HAZOP and SEQHAZ® methods as input data producers to Safety Integrity Level evaluations

Daniel Björkhem

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

Brandteknik och Riskhantering
Lunds tekniska högskola
Lunds universitet

Report 5250, Lund 2008

The report has been financed by Neste Jacobs Oy

HAZOP and SEQHAZ® methods as input data producers to Safety Integrity Level evaluations

Daniel Björkhem

Lund 2008

Title
HAZOP and SEQHAZ® methods as input data producers to Safety Integrity Level evaluations

Author / Författare
Daniel Björkhem

Report 5250
ISSN: 1402-3504
ISRN: LUTVDG/TVBB--5250--SE

Number of pages: 111
Language: English
Illustrations: Daniel Björkhem

Keywords
evaluation, HAZOP, hazard study, LOPA, process industry, risk graph, SEQHAZ, SIL

Sökord
HAZOP, klassificering, LOPA, processindustri, riskanalys, riskgraf, SEQHAZ, SIL

Abstract
Today hazard studies are a self evident part of a project plan while creating a new process or making changes in an existing one in the chemical industry. Therefore it is important to make the hazard studies as efficient as possible. The objective for this thesis was to optimise the hazard study processes based on the main methods presently used at Neste Oil Oyj, Neste Jacobs Oy and Borealis Polymers Oy. This thesis focuses on SEQHAZ® and HAZOP methods as input data for safety integrity level (SIL) evaluation with risk graph and LOPA (layer of protection analysis) methods. The hazard study process has been investigated by interviews, participation in hazard studies, studying of hazard reports and a seminar day. Based on the results three models for optimising the process are suggested, two based on LOPA and the third based on risk graph. LOPA was found to be the best method for SIL evaluation and the suggested models are a step towards performing both the HAZOP/SEQHAZ® study and the SIL evaluation in the same session.

Brandteknik och Riskhantering
Lunds tekniska högskola
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

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

Summary

Hazard studies are today a self evident part of a project plan while creating a new process or making changes in an existing one in the chemical industry. For most projects one or more of these studies must be conducted. Therefore it is important to make the hazard studies as efficient as possible to save time and money, but without jeopardizing safety.

The objective for this thesis was to optimise the hazard study processes based on the main methods presently used at Neste Oil Oyj, Neste Jacobs Oy and Borealis Polymers Oy. Neste Jacobs Oy is Neste Oil Oyj's in-house engineering company and belongs to the corporate development unit. It is a Finnish company with over 40 years of experience working with various process plant investment projects in oil refining, petrochemicals and chemicals processes in Europe, North America and the Middle East.

In hazard study processes at Neste Oil Oyj and Neste Jacobs Oy, two methods, Hazard and Operability study (HAZOP) and Seqhaz Hazard Mapping (SEQHAZ®) are currently the most used methods for hazard identification and risk estimation. Part of the information from HAZOP and SEQHAZ® studies are then used to perform a Safety Integrity Level (SIL) evaluation. The SIL evaluation establishes whether or not the risk reduction measures are enough according to the tolerable risk level. If not, further protection has to be added which can be in the form of mechanical protection or a safety instrumented function (SIF). For the SIF the proper SIL must be assigned. This is a measure of how advanced automation and interlock systems need to be installed in order to live up to the tolerable risk level. The SIL evaluation method used by Neste Jacobs Oy is risk graph whereas Borealis Polymers Oy utilises layer of protection analysis (LOPA).

Based on HAZOP, SEQHAZ®, risk graph and LOPA the key elements of the hazard study processes at Neste Jacobs Oy have been identified through interviews, participation at hazard studies, studying of hazard reports and a seminar day. Based on the results three models have been suggested for optimisation of the process.

For optimisation of the hazard study process, other methods for SIL evaluation have also been evaluated and a comparison between risk graph and LOPA has been done. LOPA was found to be the best method for SIL evaluation, however risk graph was also deemed a suitable method. The main problem has been how the information should be passed on from HAZOP and SEQHAZ® in an effective manner to the SIL evaluation. The models have been designed with improving this as a goal. Two of the models are based on LOPA methods and the third is based on a risk graph method.

The suggested models are designed to facilitate the work for the SIL evaluation team at the expense of more work for the HAZOP/SEQHAZ® team. Within the limited time of this master's thesis, it was not possible to test in a practical manner whether the improvements are better in a larger perspective for the entire hazard study process. An evaluation of the models has therefore not been possible and the models may have to be modified to suit other companies than Neste Jacobs Oy. The proposals in the models are a step towards performing both the HAZOP/SEQHAZ® and the SIL evaluation together in the same session.

Sammanfattning (Summary in Swedish)

Riskanalyser är idag en självklar del av en projektplan för en ny process eller vid förändringar i en befintlig inom den kemiska processindustrin. Därför är det viktigt att riskanalyserna görs så effektivt som möjligt i mån om att spara tid och pengar men utan att det leder till negativa konsekvenser för säkerheten.

Målet för detta examensarbete vara att optimera riskhanteringsprocessen hos Neste Jacobs Oy baserat på de metoder som används i dagsläget av Neste Oil Oyj, Neste Jacobs Oy och Borealis Polymers Oy. Neste Jacobs Oy är Neste Oil Oyj's interna ingenjörsföretag och hör till koncernens utvecklingsenhet. Det är ett finskt bolag med över 40 års erfarenhet av arbete med olika processanläggningars investeringsprojekt inom oljeraffinering, petrokemi och kemiska processer i Europa, Nord Amerika och Mellanöstern.

Vid riskhanteringsprocessen på Neste Oil Oyj och Neste Jacobs Oy används i huvudsak, två metoder, Hazard and Operbility Study (HAZOP) och Seqhaz Hazard Mapping (SEQHAZ®) för riskidentifiering och riskuppskattning. En del av informationen från HAZOP och SEQHAZ® används sedan för att utföra en "safety integrity level"(SIL)-klassificering. SIL-klassificeringen fastställer om riskreduktionen är acceptabel utifrån den tolerabla risken, om inte, behöver säkerhetsbarriärer läggas till. Dessa kan vara av mekaniskt slag eller bestå av säkerhetskritisk instrumentering varvid dess integritetsnivå (SIL) måste bestämmas. För SIL-klassificeringen använder Neste Jacobs Oy sig av en Riskgrafmetod och Borealis Polymers Oy som också har varit inblandat i projektet en säkerhetsbarriäranalys (LOPA).

Med HAZOP, SEQHAZ®, Riskgraf och LOPA som utgångspunkt har de viktigaste delarna av riskhanteringsprocessen vid Neste Jacobs Oy's projekt identifierats genom intervjuer, deltagande vid riskanalyser, studerande av riskanalysrapporter och en seminariedag. Med resultaten som grund har tre modeller föreslagits för optimering av processen.

För optimering av riskhanteringsprocessen har även andra metoder för SIL-klassificering undersökts och en jämförelse mellan Riskgraf och LOPA har gjorts. LOPA visade sig vara den bästa metoden för SIL-klassificering men även Riskgraf har funnits vara en lämplig metod. Huvudproblemet har varit på vilket sätt informationen skall föras vidare från HAZOP och SEQHAZ® analyserna på ett effektivt sätt som möjligt till SIL-klassificeringsteamet. Modellerna har därför utformats med detta som mål och två av modellerna är baserade på LOPA-metoder medan den tredje är baserad på en Riskgrafmetod.

De föreslagna modellerna leder till att SIL-klasssificeringsteamets arbete förenklas, medan HAZOP/SEQHAZ® teamet belastas. Huruvida denna förbättring är bättre i ett större perspektiv för hela riskhanteringsprocessen har inom ramen för detta examensarbete av tidsskäl inte varit möjlig att testa praktiskt. En utvärdering av modellerna har därför inte varit möjlig och modellerna kan behöva modifieras för att passa andra företag än Neste Jacobs Oy. Förslagen som gjorts i modellerna går i riktningen mot att genomföra både HAZOP/SEQHAZ® analysen och SIL-klassificeringen gemensamt i en och samma analys.

Foreword

This thesis has been conducted to meet the requirements for a Master of Science degree in Risk Management and Safety Engineering at the Department of Fire Safety Engineering, Lund University, Sweden. The thesis was written at Neste Jacobs Oy in Porvoo, Finland during September 2007 to February 2008.

During the work with this thesis I have received help from many persons and for that I would like to give my gratitude. I thank my tutor at the department of Fire and Safety Engineering Anders Jacobsson for all valuable comments and discussions.

I give my appreciation to my tutors Rainer Salo and Hanna Honkanen at Neste Jacobs Oy for all your help and support. I also thank others involved in my project Ari Aitolahti, Kari Matilainen, Irmeli Vauhkonen, and especially Erkki Turkkila for always taking your time to discuss.

I give my gratitude to all the interviewees and participators of the seminar day Hanna Honkanen, Erkki Turkkila, Kai Ingman, Rainer Salo, Irmeli Vauhkonen Kimmo Virolainen, Yngve Malmén, Seppo Koskinen, Jukka Korvenoja, Rune Strahl, Tuomas Viskari, Kari Matilainen, Brian Tibbs, Sami Matinaho, Leena Hannonen, Olavi Haapalehto, Emmi Laiho, Sari Laanti, Jari Lyytinen, Johannes Maaskant, Asko Heikkinen, Marjut Aho, Timo Bergström, Tapio Kokko and Anders Jacobsson. Without your participation the writing of this thesis would not have been possible.

I thank Alex Kuuskoski, Sinead Fitzpatrick and James Law for your help to read through the thesis.

I would also like to thank all personal at Neste Jacobs Oy for helping with all small things and for the coffee breaks and lunch times. Finally I would like to thank my family, friends and especially Ann-Sofie for being there when needed.

Daniel Björkhem

Porvoo, February 2008

Acronym

AEA - Action Error Analysis

BPCS- Basic Process Control System

E/E/PE - Electrical/Electronic/Programmable electronic

FMEA – Failure Mode and Effects Analysis

HAZOP – Hazard and Operability Study

IPL- Independent Protection Layer

LOC – Loss of Containment

LOPA- Layer of Protection Analysis

P&ID - Piping and Instrumentation Diagram

PFD - Probability of Failure on Demand

RCM -Reliable Centre Maintenance

SEQHAZ® - Seqhaz Hazard Mapping

SIF - Safety Instrumented Function

SIL – Safety Integrity Level

SIS- Safety Instrumented System

Contents

1 Introduction

1.1 Background

Hazard studies are today a self evident part of a project plan while creating a new process or making changes in an existing one in the chemical industry. For most projects one or several have to be done. Therefore it is important to make the hazard studies as efficient as possible to save time and money, but without jeopardizing the safety.

In hazard study processes at Neste Oil Oyj and Neste Jacobs, two methods, Hazard and Operability study (HAZOP) and Seqhaz Hazard Mapping (SEQHAZ®), are currently the most used methods for hazard identification and risk estimation. Part of the information from HAZOP and SEQHAZ® studies are then used to perform a Safety Integrity Level (SIL) evaluation. This evaluation is a measure of how advanced automation and interlock system needs to be installed in order to have a safe process. The SIL evaluation method used by Neste Jacobs is risk graph, and the one used by Borealis Polymers Oy is layer of protection analysis (LOPA). There is an overlap between the teams making the HAZOP/SEQHAZ® studies and the SIL evaluation team. This is necessary as they better understand what is important for their respective team.

1.1.1 Neste Oil Oyj, Neste Jacobs Oy and Borealis Polymers Oy

Neste Oil Oyj Corporation is a refining and marketing company focusing on advanced, clean traffic fuels. Neste Oil Oyj has 4,740 employees and its shares are quoted on the Helsinki Stock Exchange. Neste Jacobs Oy is Neste Oil Oyj's in-house engineering company and belongs to the corporate development unit. Its main tasks are: Responsibility for executing Neste Oil Oyj's investments projects in Finland and abroad, to develop and market technologies and to operate as a technology expert. In addition to Neste Oil Oyj, the main customers are Gasum, Borealis, Dynea, Ashland and Styrochem. The number of employees is about 750 and the head office is situated in Kilpilahti, outside Porvoo, Finland. About 40 of the employees are situated in Naantali, Finland, where Neste Oil Oyj has a smaller refinery. In January 2008 Neste Jacobs Oy bought Rintekno Oy which increased the number of employees by 230.

Borealis Polymers Oy is producing and selling polyolefins and petrochemicals. The company has 1000 employees and the production sites are also situated in Kilpilahti, Finland. Borealis Polymers Oy is the affiliated company of Borealis group. Borealis group produces plastic materials to the infrastructure, automotive and advanced packing markets in Europe, the Middle East and Asia. The company's turnover was 5,7 billion euro 2006 and the number of employees 4500.

1.2 Objective

The objective of this thesis is to first identify and document the key elements of optimal hazard study processes based on the main methods presently used at Neste Oil Oyj, Neste Jacobs Oy and Borealis Polymers Oy. And secondly to define which resources are needed for each step. The final but most important objective is to develop new models where HAZOP/SEQHAZ® studies and risk graph/ LOPA are optimally implemented.

1.3 Problem formulation

A schematic picture of hazard study processes at Neste Jacobs Oy is illustrated in Figure 1. The problem is to improve this process with the focus laid on HAZOP/SEQHAZ® studies and SIL evaluation methods, also marked with a dashed line in Figure 1.

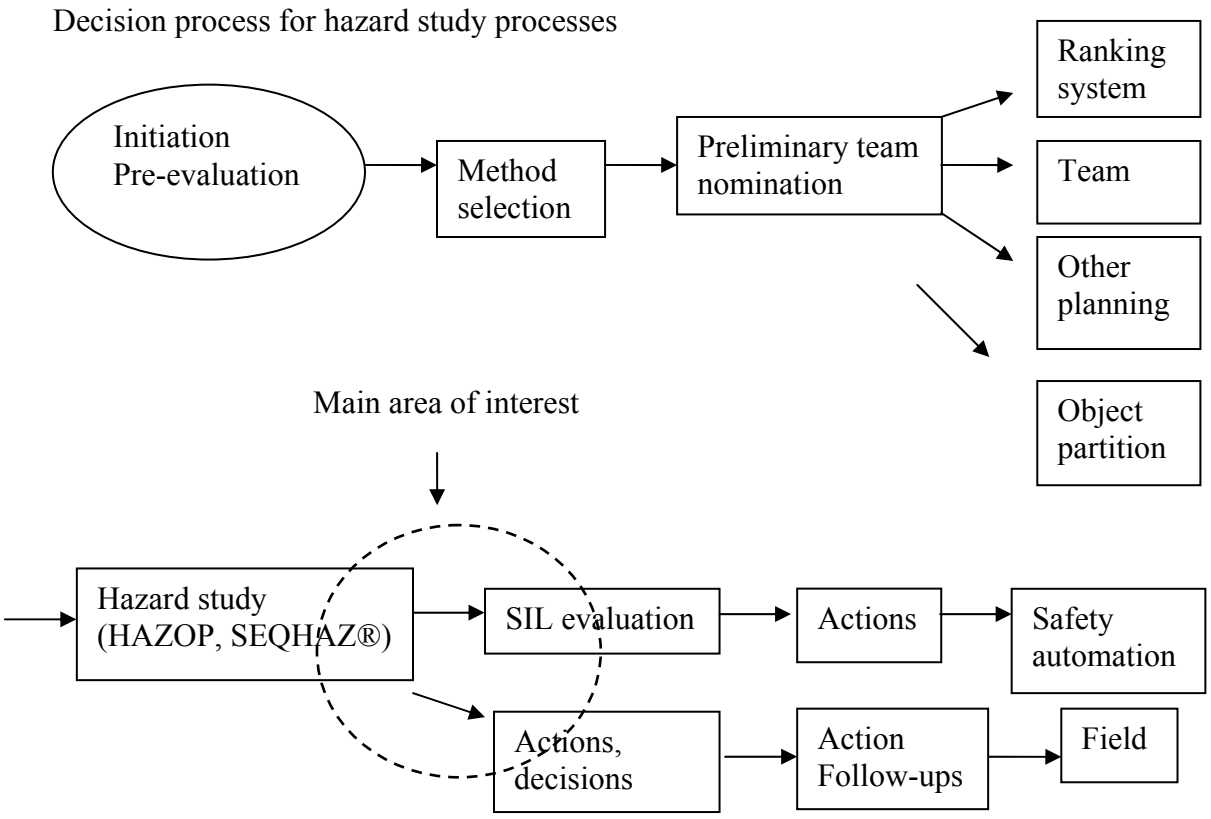

Figure 1. Schematic picture of hazard study processes at Neste Jacobs Oy, the main area of interest illustrated with a dashed line.

The key questions at issues for this project are:

- Which are the key elements in the HAZOP/SEQHAZ® study which serve as inputs for SIL evaluation?
- What information is the most important from the SEQHAZ® and HAZOP study for the SIL evaluation?
- Can any of the two methods (SEQHAZ®/HAZOP and risk graph/LOPA) be integrated into one?
- How can the hazard study process be improved?

- What are the main differences in data requirements between risk graph and LOPA?

1.4 Method

The project can be divided into two main parts. The first phase is a combined literature- and field study. In this phase Neste Oil Oyj, Neste Jacobs Oy and Borealis Polymers Oy hazard study methods are studied both theoretically and by participation in real hazard studies. Other relevant literature also has to be studied to get ideas for the model development. In the second phase new models are developed and suggestions for new implementation are proposed based on the information gained in the previous phase.

1.5 Limitations

The new model uses HAZOP and SEQHAZ® methods as basis for hazard identification and risk estimation. For SIL evaluation, risk graph and LOPA are used as basis.

1.6 Outline of the report

This report is divided into three major parts. Introduction and theory in chapters 1-3, the field study and its results and analysis in chapters 4-6 and optimised models for hazard study processes and final conclusions in chapters 7 and 8.

2 Hazard study processes

2.1 Definitions

Safety analysis in the chemical process industry has been performed for around 50 years. During these years many different terminologies have come up for the same thing. A consensus of which terms to use do not seem to exist. Therefore I have chosen to use the terms most commonly used in the chemical process industry and standard terminologies for Neste Oil Oyj. Below a definition of some key terminologies have been listed. The terms marked with (*) are defined as in the IEC Risk Analysis standard SFS-IEC 60300-3-9 (1995).

Availability - The probability that a device is operating successfully at a given moment in time.

Harm* - Physical injury or damage to the health, property or the environment.

Hazard* - Source of potential harm or a situation with potential for harm.

Hazardous event* - Event which can cause harm.

Hazard identification* - Process of recognizing that a hazard exists and defining its characteristics.

Hazard study - in the chemical process industry the terminology hazard study is often used instead of risk analysis (see Figure 2.). In this report, to be consistent mainly the term hazard study is mainly used, which includes both hazard identification and risk estimation. Other synonyms for hazard study according to CCPS (1992) are hazard evaluation, hazard assessment and process hazard analysis.

Hazard study processes - In this report the term refers to all parts shown in Figure 1. These are pre-evaluation, method selection, team selection, hazard study and SIL evaluation.

Risk* - Combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.

Risk analysis* - Systematic use of available information to identify hazards and to estimate the risk to individuals or population, property or the environment. (see Figure 2.)

Risk assessment* - Overall process of risk analysis and risk evaluation. (see Figure 2.)

Risk estimation* - Process used to produce a measure of the level of risks being analysed. Risk estimation consists of the following steps: frequency analysis, consequence analysis and their integration.

Risk evaluation* - Process in which judgements are done on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects.

SIL evaluation - Systematic analysis of reducing the risk to a tolerable risk level for the safety instrumented functions by determining the SIL for the functions. Other terms for SIL evaluation in the literature are SIL determination, SIL assessment or SIL assignment and therefore also these terms are also used as equivalent in this report.

