of numbers, with the heading “chance”, state the combined risk (probability multiplied with consequence, in million Euros/year) of each change nod.

8.1.2.4 Result of fire scenario 2.

From Figure 21 the risk can be thought to be 1.78 million Euros/year, though this might cause some problems. The result should not be interpreted as an absolute truth since the different components of the equation consist of estimations in the form of distributions. In the following Figure 22, the yearly fire damage in million Euros is presented as a distribution, which gives a better picture of the risk.

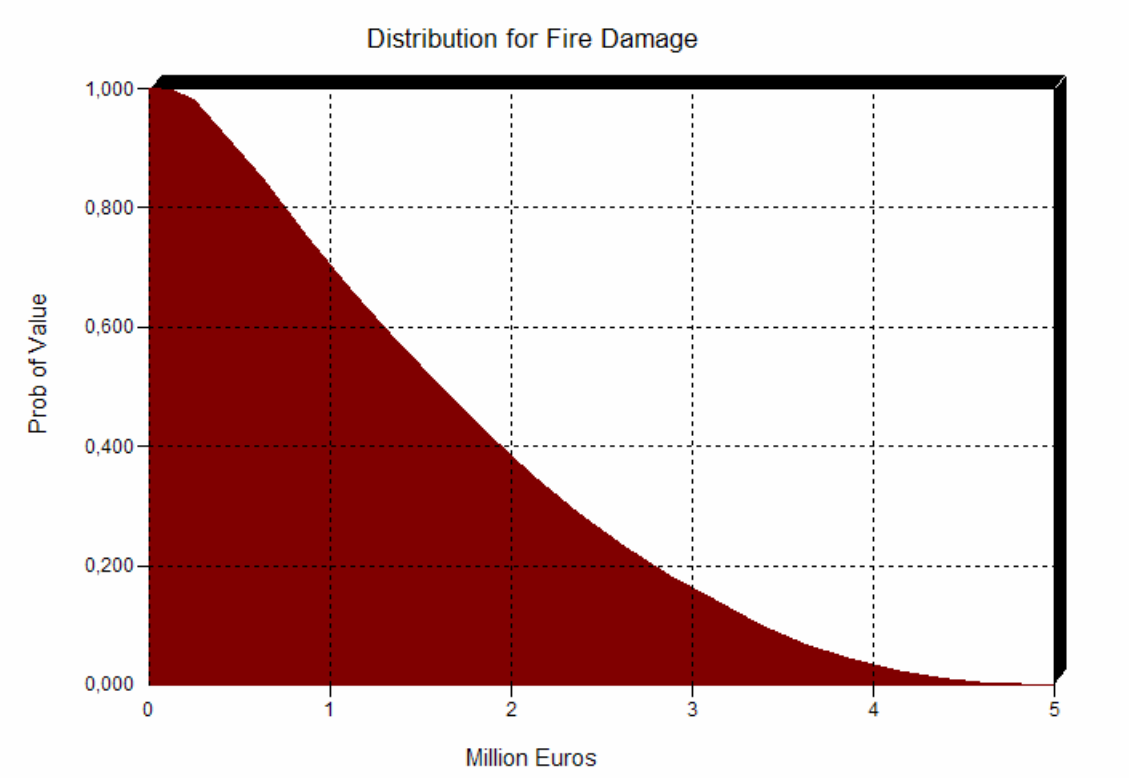


Figure 22 The chart demonstrates the distribution of the yearly fire damage in million Euros.

Another way to more easily understand the variation in the result due to the distribution of the components in the equation is presented in Figure 23 below.

Probability distribution of yearly fire damage [Million Euros]

5th percentile	0.37
Mean value	1.78
95th percentile	3.78
Standard deviation	1.08
Variance	1.16

Figure 23 Probability distribution of yearly fire damage

The result presented in this way suggests, up to the 95th percentile, that the average yearly fire damage will not exceed 3.78 million Euros. One should not interpret this result by believing there will be a fire every year which causes a cost of 3.78 million Euros. Since the FGD is likely to either sustain total damage (50 million Euros) or very little (assumed here to be 1 million Euro), rather should one understand it to mean that a few fires, occurring over an extensive time period and divided over that time period, would cause a loss of 3.78 million Euros per year.

In combination with the calculation of the event tree, a regression analysis has been performed and is presented in Appendix 7. It shows that the fire occurrence distribution is responsible for 99.8 % of the variability of the result.

8.2 Vulnerability analysis

This part presents first an overview of the internal and external risk factors and then a more in-depth study of the vulnerabilities that seems to be most relevant. The second step is of a semi-qualitative approach.

8.2.1 Overview of the internal and eternal risk factors

The hazard identification step of the analysis is based on the questions presented in Appendix 3. The best way of presenting the result is thought to be in a deliberative way, since it is considered to be less confusing because the answers are overlapping.
The questions will be answered according to the different risk factors taken from Appendix 3.

Internal factors

8.2.1.1 System attributes

The FGD is a fairly simple and straight forward industrial process. The flue gases go through a heat exchanger, then an absorber and then out through the chimney. The limestone slurry is first mixed with water in large silos and then transported to the nostrils in the absorber and sprayed over the flue gases. In other words there are few interconnected parts to the process. The purely mechanical parts are also few; a few fans and dampers are enough to make it work smoothly. The weak spot is then instead the electronic control system, which is normally operated automatically and is highly interconnected in a computer network within the control room.

The process is fortunately rather robust in the way that it is not very sensitive to disruptions in other parts of the plant. If the boiler of the unit shuts down, the FGD keeps running as usual without any problems. Also, the internal dependence is not crucial but can afford some variations of temperature and concentration levels in the flue gases and the limestone slurry.

8.2.1.2 Technical Failures and Technical Hazards factors

The Health, Safety and Environment (HSE) department at the company controls and handles safety issues and works with preventing accidents and hazards. Within the department, fire have been identified to be the main risk during repair work at the FGD, with explosion risks with Toluene also being a prioritised risk. A checklist *for works and measures upon start of inspection/overhaul works* is included in the safety regulation and is supposed to be used before repair work is about to commence. In this way, proper tools and equipment are used, so that technical failures are kept at a minimum. There are, however, occasions where the contract workers have been spotted using improper tools and equipment. The safety-engineer makes control rounds two times a day and reminds the workers of the checklist and the regulations. The combination of the instructions and the control rounds generates a good but not fault-proofed risk prevention concept.

8.2.1.3 Human factors

During normal operation accidents or “near misses” practically do not occur, according to the company, the insurance company and as well VGB – PowerTech (1998). There is enough time to put in counter measures and deal with problems that arise during operation. Workers are on duty with both cameras and instruments which help to identify problems before they become accidents. Hidden dangers are, in that sense, therefore impossible, according to the company. Thus, regular work to find underlying hidden dangers and hazards is not performed.

It is likely that incidents are very rare during normal operations, but it is nevertheless not impossible. The danger is that accidents are regarded so rare that the risk is forgotten and not dealt with adequately.

The attitude towards finding problems and dealing with hazards is of a higher ambition level when the FGD is revised and under repair work. Regular meetings once a week are organised with the responsible engineer, the safety engineer, shift leaders and the internal fire department chief, to discuss problems with the safety level. The problems that are identified are then dealt with right after the meeting. Actions are taken right on the spot where they are discovered as well. There is, however, no program for identifying latent errors within the FGD and its safety management.

The company works according to a form of the PDCA-Circle, in Germany called "Kontinuierlicher Verbesserung Process (KVP)", to minimise human errors, e.g. when a contractor is about to get hired. The circle begins with the company making an order and employs an appropriate contractor. The contractor is then educated according with the company's safety standard. His tools and equipment are checked and for each work place within the plant specific instructions are assigned. The work is then regularly checked and information and discussion with the contractor and the company is executed every morning and a larger meeting is held every week.

Workers' errors and mistakes are in general treated as something that is unavoidable, but not desired. The workers are reminded of the safety instruction they signed before starting the repair work when they are discovered to have broken a regulation. To reduce errors, the employees have special training twice a year for more dangerous (such as welding and cutting) work and once a year for less dangerous work (see also chapter 8.1.1).

8.2.1.4 Management and Organisation factors

Safety is a prioritised issue on the company's agenda and safety matters are discussed on the highest level within the company and as well on the board of the parent company, which has around 100 000 employees. The health, safety and environment (HSE) department within the company is working with the aim of bringing safety issues up from the low levels to the highest level. The HSE department is reporting directly to the board and not to the different power plants within the company. In this way the company hopes to obtain an independent and objective safety prevention work that is not pressured by economical aspects. The HSE department is then divided up into seven major responsibility groups – emission protection, water protection, dangerous goods, radiation protection, work and health protection, fire protection and breakdowns/accidents. Representatives from the board for each group are in communication with representatives for each group from the single power plants. They are in direct connection with the power plant director who gives orders and instructions to the ground personnel. Emphasis has been put into making responsibility areas clear and stressing the importance with communication and reports. Hence, the HSE management is therefore regarded to function well.

8.2.1.5 Maintenance factors

The guideline "*Fire prevention measures during erection, repair and maintenance works on flue gas desulphurisation plats*" is a 15 pages long description on safety regulations dealing with organisational measures, design and structural measure, fire detection / fire alarm and

fire extinguishing systems / fire fighting for all power plants with a FGD within the company. Safety checks that the regulations are followed are conducted by the safety engineer two times a day. When he/she discovers that they are not, a warning can be given to the worker and, in more severe cases, a direct report to the workers' foreman is given and if he is a contractor he will be sent home from work and the contract company will not be given renewed trust.

8.2.1.6 Staff factors

It is very important to have appropriately trained and motivated staff working in an industry for safety reasons. The availability of qualified personnel is therefore of big importance. As the company has several coal power plants in the same region, extra personnel are available, in case of sickness or other reasons for losses of personnel. Aspects such as strikes and recruitment of new staff are not further discussed in this paper but the competition seems high amongst the contractors and is therefore regarded as well.

A high confidence in their own safety organisation is present at the company, since they see themselves as one of the leaders of safety thinking in their own branch. Fire detection and fire fighting equipment have been improved by the company, which were later also adopted in other companies due to insurance companies' demands. Self criticism seems therefore to be fairly low, there is, however, continuous work done in decreasing risks further. Such an attitude from the management may influence the workers, which may relax their own safety thinking.

The likelihood that a worker would deliberately want to cause an accident is very small. Workers within the more sensitive zones (such as the ammoniac storage at this plant) of an industry have to, according to German law, go though a security check where the company checks the worker's previous history with the German agency of economy (BMWA) before employment.

