RAMS


# Determination of Safety/Environmental Integrity Level for Subsea Safety Instrumented Systems

Jun Zhou

July 18th 2013

Master thesis

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Supervisor 1: Jørn Vatn

Supervisor 2: Stein Hauge

NTNU

Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

Date 2013.04.10

Our reference JV/KEDA

# MASTER THESIS

**2013**

**for**

**stud. techn. Jun Zhou**

**Determination of safety integrity levels for subsea safety system based on environmental risk acceptance criteria**

**(Fastsettelse av integritetskrav for undervanns sikkerhetssystemer med utgangspunkt i risikoakseptkritierier for miljøforhold.)**

In recent years much work has been carried out to develop concepts and methods to assess reliability of safety instrumented systems (SIS). The focus has mainly been on so-called low demand systems operated under static conditions. The Deepwater Horizon disaster has demonstrated also the importance of the reliability of subsea components such as the blowout preventer (BOP) where the dynamic nature of drilling and well activities has to be taken into account. It is also recognized that less work has been done in relation to determine the reliability requirements, or the so-called safety integrity level (SIL) for a SIS. In this master thesis the candidate shall therefore investigate methods for determination of safety integrity levels for subsea safety systems. Especially the candidate shall:

1. Carry out a literature study of different SIL determination methods like risk graph, safety layer matrix, and LOPA
2. Discuss pros and cons of different SIL determination methods
3. Discuss in particular challenges with applying LOPA when there is dependencies between the SIS and other layers of protection
4. Identify challenges encounters when the consequence dimension is environment in contrast to the more familiar personnel risk
5. Based on the results obtained, propose a method for determination of SIL in the given context, and test the method in a simple case study

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

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

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

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

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

The candidate shall follow the work regulations at the company's plant. The candidate may not intervene in the production process in any way. All orders for specific intervention of this kind should be channelled through company's plant management.

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

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

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

Deadline: 1st August 2013.

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

Responsible supervisor:

Professor Jørn Vatn
E-mail: jorn.vatn@ntnu.no
Phone: 73 59 71 09

**DEPARTMENT OF PRODUCTION AND QUALITY ENGINEERING**

Per Schjølberg
Associate Professor/Head of Department

Jørn Vatn
Responsible Supervisor

## Pre-face

The master thesis was written during the spring semester 2013, at Department of Production and Quality Engineering, Norwegian University of Science and Technology (NTNU). It is the final part of graduating as an Engineer from Master of Science in RAMS (Reliability, Availability, Maintainability and Safety).

The title of this thesis is "Determination of Safety/Environmental Integrity Level for Subsea Safety Instrumented Systems". The main objective is to investigate the risk based approaches of SIL determination for subsea applications where the environmental consequences shall be included in the analysis. Relevant challenges in such SIL determination context are identified and some approaches are proposed following the discussions. It is assumed that the reader has some knowledge in risk and reliability analysis and safety instrumented systems. It is preferable to have some knowledge of IEC 61508 and IEC 61511.

I wish to thank my supervisor Professor Jørn Vatn at Department of Production and Quality Engineering for his invaluable guidance throughout the entire master thesis project. I am also very grateful to Stein Hauge from SINTEF for his constructive comments on some important chapters of this thesis.

Jun Zhou

Trondheim, Norway. 18th July 2013

## Summary

The master thesis describes, compares current methods in the literature, and proposes new methods for determination of safety/environmental integrity level of safety instrumented systems (SISs). These systems are used widely in many industry sectors to detect the onset of hazardous events and mitigate the consequences to humans, the environment and material assets.

The main objective of this thesis has been to investigate the risk based approaches for determination of safety /environmental integrity level of SISs. The focus of the thesis is the risk graph and layer of protection analysis approach for subsea applications where the failure of such systems could lead to significant environmental consequences. The thesis builds on concepts, methods and definitions adopted in two main standards for SIS applications: IEC 61508 and IEC 61511. The proposals of new methods are inspired by these two standards and other relevant literature found during the master thesis project.

The main contributions of this thesis are:

1. Discussion on current environmental risk acceptance criteria used on Norwegian Continental Shelf and proposal of new environmental risk acceptance criteria based on release volume for subsea SISs applications where the consequences of hazardous events include environmental damages.
2. A modified risk graph approach suited for SIL/EIL determinations for subsea SISs. This approach is demonstrated and tested in a case study.
3. Detailed discussion on the effect of common cause failures between the designated SIS and the existing protection layers during SIL/EIL determination. A framework for determining SIL/EIL considering such CCFs is developed. This framework includes CCFs quantification in two phases: SIL determination phase and SIL realization phase. A checklist is developed for CCFs quantification in the early phase.

## Table of Contents

Pre-face ..... 1
Summary ..... 2
Chapter 1 Introduction ..... 7
1.1 Background ..... 7
1.2 Objectives ..... 9
1.3 Research approach ..... 10
1.4 Limitations and structure ..... 10
Chapter 2 SIL determination methods in the literature ..... 12
2.1 Hazard matrix ..... 12
2.2 Safety layer matrix ..... 14
2.3 OLF approach ..... 16
2.4 Risk graph ..... 18
2.5 Calibrated risk graph ..... 21
Chapter 3 Environmental risk acceptance criteria – literature review and discussion ..... 24
3.1 Introduction ..... 24
3.2 MIRA environmental risk acceptance criteria ..... 24
3.3 Discussion ..... 27
3.2 Alternative ERAC related to requirements for technical safety barriers ..... 27
Chapter 4 Calibrated risk graph for subsea applications ..... 30
4.1 Introduction ..... 30
4.1 A proposed method --- marinized risk graph ..... 30
4.2 A case study on drilling BOP ..... 35
Chapter 5 Layer of protection analysis (LOPA) ..... 37
5.1 Introduction ..... 37
5.2 The LOPA team ..... 38
5.3 The LOPA work sheet ..... 39
5.4 The LOPA process ..... 41
5. 5 Strength and limitations of LOPA ..... 43
5. 6 HAZOP and the interface with LOPA ..... 44
Chapter 6 Considering CCFs in SIL determination ..... 46

6.1 Introduction ..... 46
6.1 Illustration of CCF affecting risk reduction ..... 47
6.2 Checklist of quantifying CCF in SIL determination phase ..... 50
6.3 Some challenges of CCFs quantification of two different protection layers in the SIS realization phase ..... 52
6.3.1 Which model to choose to quantify the CCFs? ..... 53
6.3.2 How to quantify CCFs among components with different failure rates? ..... 53
6.3.3 How to Select Beta factors for non-identical components ..... 54
6.3.4 How to select test interval for components with non-identical intervals ..... 54
6.4 A case study on LOPA taking into account CCFs ..... 55
Chapter 7 Discussion ..... 58
Chapter 8 Conclusions and further work ..... 59
References ..... 61
Appendix I – Acronyms and Abbreviations ..... 63
Appendix II – LOPA results for the case study ..... 65
Appendix III – Checklist results for the case study ..... 65

Table 1 Safety/Environmental Integrity Levels (adapted from IEC 61508, 2010) ..... 7
Table 2 The sources of scientific literature ..... 10
Table 3 An example of consequence categories for hazard matrix ..... 13
Table 4 An example of likelihood categories (adapted from Marszal and Scharpf 2002) ..... 13
Table 5 Minimum SIL requirements - subsea safety functions (OLF 070, 2004) ..... 16
Table 6 Example of categorization of risk parameters (IEC 61508, 2010) ..... 19
Table 7 An example of risk graph calibration (IEC 61511, 2004) ..... 21
Table 8 Current risk acceptance criteria for environmental risk (adapted from Vinnem, 2007) ..... 25
Table 9 Possible ERAC when defining 5% as “insignificant” frequency of harm to the environment (MIRA guideline 2007) ..... 26
Table 10 Recommended ERAC for different categories of vulnerability area (inspired by Hauge, et al, 2010) ..... 28
Table 11 An example of categorization of environmental damage based on release volumes ..... 29
Table 12 Recommended ERAC for medium vulnerability environment (Adapted from Hauge, et al, 2010) ..... 29
Table 13 An example of categorization of environmental damage based on release volume ..... 31
Table 14 Vulnerability categorization based on scoring of influencing factors ..... 32
Table 15 Scoring results of vulnerability factors for the case study ..... 35
Table 16 ERAC for high vulnerability environment ..... 35
Table 17 An example of LOPA worksheet (IEC 61511, 2004) ..... 40
Table 18 Results of fault tree calculation ..... 48
Table 19 Checklist for CCFs in SIL determination phase ..... 51
Table 20 CCFs fraction in relation with checklist scoring ..... 52
Table 21 HAZOP study results (adapted from IEC 61511, 2004) ..... 55
Table 22 LOPA worksheet for the case study ..... 65
Table 23 Checklist results for the case study ..... 66

Figure 1 Safety lifecycle (IEC 61508, 2010) ..... 9
Figure 2 Risk reduction model (IEC 61508, 2010) ..... 12
Figure 3 Typical hazard matrix for SIL selection (adapted from Marszal and Scharpf, 2002) ..... 14
Figure 4 An example of safety layer matrix (adapted from IEC 61511, 2004) ..... 15
Figure 5 Flowchart – development of SIL requirements (OLF 070, 2004) ..... 17
Figure 6 Risk interpretation in general risk graph approach ..... 18
Figure 7 Risk graph (Adapted from IEC 61508) ..... 21
Figure 8 Illustration of the MIRA guideline example of assumed activity level (Hauge et al., 2010) .. 26
Figure 9 General scheme of marinized risk graph ..... 31
Figure 10 An example of SIL calibration ..... 33
Figure 11 Calibrated risk graph for subsea applications ..... 34
Figure 12 SIL determination illustration ..... 36
Figure 13 Protection layers (adapted from IEC 61511, 2004) ..... 37
Figure 14 LOPA as a special type of event tree (adapted from Marszal and Scharpf, 2002) ..... 38
Figure 15 Types of initiating events (adapted from CCPS, 2001) ..... 42
Figure 16 HAZOP workflow and the interactions with LOPA ..... 45
Figure 17 Risk reduction for high demand applications(adapted from IEC 61508, 2010) ..... 46
Figure 18 Illustration of risk reduction considering CCF (adapted from IEC 61508, 2010) ..... 47
Figure 19 Fault tree accounting for CCF ..... 48
Figure 20 Framework for SIL determination incorporating CCF ..... 49
Figure 21 Timeline process of SIL determination in relation with safety lifecycle ..... 50
Figure 22 Illustration of CCF fraction ..... 52
Figure 23 Illustration of the process ..... 55
Figure 24 General concept of the new SIS ..... 57

# Chapter 1 Introduction

## 1.1 Background

Safety instrumented systems (SISs) are widely used in petroleum and process industry to prevent hazardous events and mitigate consequences to humans, the environment and material assets. A SIS is generally composed of input elements (e.g. sensors, transmitters), logic solvers (e.g. programmable logic controllers, relay logic systems) and final elements (e.g. safety valves). IEC 61508 as a generic standard has gained wide acceptance across a range of industries to facilitate the design and implementation of such safety systems. One important aspect of this standard and the industry specific standards, e.g. IEC 61511 for process industry, is how to systematically develop safety requirements for these systems to meet the risk acceptance criteria.

Safety integrity level (SIL) is a fundamental concept in IEC 61508, and per definition it is "probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period of time" (IEC 61508). The term Integrity level (IL) is also used in the petroleum industry. It can either be Environmental integrity level (EIL) or Safety integrity level (SIL). It is further stated in the report by Eni-Norge that when analyzing systems with regard to safety and environment, the final integrity level will be the higher of the two determined levels (Eni-Norge, 2010). As both IEC 61508 and IEC 61511 mainly concern risk to personnel, the term SIL is used. It should be noted that, in this thesis report, both terms are used and in some cases they are not specifically differentiated, as both of them refer to the same concept. The reader may also find that the title of the thesis has been changed to include both SIL and EIL in SIL determination context considering both personnel and environmental risk instead of only referring to SIL.

IEC 61508 defines four discrete integrity levels for SISs. SIL 4 is the highest integrity level and SIL is the lowest. Each integrity level corresponds to a range of average probability of failure on demand (PFDavg) for low demand SIS and probability of a dangerous failure per hour (PFH) for high demand SIS. The four SILs/EILs are shown in Table 1.

**Table 1 Safety/Environmental Integrity Levels (adapted from IEC 61508, 2010)**

| Safety/Environmental Integrity Level (SIL, EIL) | Average probability of failure on demand ($PFD_{avg}$) | Probability of a dangerous failure per hour (PFH) |
|---|---|---|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | $\geq 10^{-9}$ to $< 10^{-8}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | $\geq 10^{-6}$ to $< 10^{-5}$ |

Lots of the literature deals with IL determination considering only personnel risk (SIL determination). The methods provided in the informative annexes of both IEC 61508 and IEC 61511 mainly deal with SIL determination situations where the consequences are harm to personnel. Marszal and Scharpf (2002) described systematic methods and techniques for determining safety integrity levels for SISs considering personnel risk. Berg (2007) discussed the applicability of LOPA method for SIL determination in the process industry. Lassen (2008) described different SIL determination methods, focusing on LOPA when the consequences are limited to harm to humans. Baybutt (2007) proposed an improved risk graph method where the consequence categories include both personnel safety and environmental impacts, but did not differentiate between SIL and EIL. SIL/EIL determination applications where the consequence of hazardous events includes environmental dimensions is less discussed. Another important issue which arises with environmental risk is the environmental risk acceptance criteria (ERAC). The ERAC in relation to SIL determination is less discussed or ignored.

IEC 61508 adopts a safety lifecycle as the basic framework in order to systematically organize requirements and activities associated with design, implementation and operation of safety instrumented systems. The safety lifecycle is comprised of 16 phases and is shown in Figure 1. IEC 61511 uses a similar safety lifecycle framework. The initial five phases (1-5) lead up to the functional safety requirements, stating what the SIS is required to do, and the safety integrity requirements, stating how well the SIS is required to perform (Lundteigen, 2008). Phase 4 deals with the overall safety function. The overall safety requirements is specified in terms of the overall safety functions requirements and overall safety integrity requirements. The allocation of SIL to the designated SISs and other risk reduction measures is conducted in phase 5.

The SIL allocation is an iterative process. If it is found that the tolerable risk cannot be achieved, then the allocation shall be repeated. IEC 61508 states that the allocation shall proceed taking into account the possibility of common cause failures (CCFs). However, the current methods do not explicitly treat the CCFs between the designated SIS and other risk reduction measures when determining the SIL. The iterative process of SIL determination in relation with CCFs is further discussed in Chapter 6.

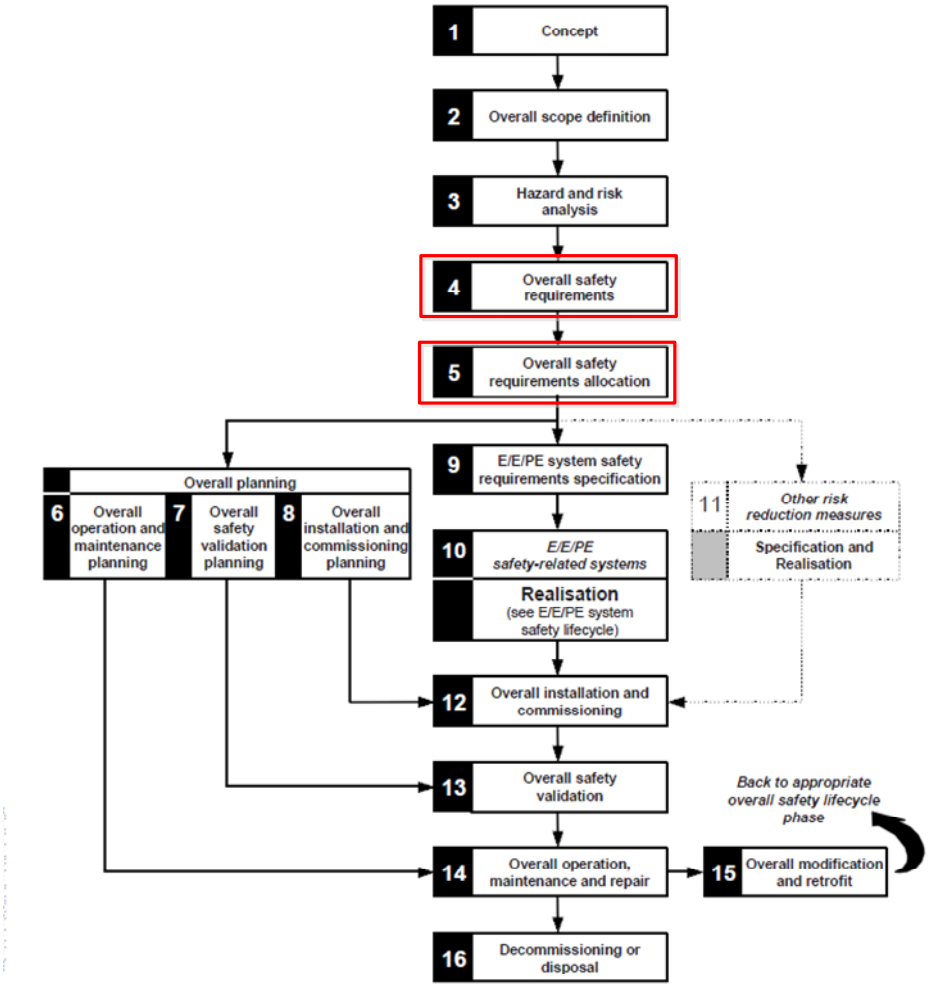



**Figure 1 Safety lifecycle (IEC 61508, 2010)**

## 1.2 Objectives

The master thesis is intended to investigate the risk based approaches for determination of safety /environmental integrity level of SISs. The focus of the thesis is risk graph approach and LOPA approach for subsea SISs where the failure of such systems could lead to significant environmental consequences. To fulfill the main objective, following tasks have been covered in the thesis:

1. Carry out a literature study of different SIL determination methods like risk graph, safety layer matrix, and LOPA
2. Discuss pros and cons of different SIL determination methods
3. Discuss in particular challenges with applying LOPA when there are dependencies between the SIS and other layers of protection
4. Identify challenges encounters when the consequence dimension is environment in contrast to the more familiar personnel risk

5. Based on the results obtained, propose a method for determination of SIL in the given context, and test the method in a simple case study

## 1.3 Research approach

In order to fulfill the objective of the master thesis, a specific research approach is adopted and followed. Based on the main objective and sub-objectives presented earlier, the most suitable approach in the beginning of the master thesis project is theoretical study based on the relevant literature. Table 2 shows the sources of the scientific literature. After acquiring knowledge of current methods in the literature, challenges and shortcoming of current methods are discussed. The development of new methods is based on literature study and discussion with the supervisors. The proposed new methods are then demonstrated and tested by case studies.