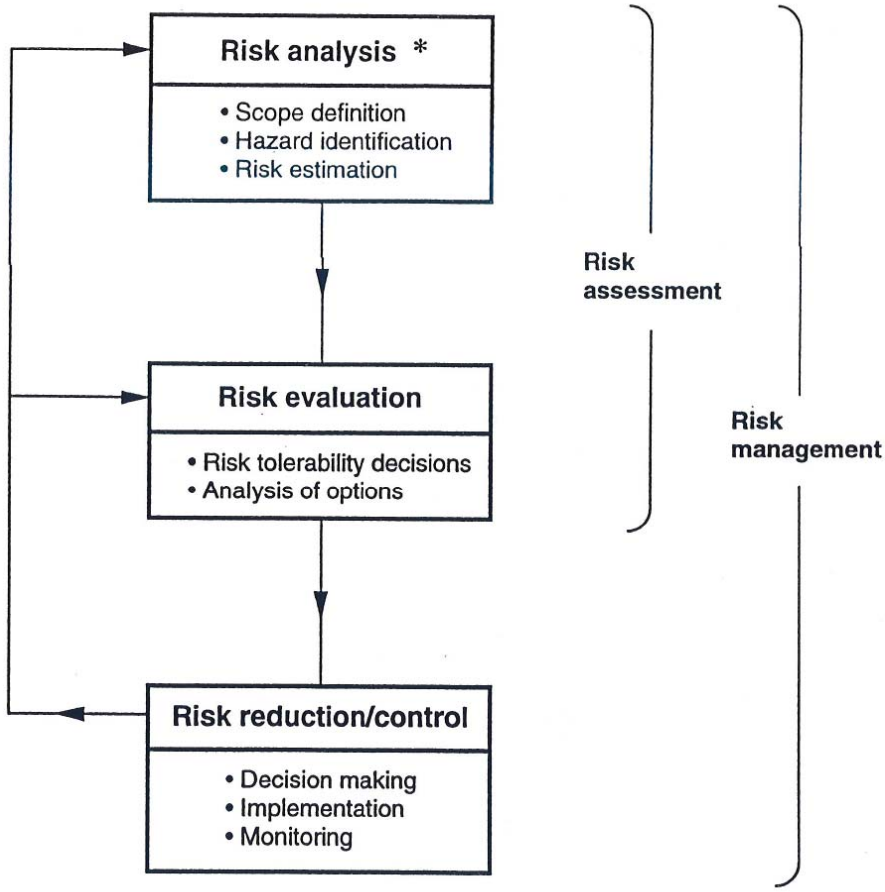

Figure 2. The relationship between risk analysis and other risk management activities. (SFS-IEC 60300-3-9, 1995)

2.2 Pre-evaluation and method selection at Neste Jacobs

The pre-evaluation is performed at the research, process development or preliminary design stage. Here it is important to get an overall view of the risks of the studied object. This can be done as soon as the first drawing of the process or any kind of object is available, and the purpose is to determine the risk level of the object by studying hazardous substances and reactions, environmental hazards and risks for explosion and fire, etc. For explosion and fire risks, Dow fire and explosion indices are calculated. In this stage the "inherent safety" principle, to make the process itself as safe as possible, is of great importance, as costs to make changes to the process still are low. In this phase the risk is classified low, medium or high depending on the consequences. (Salo, 2004)

For high risk level objects at least a HAZOP is performed. However, if there is a substantial amount of operational experience available and the object's risk level is low in respect to its class, a SEQHAZ® can be performed instead. On possible severe accidental discharges, consequence analyses are performed. These can be used to compare location and layout alternatives as well as locations of detectors and in preparing and adjusting rescue plans. For the most hazardous and difficult operational situations, human error and sequential errors are analysed with Action Error Analysis (AEA). For batch processes (when the concentration is not consistent over time), and especially during their cooking stage, a HAZOP version called Profile Deviation Analysis has been developed. Special risk assessments are done for pressure equipment and machines located in high risk areas. (Salo, 2004)

For moderate risk level objects SEQHAZ® is used as hazard study method. However if there are none or little operational experience available, there is not enough input data to achieve reliable results with this method. In these cases HAZOP and/or AEA is used. Certain risks identified in the HAZOP may require a consequence analysis. For low risk level objects there is usually no need for detailed hazard studies, but at least a SEQHAZ® or a HAZOP is recommended. (Salo, 2004)

2.3 Team selection

The team selection is an important stage in every hazard study. Even if a proper method is chosen for the study the end result is still depending on the team and how the people in the group interact with each other. The team is normally nominated in a preparation meeting between Neste Jacobs Oy and the client. The composition of the team depends on which method is used, but in general the following team composition is proposed, based on the information regarding team composition in HAZOP (Salo, 2005).

- process designer
- automation/instrument designer
- operating engineer
- maintenance engineer
- safety specialist
- team leader
- scribe

The required persons for the hazard study, as shown above, can be categorised in three groups: (1) leader, (2) scribe and (3) experts. The team leader provides direction for the analysis organizes and executes analysis activities and is responsible for hosting any meeting that may be held as a part of the study. It is essential that the team leader is experienced in the technique used, and a person from outside the project is preferred to obtain objectivity. Good interpretation skills are also important and a profound understanding of the objective of the study. The success of the study depends in many cases on the skill of the team leader. The scribe's task is to be the individual who documents the discussion that takes place at the hazard study. Typically the scribe may be someone who is not as experienced as the team leader but has some basic hazard study training and experience. It is important that the scribe has good writing and organisational skills. Scribes with more process experience can better sort out what should be documented from what should not. The rest of the team consists of experts from various areas. In this way they provide specific knowledge for their own area. This is the core of a hazard study; that people with different knowledge together can find out which risks the process has. Another important aspect is to have someone with practical experience of the process present at the analysis. This gives the others the "reality" aspect of how long time it takes to react if e.g. an alarm goes off. (CCPS, 1992)

2.4 Hazard identification and risk estimation methods used at Neste Jacobs Oy

Hazard studies consist of two parts; hazard identification and risk estimation. The purpose of hazard identification is to identify the source of the risk in terms of danger to Health, Safety, Environment (HSE) or economy. Then the risk is judged in terms of probability and consequence in the risk estimation. (Jacobsson, 2003)

There are today many hazard study methods available for hazard identification and risk estimation in the chemical process industry The most frequently used are estimated by Jacobsson (2003) to be What-if, HAZOP, Action Error Analysis (AEA) and Failure Mode and Effect Analysis (FMEA) or a combination of these. According to Laul et al. (2005) all are accepted methods for evaluating the risks and they have different strengths and weaknesses. Because of this it is more efficient to use a combination of the methods. It is up to every company itself to choose which method they prefer but laws and standards often enforce them. Salo (2004) states that during the many years in

use numerous variations of the existing methods have been developed and that ones used by Neste Jacobs Oy are two of these variations. In this chapter HAZOP and SEQHAZ®, the methods mainly used by Neste Jacobs Oy for hazard studies, are presented.

2.4.1 HAZOP

The Hazard and Operability Study (HAZOP) was developed by Imperial Chemical Industries Ltd and the earliest work was published by Elliot et al. (1968). It is the most frequently used method for identifying hazards in the chemical process industry today.

The method is team work based, and it is a systematic method for identifying process abnormalities or hazards. The team typically consists of a team leader and persons with special knowledge of the process as process designers, automation/instrument designers, operating engineers, operators, maintenance engineers and safety specialists. The HAZOP needs extensive design information e.g. process description, piping and instrumentation diagrams (P&IDs) and flow sheets before the analysis can be started. The team studies deviations of process parameters for example flow, temperature and pressure under the guidance of the team leader, where the concept is to work with guidewords e.g. “no”, “more” or “less”. For each deviation, the consequences are noted and if the consequence is severe, the preparedness is checked. Sometimes a more thorough analysis is needed and one person is then appointed responsible for seeing to it that this analysis, e.g. a consequence analysis is performed. When the team determines that inadequate protection exists for a credible deviation, it usually recommends action to be taken to reduce the risk. This is done for the parameters with one guideword at a time, and the team leader decides the carefulness with which each guideword is analysed. (Salo, 2005)

This process is continued until all the process parameters have been treated. The results are filed in spreadsheets (Appendix 1). The advantages of HAZOP are offering a creative approach for identifying hazards which thoroughly evaluates the potential consequences of process upsets or failure to follow procedures. It is also systematic and provides a good understanding of the system to the members. On the other hand it is a time consuming process and requires extensive engineering documentation and

procedures. Another drawback is that it requires trained engineers from different areas, and focuses on one event causes of deviations or failures. (Laul et al, 2005)

2.4.2 SEQHAZ®

Another hazard study method used at Neste Jacobs Oy is Seqhaz Hazard Mapping, SEQHAZ® for short. The method was developed in 1995-97 by Neste Engineering (presently Neste Jacobs) in a special project that was carried out in co-operation with Neste Oil Oyj, Neste Chemicals Division and the Danish Institute for Technical Systems Analysis. SEQHAZ® is applicable to all types of industrial objects and can be modified to fit other kinds of systems as well. It serves best as a preliminary hazard analysis at conceptual or basic design, or as a coarse method for medium or low risk objects. It has also been proven well suited for high risk objects, when the goal is to achieve a broad understanding of the risks. If there is considerable operational experience available, the method also suits a detailed design analysis of high risk objects. SEQHAZ® has been in use at Neste Oil Oyj for almost ten years and has been applied with satisfactory result both to design/investments projects and for already operating objects. (Salo, 2006)

SEQHAZ® uses the good properties of What-if?, Potential Problem Analysis and Checklists. A core property is to generate What-if? questions relevant to the object. SEQHAZ® is based on three types of short "checklists: consequence classes, cause groups and (main) parts of the activity. The main part of the activity is generally divided into physical, like process stages or main equipment, and operational ones, like maintenance, start-up and shutdown. (Salo, 2006)

This method also needs a team leader, but the big difference from HAZOP that is based on teamwork, is that the hazard identification and risk estimation is carried out individually. Therefore it is important to define what concretely is meant by the consequences catastrophic, very severe and severe in the team, before the study starts. Every person can then for themselves choose an area to evaluate. And the team leader checks that there is an overlap of a minimum of two to three persons evaluating each area. This has the advantage that the time is used more efficiently and the persons can focus on the area in which they are specialists. The results are documented in special spreadsheets shown in Appendix 2. This method is substantially faster than HAZOP,

but, on the other hand, the analysis is not as detailed. The method suits low to medium risk objects well, but also high risk objects when substantial operator skill is available. (Salo, 2006)

2.5 Other hazard identification and risk estimation methods

In this chapter What if?, AEA and FMEA, which are other hazard study methods often used in the chemical industry, are presented. For practicality many methods have been left out. For a more complete review and description of the available methods see for example (CCPS, 1992), (Kemikontoret, 2001) or (Laul et al, 2005).

2.5.1 What-if analysis

What-if analysis is a brainstorming approach where a team of experienced people familiar with the process investigated ask questions about possible undesired events. It is not as structured as HAZOP and demands more experience from the analysts for a success result. The concept encourages the team to come up with questions that begin with "what-if". In this way any process safety concern can be voiced, even if it is not phased as a question. The scribe records all the questions on a chart pad. Then the questions are divided into specific areas of investigation, such as fire protection or personnel safety. The questions are formulated based on experience and the questions are applied to existing drawings and process descriptions. (CCPS, 1992)

The purpose is to identify hazards, hazardous situations or specific accidents that could produce an undesirable consequence. The experienced team identifies possible accident situations, their consequences and existing safeguards, then suggests alternatives for risk reduction on a spreadsheet as shown in Appendix 3. The analysis can be performed at any stage of the process's life cycle, using the process information and knowledge that is available at the time. The more complex the process, the more team members are recommended for the analysis. The analysis method is fast and flexible, which means that it is also cost efficient. But as it is less systematic, it is not as complete as e.g. a HAZOP. (CCPS, 1992)

2.5.2 Action error analysis

Action error analysis is a technique of identifying operating errors and was developed by J.R. Taylor in 1979. The method analyses operating procedures to discover possible

errors in carrying them out. The actions to be carried out on the process interface are listed in turn, each action being followed by its effects on the plant, so that a sequence is obtained (Lees, 2001):

Action - Effect on plant – Action – Effect on plant…

The actions are interventions in the plant such as pushing buttons, opening / closing valves etc. The effects of possible errors are then examined using guide words for action, similar to HAZOP. The main guidewords are: TOO EARLY, TOO LATE, TOO MUCH, TOO LITTLE, TOO LONG, TOO SHORT, WRONG DIRECTION ON WRONG OBJECT, WRONG ACTION. It is important to consider whether the effects of an error can be observed or not and the number of wrong actions to be considered has to be kept small. Multiple errors are considered only to a limit extent. The action error analysis has been quite widely used in the Nordic countries but much less so elsewhere. (Lees, 2001)

2.5.3 Failure Mode and Effects Analysis

The purpose of a Failure Modes and Effects Analysis (FMEA) is to identify in a table failure modes of equipment and their effects on a system or a plant. The failure descriptions then give the analysts a basis for where changes can be made to improve the system design. In the FMEA the potential consequences found are related to the equipment failure, they rarely treat damage or injury that could arise from the system functioning successfully. Each individual failure is considered as independent, with no relation to other failures in the system. FMEA is generally used as qualitative technique and the results are listed in tabular format, equipment item by equipment item. (CCPS, 1992)

The FMEA procedure contains three steps: defining the problem, performing the review, and documenting the result. First it is important to specify which items are to be included in the analysis, and under what conditions they should be analysed. Then the review is performed and a table with item, identification, description, failure modes, effect safeguards and actions are filled in item by item. A standard table shown in Appendix 5 helps the analysis to be performed systematically, which enhances the result of the analysis. An advantage is that the analysis can be performed by a single person,

but these analyses should be reviewed to ensure completeness. The resources needed for the analysis is a system or plant equipment list or P&IDs, knowledge of equipment function and failure modes and responses to equipment failures. (CCPS, 1992)

2.6 SIL evaluation methods used by Neste Jacobs Oy and its clients

In this chapter risk graph and LOPA, the techniques used for Safety Integrity Level evaluation at Neste Jacobs Oy, Neste Oil Oyj and Borealis Polymers Oy, are presented. The SIL evaluation is done in order to ensure that the safety instruments that are planned to be installed in the process work safe enough. The goal is to reduce the risk to a tolerable risk level shown in Figure 3.

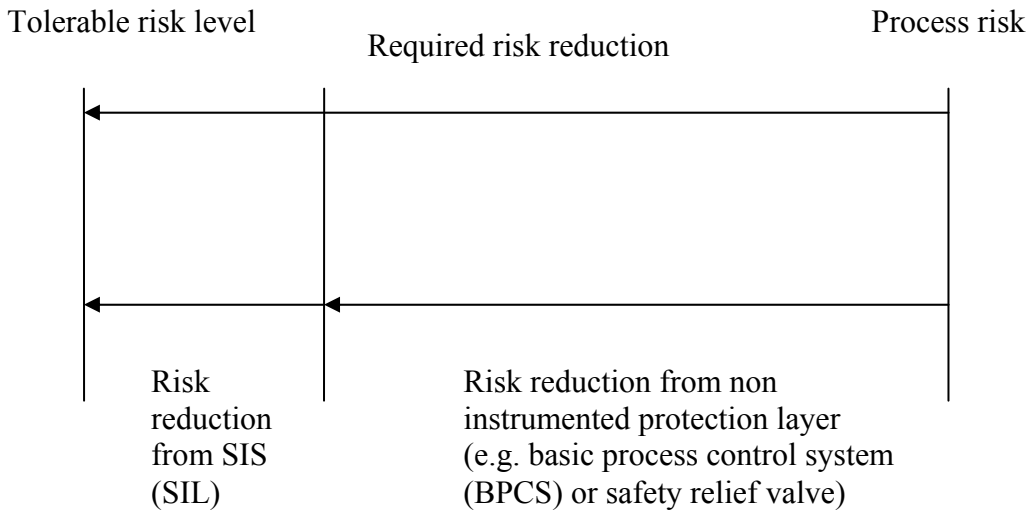

Figure 3. SIL in a risk reduction perspective.

The SIL is determined for the safety instrumented functions (SIFs) that make up the safety instrumented systems (SISs) for processes. A safety instrumented function consists of the instrumentation and functions that are necessary to detect and protect against a specific process deviation that has a potential to cause harm. This could be e.g. a level indicator controller (LIC) that opens a valve when the level is too high. A SIF is put in its context in Figure 5., which is a description of the layer of protection analysis barrier "thinking". According to Baybutt (2007) LOPA has been the dominating method for SIL evaluation in the United States while risk graph methods have achieved more popularity in Europe. The different levels of SILs are defined in Table 1.

Table 1. Definition of the different Safety Integrity Levels (IEC 61511-1, 2003)

SIL	Probability of failure on demand	Risk reduction
4	10^{-4}-10^{-5}	10 000-100 000
3	10^{-3}-10^{-4}	1 000-10 000
2	10^{-2}-10^{-3}	100-1 000
1	10^{-1}-10^{-2}	10-100

2.6.1 Risk graph

Risk graph approaches for SIL determination originates from methods described in the German standard DIN V 19250 (1994). The risk graph method used by Neste Jacobs Oy is based on the method described in International Electrotechnical Commission (IEC) standard IEC 61511-3 Appendix D (2003) and IEC 61508-5 (1998). The risk graph method in practice at Neste Jacobs Oy is a semi-qualitative model for SIL evaluation (Turkkila, 2004).

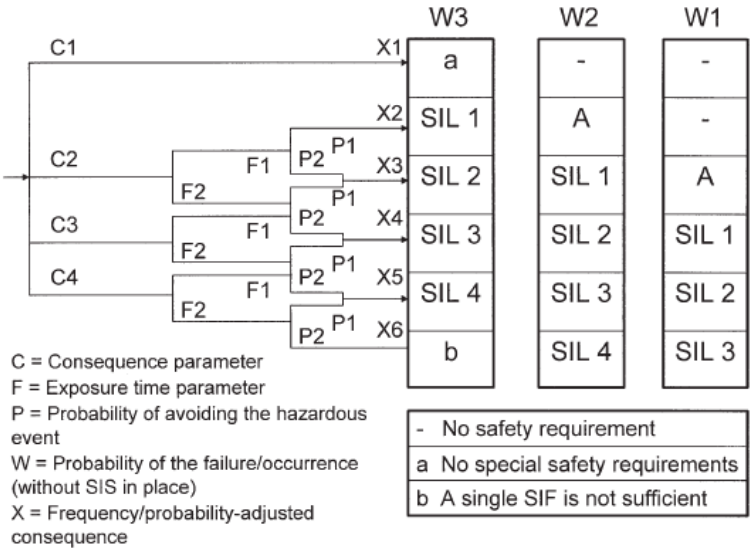

Figure 4. Risk graph method general scheme. (IEC 61511-3 Appendix D, 2003)

The risk graph method works with four parameters: consequence, C, exposure time, F, probability of avoiding the hazardous event, P and probability of the failure without SIF in place, W. They are illustrated in Figure 4. These parameters are derived from "best practice" in the chemical industry of the parameters to best describe a hazardous situation.

In this model the first step is to calibrate the risk graph. To calibrate means to make something reflect the actual situation. For risk graph the limit for the four parameters has to be set in a manner that different situation receives adequate SIL. For the consequence parameter, C, categories for what are low, medium or high consequences has to be decided. This involves setting a level for what is a tolerable risk for the company in different disciplines. At Neste Jacobs Oy the risk graph is calibrated for personal-, environmental- and economical risk. The calibration is something done by the organisational managers and it may have to be recalibrated for specific objects. The calibrations as well as further explanation of the parameters are shown in Appendix 5. A correct risk graph is very important and Neste Jacobs Oy's risk graph is calibrated close to industrial practice. (Turkkila, 2004)

The analysis is performed in a team by a group of experts almost identical to the HAZOP study. According to the IEC 61511-3 Appendix D (2003) the team should consist of: process specialists, process control engineers, operational management, safety specialists and a person with practical experience of operating the process under consideration.

When the risk graph is calibrated the analysis can start. The team first calculates the value of the consequence C as a combination of vulnerability and the number of persons present at the plant. The vulnerability V is given a different value depending on how severe the accident is. The next step is to set the value for exposure time F, which is judged as F1 or F2 depending on how often there are people present in the risk area of the object studied. If people are present in more than 10 % of the time the parameter is set to F2 otherwise F1. The next parameter to decide is P, which is based on three criteria. Only if all of them are fulfilled the value is given P1, otherwise P2. The last parameter to decide is W, the probability of the occurrence without SIF in place. This means how often for example a pressure relief valve malfunctions. These values are taken from industrial practice values and from the IEC 61511-3 (2003) standard and are categorised into three levels, W1, W2 and W3. (Turkkila, 2004)

The same risk graphs as in Figure 3 are used for estimating the environmental and economical risks except that the factor F is always set to F2, and the consequence C is then calculated according to calibration of environmental- and economical risks. The

result from this analysis is then a measure of how advanced SIF have to be installed in order to meet the tolerable criteria for safety-, environmental- or economical risks set by the company. The results ranging from “No safety requirement” to “A single SIF is not sufficient”, can be seen in Figure 3. (Turkkila, 2004)

According to Timms (2003) a proper risk graph is as good as e.g. LOPA for determining risk reduction. The risk graph also has the advantage that it can take into account both personal, environmental and economical risks separately. In an article by Kirkwood et al (2005) the strengths and weakness of risk graph are discussed. The strengths they point out is that the method is relative intuitive to plant operators without requiring detailed risk assessment training. It is also a relatively fast method of assessing SIL, which is an important factor in larger projects and it gives a conservative result which increases the confidence that the design will meet the safety requirements.

Kirkwood et al also point out the weaknesses with the risk graph method. Some users do not appreciate the detail behind the method and therefore can use it incorrectly. They continue saying that the conservativeness also is the methods weakness, as it leads to, too many SIL rated safety functions being installed, or that a higher SIL than necessary is chosen. This extra cost of installation could instead used for on obtaining a more detailed SIL evaluation, with another method. Risk graph is also poor at identifying common cause failures that exist between different protective systems or between an initiating cause and the SIF.