Contractors are chosen on the basis of their risk attitude, and the one with the right attitude is picked. The company changes contractors if it turns out that they do not live up to the company's desired risk attitude level. Risk attitude is here an expression that include both in what manner the contractors performs the work and what risk perception they uphold.

External factors

8.2.1.7 Environmental factors

Germany is not targeted by many natural disasters in comparison to the world at large. The big flooding of the rivers Elbe and Danube (Swedish/German - Donau) 2002 are the latest examples of such exceptional severe incidents. For the power plant in question and the canal next to it there is no risk for flooding as it is man made and possible to be shut off. According to the World Map of Hazard of the Nature, which has been developed by the German insurance company Münchener Rück, it is storms, lightning and hail that offer the greatest environmental threat to the plant (see Appendix 2). The same should be valid for the FGD since it shows the same construction characteristics (steel and concrete and dependence on electrical cables and equipments).

Biological hazards are the only other threat, when bird flu is becoming more and more frequent. There are some predator birds that have built a nest within the plant perimeter and

when those are accidentally killed, they are cleaned away by men with full safety protection equipment and clothes.

8.2.1.8 Societal factors

Germany is presently in a very safe position looking from a perspective of hostile attacks by its neighbours. Terrorism has, in the last years, been a more sensitive issue for the country, ever since the 11th of September and since Germany has sent troops to Afghanistan. The terrorist threat towards the company and its specific plants is unsure and very hard to estimate, and is not further discussed in this paper. Vandalism is prevented with the help of a fence around the perimeter of the plant and with camera surveillance that is shown in the security boot by the main entrance. Security cards are also provided for all the employees and visitors, and both a check-in and a check-out control are mandatory.

8.2.1.9 Infrastructure factors

There are a few infrastructural factors that have to be kept in mind when discussing the FGD's vulnerability. For the FGD to function, limestone and water are necessary. The quality of limestone is daily tested in the plant's laboratory, whiteness tests are performed and compared with the supplier's reports. The company has a contract only with one limestone supplier, but for the water supply there is both the channel and the community water available. The gypsum production is also controlled daily, with a large number of high accuracy tests in the plant's laboratory.

Accessibility to the plant is high since it is situated in the Ruhr region with a great number of highways and other roads. There should therefore be no problem for both emergency units or workers and delivery contractors to reach the plant at any times.

The plant does not keep spare parts for the FGD in stock. This as continuous measures and tests are performed on the FGD to guarantee that no unexpected events occur, due to wear down of elements in the FGD. Repair work can be planned long in advance and spare parts can be ordered.

8.2.1.10 Legal factors

The laws that are of importance for the FGD can cause the company considerable economical losses if altered. Large economical losses might be due, as well, to the breaking of set emission limits. According to the expert at VGB – PowerTech the industry does not expect a big change in the legal situation concerning FGDs within the coming 10 years.

8.2.1.11 Market factors

The dominant power production in the European Union stems from coal. In 2004, 50% of the electricity in Germany was generated from coal. Both in Germany and in the EU the power generation is well mixed of different primary energy types, such as nuclear, gas and hydro power. Thus diversity is a strength. How will the market look in the future? Coal has a long tradition in Germany, and against the background of work to decrease the CO_2 emissions, rising prices of oil and gas as well as the legally enacted phase out of nuclear power plants; coal power has even the potential to grow (Hartung 2006). The coal power market can therefore be regarded as fairly safe, and there are plenty of economical buffers that can be

used for safety measures. The company had 11 accidents (2006) per million working hours, which is just over half of the average accident frequency for the total industrial and trade in Germany (Hartung 2006).

8.2.1.12 Financial factors

The company's vulnerability is dependent on its financial situation. This factor is closely linked to market factors. The market is, in fact, a decisive force for the decisions of how much financial room a company has to invest in safety. During the last years the company has been able to present a rising profit (after tax and financial costs) to 180 million Euros in 2004 and 280 million Euros in 2005, and as well a rising turn-over of 1,400 million Euro in 2004 and 5,000 million Euro in 2005. The company has long term contracts with its parent company for indigenous coal deliveries and can feel safe in its position as one of Germany's leading coal power companies.

In case of a fire in the FGD, the insurance company will go in and cover both the reconstruction and the loss of income while the plant is not in operation. A reconstruction is estimated to take one year to complete. In 1995 a FGD in a hard coal power plant in Scholven (Germany), burned down due to a hot lamp being in contact with the rubber. The same insurance company as our company's went in and paid 85 million DM (around 42 million Euros). A FGD is, in other words, both a very expensive unit and one that takes a long time to replace.

8.2.2 In-depth study of human errors

This chapter first presents background information of human errors and how they are connected with safety culture and safety management. Furthermore follows a presentation of representative vulnerability scenarios for the FGD, according to Einarsson and Rausand's (1998) first step in their approach to a vulnerability analysis. The result of the first part is then presented before a deeper study is applied to two of the scenarios, according to Einarsson and Rausand's second step.

8.2.2.1 Background theory of human errors

As many terms in the world of risk society are not measurable or quantitative, there are only rare unified definitions existing. Human error is one of these, and has been subject to a vast debate for many years. The understanding most people have is presented in mass media that often leads the audience to believe that the accident that took place is only the error-committing person's fault, while neglecting the context in which the error was committed (Einarsson 1999b). Somewhere between 70 to 90% of all past accidents are regarded, by most analyses, to be caused by human errors (AIChE 1994). This combination attracts the interest of the many risk/vulnerability experts to human error.

One of the leading scholars in this area is James Reason. He has written a highly regarded book called *Human Error*. His theories, originating from *Human Error,* present the whole spectrum from the definition of errors and mistakes to his own model of organisational accidents in a complex system. Reason's (1990) definition of human errors is:

A generic term to encompass all those occasions on which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to the intervention of some chance agency.

The interesting question of *why* these errors are committed arises at this point. To only blame the individual is an unfortunate but common mistake. The root causes of human errors can be pinpointed to stream from management system breakdowns. Motive such as poor procedures, poor man-machine design and lack of training are of this kind, and are also known as *organisational errors* (AIChE 1992). Below follows figure 24, which describes both organisational errors and how they relate to human errors.

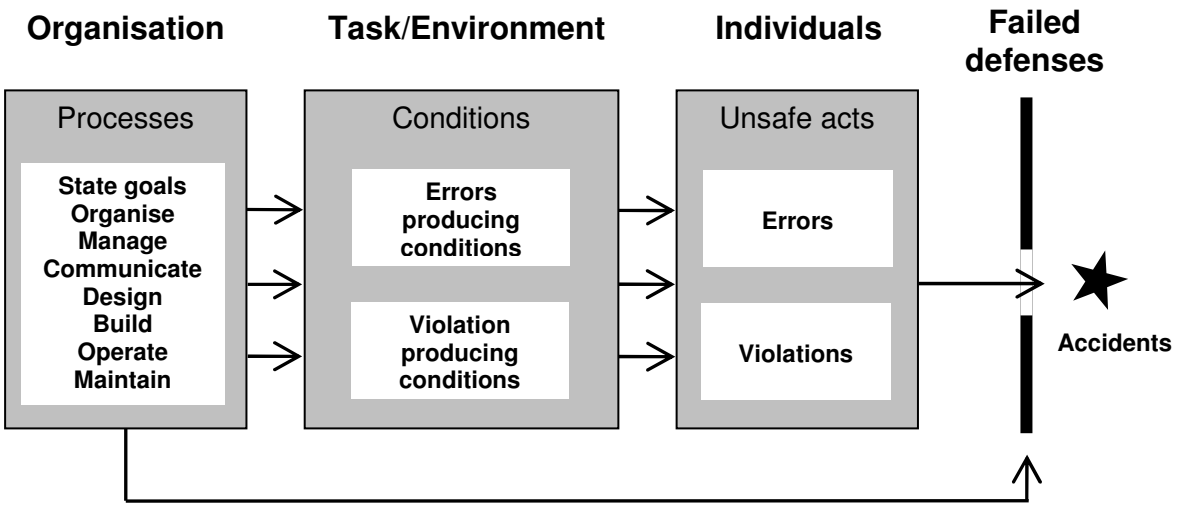


Figure 24 Reason's model of organisational accidents in a complex system (Reason 1993).

As shown in Figure 24 errors and violations by individuals are the last step in the chain before an accident occurs. It is important to understand that "unsafe acts" are not the only reason for an accident, even if it is the last step in the accident chain above. An unsafe act is always preceded by a "latent failure". Latent failures are usually fallible decisions, taken at higher levels of the organisation. They are built-in circumstances in systems that are the root causes of accidents. The effects of these kinds of decisions can be overlooked for very long time before they lead to an accident, triggered by an unsafe act also known as "active failure". Latent failures cannot be avoided, they are always present. The effective way of dealing with latent failures are not to try to eliminate them, but for those who lead and operate the system in question to visualise their negative effects (Akselsson 2006).

Active failures may as well be divided into two different categories: errors and violations. *Errors*, what we in everyday language call human errors, are committed unintentionally. As they are unintentional, they are also hard to predict and prevent. It is naturally of high importance to try to minimise them, but it is not the most effective to concentrate all the efforts on that aspect. As mental conditions (such as temporary lack of concentration or forgetfulness) due to their lack of intention and difficult to predict, are the last and least controllable link in the accident chain, it is easier to deal with the latent failures once they have been identified. Below follows Figure 25 with error-producing conditions, which are put into a random order. The list of error-producing reasons can be made longer; the difficulty lies not in identifying new reasons but in estimating which of the reasons is of highest importance (Einarsson 1999b).

1. Unfamiliarity with the task
2. Time shortage
3. Poor signal: noise ratio
4. Poor human system interface
5. Designer-user mismatch
6. Irreversibility of errors
7. Information overload
8. Negative transfer between tasks
9. Misperception of risks
10. Poor feedback from system
11. Inexperience (not lack of training)
12. Poor instructions or procedures
13. Inadequate checking
14. Educational mismatch of person with task
15. Disturbed sleep patterns
16. Hostile environment
17. Monotony and boredom

Figure 25 Error-producing conditions (Reason 1990).

Violation is another important aspect and involves, at least to some extent, deliberate actions deviating from the regular code of practice or procedures. The term can be divided into four different subcategories: *routine violations* which involve shortcuts between different task points, *optimising violations* where the individual aims to optimise a goal other than safety, *exceptional violations* which are the products of a wide variety of local and unusual conditions, and *deliberate sabotage* which aims to intentionally destroy something and is not as the others where the intention is not bad (Reason 1993; Einarsson 1999b). The two first violations are of highest interest, since they are known to cause a lot of problems in industries (Einarsson 1999b). Landscape architects give a good understanding of the problem. The artistic side of their products creates pathways that are satisfying to the human eye. What they seem to miss is the innovative side of people who will soon create new more efficient pathways through the protected grass. The example can be labelled as an optimising violation. See also figure 26 for further violations reasons.