**Table 2 The sources of scientific literature**

| | Literature sources | | | | |
|---|---|---|---|---|---|
| Search engines | Google scholar | Google | | | |
| Databases/ Journals | Scopus[1] | Scirus[2] | Science direct[3] | Springer Link | Reliability engineering & system safety |
| Books/Previous master thesis/ Standards | NTNU library | ROSS Gemini Centre - master thesis[4] | NS, NEK, ISO and NORSOK standards[5] | | |

1. http://www.scopus.com/home.url
2. http://www.scirus.com/
3. http://www.sciencedirect.com/
4. https://www.ntnu.edu/ross/publications/msc-thesis
5. http://www.standard.no/

## 1.4 Limitations and structure

This thesis is mainly concerned with SIS applications in petroleum and process industry. Most SIL determination methods have been covered, but the quantitative risk analysis (QRA) approach for SIL determination is not discussed. The thesis is mainly concerned with SIL/EIL determination applications for subsea safety instrumented systems where the consequence includes environmental damages to the sea. Relevant issues and challenges related with this are discussed in greater details, e.g. ERAC, CCFs.

The thesis is organized as follows. An introduction to the thesis is given in Chapter 1, including background, objectives and limitations. Chapter 2 presents the various SIL determination methods found in the literature. Pros and cons of each method are discussed

following the presentation of each method. In chapter 3, the ERAC related with subsea applications where the consequences of hazardous events include acute release to sea have been thoroughly discussed. Alternative ERAC are proposed to suite developing requirements, for instance, SIL/EIL requirements for technical safety barriers. In chapter 4, a new risk graph method specifically considering environmental consequences of subsea applications is proposed and tested in a drilling BOP case study. Chapter 5 presents LOPA approach for SIL determination followed by discussion of its strengths, limitation and interfaces between LOPA and HAZOP. Common cause failures between the designated SIS and existing protection layers are discussed in details and a framework for including CCFs analysis in SIL determination is proposed in Chapter 6. The framework and checklist of initial CCFs quantification is demonstrated and tested in a case study. A discussion on the proposed methods, especially the weaknesses are presented in Chapter 7. Chapter 8 gives conclusions and recommendations for further work.

# Chapter 2 SIL determination methods in the literature

A safety instrumented system implements the required safety functions necessary to achieve a safe state for the equipment under control (EUC) or to maintain a safe state for the EUC (IEC 61508, 2010). It is installed to provide necessary risk reduction in order to meet the tolerable risk. Figure 2 illustrates the risk reduction concept adopted in IEC 61508. The SIL determination starts from assessing EUC risk. The EUC risk is a function of the risk associated with the EUC itself but taking into account the risk reduction brought about by the EUC control system. The necessary risk reduction is the gap between the EUC risk and tolerable risk. It is normally achieved by a combination of different risk reducing measures. If the risk is found unacceptable, a safety instrumented system may be required and a safety integrity level must be determined. The SIL shall correspond to the average probability of failure on demand (PFDavg) for low demand SIS and probability of a dangerous failure per hour (PFH) for high demand SIS.

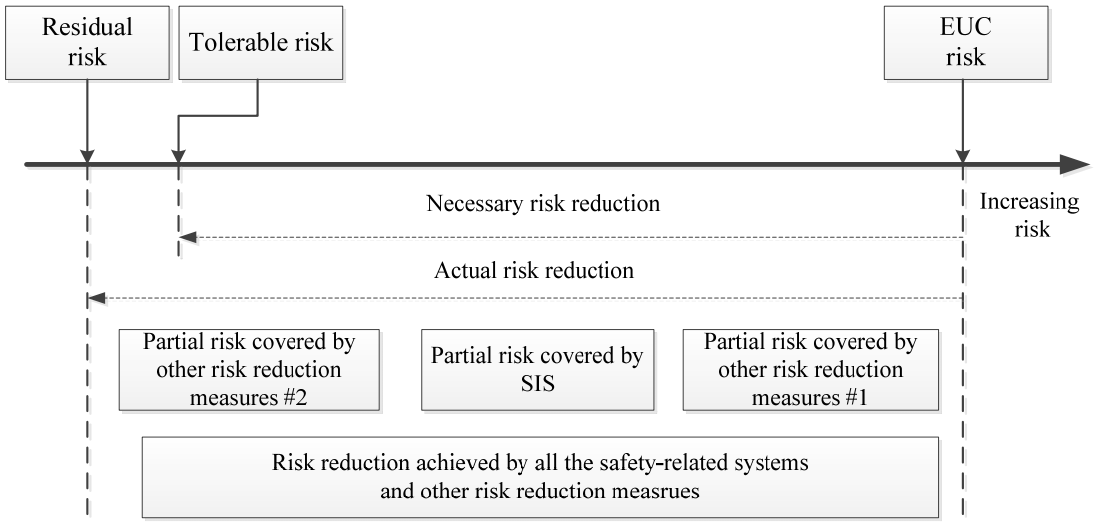



**Figure 2 Risk reduction model (IEC 61508, 2010)**

There are different methods in the literature for SIL determination, which include hazard matrix, safety layer matrix, (calibrated) risk graph and LOPA. These methods are presented in the following sections.

## 2.1 Hazard matrix

The hazard matrix method of determining SIL is one of most popular SIL assignment method, because it is straightforward and can be applied easily (Marszal and Scharpf, 2002). It is also denoted risk matrix in some literatures. The following presentation of hazard matrix for SIL determination is based on Marszal and Scharpf (2002).

The hazard matrix is qualitative and category based method. In order to use this method, the user should first assign categories to the consequence and likelihood components of the risk.

For instance, consequence can be divided into categories as “minor”, “serious”, or “catastrophic”. The likelihood categories can be assigned as “low”, “moderate” or “high”.

The consequence categories can be expressed in terms of fatalities, environmental damage or financial losses. Usually the analyst selects the category completely qualitatively, based on his or her own engineering judgment. Sometimes the analyst makes the assignment with the help of consequence analysis and calculation. Table 3 shows an example of consequence categorization based on environmental damage to the sea. The restitution time in the table is the time needed for the sea to return to its original state after being affected by the pollution.

**Table 3 An example of consequence categories for hazard matrix**

| Consequence category | Description |
|---|---|
| Minor | Environmental damage with restitution time between 1 month and 1 year |
| Serious | Environmental damage with restitution time between 1 and 10 years. |
| Catastrophic | Environmental damage with restitution time in excess of 10 years. |

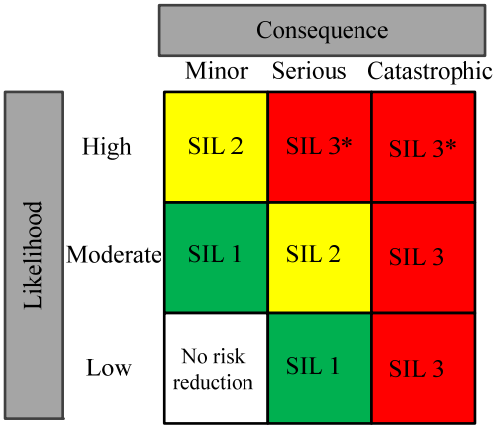
Similar to consequence, the likelihood component of the risk is also divided into different categories. Most commonly, 3 to 5 categories of likelihood are used in hazard matrix (Marszal and Scharpf, 2002).. Table 4 shows an example of three categories. Expert judgment is often used to select the proper category of likelihood. In some cases, quantitative tools, such as layer of protection analysis, are used to facilitate the selection of proper likelihood category (Marszal and Scharpf, 2002). It is important to note that the likelihood selected to this stage is the likelihood at which the event would occur without considering the effect of SIS under consideration. However, the existing protection layers in the process must be considered.

**Table 4 An example of likelihood categories (adapted from Marszal and Scharpf 2002)**

| Likelihood category | Frequency (per year) | Description |
|---|---|---|
| Low | Less than $10^{-4}$ | A failure or series of failures with a very low probability that is not expected to occur within the lifetime of the installation |
| Moderate | $10^{-2}$ to $10^{-4}$ | A failure or series of failures with a low probability that is not expected to occur within the lifetime of the installation |
| High | Higher than $10^{-2}$ | A failure or series of failures can reasonably be expected within the lifetime of the installation |

Figure 3 illustrates a typical hazard matrix which incorporates 3 categories for both consequence and likelihood. The consequence and likelihood each form an axis of the matrix, while each box of the matrix contains an SIL level. The analyst determines which box of the

matrix corresponds to the selected categories of consequence and likelihood and selects the SIL in that box to reduce the risk under consideration. The SIL represents the amount of risk reduction required. The tolerable level of risk is implied by the structure of the matrix based on which SIL is in which box (Marszal and Scharpf, 2002).




*One SIL 3 SIF may not provide enough risk reduction

**Figure 3 Typical hazard matrix for SIL selection (adapted from Marszal and Scharpf, 2002)**

The advantage of hazard matrix is its simplicity and straightforwardness to use. It can be applied to different types of consequence, e.g. fatalities, property and environmental damage. It is also limited by its simplicity and qualitative nature. The selection of proper SIL relies on the engineering judgment of the analyst to a large extent. It doesn't have a separate dimension to represent and assess existing layer of protection. In order to make a reasonable and objective judgment, the analyst has to use other quantitative tools such as LOPA to quantify the effect of existing protection layers (Marszal and Scharpf, 2002).

## 2.2 Safety layer matrix

Safety layer matrix is a variation of hazard matrix which uses a third dimension to represent the protection layers available to prevent the hazardous event under consideration. It is described in Annex G of IEC 61508 (denoted as hazardous event severity matrix) and more extensively in Annex C of IEC 61511-3, which the following presentation is based on.

According to the definition in IEC 61511-3 Annex C, a Protection Layer (PL) is a grouping of equipment and/or administrative controls that function in concert with other protection layers to control or mitigate process risk. A PL meets the following criteria (IEC 61511, 2004):

- Reduces the identified risk by at least a factor of 10.
- Specificity – designed to prevent or mitigate the consequences of hazardous event.
- Independence – independent of other protection layers. There is no potential for common cause or common mode failure with any other claimed PL.
- Dependability – can be counted on to do what it was designed to do.

- Auditability – designed to facilitate regular validation of the protective functions.

The implementation of safety layer matrix starts from establishment of the process safety target level. The process safety target level is specific to a process, a corporation or industry and therefore should not be generalized unless existing regulations and standards support for such generalization. The second step is to perform a hazard analysis, using qualitative tools such as what if analysis, HAZOP and FMECA. After the HAZOP study, the analyst should assess the likelihood, consequences and impact of potential hazardous events. Guidance on how to estimate the likelihood and consequence severity of hazardous events has been provided in the IEC 61511-3, in the form of tables. It should be noted that the likelihood is estimated without considering the effect of existing PLs. The estimates of likelihood and consequence should be preferably based on plant specific data, expertise and experience. Figure 4 illustrates an example of safety layer matrix.

| Number of PL's | SIL level required | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | - | - | - | | | | c) | SIL 1 | SIL 1 |
| 2 | c) | c) | SIL 1 | c) | SIL 1 | SIL 2 | SIL 1 | SIL 2 | SIL 3 b) |
| 1 | c) | SIL 1 | SIL 2 | SIL 2 | SIL 2 | SIL 3 b) | SIL 3 b) | SIL 3 b) | SIL 3 a) |
| Hazardous event likelihood | Low | Moderate | High | Low | Moderate | High | Low | Moderate | High |
| | Minor | | | Serious | | | Catastrophic | | |
| | Hazardous event severity rating | | | | | | | | |

a) One level 3 SIF does not provide sufficient risk reduction.

b) One level 3 SIF may not provide sufficient risk reduction.

c) SIS independent protection layer is not needed.

**Figure 4 An example of safety layer matrix (adapted from IEC 61511, 2004)**

Compared to hazard matrix, the safety layer matrix is a more comprehensive approach. It has a third dimension to represent the existing protection layers. However, it still relies largely on subjective judgment of the analyst when considering the consequence and likelihood of a hazardous event. Plant specific data and operation experience shall be developed and consulted.

## 2.3 The OLF approach

The following presentation of the OLF approach for SIL determination is based on the guideline OLF 070 (2004). OLF 070 guideline was originally developed by operators and the various suppliers of service and equipment to simplify the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum industry. Whereas IEC 61508 describes a fully risk based approach for determining SIL requirements, OLF 070 adopts minimum SIL requirements for most common safety functions on a petroleum production installation (OLF 070, 2004). The minimum SIL requirement is a deterministic approach based on the current technology and safety level in the Norwegian Petroleum industry. The calculation of minimum SILs are performed with "reliability of computer-based safety systems" (PDS) method developed by SINTEF. The minimum SIL levels are given in tables in chapter 7 of OLF 070. Table 5 shows an example of minimum SIL requirement of subsea ESD function.

Table 5 Minimum SIL requirements - subsea safety functions (OLF 070, 2004)

| Safety function | SIL | Functional boundaries for given SIL requirement /Comments |
|---|---|---|
| Subsea ESD Isolate one subsea well | 3 | Shut in of one subsea well.<br><br>The SIL requirement applies to a conventional system with flow line, riser and riser ESD valve rated for reservoir shut in conditions.<br>Isolation of one well by activating or closing:<br>- ESD node<br>- Topside Hydraulic (HPU) and/or Electrical Power Unit (EPU)<br>- Wing Valve (WV) and Chemical Injection Valve (CIV) including actuators and solenoid(s)<br>- Master Valve (MV)<br>- Downhole Safety Valve (DHSV) ) including actuators and solenoid(s)<br><br>Note) If injection pressure through utility line may exceed design capacity of manifold or flow line, protection against such scenarios must be evaluated specifically. |

OLF 070 also gives guidelines on handling of deviations from the minimum SIL requirements. A deviation, for instance, may be a safety function not covered by the minimum SIL table. These deviations need to be treated according to IEC 61508/61511 methodology. The overall methodology of OLF approach is illustrated in Figure 5.