2.6.2 Layer of protection analysis

A qualitative risk graph approach based on IEC 61511-3 Appendix E was also being used at Borealis Polymers Oy. However, the method is slightly different from the one used at Neste Jacobs Oy because it is a more qualitative one. Borealis Polymers Oy is the affiliated company of Borealis group in Finland. The LOPA procedure is a Borealis group procedure and therefore not only applicable to Borealis Polymers Oy but in the entire Borealis group. After finding the method as being a too subjective and inconsistent way of determining SIL, Borealis group have been searching for alternatives and have three to four years ago started the implementation of layer of protection analysis (LOPA). This was done because their risk graph method gave different results for identical installations, depending on which group performed the

analysis. This resulted in situations where equipment were over or under protected and in case of overprotection. Experience revealed that it was most of the time overprotection because people tend to think conservative. Considering instrumented protection systems (SIS), it is a fact that e.g. a safety instrumented system (SIS) with SIL 2 classification is much more expensive than with a SIL 1 classification, this is an undesirable economical factor if not needed. Furthermore, more complex protection systems, despite being well designed, may cause spurious trips impacting on the operability of the plant. This is something to be avoided while using LOPA. (Aerts, 2007)

The LOPA methodology originates from the Guidelines for safe Automation of Chemical processes in 1993 where it was first presented, though under the name "the risk based SIS Integrity Level method" (CCPS, 1993). It is important to understand that LOPA is a risk assessment tool that can be applied on many different areas, one of which is SIL evaluation. The LOPA method used by Borealis Polymers Oy is an applied method which is modified from the one presented in the IEC 61511-3 standard.

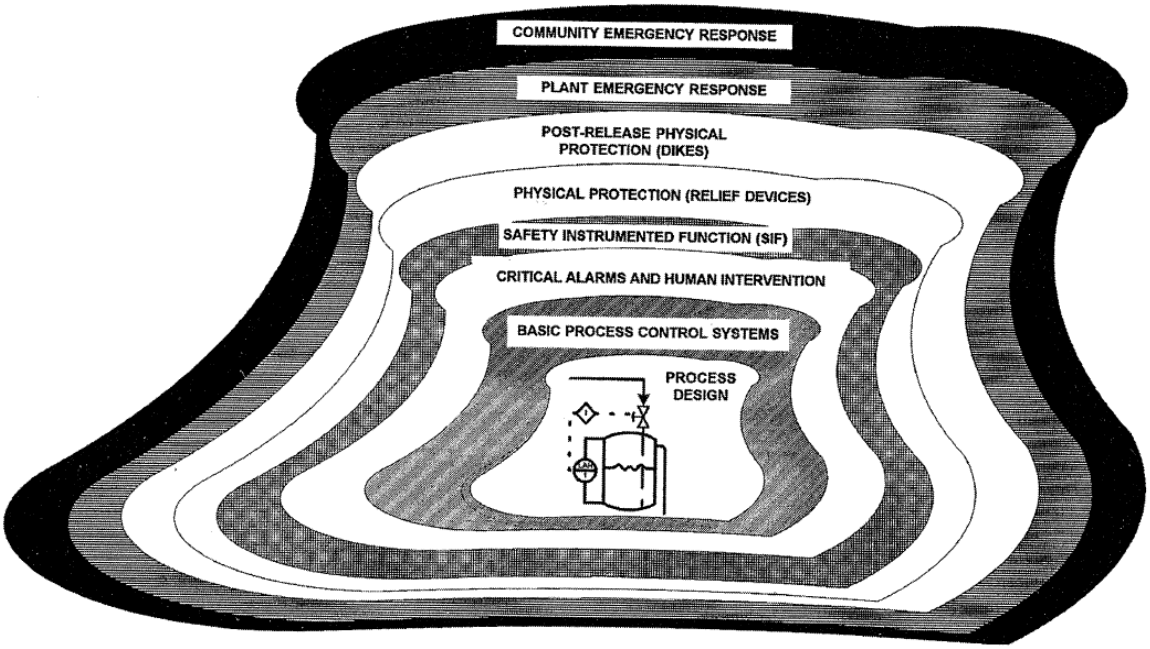

Figure 5. Layers of protection against a possible accident according to LOPA. (CCPS, 2001)

The principle of LOPA is, as the name denotes to work with protection layers as seen in Figure 5. The first step is to identify the hazards and safeguards, which is typically done with a HAZOP, What if? or a similar method. From the hazard study the most relevant

scenarios have to be selected. These are process deviations beyond the window of design, caused by either human error or equipment failure, leading to serious consequences. Borealis group's method for LOPA is based on Loss of Containment (LOC), which means that only the scenarios leading to chemicals being let out to the air, soil or sewer system are treated. The primary goal is to handle safety risks. Economical or environmental risks are not separately considered. Economical risk is covered by Reliable Centre Maintenance (RCM), which is an industrial improvement approach focused on identifying and establishing the operational, maintenance, and capital improvement policies that will manage the risks of equipment failure most effectively. In this approach failure mechanisms of each equipment and the likelihood of their occurrence are identified and as a result preventive programs are established to avoid these failures. In a way environmental risks are treated because, LOC covers almost all scenarios that will lead to environmental consequences. (Aerts, 2005) (Aerts, 2007)

The calibration for Borealis groups LOPA method, including all standard tables with category classes, initiating events, Borealis risk matrix and risk reduction values for protection layers, are all shown in Appendix 6. How LOPA works is explained further below.

First the scenario is considered without safeguards, and the initiating events are identified. The failure frequency for the initiators is then calculated if needed or standard values are used directly. The consequences are then categorised according to a table set by the company. This is a part of the calibration of the method. The frequency and consequence of the hazard give the required risk reduction from a table, which differs depending on the company’s tolerable risk level. The next step is to consider the scenario with safeguards and to identify all independent protection layers (IPLs). Independent means independent from each other and independent from the events initiator. Also here, standard values are defined for the risk reduction factor of the protection measures. (Aerts, 2007)

The risk is mitigated if the required risk reduction is higher than the sum of the risk reduction offered by the protective layers present. For example, if the consequence of the scenario in question is acceptable once every 1 000 years, the frequency of the initiating event is once every ten years, and the current IPLs in place are reducing the risk a factor ten, then this means that the event will occur once every 100 years. This is

ten times too often, according to the company's tolerable risk. This means that an additional safeguard has to be installed or the IPL in place has to be improved to reduce the frequency by a factor of ten. This could be done by installing a SIF with SIL 1, but this is not the only possibility. Also another non instrumented protection layer must be considered. The scenarios should also be documented one at a time. There are special spreadsheets in use for this, as can be seen in Table 2. (Aerts, 2007)

Table 2. Example for spreadsheet for LOPA documentation.

	1	2	3	4	5	6	7	8 Protection Layers						
	Scenario	Consequence category	Initating event	Freq-uency	Enabling event	Final initating event frequency	Required risk reduction							

There are weakness and advantages with LOPA, as with every other method. One advantage is that it puts the focus of risk reduction effort to impact events with high severity and high likelihood. It ensures that all the identified initiating causes are considered and it confirms which IPLs are effective for each initiating cause. It also gives the possibility to allocate the resources where they are needed mostly. LOPA gives clarity in the reasoning process and it documents everything that was considered. While this method uses numbers, judgement and experience are not excluded. In some cases the team's "gut feeling" was uncomfortable with the SIL number calculated, and the team went back and reviewed the assumptions for the frequency of the initiating event and came to another solution. (Dowell, 1998)

According to Aerts (2008) one big advantage with LOPA in comparison with their old risk graph based method is the evaluation of the independency of all the protection layers. He also points out that the reliability of protective measures is more thoroughly evaluated, such as for overprotection/insufficient protection, while earlier it was taken for granted that a pressure relief valve gave adequate protection for overpressure in all kinds of service.

LOPA also helps to resolve conflicts in decision making by providing a consistent, simplified framework for estimating risks of a scenario. It provides a better risk decision

basis compared to subjective or emotional arguments such as “the risk is tolerable to me”. (CCPS, 2001)

Other benefits compared with other SIL assignment methods have been identified by Summers (2003). Due to the scenario-related focus LOPA often reveals process safety issues that were not identified in previous qualitative hazard analysis. It also often identifies acceptable alternatives to the SIS, such as adding other layers of protection, modifying the process, or changing procedures. This gives the team a possibility to evaluate options using cost/benefit analysis, which allows the most cost effective means of risk reduction to be used.

On the other hand LOPA is just another risk analysis tool and has to be applied correctly. LOPA is a simplified approach and should not be applied on every scenario. It is not intended to be a hazard identification tool. The numbers generated from a LOPA analysis are not precise risk values for a scenario, which is a limitation in every quantitative risk analysis method. Differences in risk tolerance criteria and in LOPA implementation between organisations means that the result cannot normally be compared directly from one organisation to another. (CCPS, 2001)

2.7 Other SIL evaluation methods

There are also other SIL evaluation methods available besides risk graph and LOPA and in this chapter a review of the most common methods mentioned in the literature (Summers, 1998) (Marszal et al, 1999) (Kirkwood et al, 2005) (Jin et al, 2003) (Weibull, 2004) are presented. These are Consequence only, Risk matrix, Modified HAZOP, Fault tree analysis and Corporate Mandate SIL.

2.7.1 Consequence only

This is the most conservative technique and uses an estimation of the potential consequence of the incident to evaluate SIL. The frequency of the incident which is the most difficult to decide is not considered. This method is the simplest one available to evaluate SIL and is appropriate when very little historical information is available. A decision table is shown in Table 3. (Summers, 1998)

Table 3. Consequence only decision table. (Summers, 1998)

SIL	Generalized view
4	Potential for fatalities in the community
3	Potential for multiple fatalities
2	Potential for major serious injuries or one fatality
1	Potential for minor injuries

2.7.2 Risk matrix

In this method both consequence and probability of the incident or initiating event are considered. During the assessment of the incident, severity and likelihood must be determined. For risk reduction consideration the layers of protection must be independent, verifiable, and dependable. An example of a two dimensional risk matrix is shown in Figure 6. For this method to be successfully used, the process and its associated risks must be well understood, so that qualitative estimation of the likelihood and severity can be performed. (Summers, 1998)

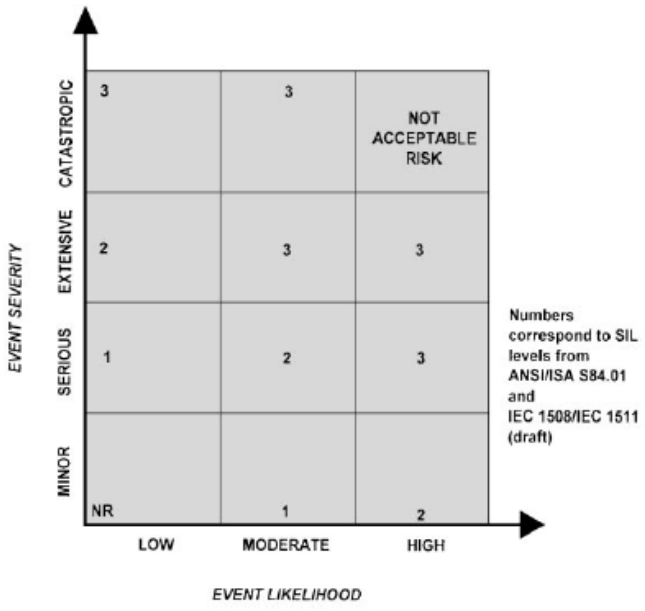

Figure 6. Two dimensional risk matrix. (Summers, 1998)

2.7.3 Modified HAZOP

The Modified HAZOP is an extension of the normal HAZOP analysis. It is based on a subjective SIL assignment of the team's qualitative understanding of the incident severity and likelihood. This method relies mostly on the experience and knowledge of

the team members, which requires extensive experience for the method to be successful. The SIL is assigned by the team's qualitative estimation of the risk. Because the method is so subjective it requires consistency between the personnel of the SIL assignment teams from project to project. (Summers, 1998)

2.7.4 Fault tree analysis

Fault tree analysis or FTA is the most common quantitative technique for detailed SIL evaluation. It can be described as a detailed mathematical analysis where diagram representation of risk and mitigating factors are used. FTA can be applied to nearly all aspects of reliability risk analysis. It allows a more advanced human factor to be included in the analysis and can model complex interactions. A drawback is that the analysis is more time consuming and costly than risk graph and LOPA but many practitioners consider that higher SIL rated functions should automatically be subjected to a detailed quantitative analysis. (Kirkwood et al, 2005)

2.7.5 Corporate mandate SIL

This is the fastest method and is adopted too small chemical plants that do not have resources to perform more advanced SIL evaluations. The approach is straightforward and works by stating "a safety system is a safety system and should therefore be SIL 3". (Summers, 1998)

3 Standards and other important requirements

There are several particular important requirements that affect the hazard study process. Laws and regulations demand that hazard studies be performed. In the last years standards have also got an increasing role in benchmarking, especially IEC 61508 (1998), which is a general standard for functional safety for safety related systems, and IEC 61511 (2003), the specific standard for the process industry sector in the same area. Another important criterion is to define a tolerable risk level, which is something left to the industry as at this moment no laws exist that define an acceptable level of risk. In this chapter laws and regulations concerning handling and storage of dangerous chemicals, important standards and tolerable risk criteria will be discussed.

3.1 Laws and regulations concerning dangerous chemicals

There are many laws and regulations in Finland that regulate the use and storage of dangerous chemicals. In Finland a major part of the SEVESO II Directive (96/82/EC) was transposed into the Decree on the Industrial Handling and Storage of Dangerous Chemicals, (59/1999 and its amendments) as well as the Act on the Safety of the Handling of Dangerous Chemicals and Explosives (390/2005). In addition, there are special legislation for e.g. liquefied petroleum gas (LPG), natural gas and explosives. (TUKES, 2006) (TUKES, 2007a)

A competent authority in safety technology in Finland is the Safety Technology Authority (TUKES). According to TUKES the aim of the operation is to maintain and promote the technical safety culture and reliability in order to protect people, property and the environment. The tasks are divided into surveillance of the products on the market and into the supervision of in-service plants, installations and technical services. (TUKES, 2007b)

TUKES also publishes e.g. guidelines in which regulations are interpreted. These clarify the meaning of the law and what minimum safety is required from the authorities.

Act (390/2005) and Decree (59/1999) enforce that the hazards that could lead to major accidents are identified. For the petrochemical industry companies in Finland this is

done with different methods depending on which stage (research, basic design etc.) the planning process is in.

An important directive for the European community concerning chemical process industry is the Pressure Equipment Directive (97/23/EC) that was adopted by the European Parliament and the European Council in May 1997. From 29 May 2002 the pressure equipment directive has been obligatory throughout the European Union. The directive refers to the Harmonised (European) Standards called EN standards that are obligatory to follow. One of these is EN 764-7 (Safety systems for unfired pressure equipments) which states that " A safety related measuring, control and regulation system shall be designed using the principles in IEC 61508." (EN 764-7, 2002). This is, so to speak, the standard of manufacturing. IEC 61508 in turn refers to IEC 61511 which is the user specific standard for the process sector industry which will be explained further in the next chapter. This means that the Pressure Equipment Directive is the law in the European Union where the authorities demand to perform SIL evaluations.

3.2 Standards IEC61508 and IEC61511

There are two standards that have a major impact on the SIL evaluation process. These are IEC 61508 (1999) *Functional safety of electronical/electronic/programmable electronic (E/E/PE) safety related systems* and IEC 61508 (2003) *Functional safety – Safety instrumented systems for the process industry sector*. IEC 61508 (2003) is a general standard for all E/E/PE which is defined in the standard as all components based on electrical and/or electronic and/or programmable electronic technology. The standard is applicable on a wide area. As this standard is if a more general nature this led to more specialised standards being established. The IEC 61511 for the process industry sector of 2003 is one of them. The IEC 61511 is the most important standard for Neste Jacobs Oy concerning the SIL evaluation process and will be discussed further below. The relationship between the two standards is illustrated in Figure 7.

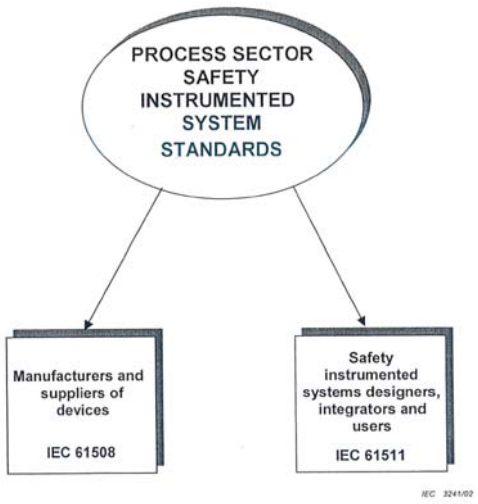

Figure 7. Relationship between IEC 61511 and IEC 61508.

The IEC 61511 standard also works out a framework which is applicable to all methods using safety instrumented systems of achieving functional safety. Two concepts "safety lifecycle" and "safety integrity level" are fundamental for the application. "Safety lifecycle" means that all stages from research, design, implementation, use and maintenance to decommission of the safety instrumented system (SIS) are embraced by the standard. Using a safety integrity level is a way to specify the safety integrity requirements of the safety instrumented functions that build up the SIS. The standard requires that a hazard study is performed to identify the overall safety requirements. (IEC 61511-1, 2003). Weibull (2004) states that the standard does not set any requirements on how the hazard study is performed but one has to be done in order to live up to the standard. This means that the companies are free to use the method they find most convenient.

The next step is to evaluate which safety integrity level is needed for the SIF, this is called SIL evaluation. The SIL evaluation is based on the results from the previous hazard study. The standard gives a guideline of five methods to use. Among theses are the risk graph method used at Neste Jacobs Oy and a LOPA method similar to the one used at Borealis Polymers Oy. There exists four SIL levels (SIL 1-SIL 4) and levels higher than SIL 4 are not recommended by the standard. Then it is recommended to go back and see if it is possible to change something in the design of the process. (IEC 61511-1,3) However in practice SIL levels of three or more occur very seldom during a SIL evaluation. If they occur, other options for risk reduction are considered as only

relying on a safety instrument function for so high critical failures is against the gut feeling. (Turkkila, 2007)

The purpose of both IEC 61508 and 61511 standards are to give the industry and others a common language for functional safety for safety instrumented systems. But also to be able to state what "good engineering practice" is when it comes to safety instrumented systems. (IEC 61511-1, 2003) IEC 61511 also defines the tolerable risk which will be discussed further in the next section.

According to Weibull (2004) the advantages employing standards are that users of components and systems can verify that the products have enough availability. Availability is defined as "The probability that a device is operating successfully at a given moment in time." (Exida, 2006). The instrumented functions can be designed for the availability needed in the specific case, so that the most effort can be put where it is mostly needed. The risk for devastating systematic failures in SIF should also decrease. Weibull also believes that the standard keeps things in order.

Weibull continues with the disadvantages of using the standards and points out that the standards requirements might lead to unnecessary bureaucracy and eventually more expensive components. It also demands investments from the companies to develop methods and educate personnel to live up to the standards. In addition the eventual return in form of easier instrument functions and higher safety are partly being eaten up lost by costs for risk evaluation, documentation and tailored design.

Timms (2003) concludes that IEC 61508 provides an opportunity to meet industry best practice while saving significant costs. An essential part is to use software tools if application of the standard is to be implemented efficiently. Finally in Timms opinion the tools should have database controls which can be audited for full life cycle management of safety instrumented systems.

3.3 Tolerable risk

Defining tolerable risk is an essential part of the hazard study process. A tolerable risk level can either be based on philosophical or political grounds. Setting a tolerable risk

level involves regarding moral, legal and financial aspects as shown in Figure 8. (Marszal, 2001)

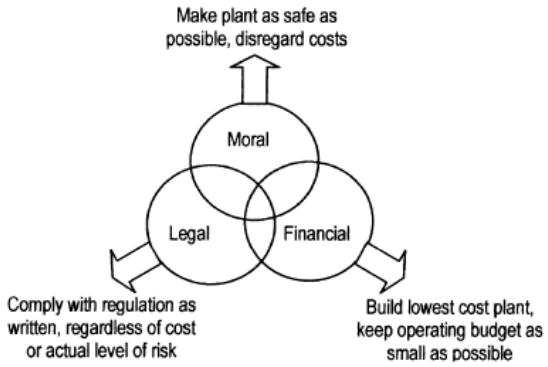

Figure 8. The risk tolerance level is set regarding moral, legal and financial criterion.