1. Manifestation or lack of an organisational safety culture
2. Conflict between management and staff
3. Poor moral
4. Poor supervision and checking
5. Group norms condoning violations
6. Misperception of hazards
7. Perceived lack of management care and concern
8. Little élan or pride in work
9. A macho culture that encourages risk-taking
10. Beliefs that bad outcome will not happen
11. Low self-esteem
12. Learned helplessness (“How gives a damn anyway”)
13. Perceived licence to bend rules
14. Ambiguous or apparently meaningless rules

Figure 26 Violation-producing conditions (Reason, 1993)

The psychological mechanisms are not the same for errors and violations. Errors originate from an information processing problem and violations have a motivational problem (Reason 1993). Effective assessments for errors are: a redesign of the work place, memory aids and retraining, etc. Violations are a social phenomenon and should be dealt at the organisational level with changing attitudes, beliefs and norms by improving moral and safety culture (Einarsson 1999b).

Improvement in safety culture is many times regarded as an effective way to handle human, latent and organisational errors. Safety culture has been the object for a number of different definitions with divergent meanings. One definition given by Booth and Lee (1995) reads as follows: “*the product of individual and group values, attitudes, competencies and patterns of behaviour that determine the commitment and the style and proficiency of an organisation’s health and safety programme*”.

There are four different sub-cultures to safety culture: reporting, fair, learning and flexible culture. To obtain a good safety culture, an organisation must be well informed. This is done through managing the four sub-cultures correctly (Reason 1997). For the organisation to receive the best information, all personnel must be involved in reporting accidents or incidents, even the person who caused it. Frank Bird has conducted an investigation of over 1.7 million reports from different companies with different industrial backgrounds. Bird's conclusion was that there are common reasons for incidents: material damages and minor/serious accidents, and that counter measures to one of the levels would affect the others as well. In Figure 27 his theory is presented, although the numbers are not to be understood as absolute. For instance, every 600 incidents you will not necessarily have one serious accident. The numbers are rather meant to indicate the relationship than to be an absolute truth (Akselsson 2006).

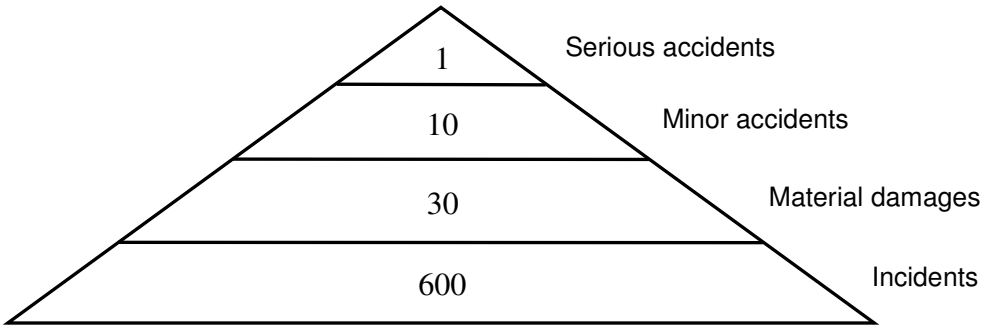


Figure 27 The Iceberg model (Akselsson 2006).

There are problems with this theory as well: the picture indicates that all incidents are equally serious while this does not necessarily have to be true. The model shows, however, how important reports are to prevent serious accidents.

For people to report incidents, the organisation must be fair, which means that human errors are not punishable, but reports are rather encouraged. To be able to draw any conclusion and make appropriate adjustments, an organisation has to study the report and investigate further when necessary. Otherwise it can not learn. Flexibility in an organisation is also necessary when an accident occurs. It is important that titles and ranks are put aside and the most suitable person for the critical situation takes charge (Akselsson 2006).

Åsa Ek (2006) at Lund University has developed these four sub-cultures and added another five to them in her effort to explain safety culture, as shown in Figure 28.

1. Reporting
2. Learning
3. Fair
4. Flexible
5. Safety attitudes
6. Safety behaviour
7. Communication
8. Working conditions
9. Riskperception

Figure 28 Nine components of safety culture (Ek 2006).

Safety attitudes reflect what understanding the employees have for the consequences of their acts and how responsible they feel toward them. The employees' interest and engagement are other aspects of safety attitudes. This is closely associated with safety behaviour. Employees who have a tendency to cross limits and take unnecessary risks are examples of people with low safety behaviour. The organisation's way to prioritise work and safety are other aspects of it.

A well functioning communication within the entire organisation depends both on the quality of the information about the present work and safety situation are spread and on the every day communication between employees. The everyday communication also influences the working conditions in the work place. A good working environment for the employees is a precondition to obtain a high safety level. Every individual's risk perception, or understanding of their own risk situation, is dependent on their view of controlling risks (Ek 2006).

8.2.2.2 Problem description and scenario presentation

Human errors are, as described above, not the simplest of matters. At the first glimpse of a human error assessment one might draw the conclusion that the only goal is to identify all possible and imaginable errors a person can commit within the system in question, and then deal with them. Reason (1990) suggests that one should look at the root causes of the problems instead of trying to imagine all possible unsafe acts. Unsafe acts are uncountable and the time for the analyst is limited, though latent failures or root causes are less concrete and harder to visualise.

Appendix 8 presents a sample of scenarios involving errors, violations and latent failures, described as Einarsson and Rausand (1998) suggest in worksheet number 1 of their Approach to a vulnerability analysis. The sample is only meant to demonstrate the range of threats, not to be comprehensive. The scenarios are regarded as important and representative for the FGD's vulnerability related to human errors. Below follows a short presentation of the scenarios:

A. The first scenario considers the risk that a worker might accidentally direct a welding tool towards the rubber and in that way might cause a fire.
B. A lamp with too high heat effect is used and forgotten inside the FGD and after some time a fire is started.
C. Someone smokes in the FGD and the cigarette is left on the rubber floor, a fire is initiated after a long time.
D. The company's use of external contractors results in a lower risk attitude which causes higher frequencies of unsafe acts, than with the company's own employees.
E. Shortcomings in the accident report system gives a decrease of learning potential for the organisation, this can result in a higher frequency of accidents.

8.2.2.3 Result of qualitative analysis (step one)

Scenario A is of high relevance since it endangers employees as well as the FGD itself. Welding is only operated under strict regulations and is supervised by the fire watch. Forgetfulness or lack of concentration can nevertheless create the opportunity for a fire. This can be due to disturbed sleep pattern amongst the welder or monotony and boredom in the work (see Figure 25 for more reasons). The underlying weakness or vulnerability is the

rubbers lack of ability to withstand fire. The organisational aspect of the accident chain in figure 24 concerns the regulations and the supervision of welding.

Scenario B is not as high in relevance since it endangers the FGD but not likely the employees. The precondition for this scenario is that someone (an employee) has to violate the regulations for which lamps are to be used in the FGD. The lamps that are allowed in the FGD have a maximum temperature of 185 ^{o}C after 24 hours, which is not enough to start a fire since the material has an flash point of 250 ^{o}C (ExxonMobil 2002). The employee might not have intentionally broken the regulations by using a lamp which generates a dangerous temperature; he can simply temporarily have forgotten the regulations. The company's efforts in demanding that each employee sign the safety regulations might in this case not be effective as a vulnerability reducing measure. The fire watch's safety rounds can nonetheless discover the lamp and correct the mistake before an accident has occurred. Credit should also be given to the safety information meetings the employees must attend before the commencing of any work at the plant.

Scenario C concerns a well known and strictly forbidden activity. It is not only in the FGD that smoking is forbidden but also at the rest of the power plant. There is no doubt that this scenario concerns an intended violation of the safety regulations. Information from the company is given that smoking is prohibited but it does not seem to work well enough as a deterrent measure. The safety rounds are not really effective since the contractors tend to violate the rules when the controller turns his back to them. The underlying reason is a lack in the company's safety culture, with safety attitude/behaviour and risk perception as subgroups.

Scenario D does not result in a factual loss but is rather an underlying reason for scenario A – C. The reason for the company to use external contractors is simply because of cost savings. Mitigation factors such as safety information and check-ups are useful. The company's policy to only contract external companies with an adequate safety attitude is another internal mitigation factor that fortunately increases the external mitigation factor of the contractors' own safety demands of their employees.

Scenario E is of the same sort as D and likewise it does not result in a factual loss. It demonstrates a weakness in the safety culture in the company, which results, according to Frank Bird and his Iceberg model, in a loss of ability to learn which can or will prevent future accidents. The communication at the plant seems to be proficient and open. It is therefore likely that the underlying reason for the lack of a good report system is due to the perception that reports on incidents or near misses are not highly important. The company's own safety organisation works for increases in safety but seems to have missed this point. Insurance and governmental interests are concentrated towards reports concerning actual accidents and not when only an incident has occurred.

8.2.2.4 Selection of which scenarios are to be quantitatively analysed

The first three scenarios show similar problematic as they all in some way concern fires. The last two are more characteristic of a root cause and do not result in any factual damage, though they might cause factual losses later on. The most relevant scenarios are to be chosen for a quantitative analysis according to Einarsson and Rausand (1998). The two last scenarios, involving latent failures, are excluded at this point due to their lack of quantitative potential. Scenario C is so similar to B regarding the potential consequences and likelihood that it is as

well excluded from quantification. In Appendix 9 (worksheet number 2 by Einarsson and Rausand 1998) is used to quantify scenarios A and B.

8.2.2.4 Result of quantitative analysis (step two)

Einarsson and Rausand's (1998) worksheet no. 2 is based on: an estimation of likelihood, four different consequence aspects, called Human, Environmental, Business and Property impacts and two mitigation, rebuilding and restore aspects, called Resources to mitigate, rebuild, restore, etc., divided up in an Internal and an External part. Each part is assigned a number from 0 to 4, 4 being the highest and 0 the lowest. If the business impact for example is very high, then a 4 would be assigned for that part. Each of the consequence ranks and the internal and external mitigation ranks may then be given a different weight that reflects the individual rank's importance in the scenario.

$$c_i = k_{hum} \cdot c_{hum.i} + k_{env} \cdot c_{env.i} + k_{bus} \cdot c_{bus.i} + k_{pro} \cdot c_{pro.i} \quad and \quad r_i = k_{int} \cdot r_{int.i} + k_{ext} \cdot r_{ext.i}$$

where c is the consequence, k the weight, r the resources of mitigation and for $i = 1, 2, \ldots$

One of their suggestions for how the result can be presented is to multiply the probability with the weighted sum of the consequences and then withdraw the weighted sum of the mitigation, as shown in formula 1 below.

