A CONCISE BEST PRACTICE GUIDE ON

RISK ASSESSMENT

A PUBLICATION OF THE
DUTCH SIL PLATFORM

NEN

SIL Platform

OCTOBER 2018

ABBREVIATIONS AND TERMS

Abbreviations

CBA	Cost Benefit Analysis
EUC	Equipment under Control Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities
HAZOP	Hazard and Operability Analysis
IC	Initiating Causes
IEC	International Electrotechnical Commission
IMEL	Intermediate Event Likelihood
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
MSP	Mechanical Safety Provision
PFD	Probability of Failure on Demand
PSP	Procedural Safety Provision
RAM	Risk Assessment Matrix
RRF	Risk Reduction Factor
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System The SIS is the tangible system that provides the SIF's functionality as set out in the SRS
SRS	Safety Requirement Specification
TMEL	Target Mitigated Event Likelihood

Terms (according to ISO/IEC guide 51:2014)

Harm	Injury or damage to the health of people, or damage to property or to the environment
Harmful event	Hazardous event which has caused harm
Hazard	Potential source of harm
Hazardous event	Event that can cause harm
Hazardous situation	Circumstance in which people, property or the environment are exposed to one or more hazards
Mitigation	Action that reduces the consequence(s) of a hazardous event
Risk	Combination of the probability of occurrence of harm and the severity of that harm
Tolerable risk	Level of risk which is accepted in a given context based on the current values of society

WHAT IS THE SIL PLATFORM?

The SIL Platform is an independent group of experienced users or adopters of the SIL philosophy, according to the IEC standards 61508 and 61511, in the Dutch process industry. The SIL Platform is linked to the Royal Dutch national standardization committee NEC 65 that follows the international work of IEC/TC65, industrial measurement, control and automation. At the time of release of this document, over 50 people, representing end-users, engineering companies, suppliers, manufacturers and consultancy firms, are a member of the SIL Platform. They frequently get together to share specific topics and challenges that occur when implementing SIL in applications in the process industry. One of which is the correct use of risk levels and matrices. This paper explains the adoption of a Risk Assessment Matrix.

SUBJECTS IN THIS BEST PRACTICE GUIDE

PURPOSE OF THIS GUIDE 01

WHAT IS THE PURPOSE OF THIS GUIDE AND HOW DOES THIS RELATE TO THE SIL PLATFORM?

The position paper of the SIL Platform (www.nen.nl) indicates that it is common practice to operate process plants at maximum performance, optimum capacity and minimum risk levels. A Safety Integrity Level (SIL) is often determined through e.g. a Layer of Protection Analysis (LOPA) [1] [2] [3], which is a means to quantify risks. However, LOPA is usually not the starting point for quantifying risks. This is often done with the use of a Risk Assessment Matrix (RAM). Contrary to LOPA and SIL, the use and type of RAM is not clearly pre-scribed or defined.

The intention of this guide is to provide guidance on RAM and show the relations between RAM, LOPA and SIL levels. What are the pitfalls? What is usually applied? What is often missed? It is not the intention to explain in detail the various available risk assessment techniques.

How to arrive at a SIL level in the correct manner leading to a qualitatively proper design and implementation is described in the EN-IEC 61511 standard [4]. Achieving a SIL requires amongst other aspects:

- Correct identification of Safety Instrumented Functions (SIF)
- Correct determination of required SIL rating of the various SIFs.

This guide strives to improve this quality by improving the quality of the risk assessment(s) providing input to the SIL determination. The targeted audience of this guide is the Dutch Process Industry Sector.

02 DEFINITIONS AND LEGISLATION

HOW ARE TOLERABLE RISK LEVELS DEFINED AND PERCEIVED BY DUTCH LEGISLATION?

The Dutch legislation does not define a tolerable risk for on-site accidents resulting in fatalities. The view of the Dutch authority Inspectorate SZW for fatalities on the workplace is founded in the legislation for public safety, in particular the Public Safety (Establishments) Decree [Besluit externe veiligheid inrichtingen - BEVI]. This Decree distinguishes between individual risk and societal risk [5] as described in Box 1.