This is very complex since human beings have demonstrated themselves to be very poor judges of risk, particularly in cases where the consequence is severe and probability low. Therefore it is found to be more effective to determine what tolerable risk is by using revealed values. This means analysing the types of risks that are currently tolerated and then quantifying the actual risk posed by those threats. (Marszal, 2001)

The philosophy most often used in industry are: "maximize the excepted utility of your investments, but do not expose anyone whether your workers or neighbours to an excessive increase in risk". Both the European Seveso II directive (1996) and IEC 61511 (2003) requires all hazards to be identified and risks to be reduced in line with the ALARP principles. The ALARP principle that is often used for determining tolerable risk means that the risk recommends to be reduced to "as low as reasonable practical" (ALARP). The principle states that there is a level of risk that is intolerable. Above this level risk can not be justified on any grounds. The ALARP principle is illustrated in Figure 9. Below the intolerable region is the ALARP region, here risks are only tolerable if risk reduction is impracticable or if its cost is grossly disproportionate to the benefit of the risk reduction gained. Below the ALARP region is the "broadly acceptable" region. In this region there is no need for detailed work to demonstrate ALARP because the risk is negligible. In addition, risk is so low that it is unlikely that any risk reduction will be cost effective, so analysis of costs of risk reduction is typically not undertaken. (Marszal, 2001)

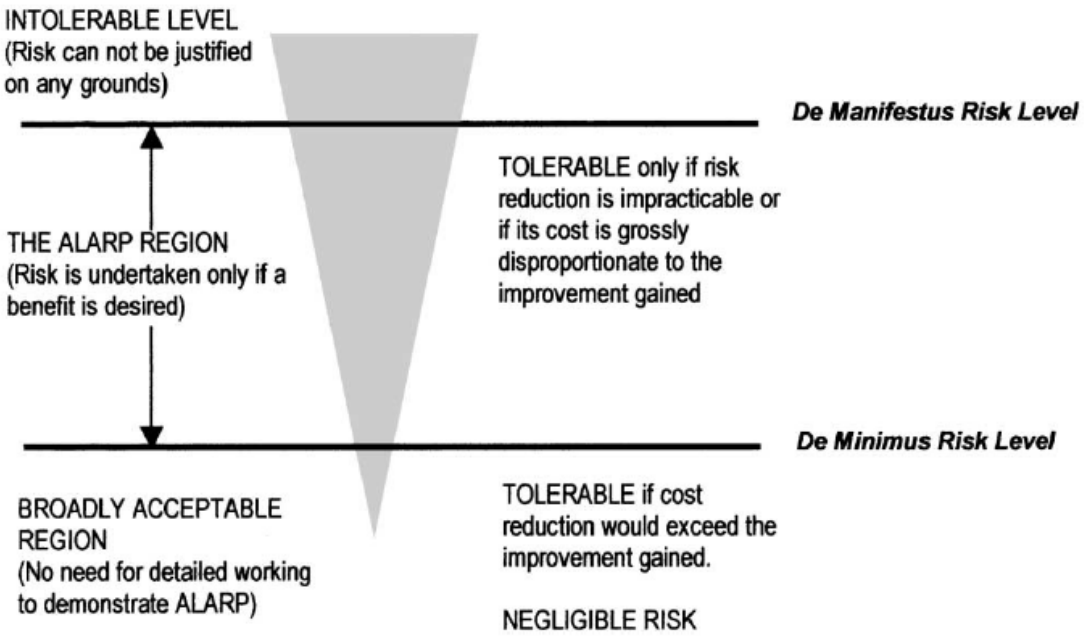

Figure 9. Tolerable risk according to the ALARP principle. (Marszal, 2001)

The word reasonable in ALARP has been interpreted by the loss prevention community to mean cost-effective which means that the principle requires cost-benefit analysis to determine which projects should be funded in the ALARP region. (Marszal, 2001)

To set the tolerable risk level is an important part of the SIL evaluation process, and the connection is illustrated in Figure 10. The process risk is first in the unacceptable region without any risk mitigation. Non SIS protection layers reduces the likelihood of the risk to the ALARP region but this is not enough. The consequence is also reduced with non SIS protection layers e.g. containment dikes. In the last step the likelihood of the risk is reduced with SIS to the acceptable risk region.

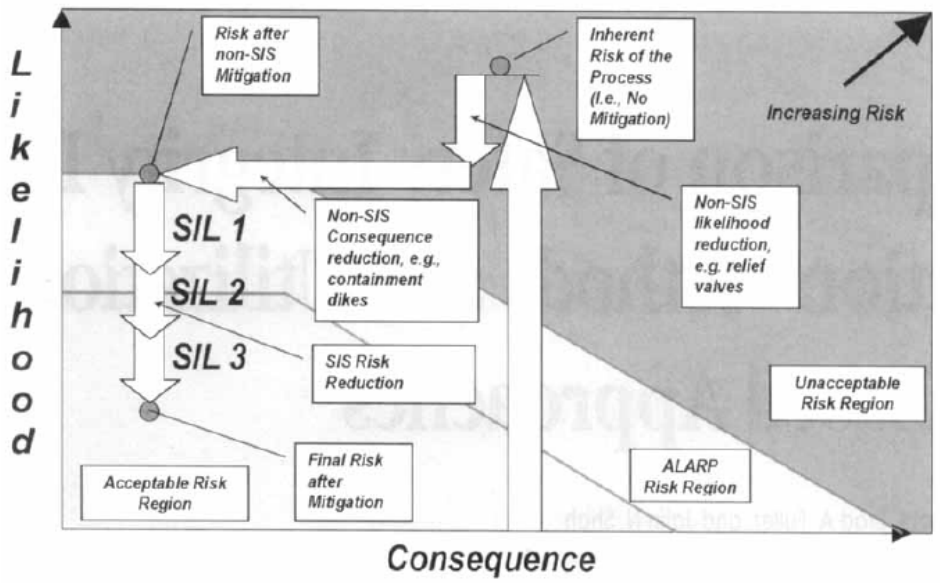

Figure 10. SIL and tolerable risk according to ALARP.

Marszal (2001) suggests cost benefit analysis to be built into the SIL evaluation process, especially for refineries where property damage losses dominates. But a plants tolerable risk level should also be in the same general range as what other operators in the same industry are using. On the other hand, White (2000), suggests the SIL level to be set on basis of only safety criteria. He believes that by preventing explosions, fires and overflows, the most major environmental incidents are also prevented. White also suggests that protection from economic loss should be provided either by the basic process control system (BPCS) or a separate system and that safety should be kept separated from other requirements.

4 Field study

4.1 Method and purpose of the field study

The purpose of the field study was to get a deeper understanding of the hazard study processes at Neste Jacobs, and to document the key elements of the hazard study processes. The information obtained will then be used as a base for the model development along with the information from the literature study. The field study was performed in three stages. Firstly HAZOP-, SEQHAZ®-, the risk graph- and LOPA reports were studied. Secondly participation in real hazard studies was undertalem, and thirdly 23 persons with experience of using the methods were interviewed. For the last part of the field study a seminar day was arranged where the interviewees was invited along with the steering group for the masters thesis. During which small sessions of LOPA and risk graph was performed and the methods where evaluated, compared and discussed. The results from the field study are presented in chapter 5.

4.2 Studying of hazard reports

The reports that have been studied are four HAZOP reports and one SEQHAZ® report obtained from Neste Jacobs Oy. The following SIL evaluation reports with the risk graph method based on the former HAZOP- or SEQHAZ® reports have also been studied. Finally, one LOPA report received from Borealis Polymers Oy was studied.

4.3 Participation in real hazard studies

The idea of this part of the thesis was to observe and see how the hazard studies are performed in practice and from these observations obtain ideas for optimising the hazard study process.

The first hazard study was performed on 24 of October 2007 from 9.00 to 12.30 and was a layer of protection analysis for determining safety integrity level. The study object was an existing polypropylene polymerisation process at Borealis Polymers Oy where changes had been made of the existing process. The purpose of the analysis was to see how these changes affected the SIS presently installed. Four scenarios were analysed and a SIL evaluation report from 2004 of the entire plant was used as base for the scenarios.

The next study that was made on 1 of November 2007 from 9.00 to 10.00 and was a "step 1" hazard study at Borealis Polymers Oy. "Step 1" is the first hazard study out of six in a life cycle procedure for a chemical plant. Which was introduced by the Imperial Chemical Industries. Depending on the project, which hazard studies (Step 1-6) that needs to be performed can change. The study object was an installation of a static mixer in a polypropylene process. The purpose of the analysis was to see which effect the installation of the static mixer had on the safety and environment. In this hazard study the level of danger of the chemicals was checked, basic screening of what effect the changes had and whether further analyses have to be done. Since no new chemicals were introduced and the safety effects were considered small the analysis went very fast.

The third hazard study was a "what if?" analysis in a Neste Oil Oyj project, the session I took part in was done on 2 of November 2007 from 8.30 to 11.30. What if? is a more general hazard study method that can be performed on basically every subject. Animal fat is one of the raw materials used for manufacturing bio diesel. The purpose of the hazard study was to find out which effect the use of animal fat and its logistics have on the bio diesel process chain. The main issues were how to keep the animal fat from being contaminated and what to do if the animal fat gets contaminated with e.g. BSE or salmonella. This was not a normal hazard study as the risks presented were totally new for the group and not only limited to treating process technical risks.

The fourth hazard study was a HAZOP done at Borealis Polymers Oy. The session was done 8 November 2007 from 9.00 to 12.40. The object of study was a phenol process where the sulphuric acid tank had been moved and the cleavage technology was new. The purpose of the HAZOP study was to evaluate if these changes added any new risks to the process. The old HAZOP report from the entire plant was used as base and the parts that were affected by the change, or that were entirely new were treated in this HAZOP session.

The fifth and last hazard study was a SEQHAZ® study of Neste Oil Oyj's loading terminal for Kilpilahti's chemical industry area. This included the loading of trains and trucks. The author participated in two sessions. The first session was on 27 of November from 9.00 to 12.00, where the method was explained and the risks were

identified The participants identified individually hazardous situations. For this the sheet illustrated in Appendix 2 was used. The second session took place on 28 of November from 12.30 to 15.30 where the proposals for action based on the identified risks were discussed.

4.4 Interviews

In total 23 interviews were done during about four weeks from 6 of November 2007 to the 3 of December 2007. A list of the people that were interviewed can be seen on Table 4.-7. People with experience of the main four methods which are considered in this thesis HAZOP, SEQHAZ®, risk graph and LOPA were interviewed. The interview questions which are shown in Appendix 7 and 8 were sent out beforehand along with an interview formula which is shown in Appendix 6. This was done in order for the interviewed to be able to prepare him or herself for the questions and to understand which type of questions that they should expect. In a few cases the interviewees answered the questions briefly beforehand by email and then during the interview the answers were discussed. Only questions regarding the method the interviewee had experience of were asked. For example, if someone had experience of using HAZOP and SEQHAZ® only questions regarding these two methods were asked. The aim was to perform the interviews face to face but in three cases telephone interviews were the only possibility due to practical reasons.

Table 4. Team leaders.

Names	**Company**	**Profession**	**Experience of methods**
Hanna Honkanen 1	Neste Jacobs Oy	Process designer	HAZOP / SEQHAZ® / Risk graph / LOPA
Kai Ingman 1	Neste Jacobs Oy	Project Manager	SEQHAZ®
Kimmo Virolainen	VTT	Senior hazard study specialist	HAZOP / Risk graph
Yngve Malmén 1	VTT	Senior Research Engineer	HAZOP
Seppo Koskinen	Inherent Engineering Oy	Process safety specialist	HAZOP / SEQHAZ®
Jukka Korvenoja	SWECO PIC	Process Consultant	HAZOP / SEQHAZ®
Tuomas Viskari	ÅF Enprima Oy	Process Consultant	Risk graph
Kari Matilainen	Borealis Polymers Oy	Process safety specialist	Risk graph /LOPA

Brian Tibbs	Brian Tibbs Unlimited	Process safety specialist	Risk graph / LOPA
Sami Matinaho	Systecon Oy	Automation Engineer	HAZOP / Risk graph / LOPA
Anders Jacobsson	AJ Risk Engineering AB	Safety specialist	HAZOP / Risk graph

Table 5. Scribes.

Names	**Company**	**Profession**	**Experience of methods**
Leena Hannonen	SWECO PIC Oy	Process consultant	HAZOP / SEQHAZ®
Yngve Malmén 2	VTT	Senior Research Engineer	HAZOP
Kai Ingman 2	Neste Jacobs Oy	Project Manager	SEQHAZ®

Table 6. Operational engineers and operators.

Names	**Company**	**Profession**	**Experience of methods**
Olavi Haapalehto	Neste Oil Oyj	Instrumentation Supervisor	SEQHAZ® / HAZOP / Risk graph
Emmi Laiho	Neste Oil Oyj	Process Control Engineer	HAZOP / SEQHAZ® / Risk graph
Sari Laanti	Neste Oil Oyj	Operational engineer	HAZOP
Jari Lyytinen	Neste Oil Oyj	Project technician	HAZOP / SEQHAZ®
Johannes Maaskant	Neste Oil Oyj	Development Manager	HAZOP / SEQHAZ® / Risk graph
Asko Heikkinen	Borealis Polymers Oy	Operator	HAZOP
Marjut Aho	Neste Oil Oyj	Process Control Engineer	HAZOP / SEQHAZ® / Risk graph

Table 7. Process designers and automation specialists.

Names	**Company**	**Profession**	**Experience of methods**
Hanna Honkanen 2	Neste Jacobs Oy	Process designer	HAZOP / SEQHAZ® / Risk graph/ LOPA
Irmeli Vauhkonen	Neste Jacobs Oy	Process designer	HAZOP
Erkki Turkkila	Neste Jacobs Oy	Automation Specialist	Risk graph / LOPA / HAZOP/ SEQHAZ®
Timo Bergström	Neste Jacobs Oy	Automation Specialist	Risk graph / HAZOP / SEQHAZ®
Tapio Kokko	Borealis Polymers Oy	Senior staff Engineer	HAZOP / Risk graph / LOPA

4.5 Seminar day

The seminar day was arranged for 10 of December from 9.00 to 16.00 at Haikko conference centre in Porvoo, Finland. Preparations for the seminar were done by the author and material from Neste Jacobs Oy and Borealis Polymers Oy was used to perform one risk graph and one LOPA session. The interviewees and the steering group were invited to the seminar. Those who participated at the seminar were:
Daniel Björkhem, Erkki Turkkila, Anders Jacobsson, Rainer Salo, Marjut Aho, Emmi Laiho, Timo Bergström, Lena Hannonen, Kai Ingman, Rune Strahl and Irmeli Vauhkonen. The purpose of the seminar was to get more familiar with the risk graph and LOPA, to identify their strengths and weaknesses and to discuss the key problems with the present hazard study processes.

5 Results

The results from the interviews are presented in chapter 5.1 and a summary of the results from the seminar day in chapter 5.2.

5.1 Interviews

In this chapter the results of the 23 interviews are presented An interview formula was used for the respondents to get basic information about their background, the formula is shown in Appendix 7. The results are based on the questions shown in Appendix 8 and 9 and are divided into seven different chapters categorised almost in the same way as the questions for the interviews.

5.1.1 HAZOP

The majority of the interviewees perceived HAZOP as both easy to use and to understand. This is due to its systematic and that it repeats itself with the same pattern. The systematic manner of identifying risks was also the advantage that most interviewees identified. The problem with HAZOP that was pointed out by all those interviewed was that it was time demanding and that the sessions are long. Whether the result of the study was considered good enough depended on the group's knowledge of the studied process. The team leader had a major responsibility to make sure that the right questions were asked in order to obtain a useful result.

HAZOP was seen as the best method for systematically identifying risks that are available for the process industry today. Many suggestions for making the method better were given. The main suggestions proposed were: To let the key participators in the study focus on the task and not be interrupted by other work. To analyse human error and special cases in a more systematic manner than presently done. Further the timing of the study was considered important; the PI&Ds should be progressed far enough so it does not become a design meeting. The importance of time managment is planned for was also a usual answer for making the HAZOP more efficient.

According to the interviewees the information needed from HAZOP when performing SIL evaluations was the hazards description and consequence. Many stated that it would

be helpful if the consequence could be ranked already in the HAZOP. It was also proposed that the ranking is demonstrated in a manner that it is useful for the SIL evaluation team. It was also pointed out by a majority that the risk ranking should be a rough one since it brings extra work to the already laborious HAZOP. It was also suggested that the likelihood should be ranked, however others felt that this was a task for the SIL evaluation team.

Most of the interviewees thought that the HAZOP should indicate what should be treated in the SIL evaluation. One proposed approach was to add an extra column "case for SIL evaluation" and if it is the case you mark it with an "X".

Whether it is possible to make a summary of the safety instrumented function needed for the process section, after a section has been analysed in HAZOP was a difficult question to answer. Some thought it is possible but only if the HAZOP is done properly.

5.1.2 SEQHAZ®

SEQHAZ® is considered easy to use and understand by those interviewed, but they stated that it demands more instructions than HAZOP, because identifying of risks is performed alone. The first advantage that was identified by all the interviewees is that SEQHAZ® is a faster method than HAZOP. Other identified advantages were that it was flexible and can easily be applied on basically, any study object. It was found to be a good alternative when a heavy risk analysis like HAZOP is not needed.

One of the problems with the method identified by the interviewees was that the same risks were often identified by different people. Several thought that the thoughts easily started to wander away from the problem at hand when you were identifying the risks on your own. Thereby irrelevant risks were identified.

It must be pointed out that the opinions about SEQHAZ® were mixed. One group was very positive while another was very negative towards the method. Therefore some thought SEQHAZ® led to a reasonable result, if the group and team leader were experienced. Some always preferred HAZOP. This depended on the majority who had the opinion that SEQHAZ® did not gave the same completeness of the result as HAZOP because of the less systematic approach.

It was difficult for the inerviewee to find improvements for SEQHAZ® but suggestions were done to synchronise the risk ranking made in SEQHAZ® with the one for the risk graph and also for HAZOP if the risks should be ranked there.

The information that is needed from SEQHAZ® when performing safety integrity level evaluations are the same as is needed for HAZOP. In SEQHAZ® the risks are already ranked in consequence and likelihood, which according to the interviewee helped the selection of relevant scenarios to be evaluated in the SIL evaluation. The interviewees did not feel it was possible to make a summary of the safety instrumented function needed for the process section, after a section has been analysed in SEQHAZ®.

5.1.3 Comparison between HAZOP and SEQHAZ®

During the interviews comparisons between HAZOP and SEQHAZ® were made. The opinions differ on whether the person interviewed was a team leader, a scribe or had another task, also the level of experience with regard using the methods played an important role for their opinions.

The main differences pointed out by the interviewees are that SEQHAZ® is faster than HAZOP, but also less systematic and thorough. But like many of the interviewee indicated, the methods are not intended to compete with one another but rather to complete each other. According to the interviewees different methods should be used for different types of projects. For hazard studies on totally new plants where little practical experience is at hand. HAZOP was suggested as the best method to be employed. SEQHAZ® was found to be best suited for updating old HAZOP reports or on a study object that is not a process technical one.

5.1.4 Risk graph

Of the persons interviewed the majority had practical experience of using the risk graph, while only several had experience of using LOPA. This may have the effect that more problems with risk graph were identified than with LOPA since the practical experience with risk graph is and longer and more extensive.

According to the interviewees the risk graph requires background information to understand the method. A majority of the interviewees found the risk graph methods template which has four parameters as one of the major advantages, as it is straightforward and easy to understand. Also the fact the three different graphs treating personnel, environmental and economical risks separately were found to be a major advantage by the interviewees.

A typical problem identified by several of the interviewees is that the calibration of the risk graphs does not fit for every occasion. Several of the interviewees also pointed out that the risk graph only takes into account the mechanical protection to a limited extent. The limits of the parameters were also pointed out as a problem by many of the interviewees when selecting e.g. if parameter F should be F1or F2. According to some of the interviewees when evaluating a SIF in the risk graph, it sometimes leads to going back and manipulate the parameters in order get a reasonable SIL for the SIF. Another disadvantage pointed out by several of the interviewees is that risk graph is a crude method for assigning SIL. It was also pointed out by the asked that the possible scale for acceptable SIL for the SIF is very limited only SIL 0, SIL 1 and SIL 2 is accepted. Although the majority of the interviewees stated that if the group have experience of using the risk graph it leads to a reasonable result. The interviewees also pointed out that a group without experience will get a higher SIL than an experienced one. According to the interviewees the result of the risk graph gives more a conservative SIL than an underrating one.

Many suggestions were proposed for improving risk graph during the interviews. One was that the calibration should be tighter in order to allow for faster decision-making, including that the limits for the parameters being set more clearly so that unnecessary discussions can be avoided. Another idea was to try to set fixed parameters for some typical process units. Furthermore one proposal was to change the Word template to an Excel one since it is easier to obtain overview in Excel and large quantities of data is better stored there.

5.1.5 LOPA

LOPA was considered easy to understand by the interviewees because of its logical methodology however, it required background training to understand the LOPA and

LOC concepts. The advantages with LOPA pointed out by the interviewees were that the method is systematic and flexible in the way that basically any type of protection layer can be included in the method. Other advantages noted by the interviewees were that the method is consistent and precise because of the use of ready tables for assigning initiating events, consequences, protection layers and risk reduction values. One of the interviewees also pointed out that LOPA was the beginning of a quantitative risk assessment and if the risks are too high it is easy to see where to start with the risk reduction.

A problem with the method identified by one of the interviewees occurs when a SIF for a compressor or an extruder are to be analysed with LOPA. Some of these SIFs risks are safety related but the main risks were economical. Economical consequences are not embraced by the current methodology used in the Borealis LOPA with the LOC approach. The majority of the interviewees have the opinion that LOPA leads to a reasonable result.

A few suggestions for improvements of LOPA were suggested by the asked. Some of the interviewees wanted that economical risk also should be included, while some did not. A suggestion was given to add a so called "Loss of money" which already has been tried with success in a few projects.

5.1.6 Comparison between risk graph and LOPA

Some of the interviewees had experience of using both the risk graph and LOPA, which made it possible to compare both methods. But it should be noted that the practical experience of LOPA was often shorter and less extensive, which may affect the comparison.