(1) Vulnerability = Likelihood $\cdot$ $(c_i - r_i)$

The different values assigned to the calculation of the vulnerability of scenario A and B are made by so called "expert estimations" by the author in discussion with company experts. The likelihood value numbers are taken from Appendix 4 and then translated to fit the new scale. The human impact is very limited for both scenarios, especially for scenario B, since no employees are assumed to be present. In scenario A at least two persons are present and are thought to assist one and other in case of injury. The environmental impact is estimated to be neglectable since only limited amounts of rubber, plastic and glue are combusted. The property impact is the same for A and B and is set with the postulation that a new FGD is estimated to cost something in the vicinity of 50 million Euros (estimation by the insurance company). The business impact is also the same for A and B and is based on calculations of lost profit. More information concerning the arguments behind the result and calculations can be found in Appendix 9.

In Figure 29 the result is presented in a consequence-likelihood matrix. The circles symbolise consequence before the mitigation parts are included and the triangles represent the final consequence when the mitigation parts have been included. The length of the line illustrates the effect of the mitigation, rebuilding and restoration parts.

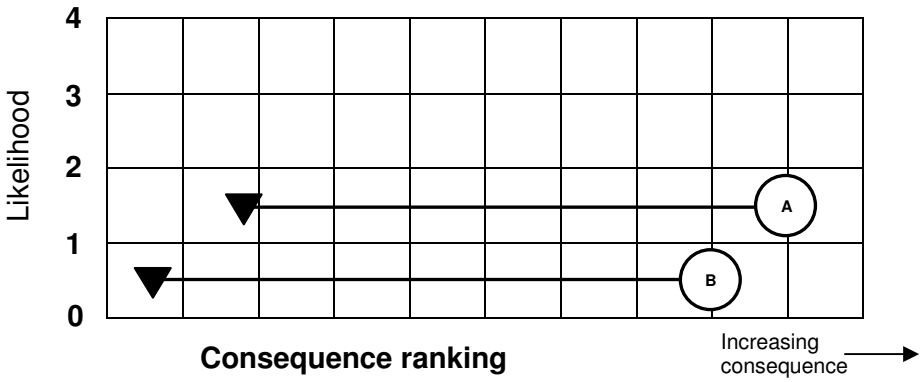


Figure 29 Consequence-likelihood matrix for vulnerability scenario A and B.

Another way of presenting the result for each scenario is to multiply each consequence rank with the likelihood estimation and withdraw a weighted sum of the internal and external mitigation factors. The result would then be for A – 8.25 and for B – 2.5 The numbers should be understood with the background of the main objective of the second step in Einarsson and Rausand's (1998) vulnerability analysis, which is to establish a ranking of the scenarios according to their criticality. With that in mind, A is more critical than B, as Figure 29 shown as well.

9 Risk evaluation

This section concerns the evaluation of risk and vulnerability of the FGD. By first describing the safety attitude at the company and the specific power plant one can get a picture of what safety ambition they have. The analysis of risk and vulnerability reducing measures can then be adopted to fit with their safety attitude. The suggestions of options can be made very long and extensive but will have to be limited here, which is why there will be only little discussion of the cost in relation to safety improvement suggestions

9.1 Safety attitude at the company and the power plant

The company has a high ambition concerning safety of both personnel and property. They even promote themselves to be leading the safety advancement in their branch in many areas. Risk and vulnerability deduction has highest priority and is said to be allowed unlimited costs if the risk level is undesirable. The company's safety department is in direct contact with the board which indicates that safety issues are dealt with in a fast and uncompromised way. Each power plant has its own safety engineer who is responsible for the plant-specific safety issues. The workers seem to have a relaxed and tolerable risk attitude. As for many other workplaces optimising violations seem to be frequent, e.g. unwillingness of using safety helmets at all times. Accident statistics of individual injuries show a relatively low frequency both in the specific power plant and the company itself in comparing with nationwide industry and trade ratings (Hartung 2006).

9.2 Suggestions of options for risk scenarios

The best approach to present the different improvements to reduce the fire risk scenarios are to divide up the scenario in its four parts.

1) Start of fire
Looking over a longer time period an ignition of the rubber is likely. The material is highly flammable and during repair work equipment is used that may easily cause a fire if handled wrongly. To decrease the likelihood of a fire is started one has mainly two different options, either alter the material or the ignition source. It is not likely that the equipment can be replaced by other less hazardous ones but the material may be changeable, see also chapter 9.3 for further possible actions, such as separating the material from the equipment.

2) Functioning of fire detection equipment
The functioning of the fire detection equipment is highly dependent upon how often functioning tests are preformed. At the present time test runs are made four times a year and the likelihood for malfunctioning is not very high. Modern detection systems in Sweden which are checked for correct functioning every fifth second has an error frequency of $2.3 \cdot 10^{-7}$ (Wettland 1991). With this detector system the likelihood for a mal functioning detector becomes almost zero.

3) Detection of fire
There are two ways to detect a fire in the FGD, through detectors or through the employees and especially the fire watch. The problem with the vicinity to the ground placed smoke detectors can be corrected easily. With detectors in the ceiling the detectors could monitor much bigger areas, even whole rooms and the probability of the detection of the fire would

increase. Additional fire guards who can oversee larger areas and more then one place at the same time are other possible and effective measures to be taken.

4) Extinguishing of fire
It is questionable if a fire can be suppressed unless the fire is in an immediate proximity of the fire watch or other personal. For fires close to the employees there are efficient equipments to suppress a fire. All three different standard nozzles should be efficient to be used for a direct fire fighting. The problem is rather if the knowledge of how to handle the hoses and fire extinguishers is sufficient enough. Since the fire watch is trained as a regular German fireman one can assume that their skill is not lacking, but the other personal might be less capable to deal with the situation.

With more modern nozzle types than the standard nozzles, such as a Fog nozzle, the response time can be made longer. The ability of the Fog nozzle to break the water droplets into a diameter of less then 1 mm triples the water extinguishing capacity. A good alternative is to exchange the nozzles of the hoses that are far from the immediate surrounding of the working personal. This should though not be interpreted as that the interior fire department is uncalled for, since they have extra protection wear and air tubes with them. Their work should however go faster since the enhanced fire equipment they usually use is at the right place from the beginning.

9.3 Suggestions of options for vulnerability scenarios

Scenario A is regarded as the most severe according to the vulnerability analysis which is mainly due to its probability estimation. The obvious action would therefore be to try to reduce the probability. One way could be to change the material in the FGD into something that is not as easily ignitable. The coating material Isobutyl rubber that is presently used is easily ignited. When welding or other similar activities are under operation, a separation of the rubber from the flame is necessary. Fireproof blankets are already in use at the FGD during maintenance work, but fireproof bricks can placed in front of the rubber for even higher fire resistance. Another action could be to enforce the fire watch by at all times, during the welding work, having a fire extinguisher in his hand rather than a few meters away, as it is now.

Scenario B has a lower probability assigned to it, but has the same potential impact as scenario A. Here it seems to be most efficient to increase the internal mitigation resources. Efforts to increase the safety culture with such subcultures as reporting, learning, safety attitudes/behaviour and risk perception, suggest that the internal mitigation would increase due to higher carefulness in following the safety regulations. A more drastic action could be to change the whole material inside the FGD into one with higher fire resistance. There is, for example, a glass material (called GI-180) which consists mainly of Borosilicate glass (ECOCERA 2007) and which is used in FGDs and is non-flammable (European Commission 2000).

Scenario C has the same problems as scenario B. The slight difference would be that the improvement of the safety culture should concentrate on increasing the subcultures of safety attitudes/behaviour and risk perception. Lack of learning or reporting culture is less evident here since the threat is a pure violation.

Scenario D has an economical background. A good guess is that it would not be economically reasonable to have all the different maintenance workers, scaffold erection workers and specially educated employees for each individual task as fulltime staff. The increased cost of safety would be too great by this approach. The company has therefore no other option than to try to enforce their own safety culture on the contractors. One good way could be through demonstrations and visualising the potential effects the hazards could have at the FGD. Another way is to require the contractor to be able to prove that his workers follow a fixed standard of safety level, for example to be certified according to the ISO 9000 standard.

Scenario E concerns the lack of an adequate report system. A standard of *how* reporting should be made, including information of *what* to report, to *whom* the report goes and *when* to report. The standard should as well include information of *why* reports are so important and what the procedure is after a report has been delivered. Information about fairness and the fact that the reports are not aimed to blame individuals is also necessary. Teaching how the system works is also essential for effective implementation. If the above information is left out, employees might regard reports as unmotivated and intimidating. The risk would then be that the report system would become nothing but a pile of papers.

10 Risk reduction/control

The last step in the risk management process consists of three parts. In this chapter a theoretical description is given consisting of the different criteria of decision making and a brief comment on two of the other parts, implementation and monitoring.

10.1 Decision making

Suggestions of how to reduce risks or vulnerabilities are useless unless a decision is made. To only identify and estimate the hazards are to stop a few meters from the finishing line. How does then appropriate and effective decision-making become sustainable? There are four main different criteria to follow and they base their decision on different background views (Mattson 2000).

The *Right-based* criteria focus on bringing the risk down to a specific level and, in extreme cases, to a risk level of zero. The problem with a set risk level is always associated with marginal cost. This means that the closer you come to reaching the desired risk level, the more the improvements will cost. It is therefore easy to be misled to use too many resources in some areas while neglecting others. The advantage is, however, that the criterion is easy for the public to accept and understand.

Another criterion is the *Technology-based*, which leads the decision maker to choose the alternative with the best available technology. This criterion is rarely used in its absolute form. Many organisations might proudly use this criterion to show to the public that they do everything possible to keep risks at a minimum, e.g. a nuclear power plant. The reality is quite different since this criterion would result in an enormous cost, if not endless. One could always argue that a new technology is available and should be applied to the risk, even if the last improvement is only a few days old. In a profit organisation, costs are always of interest compared to the utility.

That leads us to the *Utility-based* criteria, which focus on what decision produces the greatest result for the least cost. This is many times regarded to be the best criteria of them all. One of the famous methods to be used in this area is the Cost-Benefit analysis (CBA), where each decision is evaluated of its utility and cost, and the one with the highest utility is chosen for the maximising of wealth. Another approach is to apply the Cost-Effectiveness analysis (CEA), which is easier to use. In contrast to the CBA, this analysis does not demand an evaluation of the utility, but instead aims to reduce a risk to a specific level (e.g. number of injured or dead) at the minimum cost. A shortcoming might be that this analysis has no way of telling if the level is appropriate or not. The third way is to make use of Multi-Criterion-Decision-Making (MCDM), which puts the problem in a multi-dimensional frame. In this way, the result is presented in many different variables, e.g. reduction of expected injuries and of property damage, and not in one variable as the CBA.