Individual risk and societal risk [5]

- Individual risk represents the risk of an (unprotected) individual dying as a direct result of an on-site accident involving dangerous substances. Individual risk is visualized by risk contours on a map. The limit value for vulnerable objects is equal to $1x10^{-6}$ per year: no vulnerable objects are allowed within this 10^{-6} risk contour. For 'less vulnerable' objects (like small offices) the 10^{-6} contour is a target value.

- Societal risk represents the risk of an accident occurring with N or more people being killed in a single accident. The societal risk is presented as an FN-curve. For the societal risk a guide value is used. The competent authority must account for the height of the societal risk in relation to socio-economic benefits.

These tolerable frequencies reflect the risk as a result of all potential on-site accidents involving dangerous substances. From here on the Inspectorate SZW reasons along the line that the labor force is subjected to a (somewhat) higher risk, due to its presence in the affected area of the on-site accident. In an internal document [6] not to be found on internet, the Inspectorate SZW states that 10^{-5} is a widely used upper limit for the individual risk where an individual fatality arises as a direct result of an on-site accident.

From here on the Dutch legislation does not provide guidance for on-site accidents resulting in fatalities for which the process industry sector claims ALARP. It is from the British Health & Safety Executives' (HSE) document Reducing Risk, Protecting People (R2P2) [7] that one can find guidance. Figure 1 shows the various limits related to people at risk as propagated by HSE UK. In section 5 additional information regarding ALARP is presented.

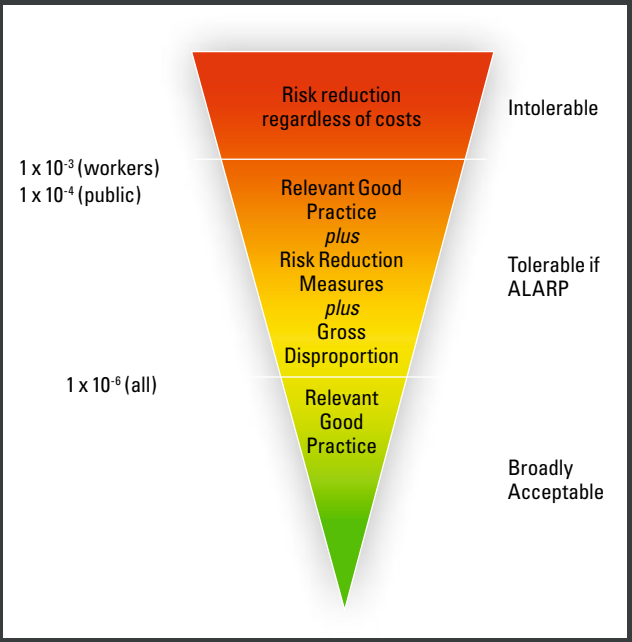


Figure 1: ALARP region according to HSE UK

RISK ASSESSMENT TECHNIQUES

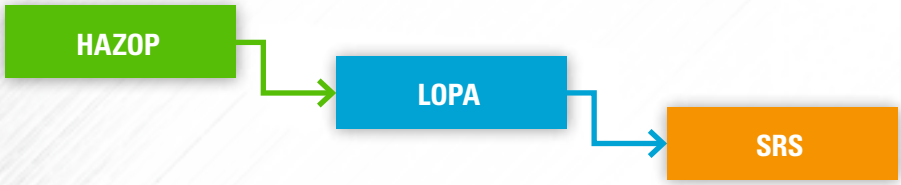
03

WHICH BASIC RISK ASSESSMENT TECHNIQUES ARE USED?

The paper from David Valis and Miroslav Koucky [8] gives a concise overview of most risk assessment techniques ranging from comparative methods (i.e. checklists and audits) to failure logics (i.e. fault tree, event tree's) up to fundamental methods such as HAZOP study [9] and FMECA.