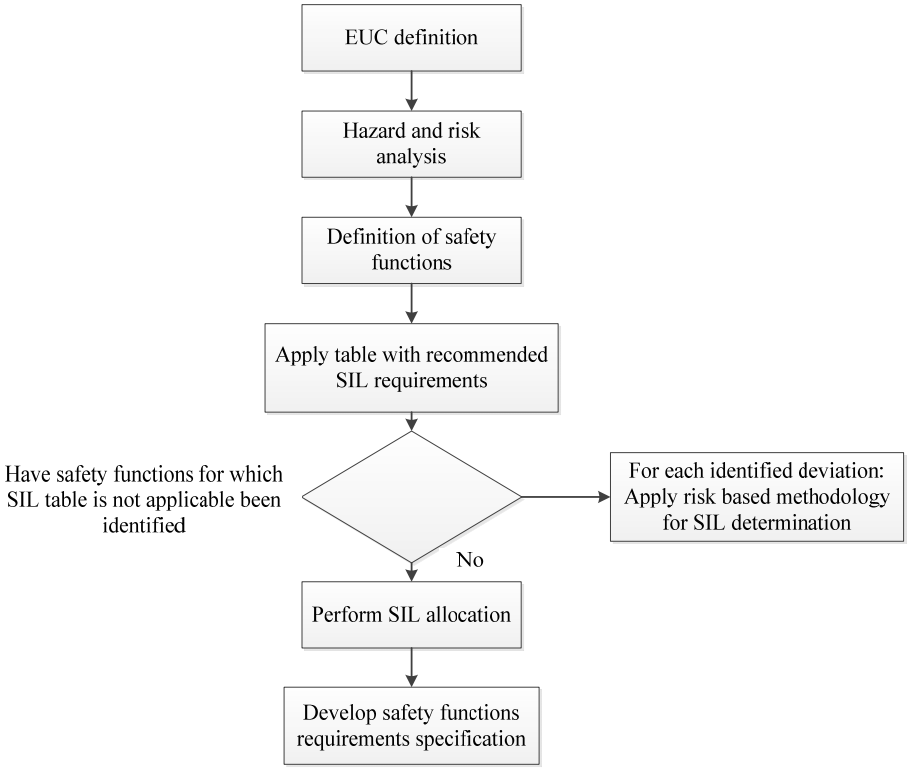



**Figure 5 Flowchart – development of SIL requirements (OLF 070, 2004)**

The advantages of OLF approach include: 1) It avoids time-consuming calculation in hazard and risk analysis; 2) It reduces documentation and simplify work process; 3) It ensures a performance level equal to or better than today's standard. However, there are also some pitfalls in this approach. It doesn't give considerations to specific conditions, design and operational philosophies of the installation under study. The minimum SIL table is based on generic reliability data, and this could give unrealistic SIL values (Cornelliusen, 2002). When using "conservative" failure rate and/or long test intervals for calculating the PFD of a given safety function, resulting in a high value (Rausand and Høyland, 2004). Thus a "low" SIL value will be claimed for the function, resulting in a "non-conservative" SIL requirement.

## 2.4 Risk graph

The risk graph presentation is based on IEC 61508 (2010) and IEC 61511(2004). Risk graph is a qualitative method which determines safety integrity level of a safety related system based on knowledge of the risk factors associated with the process and basic process control system. This approach assumes the safety instrumented systems under consideration fail or are not available in a hazardous situation, although typical non safety instrumented systems such as basic process control system (BPCS) and monitoring systems are in place. It uses a number of parameters which together describe the nature of hazardous event. One parameter is chosen from each of four sets and the selected parameters are then combined to determine the safety integrity level allocated to the safety instrumented function.

Risk graph is based on the principle that risk is proportional to the consequence of a hazardous event and its frequency. Typically in the risk graph approach, following four risk parameters are used to describe the nature of a hazardous event and select the SIL.

- consequence of the hazardous event (C)
- frequency of, and exposure time in, the hazardous zone (F)
- the possibility of avoiding the hazardous event (P)
- The probability of the hazardous event taking place without the addition of any safety related systems (but having in placed other risk reduction facilities) – this is termed the probability of the unwanted occurrence. (W)

Parameter values are combined together in order to estimate the risk of the hazardous event. The combination of C with F and P actually represent the effective consequence. W is the frequency of the hazardous event without the SIF under consideration in place but with other safe guards operating, hence the effective frequency. Risk graph combines the effective consequence with the effective frequency of the hazardous event to determining a SIL that will reduce the risk to a tolerable level (Baybutt, 2007).

Figure 6 illustrates the interpretation of risk by the four risk parameters in risk graph approach.

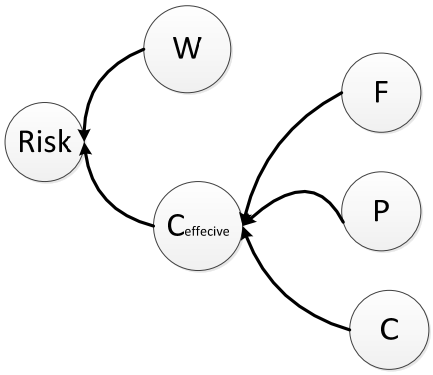



**Figure 6 Risk interpretation in general risk graph approach**

The risk graph is a category based method. Table 6 shows an example of categorization of the four risk parameters.

**Table 6 Example of categorization of risk parameters (IEC 61508, 2010)**

| Risk parameter | | Classification |
|---|---|---|
| Consequence (C) | $C_1$ | Minor injury |
| | $C_2$ | Serious permanent injury to one or more persons; death to one person |
| | $C_3$ | Death to several people |
| | $C_4$ | Very many people killed |
| Frequency of, and exposure time in the hazardous zone (F) | $F_1$ | Rare to more often exposure in the hazardous zone |
| | $F_2$ | Frequent to permanent exposure in the hazardous zone |
| Possibility of avoiding the hazardous event (P) | $P_1$ | Possible under certain conditions |
| | $P_2$ | Almost impossible |
| Probability of the unwanted occurrence (W) | $W_1$ | A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely |
| | $W_2$ | A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely |
| | $W_3$ | A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely |

Consequences are related to harm associated with health and safety of personnel or harm from environmental damage. In the example above, consequence parameter is defined as the expected number of fatalities and/or serious injuries likely to result from a hazard when the area is occupied. The parameter should include the expected size of the hazard and the

receptor's vulnerability to the hazard. It is determined by calculating the numbers in the exposed area when the area is occupied taking into account the vulnerability to the hazardous event (IEC 61511, 2004). This category ranges from minor injuries to multiple fatalities.

Occupancy is the probability that the exposed area is occupied at the time of the hazardous event. It is determined by calculating the fraction of time the area is occupied. (IEC 61511-3 2004)

The probability of avoidance parameter reflects the probability that the exposed persons are able to avoid the hazardous situation if the safety instrumented function fails on demand. It depends on the existing independent methods of alerting the exposed persons prior to the hazard occurring and methods of escape. The table 6 adopts two categories, P1 and P2, which is typical in risk graph analysis. In essence, the analyst selects the probability of avoidance category by evaluating a checklist that will determine whether avoidance credit can be taken or not. If credit for probability of avoidance can be taken, the analyst selects P1. Based on the example in IEC 61511-3, following conditions should be all met in order to select P1.

- The operator will be alerted if SIS has failed
- Facilities are provided for avoiding the hazard that are separate from the SIS and that enable escape from the hazardous area
- The time between operator's alert to a hazardous condition and the occurrence of the event is greater than on hour or is definitely sufficient for the necessary actions.

The last parameter is the demand rate of the hazardous situation. It is expressed in number of times per year that the hazardous event would occur in the absence of the safety instrumented function being studied, but considering all other non-SIS protection layers. It can be determined by considering all failures in which can lead to hazardous event and estimating the overall rate of occurrence (IEC 61511, 2004).

A typical risk graph is shown in Figure 7.

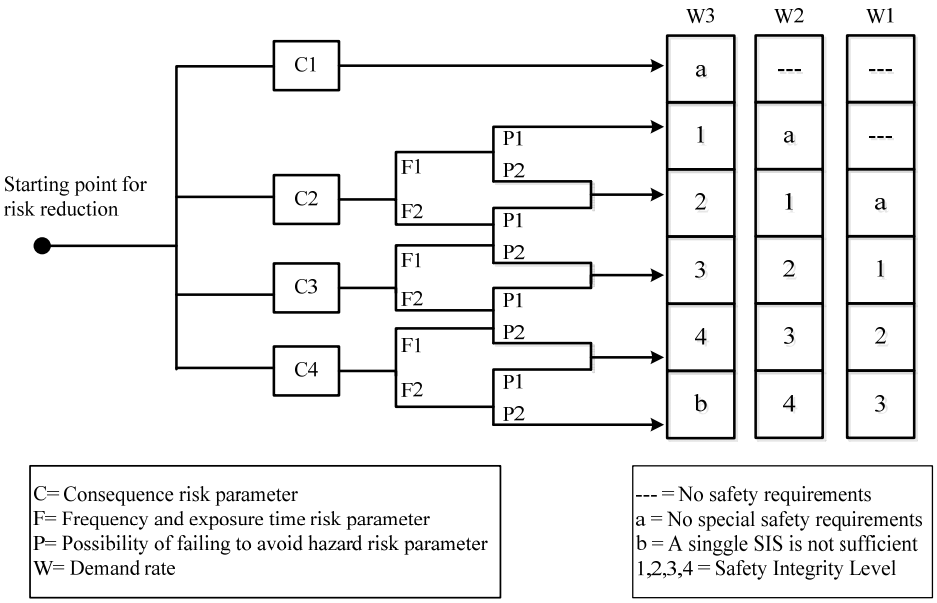



**Figure 7 Risk graph (Adapted from IEC 61508)**

## 2.5 Calibrated risk graph

Calibrated risk graph is a semi-qualitative and category based approach for determining integrity level of safety instrumented functions. As with the conventional risk graph, the 4 risk parameters are also used to select the SIL: consequence, occupancy, probability of avoiding the hazard, and the demand rate. Note that for risk graph application of SISs operating in continuous mode, the parameters used in risk graph shall be altered.

But each parameter is calibrated according to the risk acceptance criteria within the organization. Calibration of risk graph is the process of assigning numerical values to risk graph parameters. This allows the SIL assessment team to make objective judgments based on characteristics of the application and ensure the SIL selected for an application is accordance with corporate risk criteria. (IEC 61511, 2004). Table 7 shows an example of risk graph calibration from IEC 61511.

When considering the calibration of risk graphs, it is important to consider requirements relating to both individual risk and societal risk. Fatal accident rate (FAR) can be used to quantify individual risk. For example, the risk acceptance criteria relating to personnel risk can be defined as the mean FAR for all personnel at the installation shall be less than 10. Tolerable societal risk criteria are usually expressed in the form of F-N curve. To calibrate the risk graph, values or value ranges are assigned to each parameter. The risk associated with each of the parameter combinations is then assessed in individual and societal terms. The risk reduction required to meet the established acceptance criteria can then be established and the integrity levels associated with each parameter combination can be determined.

**Table 7 An example of risk graph calibration (IEC 61511, 2004)**

| Risk parameter | | Classification |
|---|---|---|
| Consequence (C)<br>Number of fatalities<br>This can be calculated by the number of people present when the area exposed to the hazard is occupied multiplying by the vulnerability to the identified hazard.<br><br>V = 0.01 (small release of flammable toxic material)<br>V = 0.1 (large release of flammable or toxic material)<br>V = 0.5 (As above but also a high probability of catching a fire or highly toxic material)<br>V = 1 (Rupture or explosion) | $C_1$ | Minor injury |
| | $C_2$ | Range 0.01 to 0.1 |
| | $C_3$ | Range 0.1 to 1.0 |
| | $C_4$ | Range >1.0 |
| Occupancy (F)<br>Percentage of time the exposed area is occupied during a normal working period | $F_1$ | Occupancy < 0.1 |
| | $F_2$ | Frequent to permanent exposure in the hazardous zone |
| Possibility of avoidance (P)<br>Probability of avoiding the hazardous event (P) if the protection system fails to operate. | $P_1$ | Hazard can be prevented by operator taking action, after he realizes SIS has failed to operate. Refer certain conditions (given in IEC 61511, 2004) |
| | $P_2$ | Almost impossible |
| Demand rate (W) The number of times per year that the hazardous event would occur in absence of SIF under consideration. | $W_1$ | Demand rate less than 0.1D per year |
| | $W_2$ | Demand rate between 0.1D and D per year |
| | $W_3$ | Demand rate between D and 10 D per year. |

Risk graph approach for SIL determination has the following advantages (Gulland, 2004):

- Precise hazard rates, consequences, and values for the other parameters of the method, are not required.
- No specialist calculations or complex modeling is required.
- It can be applied by people with a good "feel" for the application domain.
- They are normally applied as a team exercise, similar to HAZOP. Understanding about hazards and risks is disseminated among team members (e.g. design, operations, and maintenance). Individual bias can be avoided.
- It does not require a detailed study of relatively minor hazards.

- It can be used to assess many hazards relatively quickly.

However, risk graph method still has its limitations. Risk graph is still a coarse tool for assessing SIL requirements. It must be calibrated on a conservative basis to avoid the danger that they underestimate the unprotected risk and the amount of risk reduction/protection required (Gulland, 2004). It is difficult for a risk graph to consider the possibility of dependent failure between the sources of demand and the equipment used within the E/E/PE safety related system. It can therefore lead to an over-estimation of the effectiveness of the E/E/PE safety related system. (IEC 61508, 2010).

# Chapter 3 Environmental risk acceptance criteria – literature review and discussion

## 3.1 Introduction

The objective of this chapter is to discuss the risk acceptance criteria concerning environmental consequences and propose suitable ERAC for subsea safety systems. As discussed in chapter 2, the necessary risk reduction can only be determined when the tolerable risk, i.e. risk acceptance criteria haven been established. There are well established risk acceptance criteria for personnel risk, e.g. FAR and PLL. For subsea SISs applications where the consequences include environmental damage, an appropriate ERAC shall be established to facilitate developing SIL requirements for such systems. However, it is not easy and straightforward to use current ERAC for developing the requirements of technical safety barriers.

The ERAC are treated in Annex A of the NORSOK Z-013 standard. According to NORSOK Z-013, the description and requirements of ERAC is as follows (Hauge et al., 2010):

- Quantitative ERAC can be defined for various operations, e.g. drilling operation, operation of installations and/or fields. More than one type of ERAC, per operation, can be established to be able to cover several analytical endpoints.
- ERAC should include frequencies of discharges to the environment that results in defined environmental consequences. As a simplification of this, frequencies of discharges to the environment of pollutants and their volume and consequence potential may be used.

## 3.2 MIRA environmental risk acceptance criteria

The current risk acceptance criteria for the environment applied on Norwegian continental shelf is based on the OLF MIRA methodology. MIRA is a method and guideline for environmental risk analysis developed by DNV on behalf of OLF. It has been used in the Norwegian offshore industry for more than 10 years and it has been continuously refined. The current version may be found in the MIRA report revised in 2007.

The development of acceptance criteria for acute releases to environmental is based on the following main principles (MIRA guideline, 2007):

1. Environmental damage is classified according to the quantities of pollutant that will reach the shoreline.
2. Duration of environmental damage (i.e. until recovery has been completed) is the main expression for environmental damage.
3. The duration of environmental damage shall be insignificant in relation to the mean time between such damage occurrences.

The environmental damage is expressed in terms of restitution time. Different terms have been used in the literature and they all refer to the same concept, which includes recovery time, restitution time and restoration time. The restitution time is the time needed for a resource to return to its original state after being affected by the pollution. Corresponding to the first and second principle, 4 categories of environmental damage are defined as follows:

- Minor harm - environmental damage with restitution time between 1 month and 1 year.
- Moderate harm- environmental damage with restitution time between 1 and 3 years.
- Significant harm- environmental damage with restitution time between 3 and 10 years.
- Serious harm - environmental damage with restitution time in excess of 10 years.

The establishment of risk acceptance criteria for environmental pollution in MIRA guideline is based on the third principle that the duration of environmental damage shall be "insignificant" compared to the consequence of the damage. A challenge is to what should be the definition of "insignificant". In the Norwegian oil industry, the responsibility of defining what corresponds to an "insignificant" frequency of harm in this context is left to the operators. Now let RT denote the recovery time, MTBD denote the mean time between damage, and let r = RT/MTBD be the ratio between these two. The OLF standard proposes to use one of the following r values: 0.5%, 1%, 2%, 5% or 10%, without giving any more guidance. An r value of 5% is used in the standard, as an illustration. As an example this leads to that an event with a recovery time of 5 years, such an event shall not occur more often than every 100 years to be insignificant. This acceptance criteria may be translated as the maximum frequency of occurrence of significant harm to the environment is $1 \cdot 10^{-2}$ per year. Similar interpretations may be applied to each environmental damage recovery, which is shown in Table 8.

**Table 8 Current risk acceptance criteria for environmental risk (adapted from Vinnem, 2007)**

| Environmental damage category | Average restitution time (year) | Tolerable frequency |
|---|---|---|
| Minor harm | 0.5 | $1 \cdot 10^{-1}$ |
| Moderate harm | 2 | $2.5 \cdot 10^{-2}$ |
| Significant harm | 5 | $1 \cdot 10^{-2}$ |
| Serious harm | 20 | $2.5 \cdot 10^{-3}$ |

The MIRA guideline shows an example of possible acceptance criteria using 5% value as tolerable frequency. It is illustrated in Table 9. The activity level in the relevant region under consideration is assumed as follows:

- 2 fields in the region
- 2 facilities per field
- 10 operations per facility per year

Operations here mean critical activities threatening the environment, including drilling operation and well intervention. The assumed activity level and relation between operations, facilities, fields and region is illustrated in Figure 8.