The strengths of the risk graph identified by the interviewees were that the template was easy to understand and that you obtain three different graphs for personnel, environmental and economical risk. This is different in LOPA where you only get one SIL for personnel risk and this was percieved as a weakness compared to risk graph by some of the asked. LOPA is regarded by the interviewees as more systematic than the risk graph and it is seen as positive that the calibration is further driven. This leads to a more consistent result, according to the interviewees. However a danger identified by

the interviewees is that far driven calibration leaves little space for discussion qualitative aspects, which is not always good. LOPA is better than the risk graph according to some of the interviewees since it is more flexible in the sense that any type of protection layer can be included in the SIL evaluation, also something unusual. In this aspect risk graph is less flexible. According to some of the interviewees LOPA is also a more popular method and the direction towards more and more users are moving when it comes to SIL evaluation. On the other hand as pointed out by the interviewees the risk graph has been in use for a longer time and is more widespread which also has advantages.

According to the asked only one method should be used for SIL evaluation, it is not meaningful to use different methods for different cases, this only makes the SIL evaluation more complicated.

5.1.7 General questions for hazard study processes

A majority of the asked have the opinion that HAZOP should state what should be treated in the SIL evaluation. Most think this should be done by risk ranking. How this ranking should be employed differs among the interviewees. Some think that both consequence and likelihood should be ranked, while others believe that consequence is enough.

If old HAZOP/SEQHAZ® reports are used when updating the hazard study, it is suggested by the interviewees that the new HAZOP/SEQHAZ® should first be made without looking at the old report. Otherwise according to the interviewees, the old report would steer the team too much. It was also pointed out that the quality of the old report and the scope is also important when deciding if it is useful or not.

The interviewees stated that the connection between the HAZOP/SEQHAZ® study and the SIL evaluation was the identified risk and its consequences. The interviewees explained that first of all the "instrumentation description" list should be used, in order to determine which SIFs should be analysed in the SIL evaluation. From this list all functions are analysed in the SIL evaluation. But to get the scenarios for what happens when the SIF malfunction the HAZOP/SEQHAZ® report is needed, and in addition in these reports more SIFs relevant for the SIL evaluation are identified.

Where the most unclear point in relation to the HAZOP/SEQHAZ® - SIL evaluation chain lie, appeared to be a difficult question to answer among the interviewees. However, most of the interviewees stated that the pass on of information from the previous HAZOP/SEQHAZ® to the SIL evaluation was a the major problem. The interviewees also thought that there should be a better system for filtering which scenarios are relevant for SIL evaluation. Finally, according to all the interviewees they felt that at sometime, stress and tiredness had affected the result of the hazard study or SIL evaluation.

5.2 Seminar day

Many subjects where discussed during the seminar day 10th of December at Haikko conference centre in Porvoo, Finland, this is a summary of the most important issues.

First the HAZOP study and its report were discussed. The key question was what information is required to determine which scenarios from a HAZOP that needs to be treated in the SIL evaluation. To determine relevant scenarios for the SIL evaluation the quality of the documentation in the HAZOP or SEQHAZ® was found to be of great importance. The safety instrumented functions are not described clearly enough in the HAZOP, for example, which safety valves should be opened if a certain level is exceeded. The identified hazard must also be written to indicate the ultimate consequence.

SEQHAZ did not always identify scenarios relevant for the SIL evaluation but risk ranking made the selection of scenarios easier. Neither HAZOP identifies always all scenarios that should be treated in the SIL evaluation but to a more complete extent than SEQHAZ® because of its systematic way of identifying risks.

When to use HAZOP and when to use SEQHAZ® was also discussed. In general HAZOP is better suited for processing technical risks, when the project is still at design stage and only a PI&D is available. On the other hand SEQHAZ® is better suited for other types of risk analysis e.g. loading/unloading. However when to use a specific risk analysis must be decided on a case by case basis. As it is not possible to make an

absolute scheme for when the different methods should be applied. The two methods complete each other and can therefore be used together at different stages or study objects.

The Neste Jacobs Oy risk graph method and Borealis group's LOPA method for SIL evaluation were performed, discussed and compared. The risk graph's strengths were that it is a flexible method which is also widespread and has been used for a long time. Furhtermore, as it determines personal, environmental and economical risk in three different graphs is also an advantage. On the other hand the risk graph was found to be subjective and the outcome of the SIL evaluation depends a lot on the group's experience. Since a group that is not experienced in using the risk graph gets a higher SIL than an experienced one, there should always be at least two experienced people present during the analysis.

LOPAs strengths were that it was straightforward, is less dependant on the group and is faster than the risk graph. It is less dependant on the groups performance as the analysis depends more on the tighter calibration by Borealis. The acceptable level of risk is also clearly defined in Borealis LOPA, while it is more vaguely expressed in the risk graph. The disadvantages with LOPA was that the two parameters F and P that are an important part of the SIL evaluation in the risk graph are not taken into account. The method was also seen as too rigid and inflexible because of the tight calibration.

During the seminar day it was decided that the thesis should focusing on which model to use. Instead the focus should lie on the implementation of changes that can be achieved during the thesis. A key question was found to be how the pass on of information should be done from HAZOP/SEQHAZ® to the risk graph. For this to be done in a more effective way risk ranking should be made in HAZOP and SEQHAZ® to have the same scale as in the risk graph. This is important as it helps to sort out which scenarios should be treated in the SIL evaluation.

Different possibilities were discussed for harmonising the risk rankings in HAZOP, SEQHAZ® and the risk graph. One possibility is to mark clearly the SIL case / possible SIL case in the HAZOP. But a better way is to rank consequence and likelihood in the same way for HAZOP and SEQHAZ®. The consequence can be the V parameter and

the likelihood the W parameter in the risk graph. The likelihood W should be estimated whit the safety valves and other non SIF are considered present, since this is how it is defined in risk graph. An argument for why both consequence and likelihood should be estimated is that they co work and affect one another.

Three consequence scales were suggested: human, environment and economy then the one with the highest consequence class should be selected. If no considerable risk is found this is noted down but the consequence and likelihood do not have to be checked for these cases. Only the consequence classes that are relevant should be treated. The likelihood would be classified taking into account non instrumented protection layers just like in the risk graph method. The names for one of the parameters V and W will then have to be changed as they are too close to each other and can be mixed up. Another idea was risk ranking based on consequence and probability type. It was decided that the harmonisation will be further developed.

To perform the hazard study and SIL evaluation in the same session is also a direction to move to in the future, if a V and W term ranking are done in HAZOP and SEQHAZ® then it was concluded that the step is not so far away.

It was suggested that the process designers should have more interaction with the automation engineers and vice verse. This was found to be one of the reasons why the move of information does not work smoothly at present. If possible the same people should participate at both the hazard study and the SIL evaluation. This is a move towards performing both analyses at the same time in one session.

What can be learned from Borealis LOPA procedure is that they clearly state their acceptable level of risk. This is a necessity when using LOPA since it is the target of the SIL evaluation to reduce the risk to an acceptable level. It was also evident that stating standard values for failure rates, initiating events and having strict specified consequence categories in tables makes the method more consistent.

Another conclusion from the seminar was that it should be clarified when the hazards study and SIL evaluation should be carried out. The timing is important since this gives continuity in the project. It was also found to be that the hazard study decides if a SIL

evaluation is needed and that the same input data is needed from the hazard study for both the risk graph and LOPA, but the way it is presented can be different. Another important conclusion from the seminar is that no matter what method that is used for the SIL evaluation the most important is that you have competent people performing the analysis.

6 Evaluation of results

In this chapter the key elements of my findings for optimal hazard study processes are presented based on the results from the field study: interviews, studying of hazard reports, participation in real hazard studies and the seminar day. The goal of this thesis is to optimize the hazard study process and this chapter discusses its key elements.

6.1 Pre evaluation and Method Selection

In the pre evaluation stage the most important part is that the biggest risks are eliminated because if this is done properly the workload in the next risk analyse stage which in general is a HAZOP or SEQHAZ® can be considerable facilitated. Another reason is that at this stage changes in the process are still considerable low as the plant still only exist on paper. Therefore, these studies should be completed as soon as enough material is available.

The method selection is done in a discussion between Neste Jacobs Oy and the client. From the interviews I conclude that it is not possible to give a scheme that definitely indicates when it is better to use HAZOP and when to use SEQHAZ®. It has to be decided for every specific project, but in general HAZOP is best suited for a completely new plant, of which there is not so much experience in running the process. SEQHAZ® which is not as heavy as HAZOP is better suited for analysing changes of processes, or, also for new projects if there is a long experience of running the process available. SEQHAZ® could also be more easily employed than HAZOP for analyses rather than soley the process technical ones, as for example an analysis of loading chemicals. Old hazard reports (HAZOPs or SEQHAZ®s) should be used if they are of good quality when the hazard study is updated.

Another important aspect of which method to choose depends on the resources and time that is given for the detailed hazard study from the client. The reality is that these studies are made in a later phase of the project because considerable background information is required before the detailed hazard studies can be performed. This often leads to too tight time schedules which many times have to be changed, and extra sessions have to be added to complete the study.

6.2 Team selection

The team selection for a hazard study is done in a preparation meeting between Neste Jacobs Oy and the client. The client usually nominates people from the operational and maintenance side and Neste Jacobs Oy assists with the team leader, scribe and process designer and in some cases the instrumentation engineers. Those chosen for the hazard study depend on the method that is being used and on which object that is being studied. In general this means people with considerable experience of the process, because, the total knowledge of the group determines the outcome of the study. Moreover the group culture is also very important for the result the team have to be open to discussion. A person must be able to speak freely without any threats of penalties for what he states.

In a HAZOP the team leader has the most important role and should be someone from the outside, so that he can ask "dumb" questions. The team leaders role is to ask the right questions and to motivate the group so it performs well. It is also essential that the team leader is someone with process understanding. The scribe should also be someone with process knowledge, for example, a process designer that should have the ability to take out the most important elements from the discussion and write it down. It is helpful if the team leader and the scribe have worked together before because their teamwork is important for the effectiveness of the whole study.

It is extremely important that operators or operational engineers are present, if possible, at the hazard study . They give the other group members a better understanding of what can really happen so that relevant scenarios are considered. Instrument engineers are needed to understand what SIF needs to be added during the HAZOP and to say what scenarios are relevant for the SIL evaluation.

In SEQHAZ® basically the same people as for a HAZOP need to participate, a difference is that the scribe do not have to be present at the session, as in this method everyone works individually filling out a SEQHAZ®-sheet, although in a group. The scribes work is then to put the information from the sheets together in the SEQHAZ®-report.

6.3 Hazard identification and risk estimation

The two main methods that are considered in this thesis for hazard identification and risk estimation are HAZOP and SEQHAZ®. In this chapter the key findings about these methods from the field study are presented.

6.3.1 HAZOP

Hazard and Operability Analysis Study or HAZOP is the most used hazard study method in the chemical process industry and has been used for a very long time. Because of this almost everyone that was interviewed had used this method with different roles the team leader, the scribe, the process designer, the instrument engineer, the safety specialist, the operational engineer and the operators. The method is relatively easy to understand. But a short introduction of the method is needed and then you get into the "thinking" quite fast since it is a very systematic and repetitive way of identifying the hazards and assessing the risks. The pre work is very important during a HAZOP, if it is possible to send out an object description of the study object and short introduction for those which are not familiar to the HAZOP methodology it is helpful. The timing of the study is important since HAZOP requires considerable background material like PI&Ds and flow sheets, which means that the planning of the process needs to have progressed to such an extent so that it does not become a design meeting.

The strengths of this method is its systematic approach, to use guidewords and then to go through all relevant deviations for the guidewords. The list of guidewords also helps the team leaders work and see that everything gets covered. Depending on which process that is studied different guidewords can be more or less important. The guidewords with their deviations are effective to use when the scope of the HAZOP study is planned. When this is done it is important that the process is divided into reasonable parts, this is one challenge for the team leader and other experts of the process when planning the study.

The scribe should be acquainted with process design, this is an essential part of understanding the discussion. One person who shares two different roles during the study is not, helpful, for example a scribe that also acts as a process designer. As a

scribe you must put your attention on what is being said and have to write down what is decided, at the same time trying to come with your own suggestions is a too demanding task.

The credibility of the HAZOP results is considered high among the interviewees. This because of its systematic approach and I believe that because these studies are time consuming it gives the person a strong feeling that every risk was considered. Old HAZOP reports are a good aid when updating the study for example during a change. It is important that the HAZOP reports are written thoroughly in order to help the work for those that were not present at the sessions and have to use the report. This has been a frequent problem for all hazard studies, the use of a computer at the session and a beamer where everyone can see what is written instantly, has increased the quality of the writing. Now the sentences and tag numbers can be corrected direct during the session.

HAZOP is a creative group process which is time consuming, and long sessions are more rule than the exception. Because of this the importance of simple things like having regular breaks and a nice meeting room with air conditioning is extremely important. Too little time is reserved for the HAZOP study. It is better to reserve too much time and then take some sessions away in the end than having to add sessions at the end, this way the group's entire calendar is difficult to manage. The study requires much time from many people from different areas. One big challenge is to plan the study in a manner that allows the key persons needed for the study to participate.

The consequences should be ranked without protection barriers and safety instrumented functions. This should be a rough risk ranking. If the risk ranking is made too detailed it becomes very time consuming. On PI&Ds it is not possible to see the proportion of reactors, pipes or what is in the surroundings, and therefore it can often be very helpful to go check out how it looks in the factory if this is possible. Not everything is shown on a PI&D. For new plants this is of course not possible, but for HAZOPs on existing plants where a change has been made it is. HAZOP also offers an excellent opportunity of learning about the process and because of this new process designers can attend as listeners, but it is recommended that the amount of outsiders which participate should be limited since this may have a negative effect on the group.

The start-up phase is seldom treated in a HAZOP which is one of its weaknesses. It depends highly on the team leader and the expertise of the group whether this is done. Two or more deviations at a time are not considered in HAZOP and it is often these scenarios that lead to big consequences. Also human error and special circumstances are not studied systematically in a HAZOP. However, no hazard study method can identify 100 percent of all risks. Something unexpected and not previously thought of are always possible outcomes. It is dangerous processes that are being treated and HAZOP is currently one of the best ways to deal with these risks.

6.3.2 SEQHAZ®

SEQHAZ® is Neste Jacobs Oy own method and it has been in use for around ten years in different types of projects. This method is not as heavy as HAZOP but also not as systematic. The method requires more introduction than HAZOP, since here the first part of the analysis is performed alone. The team leader also plays an important role but not as important as in a HAZOP. The approach requires a group with considerable user experience of the study object to obtain a good result. When this is the fact the credibility of the result is high and the study takes considerably less time than for example a HAZOP. SEQHAZ® is a flexible method and can be used on basically any study object which doesn't necessarily have to be a process technical one. The method can also be efficiently used to improve old HAZOP reports.

The method is faster than HAZOP but is at the same time less thorough. Therefore SEQHAZ® suits well as an alternative for smaller projects or projects where the risk level is lower. The big difference from HAZOP is that the first part of the study is performed alone even though the study is performed together. In this regards you are on your own identifying the hazardous situations for different parts of the study object, filling in a sheet which is shown in Appendix 2. The idea is that you analyse the parts of the study object of which you have the most knowledge. This allows for the analysis to be more time efficient, however at the same time it is one of its weaknesses. The reason is that when you are considering something on your own it is more difficult to concentrate on the problem at hand and scenarios that are irrelevant are more likely being considered. Different people often come up with the same risks which often are the most obvious ones.

The second part is a group discussion of action proposals based on the hazardous situations identified in the first step. In this stage the consequence and risk class of the identified hazardous situations are measured differently by different people, because their reference scales are different. This is a problem in all hazard studies that include some sort of risk ranking. But since the action proposals are discussed in group the consequences and risk classes can be changed and harmonised. The moment of categorising into consequences classes and risk classes is time consuming, even if the classes are predefined in the procedure. A disadvantage when letting people write on their own is that, some are more talented in speaking than writing and because of this it is not always clear what the person meant, but this is clarified if needed at the action proposal meeting.

The scribe needs to have good Excel knowledge since there are many useful functions which can ease the work to fill out the report formula. The method also gives an excellent opportunity of learning from areas other than your own which makes it easier to understand the other workers situation. Also for SEQHAZ® thorough documentation is essential. Since the people themselves choose which area to assess it is important that the team leader makes sure that enough overlap is made. An idea is that if for example more than 10 % of the study object areas are not assessed. The project manager should as the control function verify with the team leader that enough risk assessment was done in order to find out if a tolerable risk level is achieved. To summarize this is a flexible hazard study method which can be used as an alternative or complement to the HAZOP study method and can be used for basically any type of project.

6.4 SIL evaluation

The SIL evaluation is performed after the hazards have been identified and the risks assessed in a HAZOP or SEQHAZ® study. The two main methods for SIL evaluation that are considered in this thesis are risk graph which is currently used by Neste Jacobs Oy and layer of protection analysis that is used by Borealis. In this chapter the key findings from the field study about these methods are presented. The information that is needed for a SIL evaluation regardless of what method that is used is the instrumentation description list, the hazards description and consequences and the piping and instrumentation diagram of the study object. The hazards description comes

in general from a HAZOP-, SEQHAZ® -or similar report. As it is now which hazards or scenarios that is to be treated in the SIL evaluation is based on experience. If risk ranking (in four levels) has been performed a thumb rule that has been used at Neste Jacobs Oy is that risks that are very serious (scale 3 of 4) or more automatically are treated in the SIL evaluation. The risk ranking helps the team leader for the SIL evaluation in choosing which scenarios should be treated in the analysis.

6.4.1 Risk graph

Risk graph is a semi qualitative method for SIL evaluation which is described in chapter 2.6.1, the method has been in use since 2000 at Neste Jacobs, but testing of the method started already in 1999. The method requires background information to understand; therefore an introduction of the method is required. A basic condition for risk graph is that all non instrumented protection layers are counted as present when the frequency of occurrence parameter, W is estimated. In the risk graph method used by Neste Jacobs Oy personal, environmental and economical risks are considered with the same method in three different graphs. Before using the method the risk graphs need to be calibrated for the type of process that is treated. The calibration is very important for the result of the analysis and typically the method has to be recalibrated now and then. Also one calibration does not suit every study object. The more the method is used the closer the calibration gets to the right value. It is important that there are enough examples for the calibration to be well understood.

The number of persons needed at a risk graph session is at least five: a team leader, a process designer, an operational engineer, a operator and someone that is familiar with the plant's controls and instruments. The team leader should be skilled in safety automation and it is very helpful if the team leader also has been participating in the previous hazard study. The other team members can also with high effectiveness take part in both the hazard study and the SIL evaluation. This gives a better understanding of the process and it is easier to say which scenarios go to the SIL evaluation if the same group has done the hazard study. The team leader usually acts as a scribe for the analysis so no special scribe is necessary. The analysis sheets are generally partly pre filled with scenarios and the consequence parameter pre calculated by the team leader to save time.

The risk graphs template is straight forward and easy to understand at first but there are many exceptions which have to be taken into account that are not so easy to understand for the first time user. If the group has experience in using the method the end result is usually reasonable. The method also works well for similar hazards, when there are many scenarios with the same risk types.

Risk graphs are based on subjective estimations of four different parameters. These estimations are often conservative, which means that a higher SIL than needed can be the outcome. But the outcome also depends on the calibration of the risk graph and on the group's experience of using the method. Therefore a group that is not experienced in using risk graph, get a higher SIL than one that is experienced. This is one of the largest problems with risk graph. Another key problem with the method is that the SIL scale is too tight. In theory it is possible to obtain SIL 0-4, which are 5 different steps. But in practice only up to SIL 2 is used out in the plant since SIL 3 is difficult to achieve in practice and is not considered reliable enough, if it occurs then a solution has to be found in the process design.

Risk graphs are also simple to use which can be dangerous if they are used without understanding the background of the analysis. The parameter values are found too close to each other which have the effect that the selection is not always clear. The estimation of the F parameter is found troublesome, and sometimes an F3 choice is desired. The estimations of the W parameter and the frequency of occurrence are difficult since there is not always people available with experience in how often components fail. But this is a problem not only for this method, but for every risk analysis method that uses frequencies. Risk graph does in a restricted way take into account mechanical protection and maintenance. Furthermore they do not cover ignition probability and it is not always clear what protection layer that can be used for risk reduction.

If the risks have been ranked in the previous hazard study it helps to sort out which scenarios that should be considered in the SIL evaluation. Now the consequence scale from SEQHAZ® and HAZOP (if made) is not synchronised with the one used in risk graph. If the C term had been calculated already in the HAZOP or SEQHAZ® it would say directly if it has to be considered in the SIL evaluation. But it is important to

remember that the SIL evaluation is not the only reason why the HAZOP or SEQHAZ® report is done and the total focus of the reports should not be misleading.

6.4.2 Layer of protection analysis

Layer of protection analysis (LOPA) is another method for SIL evaluation that is described in chapter 2.6.2. An applied version of LOPA has been in use at Borealis Polymers Oy in Finland since 2006. Because it is a quantitative method where frequencies are used some of the necessary calculations may at first be difficult to understand. LOPA is scenario based and a basic condition is to look at the system without any protection layers when estimating the frequency for the hazard. The frequency and consequence of the hazard gives the required risk reduction from a table. This means that the company has to state their acceptable level of risk for different consequences in numbers. This is the most difficult part with using LOPA because by stating specific values for the acceptable risk level you indirectly put a value on a human life, and this is controversial. For Borealis group the acceptable level of risk is shown in Figure 11. for different categories. The different categories are defined in the LOPA calibration shown in Appendix 6. Every company has not specified the acceptable level of risk this clearly which is a necessity if LOPA is going to be used. This may be a problem when using LOPA.