A SIL rating usually takes place during a risk assessment method such as LOPA (Layer of Protection Analysis). After the SIL rating (LOPA) a Safety Requirement Specification (SRS) shall be made.

Figure 2: Example showing some typical steps for a Safety Requirement Specification (SRS)



To obtain a reliable SRS it is therefore important that both HAZOP study and LOPA are carried out in a correct manner. How to conduct a HAZOP study or LOPA has been described in many papers & training materials and will not be repeated here.

The results of HAZOP study and LOPA, and, as a consequence, of the SIL determination, depend on the choice (and use) of the Risk Assessment Matrix (RAM). There are, to some extent, objective criteria for a RAM to be found in national legislation and European legal systems. The calibration (design) of the RAM is straight forward and discussed by Timms [10]. Since this paper intends to give guidelines in this area, this will be further discussed in the next sections.

04

RISK ASSESSMENT MATRIX

HOW TO DEFINE A RISK ASSESSMENT MATRIX?

The primary reason we focus on Risk Assessment and Risk Management is that we need to quantify risk in order to be able to determine the effectiveness and extent of the risk reduction measures we need to implement to operate a plant. Hence, it is important to define risk.

Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm. Risk is essentially the product of cause and effect on a defined scale. Engineering practice requires to express risk in two metrics: Severity and Likelihood.

Taking these metrics into account, we can develop a scale in which to measure risk. This can be numeric. Below is a list in colloquial language and ordinal scales [11].

	SEVERITY CATEGORIES				
	1 Negligible	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
Safety and Health	**Minor Injury,** Medical Treatment Case with/or Restricted Work Case	**Serious Injury** or Lost Work Case	**Major or Multiple Injuries,** Reversible injury or non-disabling permanent injury	**Single Fatality,** Permanent disability	**Multiple Fatalities,** Up to 10 fatalities

Table 1: Severity Categories Description

LIKELIHOOD CATEGORIES						
7 Very frequent > 1 /year	**6 Probable** 10^{-1} - 1 /year	**5 Sporadic** 10^{-2} - 10^{-1} /year	**4 Remote** 10^{-3} - 10^{-2} /year	**3 Improbable** 10^{-4} - 10^{-3} /year	**2 Very Unlikely** 10^{-5} - 10^{-4} /year	**1 Insignificant** 10^{-6} - 10^{-5} /year
Incident is very likely to occur on this location, possibly several times per year	Incident is likely to occur on this location	Incident has occurred on a similar location or within company	Incident is unlikely to occur within company and has occurred in industry	Incident is unlikely to occur on this location and has occurred in industry	Incident is highly unlikely to occur within company, but heard of in industry	Incident is highly unlikely to occur on this location, but heard of in industry

Table 2: Likelihood Categories Description

One of the objectives of this paper is to examine risk matrices used in the industry and determine a more general severity and likelihood scale that can be used in any generic risk assessment task.

Plotting these scales creates an ordinal matrix to quantify the Risk "zones". In many cases developers tend to multiply (or some other mathematical method) the ordinal value on the axis as if it were an interval scale:

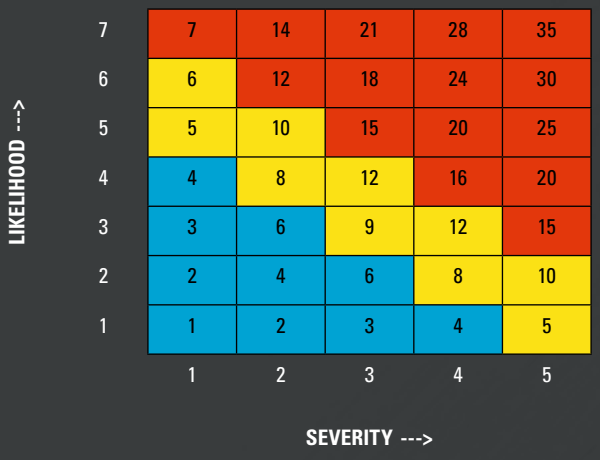


Figure 3: Example Risk Matrix

Blue indicates the Low-risk or Tolerable Risk zone, and Red the high-risk or Intolerable Risk zone. Risks can be reduced by measures that prevent the event from happening or by measures that mitigate the consequences as the event happens.