The last one is the *Hybrid* criteria which is a mixture or combination of two or three of the other criteria.

10.2 Implementation and Monitoring

After a decision is made on which measure to take, the work of implementation of the measure starts. Orders are given from the management of the organisation down to the last

executing employee. Efforts to explain the goal or expected benefits and why they are taken are very important. The work of monitoring is then initiated, and this is actually the step that makes risk management valuable, something that never ends but strives for continuing progress. Evaluation of how effective the risk and vulnerability measures are working should be made. As time goes on and the organisation and plant changes, the process needs to start from its beginning again in order to be a valid and efficient tool for risk and vulnerability deduction.

11 Conclusions

Through the process of conducting the two analyses, different advantages and disadvantages have become evident. Since this thesis has concentrated towards two specific analyses applied to only one object, the results and discussion might be misleading when attempting to be applied to other cases. The conclusions are divided to deal first with each analysis separately and then it will be tied together in the concluding remarks. This approach is thought to give an easier overview for the reader, than joining the conclusions into one combined section.

11.1 Risk analysis

Risk analyses have been used for a long time now in many different areas of society. This has resulted in there being almost countless methods available. For the unfamiliar analyst, such as the author, this caused an initial problem of feeling lost in the jungle of alternatives. Once the author was able to create a comprehensive system of the alternatives, the number and availability of options was considered a strength of the risk analyses, so that the most appropriate method could be chosen.

One of the event tree analysis advantages was the possibility of combining many risk scenarios into one. The larger an event tree is made, the more aspects can be considered. By adding an extra branch, the functionality of the fire alarm system could be added into the risk estimation. This way both the risk scenario for a functional and a non-functional fire alarm system were able to be presented in the same overall risk scenario.

The event tree presents a straightforward and easily overviewed way of understanding a risk scenario. The way the different aspects are connected and what the different outcomes result in are both understood by the reader without difficulties. It should be pointed out, however, that it might be interpreted in a too simple way. For the untrained eye the uncertainties with the probabilities and the consequences could be neglected since this is not shown within the tree itself. The analyst is therefore required to stress this point and clearly demonstrate how and why the result may differ.

The potential for the event tree analysis is very large in calculating an exact risk value. The other side of the coin goes together with what is written above, that the higher accuracy the analysis aims towards, the more problems it will have in dealing with uncertainties. This became more and more evident throughout the work, also with each new branch of the tree. One might argue that an event tree analysis is a form of QRA and therefore by nature aims towards as exact a risk estimation as possible, and if someone wants to avoid uncertainties he/she should choose another less quantitative analysis. The fact remains, however, that risk analyses tend to strive (in Sweden) towards a quantitative approach in a higher degree than vulnerability analyses do.

The thesis has shown that human errors and external threats are somewhat neglected in traditional risk analyses. There are certainly methods to involve human errors in a risk analysis, e.g. the Human Risk Assessment (HRA) method. In the same way is it not hard to extend the threat scope of a risk analysis. The point is, nevertheless, that it is common for risk analyses to disregard these aspects.

11.2 Vulnerability analysis

Einarsson and Rausand's (1998) approach to a vulnerability analysis is less quantitative in its nature than the event tree analysis. It is more similar to the index-methods for risk analyses in its way of assessing the consequence of the scenario, the likelihood estimation is however more of a quantitative (QRA) form. This should be kept in mind when discussing the advantages and disadvantages for this vulnerability analysis versus the risk analysis.

The first advantage one encounters, when applying the analysis, is that the scope of the analysis is very wide. The internal threats that are commonly examined in a risk analysis are complimented with external events that can threaten the system. It could be argued that the scope is too wide at times and that irrelevant threats are discussed. The obvious solution to that problem is to swiftly disregard those irrelevant threats to focus on the more severe ones. To avoid the risk that one disregards the wrong threats one has to justify why they are excluded from further studies. The problem can, in that way, go in a circle since the work behind the justification of exclusion may demand considerable resources.

The human influence is likely the internal factor that is emphasised the most in Einarsson and Rausand's vulnerability analysis. Compared to the IEC standard the vulnerability analysis uses an expanded view of human errors, including more than only errors from operating and maintenance staff but also the root causes that often lay within the organisation.

The vulnerability analysis supposedly has a larger scope than the risk analysis in the sense that it analyzes a longer timeframe of accidents or threats. This thesis has confirmed this standpoint, but only to some extent. The vulnerability analysis emphasizes the survival of the system and includes external mitigation aspects such as insurances and the local town fire department. The local town fire department and other interior mitigation aspects can easily be included in the event tree. The branch of the event tree for this thesis called "Extinguishing of fire" is an example of this. The unique thing with the vulnerability analysis it that the insurance aspect is included in the scenario and is said to decrease the potential impact of the threat. Insurances are, for the most part, excluded from the risk analysis since they do not decrease the risk but can, however, be a means of handling the risk.

One of the mutual problems that risk and vulnerability analyses have is the degree of risks covered by the analyses. It can hardly be said that all risks are followed up and covered in this thesis, however this was never the aim. It is nonetheless evident that both methods have shown weakness in the decision making of what threats are to be examined further and which are to be neglected. Einarsson and Sigbjörnsson (1999) are making use of something that is similar to *right-based* criteria when deciding what threats are to be further studied. Their risk level rating disregards probabilities that exceed 10^{-5} and consequences of less than 1 unit. The numbers can naturally be altered as found appropriate, but the problem of where to draw the line for what threats are still present both for risk and vulnerability analyses

The most severe problem with the vulnerability approach is the presentation of the result. One of the suggested manners is to assign different weights to each impact rank as well as to the internal and external recourses ranks. The way they (Einarsson and Rausand 1998) like to combine these ranks into a total criticality (also called risk) is not clear. Their way reads *"…, to multiply the likelihood rank with the consequence rank c_i and then subtract a weighted sum of the ranks for the internal and external recourses."* To subtract the weighted sum of the internal and external recourses (r_i) *after* the likelihood rank is multiplied with the consequence rank causes r_i to fall outside the common definition of Risk = consequence · probability,

which Einarsson and Sigbjörnsson (1999) apply in a case study of the vulnerability of a hydroelectric power system. This thesis has used a slightly different interpretation for those reasons.

A consequence-likelihood matrix was the second option suggested for presenting the final criticality. However, this approach generates some difficulties as well. The different impacts and resources are originally measured in different units (e.g. human impact – number of injured and property impact – cost in Euros). Each impact or recourse has in addition designated weights. This combination of different units and weights makes the x-scale in the matrix impossible to define. The question arises then of how useful this matrix is in reality. The advantage of the matrix is that it shows the criticality before and after the recourses are included, which is one of the major points of a vulnerability analysis.

11.3 Concluding remarks

It has been evident throughout the study that traditions and common practice matter when conducting specific types of analyses. The vulnerability analysis suggested by Einarsson and Rausand (1998) has indeed its advantages but it is clear when looking at the big picture that the method is in need of some improvements.

The need of improvements is not as apparent regarding the risk analysis. The longer development of the analysis provides a more solid method then the vulnerability analysis; however are there sides with the method that can be enhanced.

11.3.1 Joining the two methods into one

As the two methods contain different strengths it is this thesis conclusion that joining the two methods into one is the best alternative, when analysing an industrial system. The base for the joint method should be the risk analysis method, as it contains the most advantages, in combination with the following points.

First, the risk identification step of the preliminary risk analysis could be enhanced with the open system approach of the vulnerability analysis. To include external threats and risk sources is possible even for a risk analysis. The same proposal is possible regarding the human factor and the root cause of the overall organisation. There is no reason why only vulnerability analyses should have this concept of thinking. The most effective way of obtaining good results is to include people with a lot of experience, concerning the system in question, otherwise it is likely that irrelevant hazards are discussed.

The second point concerns the length of the analysis timeframe. The thesis has shown that internal mitigation factors, such as internal fire fighting, are possible to be included in a risk analysis. To expand this thinking to also include the external mitigation factors should be manageable. The difference is simply to expand the analyst's imagination and force him or her to include factors as local fire department or insurance firms into the last step of the risk estimation.

Thirdly the result from the joint analysis could be presented in an event tree. The only difference is that the last branch contains the external mitigation factor. This branch should as well possible to estimate with a probability distribution. The results could also be presented in a risk matrix, similar to how the vulnerability analysis proposes. To avoid the earlier

discussed problems one could instead present the result in three different matrixes, one for each consequence impact. The scale could for example be for the human impact, number of lost lives or number of injured and the property impact could be monetarily measured. Another proposal could be to present the result in one matrix with different scales on the consequence axes. The best way is perhaps to make use of both the event tree and the risk matrix for the presentation of the results. This since the uncertainties associated with the result are clearly demonstrated in an event tree, where as the mitigation factors, with the above additions, are clearly demonstrated in Einarsson and Rausand's risk matrix.

14 References

Books, reports, journal articles and conference papers

Abrahamsson, M. and Magnusson, S.E. (2004), *Risk- och sårbarhetsanalyser – utgångspunkter för fortsatt arbete.* Swedish Emergency Management Agency.

AIChE (1992), *Guidelines for Investigating Chemical Process Incidents*. New York: Center for Chemical Process Safety, American Institute of Chemical Engineers.

AIChE (1994), *Guidelines for Preventing Human Error in Process Safety*. New York: Center for Chemical Process Safety, American Institute of Chemical Engineers.

Akselsson, R. (2006), Compendium in "*Människa, teknik, organisation och riskhantering*", Lund Institute of Technology, Lund University, Sweden.

Andersen, E. (2003), Be prepared for the unforeseen. *Journal of contingencies and crisis management*, vol. 11, nr 3, pages 129-131.

Arbetsmiljölagen (1977:1160), Swedish Government, Stockholm, Sweden.

ArbSchG (1996), *Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit*, German Government, Berlin, Germany.

Aug. Hedinger GmbH & Co (2003), *Sicherheitsdatenblatt – Toluol*, Aug. Hedinger GmbH & Co, Stuttgart, Germany.

Booth, R.T. and Lee, T.R. (1995), *The role of human factors and safety culture in safety management*, Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture 209, 393–400.

Buckle, P. (1998), Re-defining Community and Vulnerability in the Context of Emergency Management. *Australian Journal of Emergency Management.*

Buckle, P., Marsh, G. and Smale, S. (2001), *Assessing Resilience & Vulnerability: Principles, Strategies & Actions – Guideline,* Emergency Management Australia, Australia.