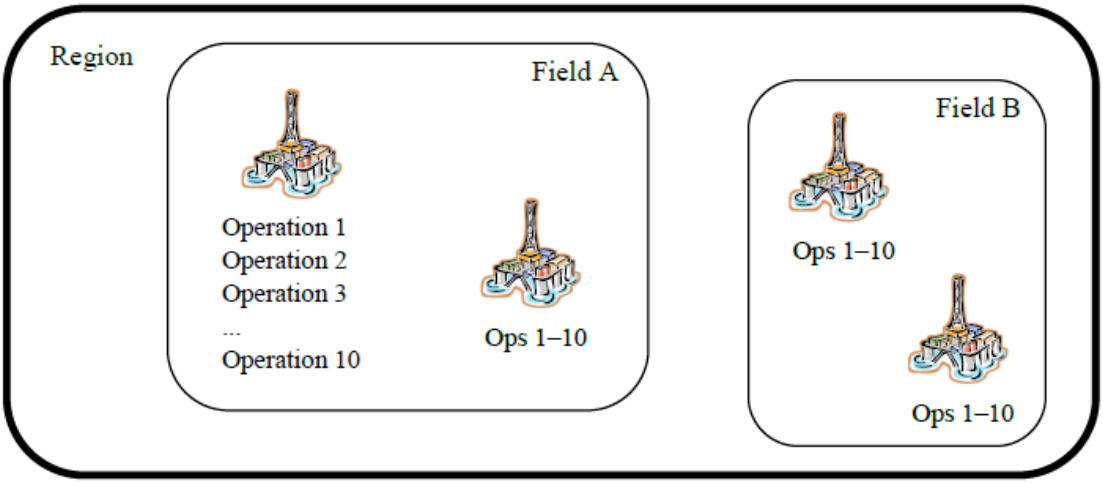



**Figure 8 Illustration of the MIRA guideline example of assumed activity level (Hauge et al., 2010)**

**Table 9 Possible ERAC when defining 5% as "insignificant" frequency of harm to the environment (MIRA guideline 2007)**

| | Consequence category | | | |
|---|---|---|---|---|
| | Minor harm | Moderate harm | Significant harm | Serious harm |
| Restitution time (years) | 0,1-1 | 1-3 | 3-10 | >10 |
| Activity specific ERAC | $1.25 \cdot 10^{-3}$ | $4.25 \cdot 10^{-4}$ | $1.25 \cdot 10^{-4}$ | $2.5 \cdot 10^{-5}$ |
| Facility specific ERAC | $1.25 \cdot 10^{-2}$ | $4.25 \cdot 10^{-3}$ | $1.25 \cdot 10^{-3}$ | $2.5 \cdot 10^{-4}$ |
| Field specific ERAC | $2.5 \cdot 10^{-2}$ | $8.5 \cdot 10^{-3}$ | $2.5 \cdot 10^{-3}$ | $5 \cdot 10^{-4}$ |
| Regional specific ERAC | $5 \cdot 10^{-2}$ | $1.7 \cdot 10^{-2}$ | $5 \cdot 10^{-3}$ | $1 \cdot 10^{-3}$ |

It should be noted that there is some inconsistency between the frequency in table 8 and table 9. It appears that MIRA guideline has adopted a more conservative approach when calculating the frequency of each harm category. The maximum restitution time for each category is used in the MIRA approach, while in table 8 proposed by Vinnem (2007) the average restitution time are used for calculation.

## 3.3 Discussion

The use of restitution time of the resources in order to assess the pollution risk is intuitively appealing since it expresses the final environmental consequences. There are some problematic issues related to using restitution time as acceptance criteria (Hauge, et al., 2010):

- The measure is well understood by biologists but appears vague and difficult to communicate to engineers and technical personnel.
- The restitution time measure directs focus towards consequence modeling but gives limited incentives to consider the frequency reducing barriers.

Apart from the disadvantages above, there are some aspects which are not taken into account in the MIRA approach. The risk to the environment can not only be measured from the restitution time perspective. The magnitude of the harm to the environment over the whole recovery time is not taken into account in the current risk acceptance criteria. For instance, the size of the fish stock affected in the area during the whole recovery time shall also be taken into account to measure the risk. The current MIRA approach does not discriminate between these different scenarios.

## 3.2 Alternative ERAC related to requirements for technical safety barriers

As discussed previously, the current ERAC is based on restitution time. The restitution time measure is not straightforward to comprehend and it depends on a large number of factors which shall be dealt with in the consequence analysis (dispersion analysis) after a hydrocarbon release. A more straightforward ERAC is lacking, in the context of specifying requirements for technical safety barriers.

It is considered easier to assess e.g., the volume of release rather than the restitution time that could be caused by such a release. This is also recognized in the NORSOK Z-013 standard, which states that “Environmental RAC should include frequencies of discharges to the environment that results in defined environmental consequences. As a simplification of this, frequencies of discharges to the environment of pollutants and their volume and consequence potential may be used.” Therefore, discharge volumes and their respective frequencies can be used as a simplification. In the following section, we discuss the steps required to use such a simplified approach.

In the MIRA guideline it is further recommended to establish specific acceptance criteria related to fields located in common emergency preparedness regions in order to achieve a good connection between environmental risk and emergency preparedness. The alternative ERAC could start from a common emergency preparedness region. The quality of the emergency preparedness may be seen as a factor of vulnerability of that region. For instance, the emergency preparedness in the Arctic area will be reduced to a large extent due to extreme weather condition compared to the oil and gas fields in the North Sea. Therefore, stricter acceptance criteria (frequency of a given volume) is required for a region with a higher vulnerability.

In addition to emergency preparedness, other relevant factors shall also be applied to decide the overall vulnerability of the area. The vulnerability of the region is divided into "Low", "Medium", and "High". The factors which shall be evaluated for categorizing vulnerability of the region include (Hauge, et al, 2010):

- Distance to shore
- Type of released oil
- Value of environmental resources
- Operation season of the year
- Competence of emergency preparedness in the region

A recommended ERAC considering different classes of vulnerability area is illustrated in Table 10.

**Table 10 Recommended ERAC for different categories of vulnerability area (inspired by Hauge, et al, 2010)**

| | Vulnerability | | |
|---|---|---|---|
| Environmental damage category | Low | Medium | High |
| Minor harm | $2 \cdot 10^{-1}$ | $1 \cdot 10^{-1}$ | $1 \cdot 10^{-2}$ |
| Moderate harm | $5 \cdot 10^{-2}$ | $2{,}5 \cdot 10^{-2}$ | $1 \cdot 10^{-3}$ |
| Significant harm | $2 \cdot 10^{-2}$ | $1 \cdot 10^{-2}$ | $1 \cdot 10^{-4}$ |
| Serious harm | $5 \cdot 10^{-3}$ | $2{,}5 \cdot 10^{-3}$ | $1 \cdot 10^{-5}$ |

The environmental damage category may further be expressed by the release volumes. A link should be established between the release volume and environmental damage in terms of restitution time. The environmental risk analysis of the region under consideration may give some information and guidance on establishing the relation between release volume and average restitution time. However, the link between release volume and restitution time shall be established based on and supported by scientific research. The justification for this is not fully grounded. Table 11 illustrates an example of categorization based on release volumes.

**Table 11 An example of categorization of environmental damage based on release volumes**

| Environmental damage category | Average restitution time | Release volume |
|---|---|---|
| Minor harm | 0.5 | 10-100 $m^3$ |
| Moderate harm | 2 | 100 -1000 $m^3$ |
| Significant harm | 5 | 1000 -10,000 $m^3$ |
| Serious harm | 20 | >100,000 $m^3$ |

When the relation between pollutant release volume and average restitution time have been established for the environment under consideration, the associate acceptable frequency can be defined for each category of release volumes. According to the activity level in the region, field, facility and activity specific ERAC can be also determined. Table 12 illustrates an ERAC example for a region with medium vulnerability. The assumption about activity level is the same as in the MIRA guideline.

**Table 12 Recommended ERAC for medium vulnerability environment (Adapted from Hauge, et al, 2010)**

| | Consequence category | | | |
|---|---|---|---|---|
| | Minor harm | Moderate harm | Significant harm | Serious harm |
| Release volume | 10-100 $m^3$ | 100 -1000 $m^3$ | 1000 -10000 $m^3$ | >100,000 $m^3$ |
| Activity specific RAC | $2.5 \cdot 10^{-3}$ | $6.25 \cdot 10^{-4}$ | $2.5 \cdot 10^{-4}$ | $6.25 \cdot 10^{-5}$ |
| Facility specific RAC | $2.5 \cdot 10^{-2}$ | $6.25 \cdot 10^{-3}$ | $2.5 \cdot 10^{-3}$ | $6.25 \cdot 10^{-4}$ |
| Field specific RAC | $5 \cdot 10^{-2}$ | $1.25 \cdot 10^{-2}$ | $5 \cdot 10^{-3}$ | $1.25 \cdot 10^{-3}$ |
| Regional specific RAC | $1 \cdot 10^{-1}$ | $2.5 \cdot 10^{-2}$ | $1 \cdot 10^{-2}$ | $2.5 \cdot 10^{-3}$ |

# Chapter 4 Calibrated risk graph for subsea applications

## 4.1 Introduction

The objective of this chapter is to propose a new risk graph method for determining EIL/SIL of subsea safety systems. The failure of such system could lead to acute release to the environment. The risk graph method presented in Chapter 2 is suitable for applications where personnel risk is of main concern. However, for SISs used in subsea applications, the consequences of failure include acute release to the environment. The integrity level required depends on the characteristics of the substance released and the sensitivity of the environment.

IEC 61511 gives an example of using risk graph where the consequences are environmental damage. However, only the consequence parameter is changed and defined in terms of environmental damage while the other 3 parameters remains unchanged as with the risk graph used for personnel risk. The occupancy parameter and probability of avoidance is especially suited for personnel risk. Occupancy is the probability that the exposed area is occupied at the time of the hazardous event. For subsea SISs, the environment is always exposed to the hazard in case of a hazardous event. The probability of avoidance parameter is also tailored for application in relation to personnel risk. As stated in the risk graph method in IEC 61511-3, the probability of avoidance parameter depends on existing independent methods of alerting the exposed persons prior to the hazard occurring and methods of escape.

## 4.1 A proposed method --- Marinized risk graph

The parameters used in risk graph for subsea SISs applications, therefore, need to be modified. The following 4 parameters are proposed to characterize the risk to the environment:

- I - Initiating cause frequency
- S - Existing safeguards risk reduction
- R - Release volume
- V - Environmental vulnerability

The proposed methodology is conducted in six steps:

The general scheme and layout of the marinized risk graph is illustrated in Figure 9. The first two parameters assess the consequence dimension of the risk and the risk matrix columns are used to determine the demand rate on the SIF under consideration. Each cell in the risk matrix contains an SIL/EIL level. The SIL/EIL represents the necessary risk reduction by the SIS under consideration.

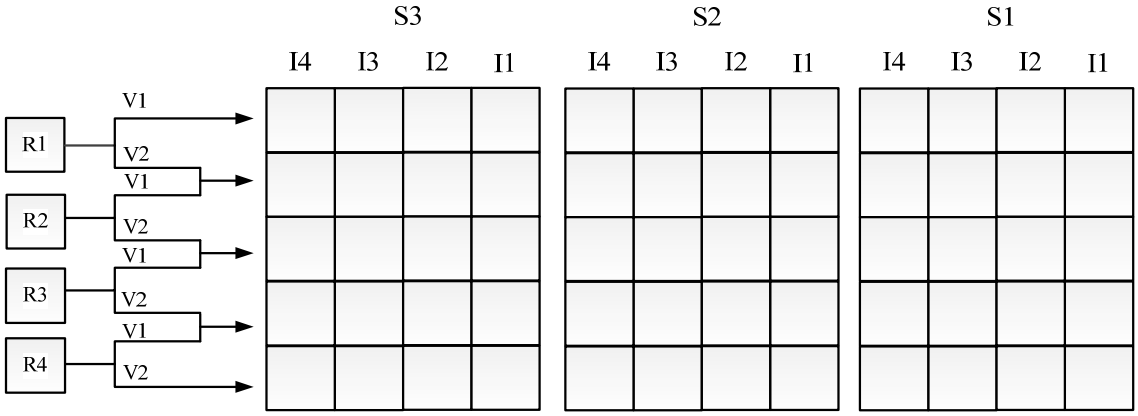



Figure 9 General scheme of marinized risk graph

### Step 1: Assign release volume (R parameter)

The analyst should first assign the release volume parameter according to the risk scenario based on his/her judgment. Release volume can be assigned according to the categories in environmental risk acceptance criteria. Table 13 shows an example of categorization of release volume.

Table 13 An example of categorization of environmental damage based on release volume

| Environmental damage category | Average recovery time | Release volume |
|---|---|---|
| Minor harm | 0.5 | 10-100 $m^3$ |
| Moderate harm | 2 | 100 -1000 $m^3$ |
| Significant harm | 5 | 1000 -10,000 $m^3$ |
| Serious harm | 20 | >100,000 $m^3$ |

### Step 2: Assign environmental vulnerability parameter (V parameter)

The vulnerability of the operation area is assessed separately in the proposed risk graph method, while the conventional risk graph approach includes the vulnerability in the consequence parameter. Based on the ERAC developed in previous chapter, the vulnerability of the environment is categorized as “Low”, “Medium”, and “High”.

The following factors need to be evaluated for categorizing the vulnerability of the region under consideration:

- Distance to shore
- Type of released oil
- Value of environmental resources
- Operation season of the year
- Competence of emergency preparedness in the region

A scoring system may be developed for categorization of the vulnerability parameter. A proposed scoring methodology is described as follows. Each factor is assessed on a scale of 1 to 10. One point corresponds to the lowest vulnerability and ten points indicate the highest vulnerability. We first assume that each factor has the same weight in the final assessment of the vulnerability. The vulnerability can be categorized according to the sum of all the five factors, which is shown in Table 14.

**Table 14 Vulnerability categorization based on scoring of influencing factors**

| Sum of all five factors | Vulnerability categorization |
|---|---|
| 5-19 | Low |
| 20-34 | Medium |
| 35-50 | High |

The parameters in the risk graph should differentiate between a level of magnitude in the selected SIL. According to the ERAC, there is one order of magnitude difference between High and Low vulnerability. Thus, two levels of vulnerability parameter are used. Higher vulnerability will require a higher value of the SIL to be allocated.

V1 - Low and medium vulnerability

V2 - High vulnerability

### Step 3: Assign parameter for the initiating event (I parameter)

Based on the types of failure, the initiating events are categorized as equipment failure, human failures and external failures. The initiating event frequency diffrentiates by an order of magnitude and ranges from 1 to $10^{-3}$ per year. Thus, four levels of initiating event frequency are used for this parameter.

Note that the initiating cause parameter implies the frequency of the initiating event which can lead to hazardous event when the exiting barriers fail. When assigning the I parameter, the enabling events/condition and other conditional modifiers shall be taken into account. Enabling condition/events do not directly cause the scenario but must be present or active for the scenario to proceed, for instance, the process being in a particular mode or phase (Baybutt, 2007). In order to be credited for risk reduction, enablers and modifiers must provide at least 1 in 10 risk reduction factor. The I parameter can be reduced according to the risk reduction provided by the enabler and condition modifiers. For example, if a scenario initiating cause frequency is $1 \times 10^{-3}$ and enabling condition and conditional modifiers for this scenario are believed to reduce the risk by 0.1, the I parameter can be assigned to I2.

### Step 4: Select risk matrix to use according to the existing safeguards (S parameter)

The S parameter is intended to credit the failure probability of existing protection layers that can prevent the occurrence of hazardous event or mitigate the consequence. The credited

protection layer will at least provide 10 fold risk reduction. Three levels are used for safeguard failure probability.

S1 - Two or more independent protection layer

S2 - Only one independent protection layer

S3 - No independent protection layer

### Step 5 Calibration according to the proposed ERAC

The next step is to assign a SIL to each cell in the risk graph in Figure 9. The objective of this calibration process is to make the SIL assignment internally consistent from cell to cell and also consistent with the environmental risk acceptance criteria. The calibration requires different risk scenarios with different consequences and likelihood to be considered and SIL to be assigned according to the necessary risk reduction. For instance, a risk scenario could be "a release of 1000 -10,000 $m^3$ oil in a high vulnerability area due to an initiating cause frequency of 0.1 per year and only one independent protection layer is able to prevent the risk scenario". Therefore, the parameters R3 and V2 are chosen to represent the consequence and the I3 column under the S2 label in risk matrix is chosen to represent the demand rate. The demand rate would be 0.01 per year. The tolerable frequency for the consequence, according to the ERAC, is $2.5 \cdot 10^{-5}$ per year. This would require the PFD of the SIS lower than 2.5·10-3 and SIL 3 is required. The corresponding cell is assigned SIL 3.