From a mindset perspective the color blue is preferred instead of green. The color green is associated with the perception that the situation is safe, which is not the case; it is only that the risk is perceived as tolerable, e.g. we tolerate one fatality every million years, however, we do not accept the fatality.

Examples

- Event:
  Rupture of a pipe due to (too) high pressure.

- Measures to reduce frequency of event (likelihood):
  Control system measuring the pipe pressure and stopping a pump or HIPPS system protecting a lower rated downstream pipe system by quick closure of a valve.
  Introducing this type of measures brings the hazard downwards in the risk matrix, from the red or yellow area towards the blue area

- Measures to limit severity of event:
  Blast wall
  Introducing a mitigation measure brings the hazard horizontally from the red or yellow area towards the blue area

In general the intention is to reduce intolerable unmitigated (raw) risks (falling in the red areas in the matrix), with the use of credible and independent safeguards, down to tolerable mitigated (residual) risks (bringing it in the blue areas).

Between the intolerable and tolerable risk there is a yellow area where the assessment of the risk is not straightforward. Smaller companies are likely to choose for a more safe solution (risk aversion) treating this area as a red zone, while larger companies, on the other hand, might follow a strict calculation. Most companies will use ALARP (As Low as Reasonably Practicable). ALARP is explained in section 5. The ALARP zone is indicated in yellow, this is why many matrices have only three colors: blue, yellow, red.

HOW TO APPLY ALARP?

05

If mitigated risks end up in the "yellow" (ALARP) area proof has to be provided that the risk can practically and reasonably not be reduced further to reach tolerable levels.

Of particular importance in the interpretation of ALARP is Edwards versus The National Coal Board (1949). This case established that a computation must be made in which the quantum of risk is placed on one scale and the sacrifice, whether in money, time or trouble, involved in the measures necessary to avert the risk is placed in the other; and that, if it be shown that there is a gross disproportion between them, the risk being insignificant in relation to the sacrifice, the person upon whom the duty is laid discharges the burden of proving that compliance was not reasonably practicable. An introduction to ALARP is written by the HSE authority in the UK [12] and on risk reduction [7].

There are three strategies that can be followed to determine that risks have been reduced to ALARP:

1. Good Practice Arguments: ALARP shall be argued by a comparison between the control measures a company has in place and the measures authorities would normally expect to see in such circumstances (i.e. relevant good practice).

2. Qualitative First Principles Arguments: The second approach to determine ALARP is from first principles, i.e. by exercising professional judgement, or experience.

3. Quantitative First Principles Arguments: there are some instances (often in high hazard industries or where there is a new technology with possible serious consequences) where the situation is less clear-cut. In these instances, a more formal Cost Benefit Analysis (CBA) may provide additional insight to come to a judgement. In any case, the outcome of a CBA is only one of several considerations that go towards the judgement that a risk has been reduced ALARP. For single and/or multiple fatalities a formal CBA is considered to be a mandatory practice so as to avoid that the repercussions of such possible consequences are taken lightly or being underestimated.

The level of detail in a risk assessment shall be proportional to the level of the hazards. In general, the greater the magnitude of the hazards under consideration, and the greater the complexity of the systems being considered, the greater the degree of rigour and robustness (and hence the greater the level of detail) a company requires in arguments to show that risks have been reduced ALARP. The level of risk arising from the undertaking shall therefore determine the degree of sophistication needed in the risk assessment.

A universal practice in the industry may not necessarily be good practice or reduce risks ALARP. A company shall not assume that it is. A company shall keep its acceptance of good practice under review since it may cease to be relevant as time goes by; new legislation may make it no longer acceptable; new technology may make a higher standard REASONABLY PRACTICABLE.