CCMD (2003), *Crises and emergency management: A guide for managers of the public service of Canada*, Canadian Centre for Management Development, Canada.

COSO (2003)*, Enterprise Risk Management Framework – Executive Summary*, The Committee of Sponsoring Organisations of the Treadway Commission, USA.

Davidsson, G. (2003), *Handbok för riskanalys*. U30-626, Swedish Rescue Services Agency, Karlstad, Sweden.

Davidsson, G., Lindgren, M., Mett, L. (1997), *Värdering av risk*, Department for Risk- and Environmental Studies, Swedish Rescue Services Agency, ISBN 91-88890-82-1, Karlstad, Sweden.

Department of Trade and Industry (2001), *Flue Gas Desulphurisation (FGD) Technologies*, London, Great Brittan.

Drysdale, D. (2002), *An introduction to Fire Dynamics*, 2nd ed., ISBN 0-8493-1300-7 Wiley-Interscience, New York, USA.

Einarsson, S. (1999a), Comparison of QRA and Vulnerability Analysis: Does Analysis Lead to More Robust and Resilient Systems?, *Acta Polytechnica Scandinavica,* Civil engineering and building construction series no. 114, Espoo, Finland.

Einarsson, S (1999b), Human error in high hazard systems: Do we treat the problem in an appropriate way? *Journal of Risk Research*, Vol. 2, No. 1, pp. 115-128.

Einarsson, S. and Rausand, M. (1998), An Approach to Vulnerability Analysis of Complex Industrial Systems. *Risk Analysis*, vol. 18, no 5.

Einarsson, S. and Sigbjörnsson, R. (1999), Vulnerability of a hydroelectric power system: A case study, submitted to *Acta Polytechnica Scandinavica,* Civil engineering and building construction series.

Ek, Å. (2006), *Safety Culture in Sea and Aviation transport*, Lund Institute of Technology, Lund University, Sweden.

ExxonMobil (2002), *Material safety data sheet of Butyl Rubber,* ExxonMobil Chemical Company - A Division of Exxon Mobil Corporation, MSDS NO.: 00003401.

Enander, A. (2005), *Människors förhållningssätt till risker, olyckor och kriser.* Swedish Rescue Services Agency, Karlstad, Sweden.

European Commission (2003), *TOLUENE - Summary Risk Assessment Report*, Joint Research Centre, Institute for Health and Consumer Protection, European Chemicals Bureau, Italy.

Frantzich, H. (1998), *Uncertainty and Risk Analysis in Fire Safety Engineering,* ISSN 1102-8246, Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

FEMA (1997), *Multi Hazards – Identification and Risk Assessment – A Cornerstone of the National Mitigation Strategy*, Federal Emergency Management Agency, USA.

Fredholm, L. (2003), *Myndighetsgemensam utgångspunkt för utformning av ledningsfunktioner och ledningsstöd vid civil krishantering.* Memorandum presented at a seminar about civil and military leadership in Enköping, Sweden, 2003-05-20.

Guymer, P., Parry, G.W., *Use of Probabilistic Methods in Fire Hazard Analysis*, IAEA-SM-305/1, USA.

Hallin, P-O., Nilsson, J., Olofsson, N. (2004), *Kommunal sårbarhetsanalys*, ISBN: 91-85053-48-1, Swedish Emergency Management Agency.

Hale, A. R., Heming, B. H. J., Rodenburg, F. G. T. and Smit, K. (1993), *Maintenance and Safety: A study of the Relation Between Maintenance and Safety in the Process Industry*, Report to the Dutch Ministry of Social Affairs and Employment, Safety Science Group, Delft University of Technology.

Hartung, M. (2006), Perspectives for the German Lignite Industry in 2006, *World of Mining – Surface and Underground*, Jahrgang 58, No. 3.

IEC (1995), *International Standard 60300-3-9, Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems*, International Electrotechnical Commission, Geneva, Switzerland.

Johansson, H. and Jönsson, H. (2007), *Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv,* Lund University Centre for Risk Analysis and Management, Lund University, Sweden.

Kaplan, S. and Garrick, B. J. (1981), On the Quantitative definition of risk
CCMD (2003), *Risk Analysis*, vol. 1, No. 1, pp. 11-27.

Karlsson, B. and Quintiere, J. G. (2000), *Enclosure Fire Dynamics*, ISBN: 0-8493-1300-7, CRC Press, LLC, Boca Raton, USA.

Kemikontoret (2001), *Riskhantering 3 – Tekniska riskanalysmetoder*, Kemikontoret (The Swedish Plastics and Chemicals Federation), Sweden.

Kluge, J. (1985), *BRAND/BVT – Tillförlitlighetsdata för brandlarmsutrustning*, ÅK-8508-10, Sydkraft AB, Sweden.

Lauridsen, K., Christou, M., Amendola, A., Markert, F., Kozine, I. and Fiori, M. (2002), *Assessing the uncertainties in the process of risk analysis of chemical establishments - The ASSURANCE project – Final summary report.* Risø National Laboratory, Roskilde, Denmark.

Levinson, S.H. and Yeater, M.L. (1983), Methodology to Evaluate the Effectiveness of Fire Protection Systems in Nuclear Power Plants*, Nuclear Engineering and Design,* vol. 76, no. 2, pp. 161-182 (54 ref.).

Malmsten, K. and Harrysson, J (2004), *Användning av risk- och sårbarhetsanalyser vid kommunal planering inför extraordinära händelser.* Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

Mattson, B. (2000), *Riskhantering vid skydd mot olyckor - Problemlösning och beslutsfattande*, Swedish Rescue Services Agency, Karlstad, Sweden.

Mattson, B. (1990), *The price for our safety*, Swedish Rescue Services Agency, Karlstad, Sweden.

Moore, W.D., (1993), *Balanced Design Concepts*, workshop editor Bukowski R.W., NISTIR 5264, Gaithersburg, Maryland, USA.

Nilsson, J. (2003), *Introduktion till riskanalysmetoder.* Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

Nystedt, F. (2000), *Riskanalysmetoder*. Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

Perrow, C. (1984), *Normal accidents - Living with high-risk technologies,* Basic books, New York, USA.

Olsson, F. (1999), *Riskanalysmetoder*. Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

Perry, R.W. (2004), Disaster Exercise Outcomes for Professional Emergency Personnel and Citizen Volunteers. *Journal of contingencies and crisis management*, vol. 12, no. 2, pp. 64-75.

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

Reason, J. (1993), The identification of latent organisational failures in complex system*, Verification and Validation of Complex systems: Human Factors Issues*, NATO ASI Series, pp. 223–37, Berlin/Heidelberg, Germany.

Reason, J. (1997), *Managing the Risks of Organisational Accidents*. Aldershot, UK: Ashgate.

Renn, O. (1998), The role of risk perception for risk management, *Reliability Engineering and System,* Vol. 59, pp. 49-62.

Rosenhead, J. (1989), *Rational Analysis for a Problematic World: Problem Structuring Techniques for Complexity*, *Uncertainty and Conflict*, Wiley, Chichester, UK.

Rosness, R. (1993), *Limits to Analysis and Verification*. In Wise, J.A., Hopkin, J.A., Stager, P. (eds): Verification and Validation of Complex Systems: Human Factors Issues. Berlin: Springer.

Sagan, S. D. (2004), *Learning from normal accidents,* Stanford University, USA.

Schlyter, J., Selvén, D. (2004), *Indexmodell som underlag vid riskvärdering.* Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

SFPE (1994), *The SFPE Handbook of Fire Protection Engineering,* Second edition, section 2-14, Quincy, MA, USA.

Sjöberg, L. (2000), Political decisions and public risk perception, *Reliability Engineering and System Safety*, Vol. 72. Is. 2, pp. 149-151.

SS-EN 1050, (1996), *Maskinsäkerhet – Principer för riskbedömning*, Sweden.

Sundelius, B., Stern E. and Byander, *F.* (1997), *Krishantering på svenska – teorier och praktik*, Nerenius and Santérus Förlag AB, Stockholm, Sweden.

Rosenberg, T. (1989), *Att skydda och rädda liv, egendom och miljö : handbok i kommunal riskanalys inom räddningstjänsten*. Swedish Rescue Services Agency, Karlstad, Sweden.

Särdqvist, S. (2006), *Vatten och andra släckmedel,* 2:a upplagan, Swedish Rescue Services Agency, Karlstad, Sweden.

Särdqvist, S. (1996), *An Engineering Approach to Fire-Fighting Tactics,* Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

Särdqvist, S., (1993), *Initial Fires: RHR, Smoke Production and CO Generation from Single Items and Room Fire Tests*, ISRN LUTVDG/TVBB—3070—SE, Department of Fire Safety Engineering, Lund Institute of Technology, Lund, Sweden.

Wettland, F., (1991), *BS-100 Reliability Analysis*, ST-91-CR-013-01, Sikte C A/S.

VGB – PowerTech (1998), *Richtlinie – Brandschutz im Kraftwerk,* VGB-R 108, Essen, Germany.

Electronic sources

Compact Oxford English Dictionary (2007), Retrieved 2007-05-25 at:
http://www.askoxford.com/concise_oed/vulnerable?view=uk

ECOCERA Co., LTD. (2007), Retrieved 2007-10-10 at:
http://www.gobizkorea.com/blog/en_catalog_view.jsp?blog_id=ecoglass&obj_id=659431&co_lang=2 and http://www.ecocera.co.kr/en/page15.html

EEX (2008), European Energy Exchange, Retrieved 2008-01-10 at:
http://www.eex.com/de/Marktinformation/Strom/Stundenkontrakte%20%7C%20Spotmarkt/spot-hours-table/2007-10-15

ESIS (2007), European chemical substances information system. Retrieved 2007-07-24 at:
http://ecb.jrc.it/esis/index.php?GENRE=CASNO&ENTREE=108-88-3

European Commission (2000a), *Iuclid dataset – Isoprene,* European Chemicals Bureau, European Commission, Italy, Retrieved 2007-11-12 at:
http://ecb.jrc.it/IUCLID-DataSheets/78795.pdf

European Commission (2000b), *Iuclid dataset - Sodium zinc potassium polyphosphate (Borosilicate glass),* European Commission, European Chemicals Bureau, Italy, Retrieved 2007-11-12 at:
http://ecb.jrc.it/IUCLID-DataSheets/65997173.pdf

Goddard, P. (2007), *A brief review of technology, legislation and economics*, Energy Focus, Retrieved 2007-05-29 at:
http://www.energy-focus.com/issue2/pdfs/flue.pdf

ICSC (2007), Inter-organisation programme for the sound management of chemicals. Retrieved 2007-07-24 at:
http://www.inchem.org/documents/icsc/icsc/eics1488.htm
and http://www.inchem.org/documents/icsc/icsc/eics0904.htm

KEMI (2007), Swedish chemical agency. Retrieved 2007-07-23 at:
http://apps.kemi.se/flodessok/floden/kemamne_eng/polyeten_eng.htm
and http://apps.kemi.se/flodessok/floden/kemamne_eng/toluen_eng.htm

Lentjes (2007) Retrieved 2007-11-13 at:
http://www.lentjes.de/LENTJES/index.php?id=174&L=1&L=1

NLM (2007), United States National Library of Medicine, Retrieved 2007-09-19 at:
http://toxnet.nlm.nih.gov/cgi-bin/sis/search/f?./temp/~t9Rk6Z:1

Oxford Dictionary (2004), Retrieved 2004-11-15 at:
http://dictionary.oed.com, search for: vulnerability/vulnerable

Seveso II Directive (2007), European Commission, retrieved 2007-10-16 at:
http://ec.europa.eu/environment/seveso/index.htm

Appendix 1 Used checklist

This checklist is based on Kemikontoret's (2001) checklist, appendix 1. The selected questions are somewhat arbitrarily selected, but based on the company's own perception of major risk sources (see also chapter 7.1.1).