Figure 11. Acceptable level of risk for Borealis group. (Aerts, 2005)

The persons needed at a LOPA session are the same as for risk graph which means at least five persons: a team leader, a process designer, an operational engineer, an operator and someone that are familiar with the plants controls and instruments. The team leader should be skilled in safety automation and it is very helpful if the team leader also participated in the previous hazard study. The other team members can also with high effectiveness take part in both the hazard study and the SIL evaluation. This gives a better understanding of the process and it is easier to say which scenarios go to the SIL evaluation if the same group has done hazard study. The team leader usually acts as scribe for the analysis so no special scribe is necessary. The analysis sheets are generally partly pre filled with scenarios by the team leader to save time.

This method also needs background information to understand the LOC and LOPA concepts, therefore an introduction of the methodology is needed. It demands more time to understand LOPA than risk graph but when you have understood it, the method is straightforward and logical. It does no leave so much space for speculations as e.g. risk graph because of the predefined tables. The method used by Borealis Polymers Oy is straightforward, fast and consistent. The predefined tables for initiating events, consequence categories, protection layers and the use of Borealis risk matrix shown in Appendix 6 leads to fast decisions and consistency.

LOPA is also more flexible than risk graph while it is possible to include almost any protection layer in the analysis. Another advantage is that LOPA is a beginning of a quantitative risk assessment, which means that if further risk assessment is required part of the job is already done. In LOPA you are listing all available layers of protection, and have a defined tolerable risk level as target which makes it easy to see where to start when extra protection layers are needed. In risk graph the non instrumental protection layers taken into account when the W parameter is estimated.

The disadvantages with LOPA are that two parameters F and P which play an important part of the risk graph method are not even taken into account in LOPA. The method is very rigid because it is based on many definite values, which are not always able to find relevant data for. These values also make the method inflexible in the sense that they do not leave much space for discussions. This depends a lot on the team leader and the group performing the analysis.

6.4.3 Comparison between risk graph and LOPA methods

The goals for risk graph and LOPA are both to reduce the risk to a tolerable level. This is done by either adding a non instrumented protection layer or a SIF for which the appropriate SIL has to be determined. The two methods are quite different risk graph are based on subjectively estimating four parameters while in LOPA which is more quantitative all values that are used are taken from tables. Therefore it is difficult to compare the methods straight off but this chapter is intended to illustrate the main difference with the risk graph method used by Neste Jacobs Oy and the applied LOPA used by Borealis.

In risk graph the four parameters are derived out of best practice in the chemical process industry of parameters describing a hazardous situation. In LOPA the basic idea is that the company explicitly has to set a tolerable risk level, and this is the target for the analysis. The tolerable risk level can be interpreted from how the parameters are calibrated in risk graph. This risk level is more vaguely expressed in risk graph. It is not clearly stated as in LOPA. LOPA is also more systematic and it is easy to see where to start when the risk has to be reduced. Because you have a required risk reduction to meet and then the protection layers are listed one by one, if the mitigation is not enough additional layers have to be added. In risk graph the protection layers are also listed, but

not all layers that can be accounted for in LOPA may be added e.g. operator response. In LOPA operator response can be counted for as a protection layer while it can't in risk graph.

The risk graph method used by Neste Jacobs Oy is based on estimating the four parameters C, F , P and W described in Appendix 5. Two of these parameters the occupancy F and probability of avoiding the hazard P are not even included in the LOPA method. The F and P parameters describe if there are persons present in the factory and if they have the possibility to escape the dangerous situations. The explanation must be that they are not considered important in LOPA. Because in a LOPA based on loss of containment the only thing that matters is if chemicals are being let out to the air, ground or water outside the factory. This means that only scenarios that include a LOC are considered and that it does not matter if there are people present or not while the consequence is still severe. Since one of the goals with LOPA is to reduce the emotionalism, this is another explanation of why the two parameters F and P are excluded from the method. It helps the team to make more accurate judgments about relative risk since it is very difficult to estimate qualitatively the number of people who might be harmed and how severe the harm might be (CCPS, 2001).

The other two parameters used in risk graph C and W are also used in LOPA but with important differences. When the demand rate W in risk graph is estimated all non instrumented protection layers must be considered because each protection layer lowers the W factor. This is an important difference from LOPA since then all the failure frequencies of the initiating events leading to the considered scenario are listed and you are looking on the naked system without any safeguards. Then the initiating event with highest failure frequency is chosen. In Borealis LOPA a pressure relief valve which is clean, well designed and tested regularly has the risk reduction of 100 (two SIL) which can be compared with risk graph where the maximum possibility to mitigate the risk is a factor 10 or one SIL / protection layer. In that sense LOPA is more flexible since a protection layer may mitigate the risk with any number it can for example be 1, 7 or 99 it do not have to be a factor 10 like in risk graph.

The consequence parameter C in risk graph is also quite different from the consequence used in Borealis LOPA. In the risk graph method used by Neste Jacobs Oy the C

parameter is semi quantified by first deciding the average number of people present then multiplying with the selected vulnerability which gives the C term. This is described more thorough in Appendix 5 Calibration of personnel risk. In LOPA which type of release is decided first then qualitative quantification of the amount and at last the category value is taken from a table for the specific release type. This means that in LOPA the type of release matter, in risk graph the type of release are taken into account in the V parameter but not to the same systematic extent.

To further illustrate the differences between the different methods, a practical example that shows how the safety integrity level for both risk graph and LOPA could be determined is done below. The same scenario will be used for the risk graph and LOPA example and is shown in Figure 12. The scenario is taken from Borealis groups LOPA procedure but has been slightly modified.

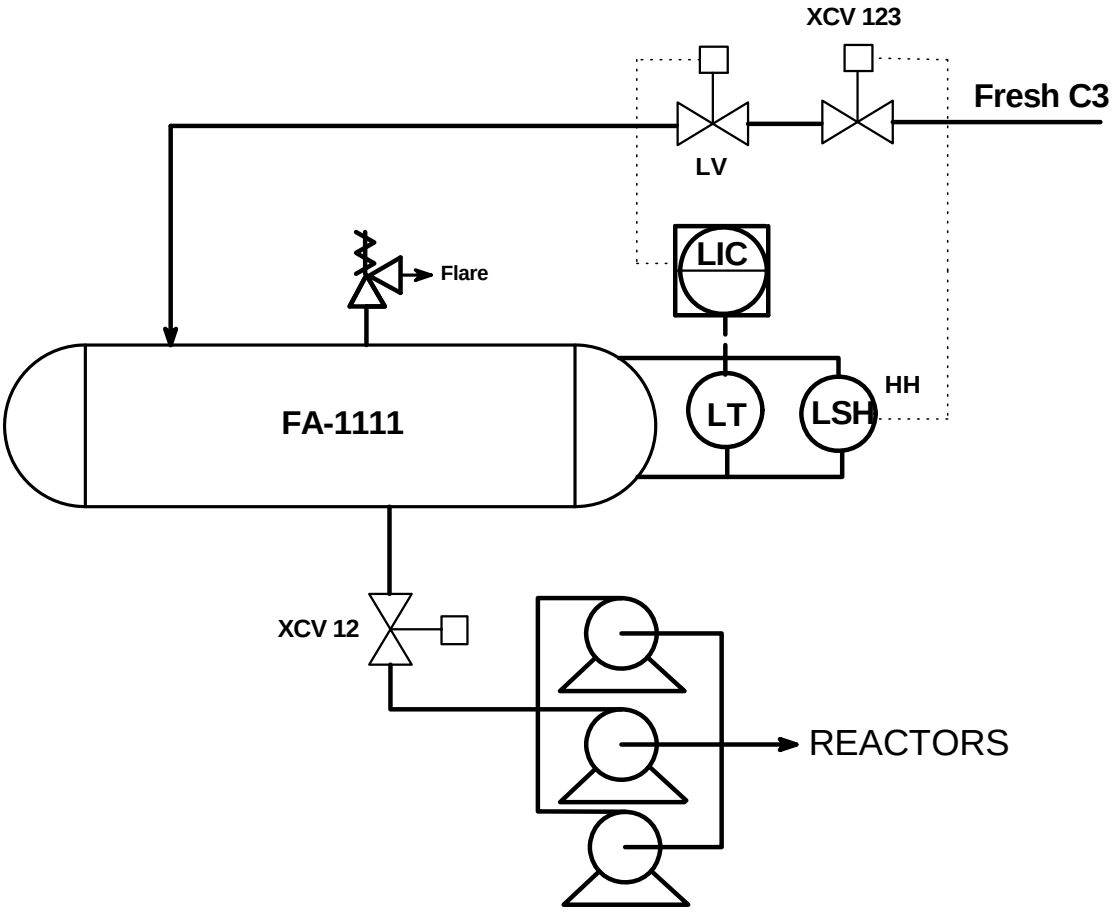

Figure 12. Simplified PI&D of propylene feed tank. (Aerts, 2005)

LIC - level indicator controller LT - level transmitter HH - high high
LSH - level switch high XCV - on/off valve LV - level control valve

Scenario description

A propylene feed tank is designed as in Figure 12. One flow with fresh C3 (propylene/propane mixture) are fed to the tank FA-1111. Three pumps suck the mixture in the tank FA-1111 towards the reactors and this line is equipped with an on/off valve The HAZOP study has identified overfilling of the feed tank FA-1111 as a scenario that may lead to high pressure in feed tank FA-1111 which in turn may lead to leakage, fire and in worst case explosion. Risk estimation shows that this would lead to catastrophic health, serious environmental and extensive economical consequences. Because of this the tank FA-1111 is protected with a safety valve and a SIF in form of an on/off valve on the fresh C3 feed line that is closed at high high level.

The causes for overfilling of the tank FA-1111 are from the HAZOP identified to be control loop failure of the LIC and outlet on/off valve failure or pump failure. The SIL evaluation for the high level measurement is first done with risk graph.

Risk graph example

First the scenario is described. The HAZOP study has identified overfilling of the feed tank FA-1111 as a scenario that may lead to high pressure in feed tank FA-1111 which in turn may lead to leakage, fire and in worst case explosion. The causes for overfilling of the tank FA-1111 are from the HAZOP identified to be control loop failure of the LIC (failure of level measurement, level valve or DCS), outlet on/off valve failure or pump failure.

The protection function that is evaluated is closing the feed to the tank FA-1111 at high level. Input signals are the high level measurement and output signal the on/off valve on the C3 feed line. The tank FA-1111 is also protected with by mechanical protection in the form of a safety valve.

The description of the parameters and calibration of the risk graph method is shown in Appendix 5.

First personnel risk is evaluated. The number of persons at the process area is estimated by the shift chief to be 1.5. For personnel risk the vulnerability parameter is set to 0,5 because the propylene are estimated to deflagrate (to burn or cause to burn with great heat and light) in the worst case. This gives the consequence, C = V * number of persons present in the process area = 1.5*0,5 = 0.75 which is equivalent to **C3**. Because of rare to more frequent exposure in the hazard zone (occupancy < 10%) **F1** is chosen. There is no possibility of avoiding the dangerous situation so the parameter **P2** is chosen. For the demand rate the equipment failure is estimated as the most common and by experience it is known to be 1/3 year which gives W2, but there is a safety valve present which allows lowering the demand rate one step to **W1**. This gives **SIL 1** for personnel risk which is shown in Figure 13.

For environmental risk the for the consequence value **C2** is chosen because the release are contained to the process are. The parameter F automatically gets **F2** since

environmental- and economical risks are always considered present in the calibration. P and W are the same as for personnel risk, therefore **P2** and **W1** is chosen giving **SIL 1** for environmental risk shown in Figure 13.

For economical risk the consequences are considered to cost 2-20 M€ which gives the value **C2.** For economical risk the value **F2** is also chosen, see above. P and W are the same as for personnel risk, so **P2** and **W1** is chosen which gives **SIL 1** for environmental risk shown in Figure 13. Now the highest SIL is chosen for the SIF which in this case is **SIL 1.**

RISK GRAPHS

Human					
C	F	P	W		
			W3	W2	W1
C1	-	-	a	-	-
C2	F1	P1	1	a	-
		P2	2	1	a
	F2	P1			
		P2	3	2	1
C3	F1	P1	2	1	a
		P2	3	2	1
	F2	P1			
		P2	4	3	2
C4	F1	P1	3	2	1
		P2	4	3	2
	F2	P1			
		P2	b	4	3
C-value		0.75			

Environment					
C	F	P	W		
			W3	W2	W1
			a	-	-
C1	F2	P1	1	a	-
		P2	2	1	a
C2	F2	P1			
		P2	3	2	1
C3	F2	P1			
		P2	4	3	2
C4	F2	P1			
		P2	b	4	3

Economy					
C	F	P	W		
			W3	W2	W1
			a	-	-
C1	F2	P1	1	a	-
		P2	2	1	a
C2	F2	P1			
		P2	3	2	1
C3	F2	P1			
		P2	4	3	2
C4	F2	P1			
		P2	b	4	3

Required SIL **1**

Figure 13. Risk graphs for human, environment and economy.

LOPA example

Now the SIL evaluation for the high level measurement is performed with the LOPA methodology for the same scenario as shown in Figure 12. The first step is to describe the scenario. The HAZOP study has identified overfilling of the feed tank FA-1111 as a scenario that may lead to high pressure in feed tank FA-1111 which in turn may lead to leakage, fire and in worst case explosion. This is a scenario with a process deviation above the design pressure that causes loss of containment of propylene/propane which means it is relevant for LOPA. The next step is to determine initiating events leading to

the scenario and their probability. The following initiating events, with their probabilities from Table 6.1 in the LOPA calibration Appendix 6, are found:

1. Closure of outlet valve 1/10 year
2. Failure of level measurement 1/10 year
3. Failure of level valve 1/10 year
4. Failure of DCS system 1/10 year
5. Failure of reactor feed pumps less than 1/10 year (more than one running)

No enabling events are applicable in this case (no extra conditions have to be fulfilled for the scenario to happen one of the initiating events are enough). The highest probability is chosen and is in this case **1/10 year**. The next step is to determine the consequence. Since the release type is liquefied pressurised gas (LPG) and the tank is a LPG feed tank, the release is considered large in case of catastrophic failure of the vessel. This gives **category 1** according to Table 6.2, Appendix 6. Now the risk matrix in Table 6.9 from Appendix 6 is used to determine the required risk reduction, the probability of 1/10 year for the scenario and category 1 gives the **required risk reduction of 1000**.

The next step is to identify all independent protection layers, values for risk reduction factors can be found in Table 6.10-11 in Appendix 6. The following protection layers are found:

Non instrumented protection layers:
1. Safety valve. **Risk reduction factor 100**.

Instrumentation protection layers:
1. SCIS[1] (safety critical instrumentation system) with high level interlock closing the critical feed. **Risk reduction factor 10 = SIL 1**

The required risk reduction is 1000, the safety valve reduces the risk with 100 since it is well designed and tested and propylene/propane is considered to be a substance where

[1] At Borealis this term is used instead of SIF but they are identical.

clean service is possible (do no plug the pipes easily). However this is not enough, since the gap is 10 to zero (1000-100), a SIL 1 interlock is required for the SIF closing the critical feed to reduce the risk to zero. This means that in this case the both methods came to the same conclusion, SIL 1. But this may not always have to be the case.

The strengths and weaknesses with the two methods have been discussed in chapter 6.4.1 and 6.4.2. A summary of that discussion is that there are strengths and weaknesses with both methods but they are both good methods for SIL evaluation. However my favourite is LOPA. The arguments for LOPA are several: it is more systematic, consistent and precise than risk graph. A more systematic approach is always an advantage when performing risk analysis while it makes it easier to that nothing is left out. Consistency is always desired when performing risk analyses. In this case more consistency which is possible in LOPA is mainly due to the tighter calibration but the risk graph methodology does not allow a tight calibration. I find the preciseness important while an inaccurate method may lead to overprotective SIS which is undesired. An argument for using risk graphs are that they have been used for a longer time than LOPA. But LOPA has also been around for a long time and is not at all a new method, it was introduced already in 1993 under another name. Today it is a widespread method for SIL evaluation and besides the direction the companies are moving today, which for me is a strong argument for using LOPA in the future.

6.5 Software tools for hazard study processes

Software tools for hazard study processes (hazard study and SIL evaluation) have been around for many years. They are nowadays very advanced and require good computer skills from the user. They save considerable time if they are used during the whole hazard study process (HAZOP- SIL evaluation) since scenarios can be automatically generated from the HAZOP study if consequence and likelihood scales are used.

On the other hand at Neste Jacobs Oy mainly HAZOP and SEQHAZ® are used for hazard studies and for SIL evaluation mainly risk graph but also LOPA are used. Since SEQHAZ® is Neste Jacobs Oy in house method there is no software tool available for this method at the market, and therefore it is not possible to find a software tool that cover all methods. There are software tools available that cover from HAZOP to risk

graph and HAZOP to LOPA but these programs have to be tested to clarify if all the input data that are needed for the program are the same as the output from the HAZOP that are currently used. Because the methods should not be modified to fit the software it should rather be the other way around.

My personal opinion is that software tools for hazard study processes are interesting since they save time when writing hazard study reports. If software tools are going to be used they should be thoroughly tested and considered before a decision is made to take them into use. Because using excel templates have the huge advantage that the software is known by almost everybody and it can be found on basically every computer and these are important practical aspects that should not be underestimated. An argument against SIL evaluation tools are that the most time consuming part are not writing things down, but the actual SIL evaluation.

7 Optimised models for hazard study processes based on HAZOP / SEQHAZ® and risk graph / LOPA methods

In the field study the key elements of the hazard study processes have been identified. The main problem was the poor quality of the documentation from the hazard studies and how the information should be passed on from the hazard studies to the SIL evaluation. This includes how to select relevant scenarios from the hazard study to be analysed in the SIL evaluation. LOPA was found to be the best SIL evaluation method which was concluded in the end of chapter 6.4.3 but also risk graph is a suitable method to use. In this chapter therefore models based on both LOPA and risk graph for optimized hazard study processes will be presented.

For the models it is first assumed that the risks are identified in either a HAZOP or a SEQHAZ® study. In chapter 5.2 it has been concluded that the documentation of these reports are extremely important to identify which scenarios to treat in the SIL evaluation. The safety instrumented functions must be clearly described and the identified hazards must be written to the ultimate consequence. The move of this information has been identified as one of the main problems for the SIL evaluation and the models will therefore focus on this interface and how the information in the HAZOP and SEQHAZ® should be presented to make the move of information as smooth as possible.

The first step to optimise the hazard study process is to let the same people perform both the hazard study and the SIL evaluation.

7.1 LOPA models

LOPA can be based on a loss of containment approach for determining relevant scenarios, like the method used by Borealis. But it may also be based on the use of a risk matrix with consequence and likelihood for determining relevant scenarios. Therefore first one model based on LOC approach is presented then one based on a risk matrix.

7.1.1 LOC based LOPA model

When HAZOP and SEQHAZ® are used for input data producers to LOPA with the LOC approach an extra column should be added with the title "LOPA case". This column will be marked with an X if the scenario in question is relevant for LOPA. The scenario is relevant if it is a LOC case, a safety instrumented function or if the group feels uncertain about if the risk reduction measures are sufficient. I have realised that it may be difficult to specify absolute rules for determining which scenarios that should be treated in the SIL evaluation but doing so is an effort towards making the selection more systematic. Also an extra column should be added estimating the consequence without safeguards. These columns should be added after the consequences stating the effect of the hazard. The consequence should specify which type of release and which category it is, just like in the Borealis LOPA method. The estimation of the consequence should help to determine if the scenario is applicable for LOPA. The release and the category is then already estimated during the hazard study, where usually a group with a more diverse knowledge is available than during the SIL evaluation, which conduce to a more accurate judgement. An example on how these extra columns could look like is illustrated in Table 8.

Table 8. Example for HAZOP template for LOPA model. Additional columns are shown in bold italic.

Stage	Part Code	Deviation	Dev. No.	Causes	Conse-quences	***Consequence without safeguard***		***LOPA case***	…
						Release type	***Cate-gory***		

The likelihood is not estimated here because this does sometimes involve calculations. Likelihood calculations are something that should be done in the LOPA, and not in the hazard study. Too many extra steps are not preferable since it would loose the flow of the hazard study.

7.1.2 Risk matrix based LOPA model

An alternative is to use a LOPA model where a risk matrix (consequence vs. likelihood) gives the input for the SIL evaluation. In the risk matrix the consequence is given on a four graded scale and likelihood on a three graded scale shown in Appendix 10 and 11. This risk ranking is done already in the HAZOP and SEQHAZ® so in the HAZOP three columns have to be added. The consequences are first categorised into human, environmental or material damage. Then the consequence and likelihood are estimated for the relevant categories. The consequence is estimated as the worst case scenario and the likelihood without considering any protection layers. The consequence and likelihood criteria must be calibrated for the specific company, depending on their tolerable level of risk. In SEQHAZ® the same consequence and likelihood categories have to be used as in HAZOP. An example for how this could look like in a HAZOP is shown in Table 9.