The depth of analysis shall be fit for purpose, i.e. more rigour is required where the risk is higher or the consequences themselves are great e.g. multiple fatalities.

Disproportion Factor (DF)

Although there is no authoritative case law which considers the question what is to be 'gross' disproportionate, it is believed that the greater the risk the higher the proportion may be before being considered 'gross'. But the disproportion must always be gross. No algorithm has been formulated that can be used to determine the proportion factor for a given level of risk. The extent of the bias must be argued in the light of all the circumstances. It may be possible to come to a view in particular circumstances by examining what factor has been applied in comparable circumstances elsewhere to that kind of hazard or in that particular industry. Taking greater account of the benefits as the risk increases also compensates to some extent for imprecision in the comparison between costs and benefits. It goes wrong on the side of safety, since the consequences of the inaccuracy have greater impact, in terms of the degree of unforeseen death and injury, as the risklevel rises.

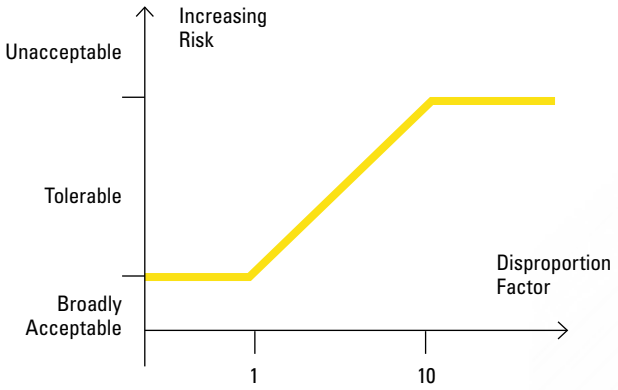


Figure 4: ALARP in relation to Disproportion Factor

LOPA, HAZOP AND SIL

06

HOW DOES LOPA RELATE TO HAZOP STUDY AND SIL?

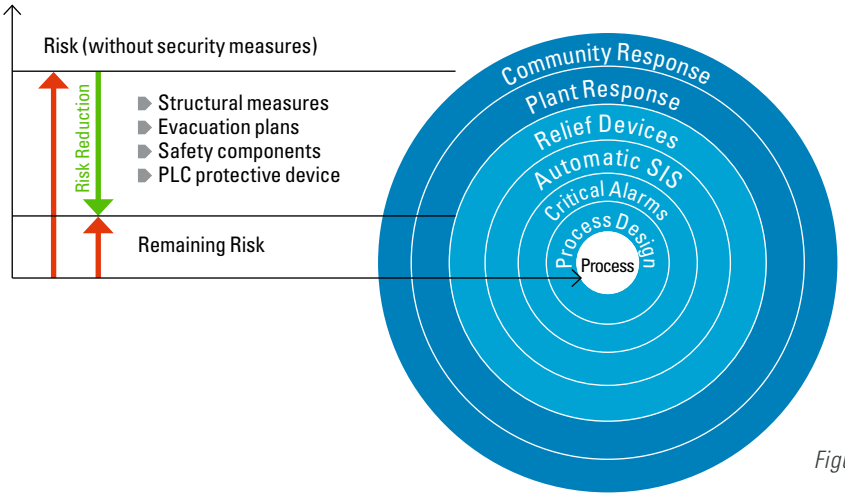


Figure 5 schematically shows the various possible safeguarding layers that can be present or could be applied to reduce the raw risk associated with a certain process. These layers vary from process design, critical alarms and operation actions (procedural safety provisions), automatic safety instrumented functions to relief devices (mechanical safety provisions) up to various response plans. Each independent and valid (credible) layer brings a certain amount of risk reduction. The sum of all such layers determines the residual risk. A LOPA is typically applied to determine the required risk reduction factor for safety instrumented functions.