Substances

- What substances are used in the FGD?
- What are the ignition temperatures for the plastic, glue and the rubber?
- What are suitable and not suitable extinguishing substances?
- If the rubber/plastic is burning what is then the concentration level that may cause serious immediately injury when inhaled?
- Are there other ways to ingest the toxic substance, other than through the lungs?
- What are the glue and plastic injury effects?
- What personal protection equipment is mandatory?
- Are there any explosive substances in the FGD?
- Are the substances corrosive?

Construction/Design

- What is the safety marginal in pressures, temperatures of the FGD?
- How is a fire prevented from expanding?
- Are operator/workers wrong actions forgiven by the system and automatically put into fail safe mode?
- Are there necessary instruments for control and emergency stop of the FGD?

Montage/Repair work

- Is the responsibility clarified according to the German law? How does it work?
- Are workers adequately educated and competent?
- Is the plant clean and in order?
- Do contractors have proper information about safety regulations, emergency actions, etc.?

During operation

- How are experiences with accidents and incidents reported and documented?
- Do the operators follow set routines for operation?
- How are new employed personnel trained and educated?
- How are the workers informed of routines that are useful for them?
- How is information of the present situation transferred to different shifts of workers?

Emergency response

- What medical treatments are available?
- How should the worker react in the event of a fire, gas leak, power cut, etc.?
- How is the fire equipment and personal protection placed and checked?
- Were earthquakes, flooding etc. taken under consideration when the plant was erected?
- Have all the safety critical equipment parts been identified and been included in a program for regular function control?
- How are the emergency exits built up?

Appendix 2 Risk chart of external natural threats

The chart presented below is used by a risk engineering group within the same corporate group as the company and taken from the World Map of Hazard of the Nature which is developed by the insurance company Münchener Rück. The risk index is a description of consequence and probability combined for the whole plant (not just the FGD) in case of a threat.

Threat	Risk Index	Description
Hail	3	Middle
Lightning	3	Middle
Storm	3	Middle
Earthquake	2	Small
Tsunami	1	None
Tornado	1	None
Volcano	1	None

Below is the assigned scale of the risk chart. The number (risk index) has a descriptive word assigned to it.

Risk Index	Description
4	High
3	Middle
2	Small
1	None

Appendix 3 Questions for the vulnerability hazard identification

The questions below are developed from Einarsson and Rausand (1998) and from Einarsson and Sigbjörnsson (1999). By extracting the content of what they mean with "risk factors," the questions have been developed to give the kind of answers they describe in their papers, but with the FGD in mind instead. For a more precise description of the background material see chapter 7.2.

Internal factors

System attributes	- Is the system designed with a high complexity? In other words, are there many components that are connected with each other in a way that is not linear? - Is the coupling between the different parts of the system tight or loose? In other words, if something malfunctions or disturbs the process, does that mean an immediate stop of the FGD?
Tech. fail/hazards	- What does the company do to prevent technical failures and hazards? Is there a program/plan to follow and/or management that organises and conducts check-ups? - What are the technological threats that are of importance?
Human	- How are the workers mistakes and errors dealt with? Is there any special training the workers have to perform regularly? - Are actions to reduce mistakes and errors trained regularly? - Is there any regular work conducted to find hidden dangers/hazards (latent errors)?
Management and Organisation	- How is the risk management organisation built up within the company? - Are there health, safety and environmental programs/systems within the company?
Maintenance	- Are there safety regulations especially for repair work? - Are the workers checked if they follow the safety regulations? - What are the consequences for workers that do not follow the safety regulations?
Staff	- How is safety culture dealt with, is there any work to increase the workers' safety culture/thinking? - Is the FGD dependent on key personnel and if so, how is it handled when the company loses important people? - How are contractors dealt with, to insure that they fulfil the safety level of the company? - Is there any sabotage threat from the employed personnel?

External factors

Environmental	- Have there been any previous flooding or earthquakes in the area?
Societal	- Does the company have any sabotage/terrorist threat aimed towards it?
Infrastructure	- How is the quality of the gypsum production secured? - How is the quality of the limestone delivery secured? - How is water supply guaranteed? - How are the delivery and quality of spare parts secured? - Are there back-up systems for the above, such as a second limestone delivery company?
Legal	- What laws are important for the FGD, today and in the future? - What are the consequences of breaking the emission limits, due to a malfunctioning FGD?
Market	- How does the coal power market look? Does the company have a small economical marginal for safety investments today and how does it look in the future?
Financial	- What is included in the company's insurance? Are both the construction and the production loss covered? - What is the cost for a total destruction of the FGD? - What is the cost for the plant, if no production of power is generated during one day? - How long can the company afford a zero production of the plant? - How much money is used for hazard prevention within the company and for the specific FGD? - How is the economical stress level for workers at the company (and its contractors)? Are they under high pressure with the danger to perform fast and careless work?

Appendix 4 Ignition check chart

The chart provided below is the first estimation of the fire risk in the FGD and is used as the first input into the event tree analysis. The column named "Location/reason" has been developed from VGB – PowerTech (1998) and the columns "Consequences" and "Probability" have been evaluated during discussions with specialists from the company's insurance firm and VGB - PowerTech and the company's own safety engineers. The scales are adopted from Kemikontoret (2001) and the consequence scale is adjusted to fit with the expected cost of a total destruction of the FGD of more than 50 million Euros.

Ignition Source	Presence? (Yes/No)	Possible? (Yes/No)	Location/reason	Consequences (1-5)*	Probability (1-5)**
Open flame	Yes	Yes	Welding, solder, burning	5	2-3
			Smoking		1-2
Mechanical Sparks	Yes	Yes	Grinding, cutting, separating	5	2
Electrical Sparks	Yes	Yes	Fire caused by damage cables	5	1-2
Electrical currents	Yes	Yes	Lamps, tools, electrical current divider	5	1-2
Hot surfaces	Yes	Yes	Heating appliances/ radiant heater	5	1-2
Hot air	Yes	No	Flue gases	-	-
Autooxidise substances	Yes	No	Insulation material	-	-

*Consequences

*Index	Description	Total cost (mil. Euros)
1	small	< 0.25
2	mild	0.25-2.5
3	medium	2.5-12.5
4	large	12.5-50
5	catastrophic	> 50

**Probability

**Index	Description	Frequency (times per year)
1	Incredible	< 1/1000
2	remote/unlikely	1/100-1000
3	infrequent/possible	1/10-100
4	probable/likely	1/1-10
5	frequent/very likely	> 1/1

Appendix 5 Fire plume calculation

The plume radius has been calculated with equation 4.16 in Karlsson and Quintiere (1999):

$b = 6/5 \cdot \alpha \cdot z$

Where b is radius in meters, α is the entrainment coefficient and z is the height of the plume in meters. This α is not to be confused with the α in a αt^2 fire. The equation is based on the "ideal plume" model. This is a rough simplification of real fire plumes and comes with several simplifying assumptions. Below is a summery of the main assumptions.

I. The fire is assumed to originate from a point source and that all energy remains in the plume and no energy is lost due to radiation. Many common fuel sources have in reality a typical radiation loss of 20 to 40% of the total energy.
II. The density difference is only assumed to be significant when expressing the buoyancy force. Looking over the whole plume, the density difference between the surrounding and the plume is regarded as small and $\rho_\infty \approx \rho$. The practical consequences of this are that the model is not good for estimations close to the source of the fire.
III. The velocity, temperature and force profiles are assumed to be of similar form and independent of the height. The temperature and velocity are as well assumed to follow a top hat profile, causing them to be constant over the horizontal section at any height with corresponding radius. Outside the plume, the velocity is assumed to be 0 and the temperature equal to the ambient temperature of the room.
IV. The horizontal velocity (ν) is assumed to be proportional to the vertical velocity (u) as $\nu = \alpha \cdot u$, with α as the entrainment coefficient of ≈ 0.15. This value is difficult to measure but corresponds well with experimental measured values.

Below are the calculated values of the plume radius at different heights above the ground.