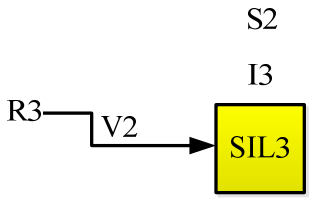
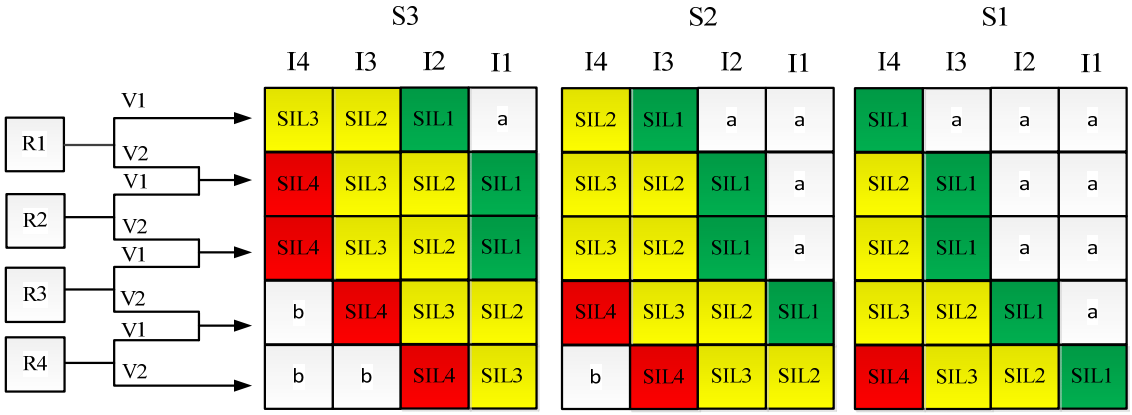



**Figure 10 An example of SIL calibration**

Figure 11 shows the calibrated risk graph. It is calibrated according the ERAC described in Chapter 5 by using the methodology described above.




I – Initiating cause frequency

V – Environmental vulnerability

S – Safeguard failure probability

R – Release volume

a – No special safety requirements

b – A single SIF is not sufficient

**Figure 11 Calibrated risk graph for subsea applications**

### Step 6 Selecting SIL/EIL for the safety instrumented function under consideration

The SIL/EIL is selected according to the scheme illustrated in Figure 11. The scheme starts from the release volume parameter and then branched by the two level environmental vulnerability parameter V1 and V2. V1 branches upwards, corresponding to a lower SIL and V2 branches horizontally, corresponding to a higher SIL. Based on the existing safeguards and initiating event frequency, each column in the three risk matrixes represents the demand rate on the SIF. The SIL is determined by the combination of these 4 parameters.

## 4.2 A case study on drilling BOP

An oil company has decided to drill a subsea oil well near Lofoten on the Norwegian continental shelf. The proposed risk graph is used to determine the SIL requirements for the drilling BOP of the subsea well.

The risk scenario under study is a blowout during drilling phase. The worst case scenario is assumed when assigning the R parameter, thus R4 is chosen. As the Lofoten area is abundant in fish resources, distance to shore is short and type of release oil will result in more serious pollution. V2 is chosen to represent the high vulnerability of the area. The scoring result of the 5 factors is listed in Table 15. As described in previous section about the scoring methodology , each factor is scored on a scale of 1 to 10. The sum of the scores of all the five factors is 35. According to table 14, it corresponds to high vulnerability, thus V2 is chosen.

**Table 15 Scoring results of vulnerability factors for the case study**

| Scoring categorizes | Scores |
|---|---|
| Distance to shore | 8 |
| Type of released oil | 8 |
| Value of environmental resources | 9 |
| Operation season of the year | 5 |
| Competence of emergency preparedness in the region | 5 |
| Sum | 35 |

As the operation area is evaluated as high vulnerability area. The corresponding ERAC shown in Table 16 is developed based on Table 10 and Table 11.

**Table 16 ERAC for high vulnerability environment**

| | Consequence category | | | |
|---|---|---|---|---|
| | Minor harm | Moderate harm | Significant harm | Serious harm |
| Release volume | 10-100 $m^3$ | 100 -1000 $m^3$ | 1000 -10000 $m^3$ | >100,000 $m^3$ |
| Activity specific RAC | $2.5 \cdot 10^{-4}$ | $6.25 \cdot 10^{-5}$ | $2.5 \cdot 10^{-5}$ | $6.25 \cdot 10^{-6}$ |
| Facility specific RAC | $2.5 \cdot 10^{-3}$ | $6.25 \cdot 10^{-4}$ | $2.5 \cdot 10^{-4}$ | $6.25 \cdot 10^{-5}$ |
| Field specific RAC | $5 \cdot 10^{-3}$ | $1.25 \cdot 10^{-3}$ | $5 \cdot 10^{-4}$ | $1.25 \cdot 10^{-4}$ |
| Regional | $1 \cdot 10^{-2}$ | $2.5 \cdot 10^{-3}$ | $1 \cdot 10^{-3}$ | $2.5 \cdot 10^{-4}$ |

| | | | | |
|---|---|---|---|---|
| specific RAC | | | | |

The initiating event is a well kick. In case of kick, the primary well barrier, the mud control system will be activated to balance the well. It is assumed that the probability of successful circulation of heavy mud is 0.8, resulting in a PFD of 0.2. The value for reliability of mud control system was justified in (Hauge, et al, 2010). Hence, the S2 risk matrix shall be used. According to drilling statistic on Norwegian continental shelf, the well kick probability is estimated by 0.2 per well operation (Hauge, et al, 2010). The initiating event parameter is hence set to I2. Therefore, the combination of the four parameters that have been chosen leads to a SIL3 requirement. This is illustrated in Figure 12.

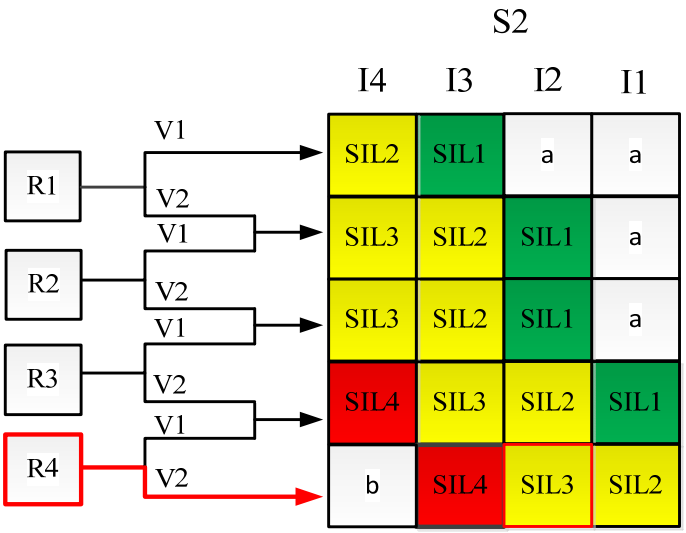



**Figure 12 SIL determination illustration**

# Chapter 5 Layer of protection analysis (LOPA)

## 5.1 Introduction

Layer of protection analysis (LOPA) is a semi-quantitative tool for analyzing and assessing risk. The method was first introduced in the process industry in 1993. It is found to have other applications in the industry, in addition to being used as a SIL determination tool, including capital improvement planning, management of change, emergence response planning and so forth (CCPS 2001).

The main objective of LOPA is to determine if there are sufficient layers of protection against an accident scenario (CCPS 2001). It requires the analyst to compare the intermediate event frequency with the corporate risk criteria, determining whether the risk is tolerable. Depending on the complexity of process and severity of consequence of the risk scenario, many different protection layers are required to prevent the occurrence of the accident. Figure 13 illustrates the typical protection layers for a chemical process.

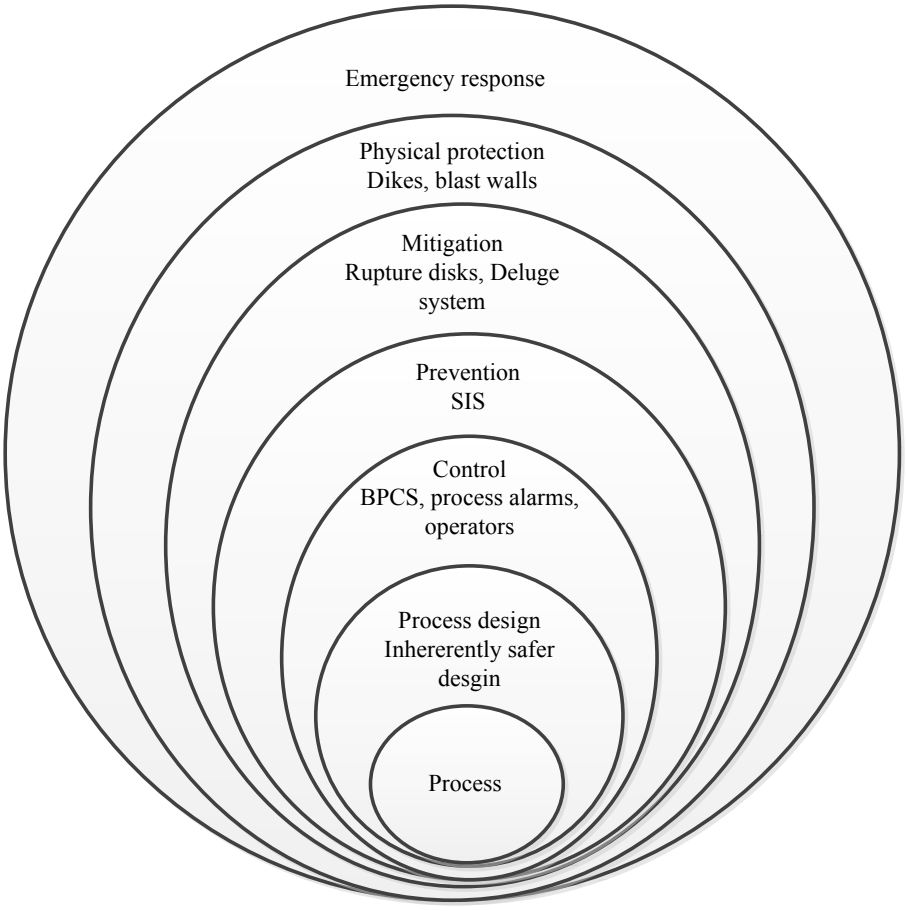



**Figure 13 Protection layers (adapted from IEC 61511, 2004)**

LOPA can be viewed as a special form of event tree analysis with the purpose of determining an unwanted event, which can be prevented by one or more protection layers. As illustrated in Figure 14, the protection layers in LOPA are analogous to the branches in an event tree. Each branch is always a set of complementary events in which the protection layer either functions successfully or fails (Marszal and Scharpf, 2002). The difference from the event tree analysis is that we are only interested in the worst-case scenario, where all the protection layers must fail in order for the consequence to occur. We then calculate the frequency of the unwanted consequence by multiplying the PFDs of the protection layers with the initiating event frequency. Comparing the resulting frequency of the unwanted consequence with a tolerable frequency of corresponding consequence severity, the necessary risk reduction and SIL allocation can be achieved and an appropriate SIL can be determined.

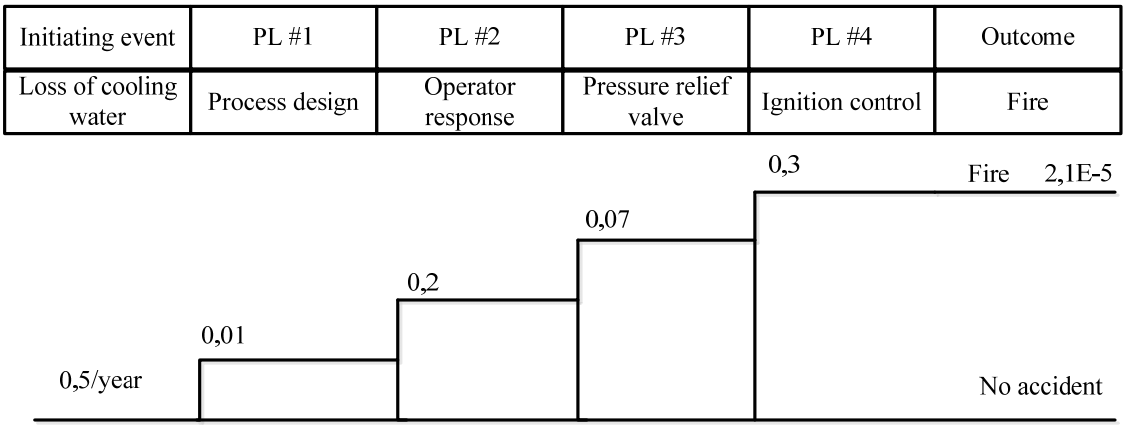



**Figure 14 LOPA as a special type of event tree (adapted from Marszal and Scharpf, 2002)**

## 5.2 The LOPA team

In order to use LOPA to determine the SIL of the SIS under consideration, a multi-disciplinary team should be established. According to IEC 61511-3, the team should consist of:

- operator with experience and knowledge from operating the process
- engineer with expertise in the process
- manufacturing management
- process control engineer.
- instrument/electrical maintenance person.
- risk analysis specialist

At least one person in the team should be trained in the LOPA methodology.

Before commencing the actual LOPA work, the team should establish a project plan and provide the necessary background information and data. Relevant data is identified in a HAZOP or preliminary hazard analysis (PHA). In addition, piping and instrumentation

diagrams, cause and effects charts, and the Safety Requirement Specification (SRS) for the existing SISs should be available (Rausand, 2011).

## 5.3 The LOPA work sheet

The data and results from the LOPA analysis are documented in the LOPA worksheet. Table 17 illustrates a typical LOPA worksheet from IEC 61511. Each column and the required information are explained in the next section about the LOPA.

**Table 17 An example of LOPA worksheet (IEC 61511, 2004)**

| | Impact event | | Initiating event | | Protection layers | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Reference nr. | Description | Severity level | Initiating event | Initiating event likelihood | General process design | BPCS | Alarms, etc | Engineered mitigation | Additional mitigation | Intermediate event likelihood | SIF integrity level | Mitigated event likelihood | Notes |
| 1 | Fire from distillation column rupture Tolerable frequency 1,00E-9 | S | Loss of cooling water | 0,1 | 0,1 | 0,1 | 0,1 | PRV 01 | 0,1 | 1,00E-07 | 1,00E-02 | 1,00E-09 | High pressure causes column rupture |
| 2 | Fire from distillation column rupture 1,00E-9 | S | Steam control loop failure | 0,1 | 0,1 | | 0,1 | PRV 01 | 0,1 | 1,00E-06 | 1,00E-02 | 1,00E-08 | Same as above |

Note: Severity level E = Extensive; S = Serious; M = Minor

Likelihood values are events per year; the other numerical values are average probabilities of failure on demand.

## 5.4 The LOPA process

### Step 1 Develop accident scenarios

The starting point of a LOPA analysis is the impact event, which is typically identified during a HAZOP study. But the accident scenario starts from the initiating event. The most efficient way of developing accident scenario is the event tree analysis. An event tree is established for each initiating event revealed by the HAZOP study. Only the protection layers that are Independent protection layers (IPLs) are included to construct the event tree for LOPA analysis (Rausand, 2011).

The analyst will screen the end events of the event tree diagram based on the consequence. If an end event does not cause any significant harm to the assets (environment, personnel or material assets), the corresponding scenario is excluded from further analysis. The end events selected (also denoted as impact events) for further analysis is entered in column 1 of the LOPA worksheet. The severity of each impact event is evaluated and classified, for instance, as "High", "Medium", or "Low". The severity level is entered in column 2 of the LOPA worksheet.

### Step 2 Identify the initiating event of the scenario and determine the initiating event frequency.

In this step, the initiating events for each accident scenario are identified and the frequencies are estimated. Initiating events are grouped into three general types: external events, equipment failure, and human failures. Figure 15 illustrates the three general types of initiating events.