Figure 5: Possible Safeguarding Layers

The term IPL has been defined by CCPS [13] in relation to its function (Box 2) and characteristics (Box 3).

When applying LOPA, the following steps are applied to the HAZOP study results:

1. Define the Target Maximum Event Likelihood (TMEL) in combination with the potential Severity
2. Determine credible initiating events (IE) for each scenario
3. Determine the expected initiating event frequency (IEF) for each IE
4. List the (maximum expected) severities from the HAZOP study results
5. Determine risk reduction achieved by known Independent Protection Layers (IPL) not being SIF
6. Determine Intermediate Event Likelihood (IMEL) [14]
7. Compare IMEL with TMEL
8. Missing risk reduction (if any), gives the target SIL of a Safety Integrity Function

Note : TMEL is recorded in the Risk Matrix.

Step 1

The TMEL requires a quantified Risk Assessment Matrix. This means the RAM must have its likelihood expressed in a ratio scale (quantitively). It is advised to set the TMEL value on the border of the tolerable (blue) and ALARP (yellow) areas.

Function of an IPL

- The evolution of an event into a unwanted situation, e.g. an explosion, independent of the cause and independent of correct functioning of other protective devices.

Characteristics of an IPL

- A system or subsystem specifically designed to reduce the likelihood or severity of the impact of an identified hazardous event by a large factor. An IPL must be independent of other protection layers associated with the identified hazardous event, as well as reliable, and auditable.

Step 5

Reference is made to the CCPS handbook for typical PFD values for non-instrumental safeguards [1] [3].

Step 6

The resulting intermediate event likelihood is the outcome of multiplying the initiating event frequency with the validated PFD of each IPL.

From the HAZOP			LAYERS of PROTECTION (PFD)				RESULT
Impact Event	**Initiating Event**	**Initiating Event Frequency (/ year)**	**Basic Process Control System (BPCS)**	**Procedural Safety provision ALARM & (2) Operator action**	**Ristricted Access**	**Mechanical Safety Provision Relief Valve (3)**	**Intermediate event likelihood**
Explosion of Vessel	High Pressure	0,2	0,2 (1)	0,5	n.a.	0,1	0,002

Figure 6: Possible Safeguarding Layers

Notes to figure 6:

1 *According to IEC61511-1 9.3.2 the risk reduction factor claimed for a BPCS independent protection layer shall be < 10. Or, in PFD terms, the PFD > 0,1. In case a PFD ≤ 0,1 is claimed, one needs to provide proof that the BPCS is as reliable as claimed. In practice though, often a PFD equal to 0,1 is chosen.*

2 *An alarm and associated operator action is an example of a procedural safety provision (PSP). It is advised to implement a strict alarm management system based on international standards like*
   - *IEC 62682 'Management of alarms systems for the process industries'*
   - *EEMUA 191 'Alarms systems: a guide to design, management and procurement'*
   - *ANSI-ISA-18.2 'alarm management lifecycle'*
   - *API RP 1167 'Pipeline SCADA Alarm Management'*

3 *A relief valve is an example of a mechanical safety provision (MSP).*

Steps 7 & 8

If the IMEL < TMEL no additional risk reduction is required. The needed risk reduction, expressed in terms of Risk Reduction Factor (RRF), for people, is found as follows:

RRF= IMEL / TMEL = 0,006 / 0,0001 = 60, which corresponds to SIL 1.

See figure 7 below.

The relation between RRF, SIL and PFD can be found in table 3 extracted from IEC61511-1 [4] below. The table is applicable for low demand mode only and is described in box 4; high demand and continuous demand are not further discussed. Further details of the various demand modes can be found in IEC61508.

DEMAND MODE of OPERATION		
Safety integrity level (SIL)	**PFD_{avg}**	**Requited risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	> 1000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	> 100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	> 10 to ≤ 100

Table 3: Relation between SIL, PFD and RRF

Definition of low demand mode of operation

Where the safety function is only performed on demand, in order to transfer the Equipment under Control into a specified safe state, and where the frequency of demands is no greater than one per year.