z - height (m)	b - radius (m)
0,6	0,108
0,8	0,144
1,0	0,180
1,2	0,216
1,4	0,252

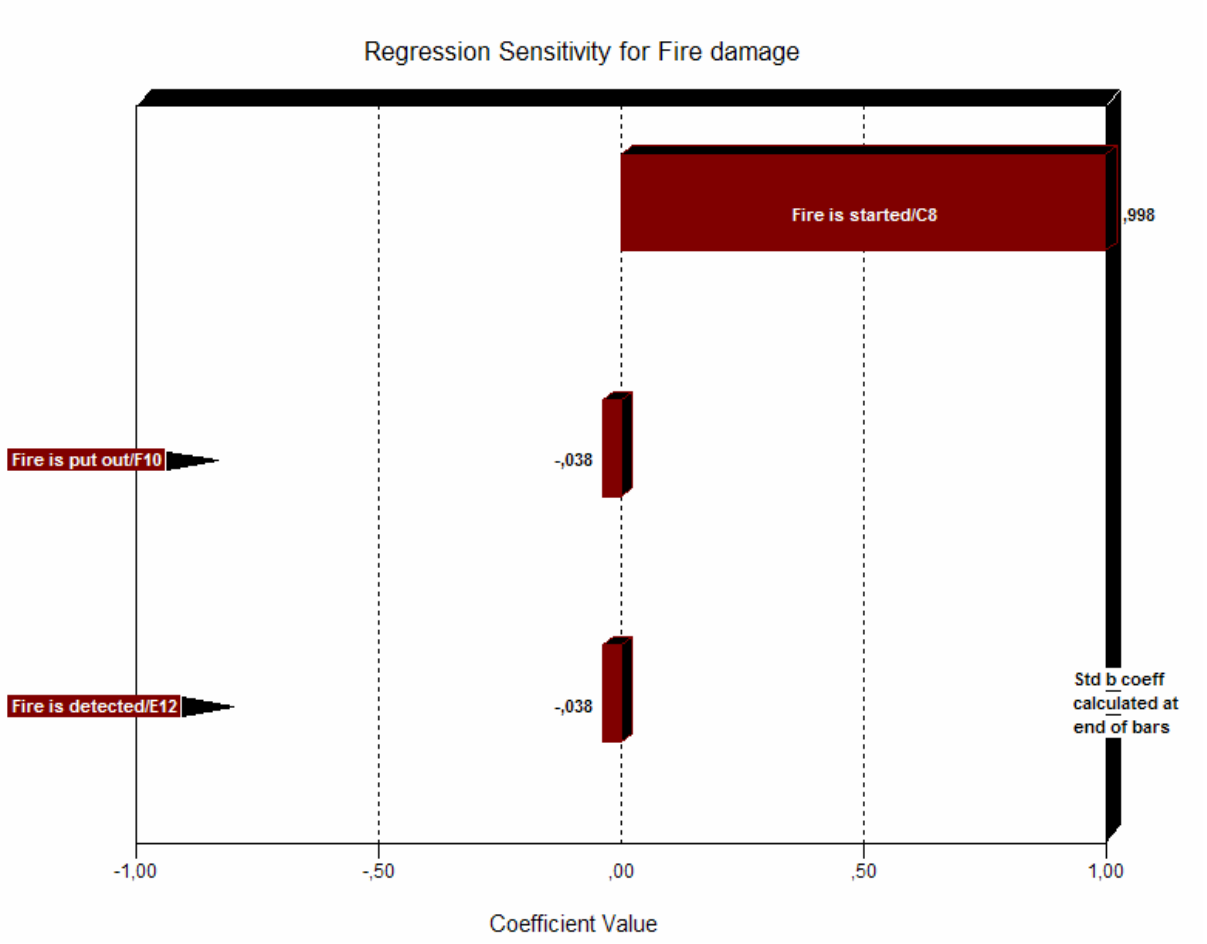
Appendix 6 Fire growth of rubber according to αt^3-curves

	Fastest		*Söderblom (Särdqvist 1993)*	
Time (s)	**α-value (MW/s^3)**	**Effect (MW)**	**α-value (MW/s^3)**	**Effect (MW)**
0	0,000005	0,00	0,0000026	0,00
30	0,000005	0,14	0,0000026	0,07
60	0,000005	1,08	0,0000026	0,56
90	0,000005	3,65	0,0000026	1,90
120	0,000005	8,64	0,0000026	4,49
150	0,000005	16,88	0,0000026	8,78
180	0,000005	29,16	0,0000026	15,16
210	0,000005	46,31	0,0000026	24,08
240	0,000005	69,12	0,0000026	35,94
300	0,000005	135,00	0,0000026	70,20
360	0,000005	233,28	0,0000026	121,31
420	0,000005	370,44	0,0000026	192,63
480	0,000005	552,96	0,0000026	287,54

	Middle		*Sundström (Särdqvist 1993)*	
Time (s)	**α-value (MW/s^3)**	**Effect (MW)**	**α-value (MW/s^3)**	**Effect (MW)**
0	0,0000016	0,0	0,00000069	0,0
30	0,0000016	0,0	0,00000069	0,0
60	0,0000016	0,4	0,00000069	0,1
90	0,0000016	1,2	0,00000069	0,5
120	0,0000016	2,8	0,00000069	1,2
150	0,0000016	5,6	0,00000069	2,3
180	0,0000016	9,6	0,00000069	4,0
210	0,0000016	15,2	0,00000069	6,4
240	0,0000016	22,7	0,00000069	9,5
300	0,0000016	44,4	0,00000069	18,6
360	0,0000016	76,7	0,00000069	32,2
420	0,0000016	121,9	0,00000069	51,1
480	0,0000016	181,9	0,00000069	76,3

	Slowest	
Time (s)	**α-value (MW/s^3)**	**Effect (MW)**
0	0,000000345	0,00
30	0,000000345	0,01
60	0,000000345	0,07
90	0,000000345	0,25
120	0,000000345	0,60
150	0,000000345	1,16
180	0,000000345	2,01
210	0,000000345	3,20
240	0,000000345	4,77
300	0,000000345	9,32
360	0,000000345	16,10
420	0,000000345	25,56
480	0,000000345	38,15

Appendix 7 Regression analysis



Appendix 8 Human error, violation and latent failure related scenarios for the FGD

Threat	Scenario (Emergency)	Potential immediate effects	Resources/plans/system for mitigation, restoration, rebuilding, etc.		Remarks
			Internal	External	
Human error	A welding tool is accidentally directed towards the rubber.	Ignition is relatively instant and fire spreads rapidly and causes catastrophic consequences if not put out.	Flame proof blankets on the rubber preventing accidental ignitions. Fire guard, fire hoses, water screens and fire extinguishers are also at hand.	The local fire department arrives at the scene 10-15 min after an alarm. Insurance covers both rebuilding costs and production losses.	
Human error/ Violation	A lamp with too high heat effect is used in the FGD.	After many hours a fire starts and the fire spreads rapidly and causes catastrophic consequences if not put out.	There are strict regulations of what sort of lamps are allowed in the FGD. Surveillance with smoke detectors and fire watch for detection of fire. Fire hoses, water screens and fire extinguishers are also at hand.	The local fire department arrives at the scene 10-15 min after an alarm. Insurance covers both rebuilding costs and production losses.	The lamp can be used due to absent-mindedness or as an intended violation.
Violation	A fire is caused by someone smoking inside the FGD.	The ignition of the fire goes slowly, but after the first flame the fire spreads rapidly and causes catastrophic consequences if not put out.	Surveillance with smoke detectors and fire watch for detection of fire. Fire hoses, water screens and fire extinguishers are also at hand.	The local fire department arrives at the scene 10-15 min after an alarm. Insurance covers both rebuilding costs and production losses.	
Latent failure	The use of external employees (contractors).	Increase of human errors and violations due to different (lower) risk attitude.	Safety management section of the company which informs and controls the safety behaviour of employees and contractors.	The contractors own controls and safety information.	Latent failures leads to human errors or violations
Latent failure	Shortcomings in report system.	Incidents as “near misses” are not considered important enough to be reported. The organisation therefore misses a lot of its learning potential and indication of how to decrease risks.	Safety management section of the company that works for a continuing increase of safety.	Insurance and governmental demands of information concerning accidents and incidents.	

Appendix 9 Quantitative analysis of vulnerability scenarios A and B

Scenario	Likelihood of scenario *	Consequences of scenario **				Resources to mitigate, rebuild, restore, etc. ***		Total
		Human impacts	Environmental impacts	Business impacts	Property impacts	Internal	External	
A) A welding tool is accidentally directed towards the rubber.	1-2	1	0	4	4	3	4	1.5·(1+0+4+4-(3+1.2·4)) = 1.8 See also figure 29
B) A lamp with too high heat effect is used in the FGD.	0-1	0	0	4	4	2	4	0.5·(0+0+4+4-(2+1.2·4)) = 0.6 See also figure 29

*The scale of likelihood factor runs from 0 to 4, 4 meaning very frequent and 0 meaning negligible. The numbers are taken from Appendix 4 and then translated to fit this scale.

** The scale for the four different consequence impacts runs from 0 to 4, 4 meaning the most critical and 0 meaning negligible. The numbers for the human and environmental impacts have been assigned by so called "expert estimations" by the author and company experts. The number for property impact is set with the postulation that a new FGD is estimated to cost something in the vicinity of 50 million Euros (estimation by insurance company) and is regarded to be most critical – 4. The business impact is based on calculations of lost profit that can be found below. The weight for the consequences' impact of the scenario has been chosen to be equal to 1, since there is no particular reason for assigning anything else.

*** The scale for the mitigation resources runs from 0 to 4, 4 meaning a strong (available and adequate) resource and 0 meaning a very weak (unavailable or inadequate) resource. The numbers have been assigned by so called "expert estimations" by the author in discussion with company experts. The internal weight is assigned to be 1, for the same reasons as for the impacts above. The external weight is assigned slightly higher (1.2) as insurance covers all lost profit and the replacement of the FGD. It does not, however, cover all losses, such as the human impact and some other economical aspects, which is why a higher number is not assigned than 1.2.

The business impact depends on lost profit, lost credibility/reputation and lost market shares. Since the company is in a long term contract with the mother company and the market is stable and the energy demand is continuing to increase, the lost market shares are therefore neglected in this case. Lost reputation and credibility can, however, be a problem if the company has continuous problem with the safety. The estimation for how large this impact can be is outside of the scope of this thesis, as it is a rather complicated economical problem. If unlucky, an accident can occur in the wrong moment and turn the public against the company, which could cause large economical damage in the long run.

The estimation of the business impact is therefore based on the loss of profit that the company may suffer in case of an accident. The lost profit is equal to the expected income of the energy subtracted with the producing cost, for the time period of the power plant has to be shut down. The production cost is simplified to only depend on the cost of coal. Additional cost would be energy, water and limestone costs, etc, but since the income of the sales of the gypsum is also neglected the two factors should even out each other to some extent. Salary to the employees is paid in any case and, is therefore not included in the calculation. Below follows a chart of what the lost profit would be for a destroyed FGD for unit 3 and 4. The estimated rebuilding time of a FGD is one year and the power price is taken from the 15th of October 2007, with a mean value of the pike price and the bottom price of that day (EEX 2008). Running time and quantity of coal used in the different units are from 2006.

	Unit 4	**Unit 3**
Energy price (cent/kWh)	5,8	5,8
Running time (h)	6,500	6,000
Effect (kW)	500,000	300,000
Lost Income (Euros)	188,500,000	104,400,000
Coal (tons)	1,000,000	600,000
Coal price (Euros/ton)	60	60
Lost production costs (Euros)	60,000,000	36,000,000
Lost profit (euros)	**128,500,000**	**68,400,000**
Profit 2005 (mil. Euros)	280	280
% of profit	**46**	**24**

As seen above, the magnitude of lost profit would be considerable and is here called to be most critical – 4. What should be kept in mind is that this calculation is not very exact but rather gives an estimate of the impact. For instance, an accident like this would have a much greater impact on the final result of the company in the year 2004, when the profit after tax and interest costs was 180 million Euros. The impact would then have been 71 respective 38 % of the total profit.