Table 9. Example how risks can be ranked in HAZOP as input data to LOPA. C stands for consequence and L for likelihood. Additional columns are shown in bold italic.

Stage	Part Code	Deviation	Dev. No.	Causes	Conse-quences	***Consequence type (H, E,M)***	***C***	***L***	Preparedness, precautions taken	…

This model is ideal if software tools are to be used for the hazard study process, since these tools are most effective if they are used during the whole process from HAZOP/SEQHAZ® to the LOPA. When the risks are ranked in both consequence and likelihood in the hazard study, the risk matrix is done and when it exceeds a certain level the specific scenario is automatically treated in LOPA. If a software tool is used with this method the LOPA scenarios are generated automatically. The drawback is that it is difficult to set this level, and irrelevant scenarios may be treated but more dangerous would be if relevant scenarios are not treated. Therefore, a sensibility check of the chosen scenarios and the ones left out would still have to be done. But I believe that a suitable level for the risk matrix that should be used to select scenarios to the LOPA would be found after testing and some time of using the method.

An Excel template is suggested to be used by the author for both the HAZOP/SEQHAZ® and the LOPA since it is easier to get an overview in Excel, and these analyses can often be up to a 100 pages, these large documents are slow to handle in Word.

7.2 Risk graph model

For the risk graph model the same risk categorisation should be used for SEQHAZ®, HAZOP and risk graph, because in this way the risk ranking can be of use in the later SIL evaluation. After studying the current risk ranking at Neste Jacobs Oy for SEQHAZ®, HAZOP and risk graph I concluded that there are not much difference in the criterions and that those with small changes can be the same for all analyses. This gives consistency and avoids double work when the risks have to be re-ranked because of the different scales.

This risk ranking is based on the one used in the current risk graph calibration since if the ranking is to be useful for the SIL evaluation this ranking have to be used. The ranking will be done both in HAZOP and SEQHAZ®. After the consequences of the risks are determined one column has to specify the type of risk: human, environmental or material damage. Only the ones relevant are considered. In the next step the risk is ranked on a five graded consequence scale defined as the term V term described in Appendix 5 for human risk. If the team leader also noted the number of persons present in the process area, the consequence parameter can be calculated after the session is done. For environmental and material damage the risk is ranked according to calibration shown in Appendix 5. In the third extra column the likelihood is ranked on a three graded scale. The likelihood is estimated with mechanical protection included defined in the same way as parameter W in risk graph shown in Appendix 11. An example for how this could look like in HAZOP is shown in Table 10.

Table 10. Example how risks can be ranked in HAZOP as input data to risk graph. C stands for consequence and L for likelihood. Additional columns are shown in bold italic.

Stage	Part Code	Deviation	Dev. No.	Causes	Conse-quences	***Consequence type (H,E,M)***	***C***	***L***	Preparedness, precautions taken	…

7.3 Validation of models

In this chapter the two proposals for LOPA models and the risk graph model are tested in an example for the same scenario used in chapter 6.4.3. The risks are first identified in the HAZOP/SEQHAZ® studies and thereafter it is shown how the extra information from the hazard studies can be useful during the SIL evaluation. This functions as a validity check of the models.

7.3.1 LOC based LOPA model

First the risks have been identified in a HAZOP report with the P&ID used shown Figure 14.

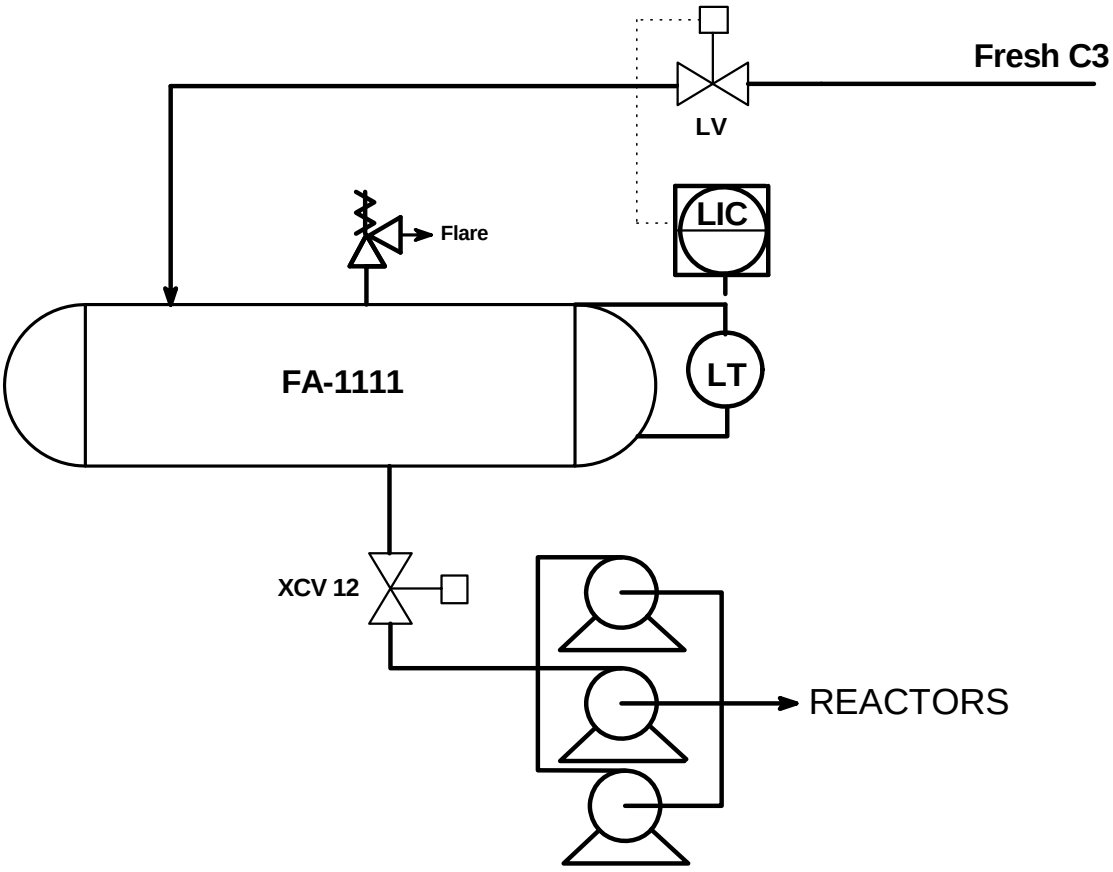

Figure 14. PI&D used at the HAZOP study for the scenario described in chapter 6.4.3.

An example on how the HAZOP report for the deviation for high level could look like for the LOC based LOPA model with the new information in italic is shown in Table 11.

Table 11. Example of HAZOP report for LOC based LOPA model with new columns shown in italic.

Stage	Part Code	Devi-ation	Dev. No.	Causes	Conse-quences	*Consequence without safeguard*		*LOPA case*	Pre-pared-ness	Proposed actions
						Release-type and amount	*Cate-gory*			
1	A	high level	1.2	Backflow from reactors Outlet on/off valve failure Control loop failure	leakage→ fire→ explosion	LPG, large	1	X	Safety valve	Install interlock that shuts feed to tank FA-1111 if level is high

The idea with the new columns is that the relevant scenarios for the LOPA already are selected in the HAZOP. The release type and category is already estimated so they can be transferred directly to the LOPA. The LOPA analysis is then performed in the same way as shown in chapter 6.4.3 for the LOPA example with the only difference that the category class is already estimated.

For SEQHAZ® it is difficult to make the same estimation, since in SEQHAZ® this part of the analysis is done alone. Because to determine if a scenario is relevant for LOPA requires much experience and discussion may be needed.

7.3.2 Risk matrix based LOPA model

The risks have been identified in a HAZOP report for one deviation based on the PI&D shown in Figure 14. an example on how this could look like for the risk matrix based LOPA model is shown in Table 12. with new columns in italic.

Table 12. Example of HAZOP report for LOC based LOPA model with new columns in italic. C stands for consequence and L for likelihood.

Stage	Part Code	Devi-ation	Dev. No.	Causes	Conse-quences	*Consequence type (H, E,M)*	*C*	*L*	Prepared-ness, precaut-ions taken	Proposed actions
1	A	high level	1.2	Backflow from reactors Outlet on/off valve failure Control loop failure	leakage→ fire→ explosion	H E M	3 2 2	2 2 2	Safety valve	Install interlock that shuts feed to tank FA-1111 if level is high

The new columns should also in this case help to sort out which scenarios are relevant for LOPA. With this model the consequence type with highest consequence is always chosen, and the consequence and likelihood should be ranked with numbers. Now the relevant scenarios are sorted out depending on the tolerable risk level set in the risk matrix. The risk matrix and its calibration used for the example in Table 12. are shown in Figure 15. with red squares going directly to the LOPA, yellow have to be under consideration and green left out. The risk matrix has to be calibrated for each company depending on their tolerable risk level and depending on which type of object it is.

RISK MATRIX		**Likelihood**		
Seriousness of consequences		Low = 1	Moderate = 2	High = 3
Catastrophic	**4**			
Very serious	**3**			
Serious	**2**			
Minor	**1**			

Figure 15. Example of risk matrix for selection of relevant scenarios for LOPA, with relevant scenarios in red, possible scenarios in yellow and irrelevant scenarios in green.

In this case the scenario is a possible LOPA scenario and analysis is done like the LOPA example shown in chapter 6.4.3. The difference with this method is that the scenarios that are relevant are chosen automatically. In SEQHAZ® consequence and likelihood is already ranked so it should not be too difficult too apply the same columns there.

7.3.3 Risk graph model

The risks have been identified in a HAZOP report for one deviation based on the PI&D shown in Figure 14. and an example on how this could look like for the risk graph model is shown in Table 13. with new columns high lighted in italic.

Table 13. Example of HAZOP report for risk graph model with new columns in italic. C stands for consequence and L for likelihood.

Stage	**Part Co-de**	**Devia-tion**	**Dev. No.**	**Causes**	**Conse-quences**	*Conse-quence type(H,E,M)*	*C*	*L*	**Prepared-ness,pre-cautions taken**	**Propos-ed actions**
1	A	high level	1.2	Backflow from reactors Outlet on/off valve failure Control loop failure	leakage→ fire→ explosion	H E M	C3 C2 C2	1 1 1	Safety valve	Install interlock that shuts feed to tank FA-1111 if level is high

The results seen in Table 13. for the consequence C, comes from first estimation of human risk (H) were the parameter V is estimated to 0.5, since propylene are estimated to deflagrate in the worst case. With the number of persons present at the process area noted by the team leader to 1.5 the consequence parameter is after the HAZOP session calculated to 0.75 which is equivalent to C3, shown in Table 5.2 in Appendix 5. The consequence for the environment (E) is estimated from Table 5.4 in Appendix 5 to C2 since the release is estimated to be confined to the process area. Finally the consequence for material damage (M) is estimated to C2 with the use of Table 5.5. The likelihood is estimated considering mechanical protection layers, in this case there is a safety valve present which lowers the likelihood. The likelihood criterion is the same as for parameter W in risk graph and is shown in Appendix 11.

Now the SIL evaluation is performed as normally with the risk graph method in the same way as in the example in chapter 6.4.3. The difference is that the risk ranking should help to sort out relevant scenarios and, that the consequence parameter, C, and

demand rate, W, beforehand are estimated and are ready to be used for the SIL evaluation. This means that only two parameters have to be estimated. For SEQHAZ® the same columns may be introduced.

8 Conclusions

Hazard study processes are complex and there are many aspects that have to be taken into account when performing risk analyses. This thesis has documented the key elements with the hazard study process at Neste Jacobs Oy, based on results from studying old hazard study reports, participating in real hazard studies, interviews and a seminar day. The focus of this thesis has been on the interface between the hazard study and the SIL evaluation. Therefore the three models for optimised hazard study processes, two based on LOPA and the third based on risk graph, are suggesting changes in the hazard study to make the move of information easier to the SIL evaluation.

This thesis has also discussed different methods for SIL evaluations. LOPA was found to be the best SIL evaluation method which was concluded in the end of chapter 6.4.3 but also risk graph is a suitable method to use. When the methods are used it is crucial to use them properly and be aware of their weaknesses. But the most important for the SIL evaluation is that there are competent people performing the analysis, not which method is used.

Everyone working with hazard study processes has their favourite methods to use, usually because these are the methods they have been schooled in, so depending on who you are talking to some prefers HAZOP and others SEQHAZ® for hazard study method. The same is true for LOPA and risk graph for SIL evaluations.

During six months of thesis work it is concluded that there exist many ways of performing the hazard study processes. Which methods to use depend on many factors e.g. which industry the company are working in, the size of the company and which tolerable level of risk that may be accepted by the company.

The suggested models are designed to facilitate the work for the SIL evaluation team at expense of more work for the HAZOP/SEQHAZ® team. Within the limited time of this master's thesis, it has not been able to test practically if the improvements are better in a larger perspective for the entire hazard study process. An evaluation of the models has

therefore not been possible and the models may have to be modified to suit other companies than Neste Jacobs Oy. But the author believe they would lead to more consistency and safer processes which are results that are beneficial to everyone. The suggestions are a step towards performing HAZOP/SEQHAZ® and the SIL evaluation in one session. This is already done in e.g. the nuclear power plant sector and is an interesting possibility which should be investigated further in future work. For future work this thesis and the book Safety Integrity Level Selection by Marszal et al (2002) can be used as a starting point.

9 References

Aerts, B. (2005) Procedure: HSE-035 Protection Layer Analysis, Borealis group.

Aerts, B. (2007-09-20) LOPA training event, Borealis group, Porvoo, Finland.

Aerts, B. (2008-01-23) Phone call, Process Safety Manager, Borealis group, Belgium.

Baybutt, P. (2007) An Improved Risk Graph Approach for Determination of Safety Integrity Levels (SILs), *Process Safety Progress*, Vol.26, No.1, 66-76.

Center for Chemical Process Safety (CCPS). (1992) Guidelines for Hazard evaluation procedures, Second Edition, New York, American Institute of Chemical Engineers.

Center for Chemical Process Safety (CCPS). (1993) Guidelines for safe Automation of Chemical processes, New York, American Institute of Chemical Engineers.

Center for Chemical Process Safety (CCPS). (2001) Layer of Protection Analysis: Simplified Process Risk Assessment, New York, American Institute of Chemical Engineers.

DIN V 19250. (1994) Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Berlin.

Dowell, M. A. (1998) Layer of protection analysis for determining safety integrity level, *ISA Transactions,* Vol.37, No.3, 155-165.

Elliot, D. M. and Owens, J. M. (1968) Chemical Engineering, 377-383.

EN 764-7 (2002) Pressure equipment. Part 7: Safety systems for unfired pressure equipment.

European Seveso Directive, 1982 (Council Directive 81/501/EC) reviewed 1996 and adopted as Seveso II Directive.

Exida (2006) Functional Safety Terms and Acronyms Glossary.
Retrieved from:
http://www.exida.com/articles/Safety%20terms%20and%20acronyms%20from%20exida.PDF (2007-12-13)

IEC (EN) 61508-5 (1998) Functional safety of electrical/electronic/programmable electronic safety related systems – Part 5: Examples of methods for the determination of safety integrity levels.

IEC (EN) 61511-1 (2003) Functional safety - Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, systems, hardware and software requirements.

IEC (EN) 61511-3 (2003) Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels.

Jacobsson, A. (2003) Val av lämplig riskanalysmetod inom processindustrin, IPS Guide.

Jin, S.H., Yeo, Y-K., Moon, I., Chung, Y., Kim, I-W. (2003) Evaluation of Safety Instrumented Systems Using Reliability Analysis, *Process Safety Progress,* Vol.22, No.3, 169-173.

Kemikontoret (2001) Riskhantering 3-Tekniska riskanalysmetoder.

Kirkwood, D. and Tibbs, B. (2005) Developments in SIL Determination, *Computing & Control Engineering Journal,*Vol.16, No.3, 21-27.

Laul J.C., Simmons, F., Goss J.E., Boada-Clista, L.M., Vrooman, R.D., Dickey R. L., Spivey, S.W., Stirrup, T., Davis, W. (2005) Perspectives on chemical hazard characterization and analysis process at DOE, ACS Division of Chemical Health & Safety, Elsevir.
Retrieved from:
http://hss.doe.gov/HealthSafety/WSHP/chem_safety/CHS-article-final9-7-05.pdf (2007-09-14)

Lees, F. P. (2001) Loss prevention in the Process Industries, Volume 1, Second Edition ,Oxford, Butterworth Heinemann.

Marszal, Edward M. (1999) Comparison of Safety Integrity Level Selection Methods and Utilization of Risk Based Approaches, *Process Safety Progress,* Vol.18, No.4, 189-194.

Marszal, E. M. (2001), Tolerable risk guidelines, *ISA Transactions*, Vol.40, No.4, 391-399.

Marszal, E. M and Scharpf, E. (2002) Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis, North Carolina, ISA (The Instrumentation, System, and Automation Society).

Salo, R. (2004) Procedure: Hazard studies, Neste Engineering Oy.

Salo, R. (2005) Procedure: Hazard and operability study, Method guide, Neste Jacobs Oy.

Salo, R. (2006) Procedure: SEQHAZ® method description, Neste Jacobs Oy.

SFS-IEC 60300-3-9 (1995) Dependability management. Part 3: Application guide. Section 9: Risk analysis of technological systems.

Stavrianidis, P. and Bhimavarapu, K. (1998) Safety instrumented functions and safety integrity levels (SIL), *ISA Transactions*, Vol. 37, 337-351.

Summers, A. E. (1998) Techniques for assigning a target safety integrity level, *ISA Transactions,* Vol.37, 95-104.

Summers, A. E., (2003) Introduction to layer of protection analysis, *Journal of Hazardous Materials* Vol. 104,163-168.

Timms, C. R. (2003) IEC 61508/61511-Pain or gain?, *Process Safety Progress*, Vol.22, No.2, 105-108.

TUKES Safety technology authority (2006) TUKES Guidebook: Dangerous chemicals in industry.
Retrieved from:
http://www.tukes.fi/Tiedostot/englanti/dangerous_goods/brochures/dangerous_chem_brochure.pdf (2007-10-08)

TUKES Safety technology authority (2007a).
Retrieved from:
http://www.tukes.fi (2007-10-17)

TUKES Safety technology authority (2007b).
Retrieved from:
http://www.tukes.fi/en (2007-10-05)

Turkkila, E. (2004) Procedure: K-150 Riskigraafimenetelmä, Neste Engineering Oy.

Turkkila, E. (2007-09-24) Discussion, Neste Jacobs, Porvoo, Finland.

Weibull, B. (2004) Säkerhetskritisk instrumentering Vad innebär IEC 61511 för processindustrin?, IPS Guide

White, R.S (2000) Easily Determine Safety Integrity Level*, Chemical Engineering Progress*,Vol. No.96, 3, 51-54.

Appendix

Appendix 1 Example of spreadsheet for HAZOP

Table 1.1 Example of spreadsheet for HAZOP. (CCPS, 1992)

Team: HAZOP Team #3 **Drawing Number:** 70-0BP-57100
Meeting Date: 6/27/81 **Revision Number:** 3

Item No.	Deviation	Causes	Consequences	Safeguards	Actions
2.0	Line - Ammonia feed line to the DAP reactor. Deliver ammonia to reactor at y gpm and z psig (dwg: Figure 6.6)				
2.1	High flow	Ammonia feed line control valve A fails open Flow indicator fails low Operator sets ammonia flow rate too high	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Periodic maintenance of valve A Ammonia detector and alarm	Consider adding an alarm/shutdown of the system for high ammonia flow to the reactor Ensure periodic maintenance and inspection for valve A is adequate Ensure adequate ventilation exists for enclosed work area and/or consider using an enclosed DAP storage tank

Appendix 2 Example of SEQHAZ® spreadsheet

Table 2.1 Example of SEQHAZ® spreadsheet. (Salo, 2006)

	Part	Cause group	Descriptions of hazardous situation i.e. how things can go wrong	Consequence class	Risk class

Appendix 3 Example of What if spreadsheet

Table 3.1 Example of What if spreadsheet. (CCPS, 1992)

Process: DAP Reactor
Topic Investigated: Toxic Releases

Analysts: Mr. Safety, Ms. Opera, Mr. Design
Date: 05/13/95

What-If	Consequence/Hazard	Safeguards	Recommendation
the wrong feed material is delivered instead of phosphoric acid?	Potentially hazardous phosphoric acid or ammonia reactions with contaminants, or production of off-specification product	Reliable vendor Plant material handling procedures	Ensure adequate material handling and receiving procedures and labeling exist
the phosphoric acid concentration is too low?	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Reliable vendor Ammonia detector and alarm	Verify phosphoric acid concentration before filling storage tank
the phosphoric acid is contaminated?	Potentially hazardous phosphoric acid or ammonia reactions with contaminants, or production of off-specification product	Reliable vendor Plant material handling procedures	Ensure adequate material handling and receiving procedures and labeling exist
valve B is closed or plugged?	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Periodic maintenance Ammonia detector and alarm Flow indicator in phosphoric acid line	Alarm/shutoff of ammonia (valve A) on low flow through valve B
too high a proportion of ammonia is supplied to the reactor?	Unreacted ammonia carryover to the DAP storage tank and release to the work area	Flow indicator in ammonia solution line Ammonia detector and alarm	Alarm/shutoff of ammonia (valve A) on high flow through valve A

Appendix 4 Example of Failure Mode and Effect Analysis spreadsheet

Table 4.1 Example of Failure Mode and Effect Analysis spreadsheet. (CCPS, 1992)

DATE: 1/21/91 **PLANT:** DAP Plant **SYSTEM:** Reaction System				**PAGE:** 5 of 20 **REFERENCE:** Figure 6.7 **ANALYST(s):** Mr. Ray Johnson		
Item	**Identification**	**Description**	**Failure Modes**	**Effects**	**Safeguards**	**Actions**
4.1	Valve B on the phosphoric acid solution line	Motor-operated, normally open, phosphoric acid service	Fails open	Excess flow of phosphoric acid to the reactor High pressure and high temperature in the reactor if the ammonia feed rate is also high May cause a high level in the reactor or the DAP storage tank Off-specification production (i.e., high acid concentration)	Flow indicator in the phosphoric acid line Reactor relief valve vented to the atmosphere Operator observation of the DAP storage tank	Consider alarm/shutdown of the system for high phosphoric acid flow Consider alarm/shutdown of the system for high pressure and high temperature in the reactor Consider alarm/shutdown of the system for high level in the DAP storage tank

Appendix 5 Risk graph calibration (Turkkila, 2004)

Table 5.1 Description of parameters used for risk graph.