From the HAZOP			TMEL (target)			LAYERS of PROTECTION (PFD)				IMEL	RESULT	
Impact Event	**Initiating Event**	**Initiating Event Frequency (/ year)**	**People**	**Environment**	**Assets**	**BPCS**	**ALARMS Operator action**	**Restricted Acces**	**Relief valves**	**Intermediate event likelihood**	**Additional Risk Reduction**	**Target SIL**
Explosion of Vessel	High Pressure	**0,2**	One Fatality	Small	> 1 Ms	**0,2**	**0,5**	**n.a.**	**0,3**	**0,006**		
			0,0001								60	1
				0,01							0,6	0
					0,0001						60	1
			TMEL	**TMEL**	**TMEL**					**IMEL**		

Figure 7: Example on Target SIL Calculation

This example shows how LOPA can provide a systematic and holistic approach to risk reduction accounting for all the available protection layers in an installation.

Following setting the SIL requirement for the SIF, a design verification should be conducted. The IEC standards set specific criteria to define what combinations of instrumentation and procedures can be claimed as a layer of protection (see for example IEC 61511 - Part I, Chapter 9.4).

PITFALLS

07

PITFALLS CONDUCTING HAZOP STUDIES

In common practice only Safety Instrumented Function (SIF) that have previously been identified in the HAZOP study are subject to Risk Assessment (by LOPA or equivalent methods). SIF's are typically included in green field designs as per engineering judgement without applying quantitative methods. If during the HAZOP no SIF's have been defined within a particular scenario AND the risk associated with that scenario was qualitatively considered by the team to be sufficiently mitigated, then the scenario is usually not evaluated futher by LOPA. The pitfall here lies in the fact that risks during HAZOP study are typically not quantified.

HAZOP study depends on subjective "expert judgement" of the team whether or not mentioned safeguards are deemed to be sufficient or not. This is a practice that is inherited from the past, before the development of semi-quantitative methods such as LOPA. Quantitative information used in a LOPA, instead, provides a consistent and more "objective" appreciation of likelihood of occurrence and level of safeguard a SIF can bring to prevent the causes leading to the consequences defined.

In other words: if a quantitative assessment such as LOPA would have been conducted as part of the HAZOP study approach for scenarios not containing any SIFs, likely a number of those scenario's would come out as being insufficient in terms of safeguards in relation to the Target Mitigated Event Likelihood (TMEL) set by a company. Merging HAZOP study and LOPA techniques together and subjecting all HAZOP scenarios to a LOPA session would lead to more consistent, factual and reproducible results.

Another pitfall is that consequences are not always thought through by the HAZOP study team up to the final ultimate consequences (often outside the node). This usually leads to lower (perceived) consequences and severities and, as a result, to the implementation of insufficient risk reduction measures

A third pitfall is that the team reports existing safeguards to mitigate a specific risk, but does not always question / verify if the reported safeguards are valid, independent and - as a whole - sufficient to mitigate the risk down to tolerable levels. An observed pitfall in proving the independence of the safeguards is often neglecting the fact that when the failure of one safeguard constitutes the demand for another safeguard for the same risk, the two safeguards cannot be considered two independent layers of protection. The overall consequence is insufficient risk reduction at site. See also the previous section on how LOPA can support a HAZOP study to answer the question if safeguards are sufficient.

HARM AND HAZARD SCALES

08

HARMS

The scales of harm differ in respect to the grading, however the minimum and maximum limits always range between: local injury treated on location by first aid and with no leave from work necessary to multiple deaths (with "multiple" being either more than one person OR more than five persons).