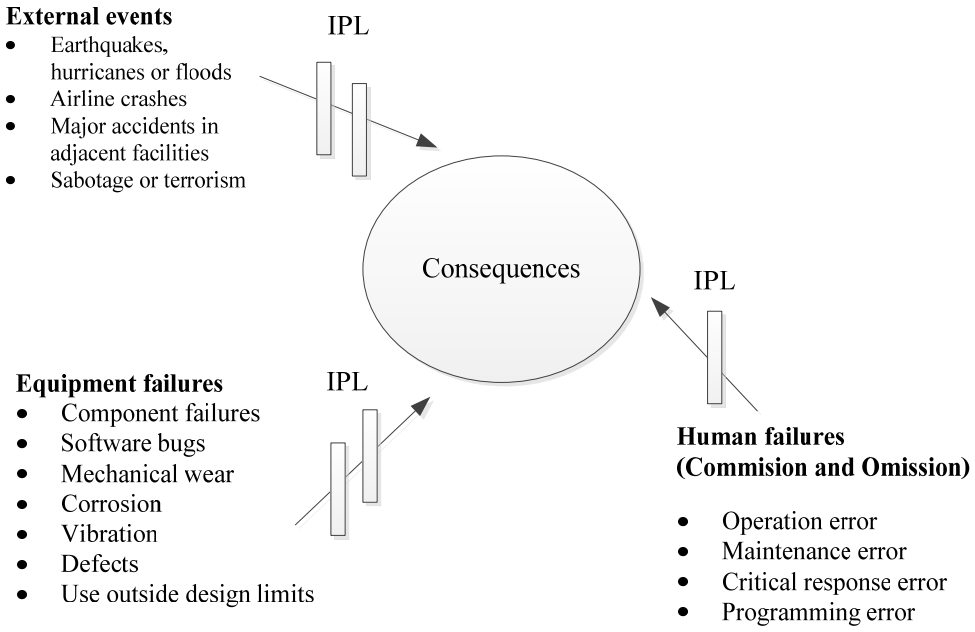


**Figure 15 Types of initiating events (adapted from CCPS, 2001)**

The main challenge of this step is to ensure that the list of initiating events are relatively "exhaustive". A checklist may be prepared to ensure this objective is achieved. An impact event may be caused by several initiating events. It is important that the LOPA team identifies all of them.

It is important to differentiate between initiating events and underlying root causes. Initiating event can be the result of various underlying root causes. Care should be taken to avoid going too far into root causes in identifying initiating events (CCPS, 2001). The LOPA team should evaluate all the causes and verify if they are valid initiating events. For example, inadequate operator training/certification is not a valid initiating event, but rather a possible underlying cause of an initiating event. Invalid initiating events should be either corrected or removed.

When the initiating events are identified, the frequency (per year) of each initiating event can be determined. This can be found in the HAZOP study. If LOPA is not done as part of the HAZOP study, the team must estimate the frequency of each initiating event. The frequency estimates, especially equipment failure rate, are based on industry data, such as OREDA. Some are based on company experience data.

The initiating events and frequency estimates are entered in column 3 and 4 respectively in the LOPA worksheet.

### Step 3 Identify IPLs and estimate the probability of failure on demand of each IPL.

In this step, the LOPA team identifies and lists all the existing protection layers related to each specific initiating event. This is usually done as part of HAZOP study, but the LOPA team should go through every protection layer and check that they understand the layers' functions and limitations (Rausand, 2011),

In LOPA analysis, only IPLs are credited for risk reduction. Therefore, the team should compare each protection layer with the IPL requirements to decide which protection layers can be credited as IPL. According to Rausand (2011), the IPLs can be classified into the following 5 main groups:

1. Process design
2. Basic process control system (BPCS)
3. Operator response to alarms
4. Engineered mitigation such as dikes, pressure relief, and existing safety instrumented systems
5. Additional mitigation in the form of restricted access. (This group is sometimes not included in LOPA worksheet).

The LOPA team must analyze the sequence of activation of each IPL in relation to the initiating event and arrange them in the corresponding order.

Next, the LOPA team should estimate the PFD of each IPL. For each main group presented above, the total PFD is then calculated and entered in column 5-9 in the LOPA worksheet.

#### Step 4 Estimate the risk related to each impact event by combining the consequence, initiating event frequency and IPL data.

There may be several initiating events for each impact event. The first step in estimating the risk related to each impact event is to determine the frequency of each accident scenario for each initiating event. This is done by multiplying the data entered in column 5-9 of the worksheet. The result is entered in column 10. It represents the estimated intermediate likelihood of each accident scenario.

The intermediate frequency of the same impact event can be found by adding the intermediate frequencies in column 10. According to Rausand (2011), adding these frequencies will give a conservative approximation since the initiating events may occur at the same time, due to a common root cause. However, it is conservative only when all the initiating events have been identified.

#### Step 5 Evaluate the risk according to the acceptance criteria

In this step, the LOPA team must compare the calculated intermediate frequency of each unique impact event with the corresponding risk acceptance criteria. If the intermediate event frequency is less than the tolerable frequency of the severity level, there is no need of additional protection layers for further risk reduction.

On the other hand, if the intermediated event frequency is higher than the tolerable frequency level, further risk reduction is required. The LOPA team should first consider inherently safer design. If inherently safer design changes can be made, the PFD in column 5 is updated and a new intermediate event frequency is calculated.

#### Step 6 Consider Options to reduce the risk

According to IEC 61508, inherently safer design and other technology protection layers should be considered before SIS as further risk reduction measures. If the evaluation implies that a SIS is needed, the PFD requirement for the SIS can thus be determined. This is done by dividing the tolerable mitigated event frequency in column 1by the intermediate event frequency in column 10. The result is entered into column 11 of the LOPA worksheet shown in table 2.1. The SIL is determined by comparing the result with the SIL table (Table 1).

## 5. 5 Strengths and limitations of LOPA

The LOPA method has the following advantages:

- It is performed as a multi-disciplinary team exercise. The accident scenarios related to the process are identified and analyzed extensively one by one.
- The risk acceptance criteria are incorporated explicitly in the LOPA process. The necessary risk reduction is found and quantified explicitly by comparing the intermediated event frequency and target mitigated event likelihood (TMEL).

- It facilitates the identification of the effective protection layers in a specific accident scenario. This information can help the organization to decide which protection layers to focus on during operation, maintenance and related training.

The limitations of LOPA are:

- LOPA is more time-consuming and requires more documentation than risk graph and other simple SIL determination methods.
- LOPA is not qualified for situations where comprehensive quantitative risk assessment (QRA) is required. It cannot substitute quantitative risk assessment tools such as event tree analysis or fault tree analysis (CCPS, 2001).
- Data uncertainty in estimating frequency of the initiating event and the PFD of IPLs. In LOPA, approximate values of all relevant parameters are used; therefore data uncertainty exits in the process and will eventually affect the result. In one approach, all relevant parameters are rounded to the higher decade range (for example, a probability of $5 \cdot 10^{-2}$ is rounded to $10^{-1}$). This is a very conservative approach and can lead to significantly higher SIL levels. For example, the multiplication of $2 \cdot 10^{-2}$ and $5 \cdot 10^{-2}$ is $1 \cdot 10^{-3}$, but if it is approximated by rounding up to the higher decade rage, the result is $1 \cdot 10^{-4}$. This would lead to a higher SIL level to be selected. In IEC 61508, it is stated that data uncertainty should however be recognized by rounding all parameter values to the next highest significant figure (for example, $5.4 \cdot 10^{-2}$ should be rounded to $6 \cdot 10^{-2}$) (IEC 61508, 2010).
- Common cause failure between the required SIS and credited IPLs is not included in the analysis.
- A main challenge is to record all the assumptions that are (necessarily) made during the LOPA session and transfer these assumptions in a proper manner to operations.
- Difficult to know/ensure whether all scenarios and initiating events are really covered.

## 5. 6 HAZOP and the interface with LOPA

A Hazard and Operability (HAZOP) study is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation (Rausand, 2007). It is usually performed by a multidisciplinary team (HAZOP team) in a series of meetings. The HAZOP approach was developed initially to be used during the design phase, but can also be applied to systems in operation. The most common HAZOP study is carried out during the detailed engineering phase (Rausand, 2011).

In the HAZOP study, the system or plant is divided into a number of study nodes. The study nodes are examined one by one. For each node, design purpose and the normal state are defined (Rausand, 2011). A set of guidewords and process parameters are used to facilitate brainstorming of possible deviations in the system. The brainstorming is normally led by a set of HAZOP questions. For instance, the guideword can be “High” and the process parameter could be “Pressure”. Thus the HAZOP question could be raised as “could there be high pressure”, “If so, how could it rise” and “what are the consequences of high pressure”.

The HAZOP procedure involves eight steps. Figure 16 illustrates the workflow of HAZOP study. The interactions with LOPA are also identified and shown in the figure.

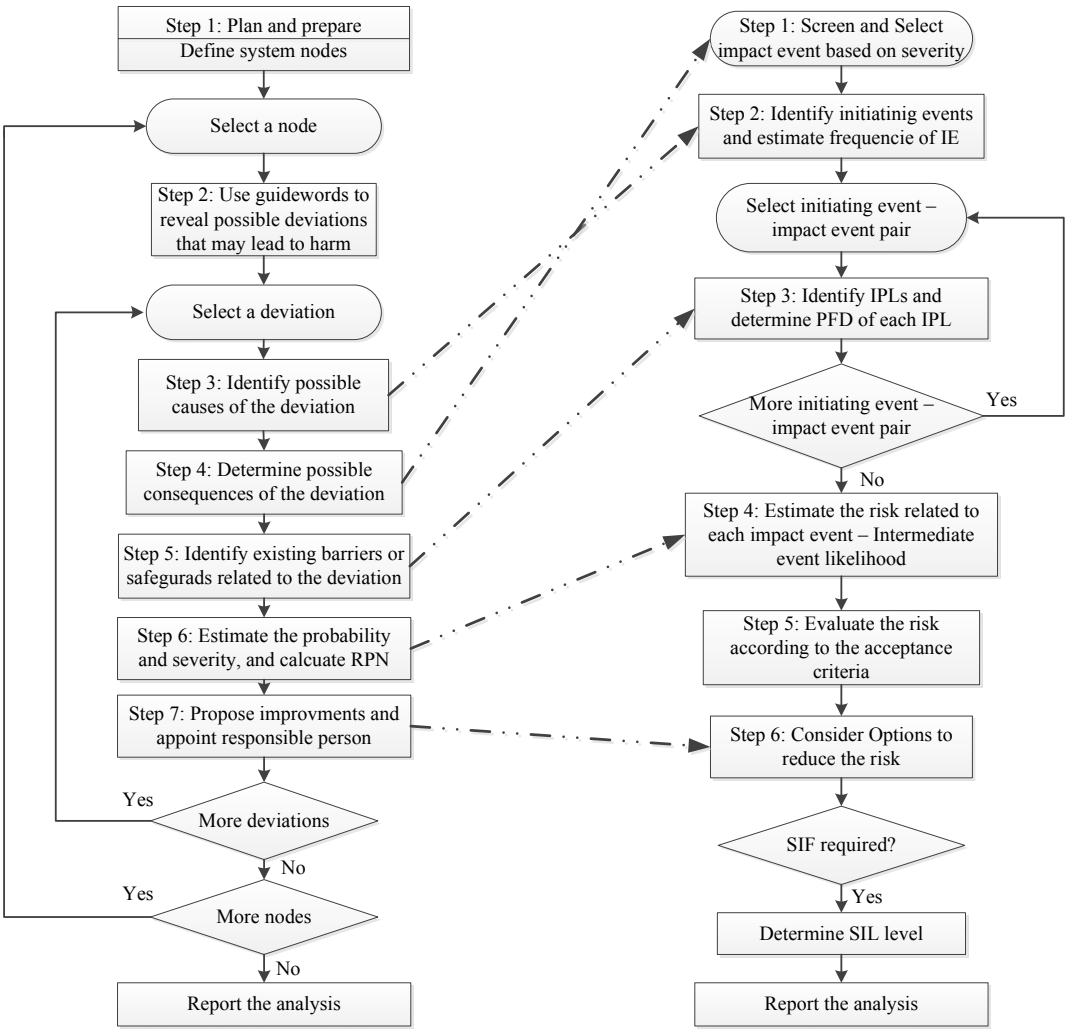



**Figure 16 HAZOP workflow and the interactions with LOPA**

As illustrated in Figure 16, LOPA receives output information and data from the HAZOP study. The HAZOP study starts from a process deviation, for instance, high pressure. Possible causes and consequences of high pressure are then identified. Possible causes can be "a blockage in the outlet pipe". The consequence could be "rupture of the vessel". The starting point of LOPA analysis is the impact event. Therefore, the LOPA team could screen the consequences identified in the HAZOP study and select the consequences based on severity level.

# Chapter 6 Considering CCFs in SIL determination

## 6.1 Introduction

The existing approaches to SIL determination assume independence between the designated SIS and the existing protection layers. In this chapter, the risk reduction situations where there are CCFs between the protection layers are discussed. A fault tree has been constructed to illustrate the effect of CCFs on the actual risk reduction. A framework of SIL determination including CCFs analysis is proposed after the discussion. The framework aligns with the different phases of the safety lifecycle adopted by IEC 61508, in which CCFs between the SIS to be implemented and the existing PLs are taken into account. In the SIL determination phase, a checklist has been proposed for CCFs quantification in this stage. The challenges encountered in CCFs quantification in SIS realization phase are discussed.

According to IEC 61508, during the determination of SIL, it is important to take account of common cause and dependency failures. The risk model adopted in IEC 61508 (see Figure 2 in Chapter 2 and Figure 17) assumes that each safety system relevant to the same hazard is fully independent (IEC 61508).

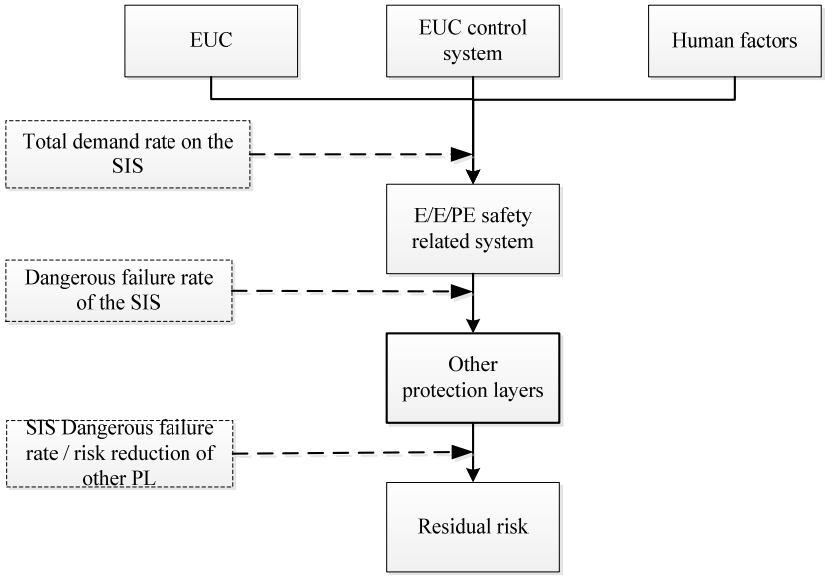



**Figure 17 Risk reduction for high demand applications(adapted from IEC 61508, 2010)**

However, there are many applications where the safety systems that provide protection against the same hazard are not independent of each other. The following non-independent situations are listed in IEC 61508-5:

1. The same cause can lead to a dangerous failure of an element within the EUC control system and an element in the safety related system. See illustration in Figure 18. For instance, separate sensors are used in the EUC control system and safety system, but common cause

could lead to failure of both (e.g. failure of heat tracing could lead to freezing of impulse lines for both sensors).

2. When there are more than one safety related systems, the same type of equipment is used within each safety related system and each is subject to failure from the same cause. For example, the same type of sensor is used in two separate protection layers for the same hazard. This situation is also illustrated in Figure 18.

3. The protection systems are diverse but proof testing is carried out on all the systems on a synchronous basis, resulting in all systems having their "peak PFD" at the same time).

4. The same component is used as part of the control system and the safety related system.

5. The same element is used in more than one safety related system (e.g. common valves for the PSD and the ESD system).

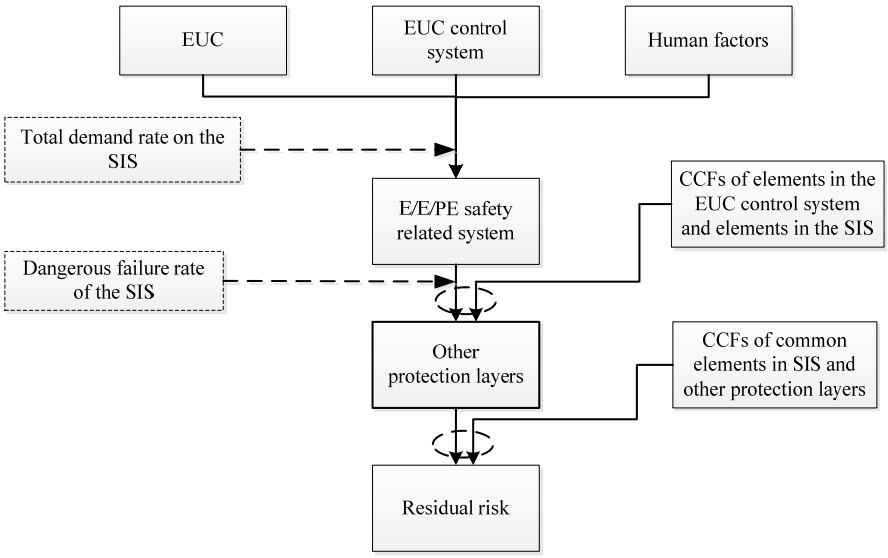



**Figure 18 Illustration of risk reduction considering CCF (adapted from IEC 61508, 2010)**

## 6.1 Illustration of CCF affecting risk reduction

Assume that one IPL has been credited for a specific accident scenario. The PFD of the IPL has been determined as 0.01. A SIS is required for further risk reduction after considering other risk reduction measures. However, the SIS which is going to be implemented may suffer from CCFs with the IPL being credited. Without considering the effect of CCF, SIL 2 requirement has been determined. It should be noted that we now assume that the PFD of these two protection layers have the same magnitude. A fault tree has been constructed to calculate the actual risk reduction of the IPL and SIS, as illustrated in Figure 19. The CARA Fault Tree has been used to calculate the unavailability of the two barriers in parallel when the CCF fraction is assumed 10%, 5% and 2% respectively. The results of actual mitigated risk are presented in Table 18.