Parameter		Description
Consequence	C	Personal risk treats the number of fatalities and/or injuries likely to result from the occurrence of the hazardous event. Determined by calculating the numbers in the exposed are when the area is occupied taking into account the vulnerability to the hazardous event. Environmental risk is treated as the size of release to the environment. Economical risk is treated as total loss in euros.
Occupancy	F	Probability that the exposed are is occupied at the time of the hazardous event. Determined by calculating the fraction of time the area is occupied at the time of the hazardous event. This should take into account the possibility of an increased likelihood of persons being in the exposed area in order to investigate abnormal situations which may exist during the build-up to the hazardous event. For environmental- and economical risk this parameter is always set to F2.
Probability of avoiding the hazard	P	The probability that the exposed persons are able to avoid the hazardous situations which exist, if the safety instrumented function fails on demand. This depends on there being independent methods of alerting exposed persons to the hazard and there being methods of escape. Environmental- and economical risk is treated by applying the personnel risk for possibility to escape the danger.
Demand rate	W	The number of times per year that the hazardous event would occur in the absence of the safety instrumented system. This can be determined by considering all features which can lead to the hazardous event and estimating the overall rate of occurrence taking into account other protection layers. Environmental- and economical risk is treated by applying the personnel risk for occurrence of hazardous event.

Calibration of the consequence parameter for personnel-, environmental- and economical risk

Calibration of personnel risk

(1) C = V * number of persons present in the process area

V = 0.01 Small release of flammable or toxic material

V = 0,05 Big release of flammable and toxic material, or small release with high probability to ignite.

V = 0,1 Large release, with high probability to ignite.

V = 0,5 Deflagration

V = 1 Rupture ,explosion or release of especially toxic material with hydro fluoride.

Numbers of persons present in the process area are calculated as an average value of when exposed to the danger.

Table 5.2 Calibration of the consequence parameter for personnel risk.

Consequence parameter	Classification
C1	>0,01
C2	0,01 - 1,0
C3	>0,1 - 1,0
C4	>1,0 - 10

Table 5.3 Personnel risk consequence parameter sensibility check.

Consequence parameter	Classification
C1	temporary disability or sickness
C2	Occurred injury, lasting disability or sickness, do not affect the ability to work
C3	Death or severe injury (>5), loss of ability to work
C4	Several deaths or several severely injured (>5)

Calibration of environmental risk

The consequence C for environmental risk is set to four levels C1,C2,C3 and C4. The calibration is shown in Table 5.4.

Table 5.4 Calibration of the consequence parameter for environmental risk.

Consequence parameter	Classification	Comments
C1	Release, with minor damage that is not very severe. Environmental strain or pollution or exceed of licence condition. Affects the process area and the inside of the plant.(Local environmental damage)	A moderate leak from a flange or a valve. Small scale liquid spill. Small scale soil pollutions without affecting ground water.
C2	Release in process area with significant damage. Limited known poisonous release. Affects the nearby surroundings.	Release of obnoxious compound travelling beyond the unit following flange gasket blow-out or compressor seal failure.
C3	Release outside the process area with major damage which can be cleaned up quickly without significant long term/lasting consequences. Major environmental damage. Severe exceeding of licence condition or regulation.	A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants or fauna. The company is obliged to restore the polluted area to the original state.
C4	Release outside the process area with major damage which cannot be cleaned up quickly or with lasting consequences.	Liquid release that could affect groundwater, release in river or sea. A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants or fauna. Solids fallout: dust, catalyst, soot, ash.

Calibration of economical risk

Economical risk consequences are estimated considering machine damage, reparation work costs and loss of production. The calibration of the question is shown in Table 5.5.

Table 5.5 Calibration of the consequence parameter for economical risk.

Consequence parameter	Total loss	Comments
C1	0,2 M€ - 2M€	Total loss includes the cost of building up the plant again and production loss.
C2	>2 M€ - 20 M€	
C3	>20 M€ - 100 M€	
C4	>100 M€	

Definition of the Occupancy parameter, F

Personnel risk

Table 5.6 Definition of the occupancy parameter, F.

Occupancy parameter	Definition
F1	Rare to more frequent exposure in the hazard zone. Occupancy <10 %
F2	Frequent to permanent exposure in the hazard zone. Occupancy ≥10%

Environmental- and economical risk

Because environmental- and economical risk is always present, this parameter always gets the value F2.

Definition of the probability of avoiding the hazard parameter, P

The probability of avoiding the danger if the protection system fails to operate is treated in the same way for personnel, environmental and economical risk graphs. The probability of avoiding the hazard parameter P has to values P1 or P2. P1 is used if the following conditions are fulfilled:

- Facilities are provided to alert the operator that the SIS has failed
- There are time and means of manually steering the process to safe condition
- There exist an escape route and enough time to safely escape the danger

If one of these conditions not are fulfilled the parameter gets value P2.

It is assumed that the facilities of alerting the operator are independent of the SIS and that the failure of the SIS can be understood by reading the process magnitude or/and the state information

Definition of the demand rate, W

The demand rate parameter W is the number of times per year that the hazardous event would occur in the absence of the safety instrumented system. The parameter is treated in the same way for personnel, environmental and economical risk graphs. The demand rate parameters W1, W2 and W3 definition is shown in Table 5.7.

Table 5.7 Definition of the demand rate, W.

Demand rate	Probability of occurrence / year
W1	$< \frac{1}{30}$
W2	$\frac{1}{30} - \frac{1}{3}$
W3	$> \frac{1}{3}$ (still ≤1 time/year)

Only one plants experience is not enough to estimate the probability of occurrence for different hazards. Because of this the process industries typical knowledge should be used as a help if available. In Table 5.8 is shown typical occurrences of failures in the chemical process industry and their frequency. This Table is a help when the W parameter is estimated with Table 5.7.

Table 5.8 Criteria for probability of occurrence of hazardous events. (Stavrianidis et al, 1998)

Type of events	Likelihood	
	Frequency/year	Qualitative ranking
Events like multiple instrument or valve failures, multiple human errors or spontaneous failures of process vessels	$<10^{-4}$	Very low
Events including combinations of instrument failures and human errors or full bore failures of small process lines or fittings	10^{-4}–10^{-3}	Low
Events like dual instrument, valve failures, or major releases in loading /unloading areas	10^{-3}–10^{-2}	Moderate
Events like process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials	$>10^{-2}$	High

If safety valves are designed properly according to the needed requirements, backlash valves as well as BCPS can be counted for as mitigating factors in the most places on the line. For example alarms that reveals the initiation of a hazardous chain event.

For mitigation of the W parameter also measurements and alarms that could prevent the hazardous event from happening even before it becomes dangerous should be counted in. For example:

- An alarm that reveals the malfunction of the control valve by detecting a too big difference between the control valves control and feedback signal.
- An alarm that reveals the malfunction of the control loop by detecting a too big difference between the control loops control and feed back signal.

W3 is chosen only for exceptionally instable continuous processes or in circumstances when there is extraordinary little experience of the process. In Neste Oil Oyj refineries at background of the long experience there should not exist cases for personnel risk that should end up with a W3 parameter. In the case where W3 is the only choice of parameter W, changes should be done in process design.

If the probability of occurrence could not be estimated by this method, it could be estimated quantitatively. This can be done by calculating different components requirements together or by analysing with a more complex method like Failure Tree Analysis. If the probability of the hazardous event is large, redo the risk graph or recalibrate.

Estimation with this method requires that all failure frequencies that may lead to that the hazard are considered and that they are calculated together.

Appendix 6 LOPA calibration (Aerts, 2005)

Table 6.1 List of initiating events and their failure frequencies.

Initiating Event	Fail frequency per year
Safety valve opens spuriously	$1x10^{-4}$
Cooling water failure (*)	$1x10^{-1}$
Electrical general power failure (*)	$2x10^{-1}$
Pump failure (motor or mechanical failure)	$1x10^{-1}$
Pump seal failure	$5x10^{-1}$
Unloading / loading hose failure	$1x10^{-2}$
BPCS instrument loop failure *Note:* IEC 61511 is more than $1x10^{-5}$/hr or $8.76x10^{-2}$/yr (IEC, 2001)	$1x10^{-1}$
Sensor failure	$1x10^{-1}$
Valve failure (control or on/off function)	$1x10^{-1}$
Manipulation of wrong valve (opened or closed)	$1x10^{-1}$
Operator failure (to execute routine procedure, assuming well trained, unstressed, not fatigued)	$1x10^{-1}$ per opportunity

Here follows a definition of the different categories used in the Borealis groups LOPA:

Table 6.2 Category definition for liquefied pressurised gas.

LPG					
Cat.	**Product - phase**	**Size of release**	**Type of release**	**Location of release**	**Remarks - examples**
1	LPG	Large	Catastrophic failure of vessel	-	LPG storage or feed tanks, polymerization reactors, distillation columns,…
2		Medium	Catastrophic failure of smaller equipment	In process installation or near buildings, public areas.	Failure of heat exchanger containing LPG
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		Opening of atmospheric PSV on LPG sphere.
3			Catastrophic failure of smaller equipment	Not near process installation nor near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
4		Small	Limited release in quantity and time.		Small leakage through packing. Sample point. Thermal safety valve.

Table 6.3 Category definition for flammable gas.

Flammable gas					
Cat.	**Product - phase**	**Size of release**	**Type of release**	**Location of release**	**Remarks - examples**
2	**Flammable gas**	Large	Catastrophic failure of vessel	-	Large gas mixing vessel.
3		Medium	Catastrophic failure of smaller equipment	In process installation or near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
4			Catastrophic failure of smaller equipment	Not near process installation nor near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
5		Small	Limited release in quantity and time.		

Table 6.4 Category definition for flammable liquid.

Flammable liquid (> C5)					
Cat.	**Product - phase**	**Size of release**	**Type of release**	**Location of release**	**Remarks - examples**
2	**Flammable liquid**	Large	Catastrophic failure of vessel	-	Hexene storage tank.
3		Medium	Catastrophic failure of smaller equipment	In process installation or near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
4			Catastrophic failure of smaller equipment	Not near process installation nor near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
5		Small	Limited release in quantity and time.		

Table 6.5 Category definition for toxic gases.

Toxic Gasses					
Cat.	**Product - phase**	**Size of release**	**Type of release**	**Location of release**	**Remarks - examples**
1		Large	Catastrophic failure of vessel	-	
2		Medium	Catastrophic failure of smaller equipment	In process installation or near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
3			Catastrophic failure of smaller equipment	Not near process installation nor near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
4		Small	Limited release in quantity and time.		

Table 6.6 Category definition for toxic liquids.

Toxic Liquids					
Cat.	**Product - phase**	**Size of release**	**Type of release**	**Location of release**	**Remarks - examples**
2		Large	Catastrophic failure of vessel	-	
3		Medium	Catastrophic failure of smaller equipment	In process installation or near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
4			Catastrophic failure of smaller equipment	Not near process installation nor near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
5		Small	Limited release in quantity and time.		

Table 6.7 Category definition for toxic solids.

Toxic solids					
Cat.	**Product - phase**	**Size of release**	**Type of release**	**Location of release**	**Remarks - examples**
3		Large	Catastrophic failure of vessel	-	
4		Medium	Catastrophic failure of smaller equipment	In process installation or near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		
5			Catastrophic failure of smaller equipment	Not near process installation nor near buildings, public areas.	
			Not from catastrophic failure but from leakage point or opening of atmospheric safety relief valve		

Table 6.8 Category definition for fire.

FIRE			
Cat.	**Size of fire**	**Consequences of fire**	**Remarks - examples**
2	Large	Large fire that may expand outside production unit.	Catastrophic failure of vessel containing large amount of flammable liquid above ignition temperature.
3	Medium	Leading to important fire that is contained within production unit.	Release of Pyrophoric liquid (e.g. teal)
4	Small	Small local fire.	Extruder fire. Small release of H_2 via atmospheric pressure relief valve.

Table 6.9 Borealis risk matrix, category class and initiating event gives the required risk reduction.

Category			10	100	1000	10.000
Cat. 1	-	-	SIL 1	SIL 2	SIL 3	SIL 4
Cat. 2	-	-	-	10 SIL 1	100 SIL 2	1000 SIL 3
Cat. 3	-	-	-	-	10 SIL 1	100 SIL 2
Cat. 4	-	-	-	-	-	10 SIL 1
Cat. 5	-	-	-	-	-	-
	Extremely rare	Rare	Possible	Occasionally	Probable	Frequent
	10^{-5}	10^{-4}	10^{-3}	10^{-2}	10^{-1}	10^{-0}

Table 6.10 Standard values of risk reduction for protection layers.

Device	Risk Reduction	Remarks
Mechanical Devices		
Pressure relief valve	100	Clean service. Well designed, fabricated, installed and tested. Test documented.
Pressure relief valve	10	Difficult application (dirt, corrosion, polymerizing product, etc.) Well designed, fabricated, installed and tested. Test documented.
Rupture disc	100	Clean service. Well designed, fabricated, installed and tested. Test documented.
Rupture disc	10	Difficult application (dirt, corrosion, polymerizing product, etc.) Well designed, fabricated, installed and tested. Test documented.
Mechanical overspeed protection	10	Tested regularly according to Vendor prescription and freq. depending on test results . Test documented.
Key-locked valve (car sealed)	10	Key-lock is used for scenarios where maloperation off valve is initiating event.
Check valve	10	Clean service. Suited for application. Well designed, fabricated, installed and with documented min. annual test Exact test interval depending on success of conducted tests

Table 6.11 Standard values of risk reduction for protection layers.

Instrumentation		
BPCS control loop (DCS or PLC)	10	Acc. to IEC-61511 max obtained risk reduction is 10
SCIS	SIL1 to SIL3	All in accordance to IEC-61508 and IEC-61511.
Human intervention		
Operator response	1	Under stress, average training
Operator response	10	Operator response to alarms and procedures, low stress, recognised event (note 1).
Operator response	100	Operator response to alarms and procedures, low stress, recognised event with more than 24 hours to resolve the problem (note 1).
Normal operator procedure	10	Procedure, depending on one operator (note 2).
Special operator procedure	100	Special procedure, depending on 2 different persons, fully independent (note 2).
Post release protection		
Dikes, fire walls, containment, etc.	100	Design and implementation must be in accordance to applicable standards. Regular inspection and maintenance required and documented.

Appendix 7 Interview formula

Lomake haastattelu/Interview formula

Nimi/Name: _____

Ikä/Age: _____

Koulutus/Education:
_____
_____
_____
_____

Ammatti/Profession:_____

Yritys/Company:
_____

Puhelin/Phone:_____
Sähköposti/email:_____

Experience of methods / Kokemusta metodia: (HAZOP/SEQHAZ/Risk graph/LOPA)
_____
_____
_____

Päivämäärä/Date: _____

Appendix 8 Interview questions for HAZOP and SEQHAZ®

This is a list of the interview questions for HAZOP and SEQHAZ® that was sent out to the interviewees before the interviews. Because of the interview was in discussion form the order of the questions was not followed strictly. Other questions were also asked that came up along with the interview but they are out of practical reason not listed here.

HAZOP

Is the HAZOP method easy to use and understand?

What are the advantages with the method?

What are the problems with the method?

Is the result of the method good enough? Is it too conservative or too careless?

How can we make the HAZOP more efficient?

What information do you need from HAZOP when performing safety integrity level evaluation?

Should the HAZOP state what should be treated in the safety integrity level evaluation?

After finishing evaluating a process section, is it possible to make a summary of the safety instrumented functions needed for the section?

SEQHAZ®

Is the SEQHAZ® method easy to use and understand?

What are the advantages with the method?

What are the problems with the method?

Is the result of the method good enough? Is it too conservative or too careless?

How can we make the SEQHAZ® more efficient?

What information do you need from SEQHAZ® when performing safety integrity level evaluation?

After finishing evaluating a process section in SEQHAZ®, is it possible to make a summary of the safety instrumented functions needed for the section?

Comparison between HAZOP and SEQHAZ®

If you compare HAZOP with SEQHAZ®, what are the differences?

Should you have different method for different types of projects?

General questions

How do you use old HAZOP/SEQHAZ®-reports in the most effective way for updating HAZOP/SEQHAZ€ reports?

What is the most unclear point in the HAZOP/SEQHAZ- SIL evaluation chain and how would you like to improve it?

Have tiredness or stress in your opinion sometimes affected the decision made in a hazard study?

Appendix 9 Interview questions for safety integrity level evaluations

This is a list of the interview questions for SIL evaluations that was sent out to the interviewees before the interviews. Because of the interview was in discussion form the order of the questions was not followed strictly. Other questions were also asked that came up along with the interview but they are out of practical reasoned not listed here.

Risk graph

Is the risk graph method easy to use and understand?

What are the advantages with the method?

What are the problems with the method?

Is the result good enough? Is it too conservative or too careless?

How can we make the risk graph method more efficient?

Is it possible to define typical process unit's risks in a way that during the SIL evaluation with risk graph they always get the same parameter values for W and P?

LOPA

Is the layer of protection analysis method easy to understand?

What are the advantages with the method?

What are the problems with the method?

Is the result good enough? Is it too conservative or too careless?

How can we make the LOPA method more efficient?

How do you include economical risk in LOPA?

Comparison between risk graph and LOPA

If you compare risk graph and LOPA, what are their strengths and weaknesses?

Is it better to use risk graph in some cases and LOPA in others?

General questions

Should HAZOP analysis state what should be treated in the SIL evaluation? By for example risk ranking?

When one process part have been analysed in HAZOP or SEQHAZ® is it possible to make a summary that defines which safety instrumented functions are needed for this process part?

What is the connection from HAZOP/SEQHAZ® to SIL evaluation, which base information from the hazard study is used?

What is the most unclear point in the HAZOP/SEQHAZ® - SIL evaluation chain and how would you like to improve it?

Have tiredness or stress sometimes affected the decision made during a SIL evaluation?

Appendix 10 Suggestion for consequence criteria for risk matrix based on LOPA model

Table 9.1 Suggestion for consequence criteria for risk matrix based on LOPA model. (Salo, 2006)

	Major accident			
Type of consequence	**C Catastrophic**	**V Very serious**	**S Serious**	**M Minor**
Consequences to humans	Several deaths or many seriously injured.	One death. Permanent disability to work. Permanent serious defect. Significant exposure to toxicants.	Long sick leave. Temporary disability. Serious injury that may heal up. Exposure leading to symptoms.	Consequences lesser than the serious ones.
Environmental damage	Large-scale destruction of the soil, groundwater, water system, flora or fauna outside the plant area. Permanent effects.	Large-scale pollution of the soil, groundwater, water system, flora or fauna at the plant area. Serious, but amendable or recoverable damage outside the plant area.	Local or minor pollution of the soil, groundwater or water system. Emission to the water system exceeding the terms of licence.	
Material damage (to be defined by case)	Over 6 months interruption of production or deliveries. Own or customer's damages over 100 million €. International or domestic media event.	1 – 6 months interruption of production or deliveries. Own or customer's damages 20 – 100 million €. Negative publicity in local media.	3 days – 1 month interruption of production. Damages 2 – 20 million €.	

Appendix 11 Suggestion for likelihood criteria for risk matrix based on LOPA model and risk graph model

Table 10.1 Suggestion for likelihood criteria for risk matrix based on LOPA model and risk graph model. (Turkkila, 2004)

Likelihood	Probability of occurrence / year
low = 1	$< \frac{1}{30}$
moderate = 2	$\frac{1}{30} - \frac{1}{3}$
high = 3	$> \frac{1}{3}$ (still $\leq$1 time/year)