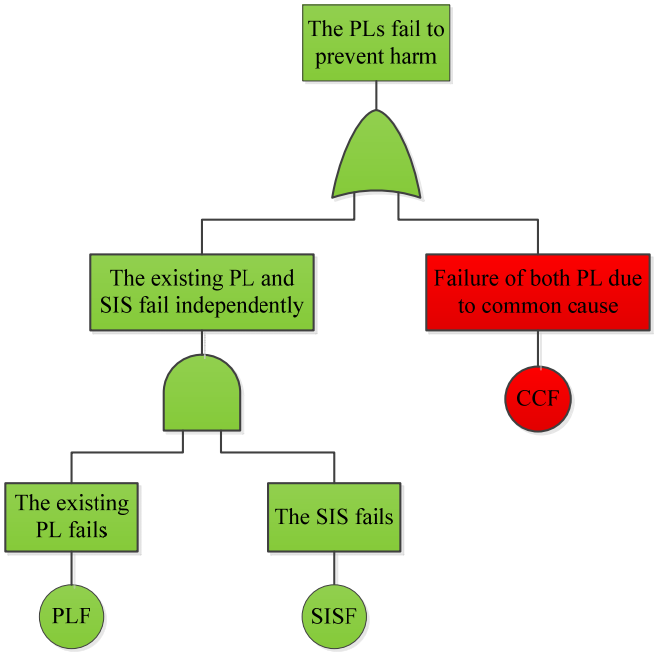



**Figure 19 Fault tree accounting for CCF**

**Table 18 Results of fault tree calculation**

| Initiating event | PFD of Existing PL | PFD of SIS | CCF fraction of the SIS | Risk reduction considering CCF | Actual Mitigated risk |
|---|---|---|---|---|---|
| 0,1/year | 0,01 | 0,01 | 10% | 1,08e-003 | 1,08e-004/year |
| 0,1/year | 0,01 | 0,01 | 5% | 5,90e-004 | 5,90e-005/year |
| 0,1/year | 0,01 | 0,01 | 2% | 2,96e-004 | 2,96e-005/year |
| 0,1/year | 0,01 | 0,01 | 0 | 1,00e-004 | 1,00e-005/year |

According to the results of the fault tree calculation, the CCFs between the SIS and the existing PL will result in a higher mitigated event frequency than in the independent situation. When the CCF fraction is 10%, the mitigated event frequency becomes one order of magnitude higher.

It is mentioned in IEC 61508-2 that "in the case of common cause failures being identified between the E/E/PE safety–related systems and demand causes or other protection layers there will need to be confirmation that this has been taken into account when the safety integrity level and target failure measure requirements have been determined."

Therefore, an additional step shall be added to the SIL determination process, which addresses the CCFs between the SIS and other PLs. Figure 20 illustrates the framework incorporating the evaluation of CCFs and LOPA during the SIL determination process.

It should be noted that using CCFs fraction of 10% as the criterion is based on the fault tree calculation presented above. It applies to the situations where PFDs of the dependent PLs are in the same order of magnitude range.

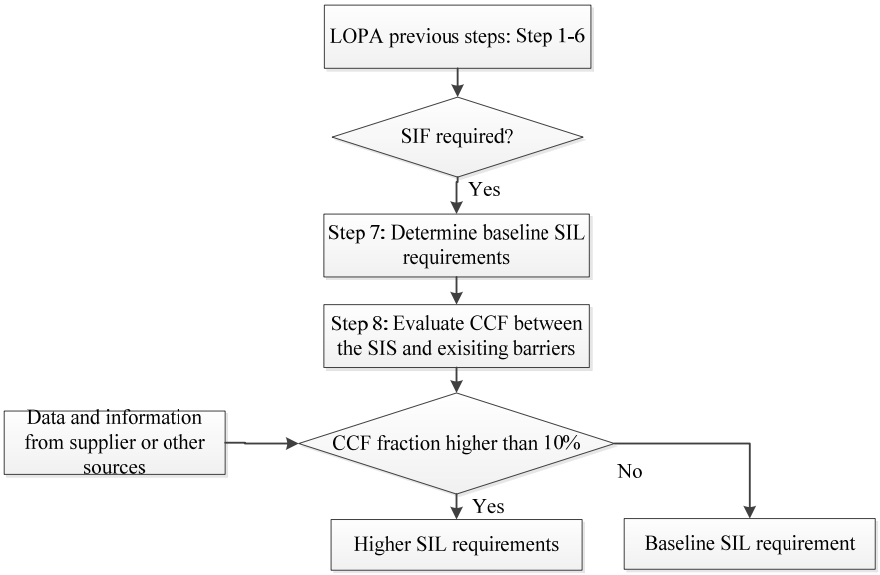



**Figure 20 Framework for SIL determination incorporating CCF**

In relation with the safety lifecycle adopted in IEC 61508, the CCFs between the required SIS and existing barriers should be considered and treated appropriately in both the SIL allocation and realization phase. As more information and data about the SIS can be acquired, the CCFs can then be updated and modeled more accurately in SIS realization phase. The SIL allocation is an iterative process. If CCF fraction is found to be sufficiently low, the baseline SIL can be applied. If the analysis that includes CCFs indicates that the tolerable risk cannot be achieved based on initial assumptions, then design changes will be needed (IEC 61508, 2010). If design changes are not possible, a higher SIL requirement shall be applied and specification for the SIS shall be modified. Figure 21 shows the timeline process of SIL requirement when treating CCFs between the designated SIS and existing protection layers.

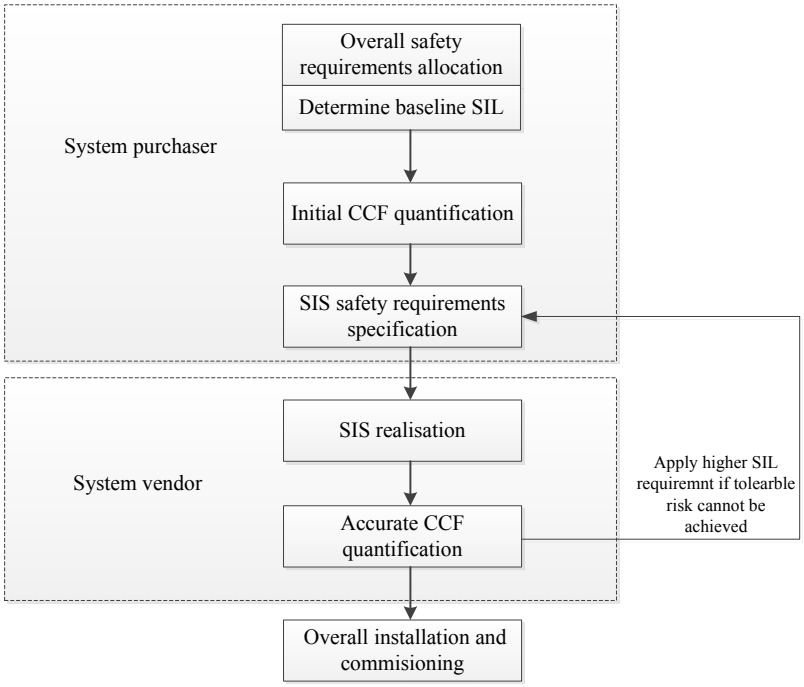



**Figure 21 Timeline process of SIL determination in relation with safety lifecycle**

## 6.2 Checklist of quantifying CCF in SIL determination phase

IEC 61508 gives the following requirements if the EUC control system, E/E/PE safety related systems and other risk reduction measures are to be treated independently (IEC 61508, 2010):

- be independent such that the likelihood of simultaneous failures between two or more of these different systems or measures is sufficiently low in relation to the required safety integrity;
- be functionally diverse (i.e. use totally different approaches to achieve the same results);
- be based on diverse technologies (i.e. use different types of equipment to achieve the same results);
- not share common parts, services or support systems (for example power supplies) whose failure could result in a dangerous mode of failure of all systems;
- not share common operational, maintenance or test procedures.

If not all of the requirements can be met, the SIS and the other risk reduction measures shall not be treated as independent for the purposes of the safety allocation. Based on the above requirements in IEC 61508 considering CCFs in the SIL determination phase, the checklist in Table 19 is proposed for initial CCF quantification.

Table 19 Checklist for CCFs in SIL determination phase

| Questions | Points | Answers |
|---|---|---|
| **Separation/segregation** | | |
| • Will the different protection layers share some common components? | 10 | ☐ Yes ☐ No |
| • Will the different protection layers share the same utility, service or support system (e.g. power supplies, heat tracing, etc.)? | 10 | ☐ Yes ☐ No |
| **Diversity** | | |
| • Do the channels employ different electrical principles/designs/technology, for example, digital and analogue, different manufacturer (not re-badged) or different technology? | 10 | ☐ Yes ☐ No |
| • Do the two different protection layers employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc? | 10 | ☐ Yes ☐ No |
| **Redundancy** | | |
| • Will separate test methods and people be used for each protection layer during commissioning? | 10 | ☐ Yes ☐ No |
| • Will there be different people to carry out maintenance on each protection layer at different times? | 10 | ☐ Yes ☐ No |
| **Competence/training/safety culture** | | |
| • Will designers be trained to understand the causes and consequences of common cause failures? | 10 | ☐ Yes ☐ No |
| • Will maintenance personnel be trained to understand the causes and consequences of common cause failures? | 10 | ☐ Yes ☐ No |
| **Environmental control/ Maintenance** | | |
| • Will there be any components in the different protection layers that are always exposed to the same environmental impacts (excessive stress on both systems)? | 10 | ☐ Yes ☐ No |
| • Will the different protection layers share common operational, maintenance or test procedures? | 10 | ☐ Yes ☐ No |

The above checklist consists of 10 questions to be asked against the CCFs between the SIS required and existing protection layers. In the checklist, each question has been weighted equally. The answers will be scored individually and the points will be given if the answer is positive to CCFs contribution. The checklist is developed based on the checklist used in IEC 61508 for determining beta value of different channels within a safety related system. The categories are similar to the ones in IEC 61508 checklist. It should be noted that this checklist

is designated to be used in an early stage, where very little information is available. At this phase, a very coarse estimation of CCFs can be achieved.

After all the questions have been answered, the aggregate score is then linked to a CCF fraction. The relation between the checklist scoring and CCF fraction is shown in Table 20. The table below broadly corresponds to the similar calculation of beta values table in IEC 61508.

**Table 20 CCFs fraction in relation with checklist scoring**

| Score range | CCF fraction |
|---|---|
| 80-100 | 10% |
| 50-80 | 5% |
| Under 50 | Less than 5% |

## 6.3 Some challenges of CCFs quantification of two different protection layers in the SIS realization phase

In the realization phase, more information and data can be acquired about the SIS under consideration; a more accurate quantification of CCFs can be achieved. In this phase, the two different protection layers can be treated as a whole system for reliability analysis. Figure 22 illustrates the reliability block diagram including different protection layers.

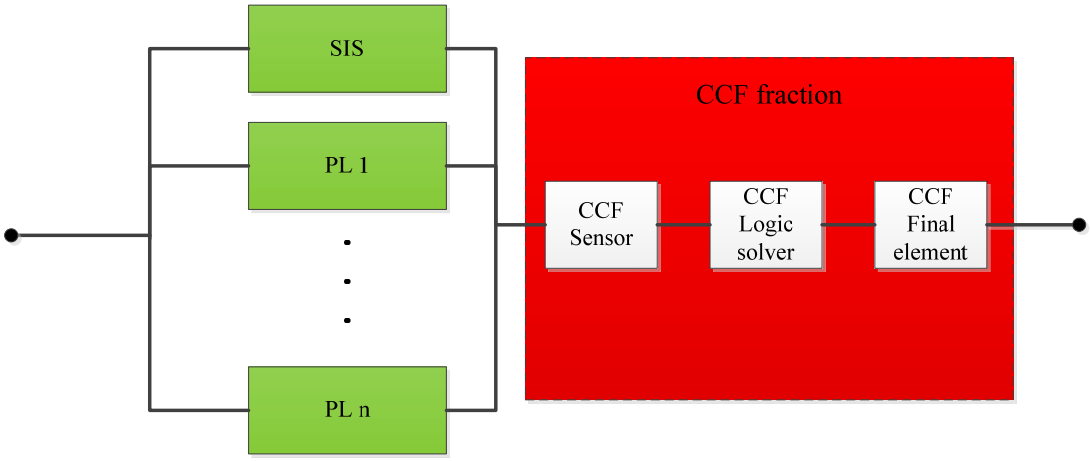



**Figure 22 Illustration of CCF fraction**

There are some challenges associated with quantification of CCFs in different protection layers. The traditional CCF models are used to quantify CCFs within the same system. However, CCFs between different protection layers have not yet been given appropriate attention. The question is how to model CCFs between non-identical components in different protection layers.

### 6.3.1 Which model to choose to quantify the CCFs?

There exist different approaches for modeling CCFs. Generally, the CCFs modeling approaches can be classified as explicit method and implicit method. The explicit method can be applied when the causes of dependency failures are identified and defined. These causes of dependency include, for example, human errors, utility failures and environmental events. By the explicit method, the cause of dependency is included into the system logic models, for example as a basic event in the fault tree model, or as a functional block in a reliability block diagram (Rausand, 2011).

However, in most situations, the causes of dependent failures are difficult or even impossible to be modeled explicitly. They are modeled using implicit method.

For reliability analysis of SISs, it is very difficult to identify all the causes of dependent failures. Thus, implicit method should be applied. The implicit models include the beta factor model, alpha model, multiple Greek letter model and binomial failure rate model. The beta factor model has gained wide acceptance in the process industry. It is also a recommended approach to model CCFs within safety instrumented system in IEC 61508. The main challenge with these models is lack of relevant data to support model parameters (Haugen et al, 2010).

### 6.3.2 How to quantify CCFs among components with different failure rates?

In most situations, components in different protection layers have non-identical failure rates for dangerous undetected (DU) failures, i.e. $\lambda_{DU,A} \neq \lambda_{DU,B}$ . To model CCFs using the beta factor model, we first need to select a "representative" failure rate for the non-identical components. We may choose between two approaches (Hauge et al, 2010):

- Use some representative average value, typically the geometric mean of the CCF failure rates of the two components, i.e. $PFD_{1oo2}^{CCF} = \beta_{A,B}\sqrt{\lambda_{DU,A} \cdot \lambda_{DU,B}} \cdot \tau / 2$
- Use the lowest failure rate of the two components, i.e. $PFD_{1oo2}^{CCF} = \beta_{A,B} \cdot Min(\lambda_{DU,A}, \lambda_{DU,B}) \cdot \tau / 2$

For redundant components with non-identical failure rates, using the geometric mean has often been the preferred method. This is an adequate approach if the failure rates are of the same magnitude. However, for components with very different failure rates (e.g. different magnitude of failure rates), the weighting of the largest failure rate will become dominant and in extreme cases the CCF contribution may exceed the likelihood of an independent failure of the most reliable component (Hauge et al, 2010).

The logical foundation for the second approach is that when having two or more redundant components, the rate of CCFs of the combined system will be governed by the component with the most reliable component, i.e. with lowest failure rate. This approach is used when the failure rates have different order of magnitude. The minimum failure rate approach, however, is not necessarily appropriate in situations with several components where the failure rates differ considerably (Hauge et al, 2010).

### 6.3.3 How to Select Beta factors for non-identical components

Fundamentally, the factor beta represents the conditional probability of the component failure given that the redundant component has failed. It is also the proportion of CCFs of each component. For example, consider two redundant and identical components A and B. The beta factors are denoted $\beta_A$ and $\beta_B$ respectively.

$$\beta_A = \text{Pr (B fails | A fails)} = \text{Pr (A fails | B fails)} = \beta_B$$

It is reasonable to determine a universal beta value for the redundant components if they are identical. But, it will be more difficult to select a beta value for non-identical components.

Hauge (2010) suggested two approaches: one is to select the lowest value of $\beta_A$ and $\beta_B$ or event lower in case of high degree of diversity; the other approach is to select a beta value based on expert judgments and failure cause analysis.

The checklist from IEC 61508 may also be used to determine the beta factor for non-identical components, although some modifications may be needed to suit for the difference with identical channels.

### 6.3.4 How to select test interval for components with non-identical intervals

For components with different test intervals, the question becomes how to select the test interval to be used in CCF quantification. Hauge (2010) suggested using the average test interval of the redundant components. For instance, there are N redundant components and each has a test interval denoted as $\tau_i$. The average interval can be determined by:

$$\bar{\tau} = \frac{1}{N}\sum_{i=1}^{N}\tau_i$$

## 6.4 A case study on LOPA taking into account CCFs

Consider a subsea process which consists of a pressurized vessel and associated control systems. The process is illustrated in Figure 23. The vessel contains hydrocarbons fed through the pipeline from a subsea well. The basic process control system (BPCS) is responsible for controlling the process. It monitors the signals from level transmitter (LT) and controls the operation of the level control valve (LCV). The existing safety system available is a non-instrumented protection layer (PL 1) to address the hazards associated with vessel overpressure. If the protection layer operates successfully, the releases from the protection layer are piped to a knock out tank, thus avoiding releases to the environment.

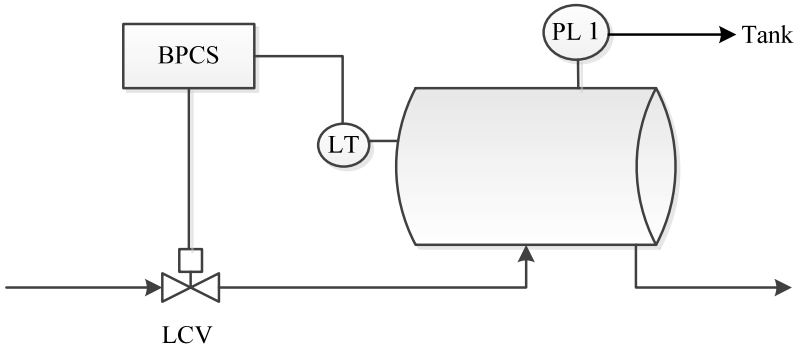



**Figure 23 Illustration of the process**

A HAZOP study has been conducted to assess the risk associated with this process. The results of HAZOP study is presented in Table 21.

**Table 21 HAZOP study results (adapted from IEC 61511, 2004)**

| Item | Deviation | Causes | Consequences | Safeguards | Action |
|---|---|---|---|---|---|
| Vessel | High pressure | High level | Release to environment | BPCS<br><br>Non-instrumented protection layer | Evaluate conditions for release to environment and consider risk reduction measures if necessary |
| | Low/no flow | Failure of BPCS | No consequence of interest | | |
| | Reverse flow | | No consequence of interest | | |

We assume that the risk acceptance criteria for the process is defined as the frequency of release to the environment due to vessel over-pressurization shall be less than $1 \cdot 10^{-7}$ per year.

The results of the HAZOP study have been used for the LOPA analysis. The LOPA team has selected release to environment due to high pressure as impact event for further LOPA analysis. The consequences due to the other deviations are not of interest.

It should be noted that there is modification of modeling approach of the scenario. Fundamentally high level is caused by failure of BPCS, which works in a continuous mode. The frequency of such failure is assumed to be 0.001 per year. However, in order to analyze the CCFs between BPCS and the SIS to be implemented, we treat the BPCS as a protection layer which works on demand and the initiating event is high level with a frequency assumed to be 0.1 per year. The IPLs which can prevent the consequence of release to environment are BPCS and the non-instrumented protection layer. The BPCS is assumed to have a PFD of 0.01 and the non-instrumented protection layer PL1 has a PFD of 0.1. The results of LOPA study are listed in Appendix II Table 22.

The intermediate event likelihood is 1.00E-04 and this is still above the acceptance criteria of tolerable frequency 1.00E-06. Further risk reduction is required to meet the risk acceptance criteria. The LOPA team first evaluated the possibility of risk reduction using non-SIS protection layers, but found that it is not feasible. Thus a SIS is needed for further risk reduction. In order to reduce the frequency of release to environment to a tolerable level, a SIL 2 safety instrumented system shall be implemented. This is determined as a baseline SIL requirement based on the assumption that the SIS is independent with the existing protection layers. A general SIS design concept has been determined. Two pressure transmitters will be used to detect overpressure in the vessel and send signals to a logic solver, which controls the operation of a shutdown valve in the supply pipeline. The two pressure transmitters are arranged in 1oo2 configuration. The design concept is illustrated in Figure 24.

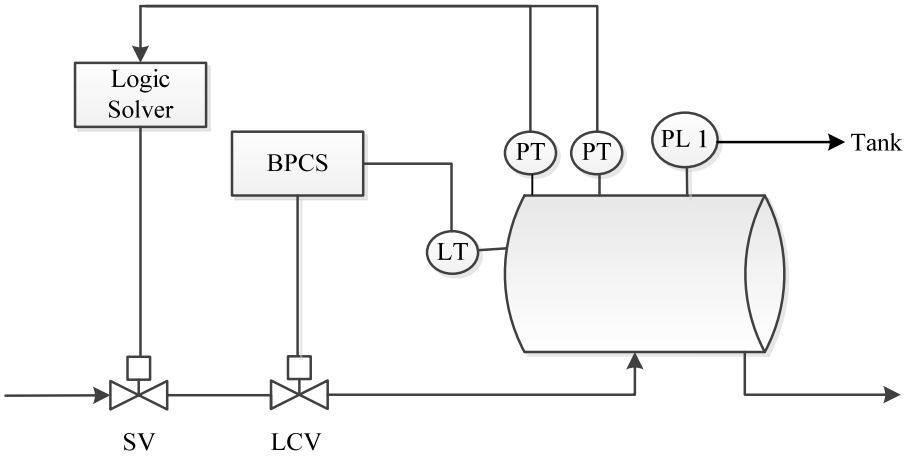



Figure 24 General concept of the new SIS

However, there exist CCFs between the pressure transmitters and level transmitter, the shutdown valve and level control valve. Although the shutdown valve and level control valve are two different types of valves, they are "seeing" the same fluid. The pressure transmitters and level transmitter are exposed in the same environment. CCFs can occur between the sensors as well as the valves which are located on the different protection layers. As the BPCS is separate with logic solver of the new SIS, it is reasonable to believe that there are no CCFs between the BPCS and the logic solver.

We can obtain an aggregate score of 30 by using the proposed checklist for initial CCFs quantification. Table 23 in Appendix III shows the results of CCF checklist. This corresponds to a CCF fraction lower than 5%. Therefore, a baseline SIL 2 is allocated to the SIS. However, further cautions should be taken against CCFs and a more accurate quantification shall be conducted in the SIS realization phase to demonstrate that the tolerable risk is achieved.

# Chapter 7 Discussion

In this thesis, several new methods have been proposed in light of SIL determination for subsea SISs. There are also some weaknesses in the proposed methods.

The alternative ERAC is solely based on release volumes. The categorization of environmental damage based on the release volumes can be questioned. Restitution time is used for categorization in the current ERAC. The link between release volume and restitution time shall be established based on and supported by scientific research. The justification for the proposed ERAC is not fully grounded.

The fault tree illustration is based on PFD value 0.01 and the two protection layers have the same order of magnitude PFD value. What if the PFD value is higher or lower than 0.01 range? What will be the difference when the PFD values of the protection layers are not in the same order of magnitude?

The checklist is proposed to quantify CCFs in the early phase. It broadly corresponds to the beta value in IEC 61508 checklist. Is the checklist a complete list of factors associated with CCFs? Are there any other factors that influence CCFs in two different protection layers?

In the case study, we modified the modeling approach for the failure of BPCS. High level is caused by failure of BPCS, which works in a continuous mode. The frequency of such failure is assumed to be 0,001 per year. In order to analyze the CCFs between BPCS and the SIS to be implemented, we treat the BPCS as a protection layer which works on demand and the initiating event is high level with a frequency assumed to be 0.1 per year. The BPCS is treated as an IPL working on demand with a PFD of 0. 01. This modification shall be questioned.

# Chapter 8 Conclusions and further work

The main objective of this thesis has been to investigate the risk based approaches for determination of safety /environmental integrity level of SISs. Hazard matrix, safety layer matrix, risk graph, calibrated risk graph, the OLF approach and LOPA have been described and discussed. Risk graph and LOPA have been the focus and recommended approach for SIL determination for subsea SISs. However, some modifications and adaptations shall be needed to suit the special situations of subsea applications. This leads to the proposal of the new methods in this thesis. The sub-objectives of this thesis are listed below and the coverage and findings of each objective is discussed.

- Literature study of different SIL determination methods like risk graph, safety layer matrix, and LOPA

Literature study of different SIL determination methods has been carried out. Different approaches and methodologies have been described and discussed in depth. The different SIL determination methods covered are hazard matrix, safety layer matrix, risk graph, calibrated risk graph, OLF approach and LOPA. However, the quantitative risk analysis approach for SIL determination is not covered. The reader can refer to IEC 61511.

- Discuss pros and cons of different SIL determination methods

This objective has been accomplished. Strength and disadvantages of different SIL determination methods have been discussed following the presentation of each method.

- Discuss in particular challenges with applying LOPA when there are dependencies between the SIS and other layers of protection

The challenges with applying LOPA when there are dependencies between the SIS and other layers of protection has been found to be how to model CCFs in the SIL determination context. The effect of CCFs between the SIS and other protection layers on the actual risk reduction have been demonstrated by a fault tree. A framework incorporating LOPA and CCFs analysis between the designated SIS and other protection layers have been proposed. The framework includes CCFs quantification in two phases: SIL determination phase and SIL realization phase. A checklist for CCFs quantification in early phase is proposed. Challenges associated with quantification of CCFs in different protection layers during SIS realization phase are discussed.

- Identify challenges encountered when the consequence dimension is environment in contrast to the more familiar personnel risk

The challenge of SIL determination situations where the consequence dimension is environment has been found to be the lack of suitable ERAC for developing requirements for technical barriers. The current ERAC on the Norwegian continental shelf is presented. The shortcomings of ERAC in the MIRA guideline are discussed in details. An alternative ERAC based on release volumes have been proposed.

- Based on the results obtained, propose a method for determination of SIL in the given context, and test the method in a simple case study

This objective is accomplished. The marinized risk graph approach is tested by a drilling BOP case study, using the alternative ERAC proposed. The LOPA approach including CCFs analysis is tested by a case study. The proposed checklist for initial CCFs quantification is demonstrated.

The weaknesses of the proposed methods are discussed in the previous chapter. Further research is required to solve those questions in the discussion section and the challenges.

## References

Anniken Reusch Berg (2007) Applicability of Layer of Protection Analysis to determine Safety Integrity Levels in the Process Industry. Master thesis, NTNU.

Baybutt, P. (2007). An improved Risk Graph Approach for Determination of Safety Integrity Levels (SILs). Process Safety Progress, 26:66–76.

Christopher Lassen (2008) Layer of protection analysis (LOPA) for determination of safety integrity level (SIL). Master thesis NTNU.

CCPS (2001). Layer of protection analysis - simplified process risk assessment. American Institute of Chemical Engineers (AIChE), Centre for Chemical Process Safety (CCPS). 3 Park Avenue, New York.

Eni-Norge (2010). Calibrated risk graph. Goliat development proeject.

Gulland W.G. (2004) Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons. 4-sight Consulting.

Hauge S. et.al. (2010) Barriers to prevent and limit acute release to sea – environmental risk acceptance criteria and requirements to safety systems. SINTEF Technology and Society, Safety Research.

Hauge S., Håbrekke S ,and Lundteigen M. (2010) Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection, 2010 Edition. SINTEF Technology and Society, Safety Research.

IEC 61508 1-7 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission, Geneva.

IEC 61511 (2004). Functional safety - safety instrumented systems for the process industry sector. International Electrotechnical Commission, Geneva.

K. Cornelliusen,2002) Approaches to the determination of safety integrity levels (SIL) for Safety Instrumented Systems (SIS); comparison and discussion. NTNU, Trondheim.

Lundteigen M. (2008). Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability. Doctoral thesis, NTNU.

Metode for Miljørettet Risikoanalyse (MIRA) (2007), OLF.

Marszal, E. and Scharpf, E. (2002). Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis. The Instrumentation, Systems and Society (ISA). Research Triangle Park, NC.

NORSOK Z-013 (2010) Risk and emergency preparedness analysis. Norwegian Technology Centre.

OLF 070 (2004) Application of IEC 61508 and IEC 61511 in the Norwegian petroleumindustry. OLF.

Rausand, M. and Høyland, A.(2004): "System Reliability Theory: Models, Statistical methods, and Applications" (2nd ed.), Wiley, Hoboken, 2004.

Rausand, M. (2007) Hazard and Operability Study slides. Retrieved on 2nd May from internet address : http://frigg.ivt.ntnu.no/ross/slides/hazop.pdf.

Rausand, M. (2011): "Risk Assessment: Theory, Methods, and Applications," Wiley, Hoboken, 2011.

Vinnem J.E. (2007) Offshore Risk Assessment Principles, Modelling and Applications second edition - Springer series in reliability engineering.

## Appendix I – Acronyms and Abbreviations

| | |
|---|---|
| BOP | Blow out preventer |
| BPCS | Basic process control system |
| CCF | Common cause failure |
| CCPS | Center for Chemical Process Safety |
| DU | Dangerous undetected |
| EUC | Equipment under control |
| EIL | Environmental integrity level |
| ERAC | Environmental risk acceptance criteria |
| FAR | Fatal accident rate |
| HAZOP | Hazard and operability study |
| IEL | Intermediate event likelihood |
| IPL | Independent protection layer |
| LOPA | Layer of protection analysis |
| LCV | Level control valve |
| MIRA | Miljørettet Risikoanalyse (English: Environmental risk analysis) |
| MTBD | Mean time between damage |
| NORSOK | Norsk sokkels konkurranseposisjon (English: Competitive position for the Norwegian continental shelf) |
| NCS | Norwegian Continental Shelf |
| OLF | Oljeindustriens landsforening (English: The Norwegian Oil Industry Association) |
| OREDA | Offshore Reliability Data |
| PFD | Probability of failure on demand |

| | |
|---|---|
| PFH | Probability of a dangerous failure per hour |
| PHA | Preliminary hazard analysis |
| PLL | Potential loss of life |
| PL | Protection Layer |
| QRA | Quantitative risk analysis |
| RT | Recovery time |
| SV | Shutdown valve |
| SIF | Safety instrumented function |
| SIL | Safety Integrity Level |
| SIS | Safety instrumented system |
| SRS | Safety Requirement Specification |
| TMEL | Target mitigated event likelihood |

## Appendix II – LOPA results for the case study

**Table 22 LOPA worksheet for the case study**

| | Impact event | | Initiating event | | Protection layers | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| Reference nr. | Description | Severity level | Initiating event | Initiating event likelihood | General process design | BPCS | Alarms, etc | Engineered mitigation | Additional mitigation | Intermediate event likelihood | SIF integrity level | Mitigated event likelihood | Notes |
| 1 | Release to environment from the vessel Tolerable frequency 1,00E-6 | S | High level | 0,1 | 1 | 0,01 | 1 | 0,1 | 1 | 1,00E-04 | 1,00E-02 | 1,00E-06 | High pressure causes release to environment |
| | | | | | | | | | | | | | |

Note: Severity level E = Extensive; S = Serious; M = Minor

Likelihood values are events per year; other numerical values are probabilities of failure on demand average.

## Appendix III – Checklist results for the case study

Table 23 Checklist results for the case study

| Questions | Points | Answers |
|---|---|---|
| **Separation/segregation** | | |
| • Will the different protection layers share some common components? | 10 | ☐ Yes ☒ No |
| • Will the different protection layers share the same utility, service or support system (e.g. power supplies, heat tracing, etc.)? | 10 | ☒ Yes ☐ No |
| **Diversity** | | |
| • Do the channels employ different electrical principles/designs/technology, for example, digital and analogue, different manufacturer (not re-badged) or different technology? | 10 | ☒ Yes ☐ No |
| • Do the two different protection layers employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc? | 10 | ☒ Yes ☐ No |
| **Redundancy** | | |
| • Will separate test methods and people be used for each protection layer during commissioning? | 10 | ☒ Yes ☐ No |
| • Will there be different people to carry out maintenance on each protection layer at different times? | 10 | ☒ Yes ☐ No |
| **Competence/training/safety culture** | | |
| • Will designers be trained to understand the causes and consequences of common cause failures? | 10 | ☒ Yes ☐ No |
| • Will maintenance personnel be trained to understand the causes and consequences of common cause failures? | 10 | ☒ Yes ☐ No |
| **Environmental control/ Maintenance** | | |
| • Will there be any components in the different protection layers that are always exposed to the same environmental impacts (excessive stress on both systems)? | 10 | ☒ Yes ☐ No |
| • Will the different protection layers share common operational, maintenance or test procedures? | 10 | ☒ Yes ☐ No |
| **Aggregate score** | 30 | |