The parameters used to distinguish grades use the following differentiating factors:

- Whether the harm involves death or only injury
- Whether the injury is permanent or not
- Whether recovery involves leave from work longer than 3 days or not
- The number of people affected

We have found that a permanent disability is typically considered the same as death, and sometimes 5 or more injuries requiring leave from work are considered equivalent to one death. A reference scale was created to compare the actual scales used in the matrices and mark the recurring scale divisions. After analysing the available graphs the following table was built to guide in designing scales of harms (low demand processes):

Risk Matrix Calibration: Harms					
Injury or Death	**At least 1 IRREVERSIBLE injury**	**Leave from work / Hospitalization**	**Number of victims**	**Resulting Harm Grade**	**Advised Harm Grade Scale (simplified based on results)**
I	N	First aid, no leave	0	Marginal	Negligible
I	N	Leave < 3 days	1 to 4	Minor	Minor
I	N	Leave > 3 days	5 or more	Medium	Moderate
	Y	Leave > 3 days	1 to 4	Moderate	
D	Y	1 death *	1	Major	Major
D	Y	2 to 5 deaths *	2 to 5	Severe	Catastrophic
D	Y	more than 5 deaths*	> 5	Catastrophic	

Table 4: Risk Matrix Calibration on Harms

(* or permanent disability)

Risk Matrix Calibration: Hazards				
Occurs in industry type	**Occurs within the company**	**Occurs at site**	**Likelihood = Events per Year**	**Resulting Hazard Grade**
			Years	
No / Never heard of	No / Never heard of	No / Never heard of	y < 1000 k	Insignificant
Yes		No / Never heard of	y < 100 k	Very Unlikely
Yes	Yes	No / Never heard of	y < 10 k	Improbable
Yes	Yes (Multiple times)	No / Never heard of	y < 1 k	Remote
Yes	Yes (Several times)	No / Never heard of	y < 100	Sporadic
Yes	Yes	Yes	y < 25	Occasional
Yes	Yes	Yes (Multiple times)	y < 10	Probable
Yes	Yes	Yes (Several times)	y < 2	Frequent
Yes	Yes	Yes (Often)	y < 1	Very Frequent

Table 5: Risk Matrix Calibration on Hazards

HAZARDS & LIKELIHOODS

Unlike Harms, the boundaries of the hazard & likelihood scales are found to vary more in the analysed matrices. Depending on the process, the minimum likelihood is found to vary between once in a hundred years to once in a hundred thousand years. The maximum frequency for low demand processes is typically once a year although we have seen a number of Risk Matrices considering frequencies below once a year). One of the possible reasons for this could be an attempt to account for possible operator mistakes and other operational faults that could occasionally make the demand rate rise above expected values.

Since it appears that in common practice the industry extends the risk assessments to these singular cases, we have included in this paper the results of the analysis of Frequent and Extremely Frequent events. These events can be labelled as "Very frequent" (refer to the tables in section 3).
It must be kept in mind that, according to IEC definitions, processes with demands exceeding once a year are to be treated as high demand and not as low demand.

The reference Hazard axis is expressed in likelihood (events per year). All available matrices are compared to it to find recurring grades. The discriminating factors for hazard are

- Whether, and to which degree, the hazard is heard of in the industry
- Whether, and to which degree, the hazard is heard of in that specific installation.

The result of the analysis is showed in table 5 and can be used as a guideline to create a general Risk Matrix that fits any process in low demand mode.

RISK ASSESSMENT MATRICES

09

EXISTING PRACTICES IN RISK ASSESSMENT MATRICES

Risk assessment matrices that are used by more than 15 companies globally were collected and analysed to find out commonalities and best practices. All the examples are for low demand process installations. The following observations are made:

- Matrices vary in number of columns and rows
- Both Hazard and Harm grading vary between matrices
- Descriptions of severity are not always consistent in same type of process industry sector.
- Descriptions of frequency are not always consistent in same type of process industry sector.
- Descriptions of frequency have both qualitative as well as quantitative measures that from proper statistical methods seem to be not validated properly
- The level of risk which is deemed to be tolerable / not tolerable varies between companies, irrespective of the sector
- Categories of likelihood are not always in steps of 10

After all company risk matrices have been analysed and "averaged", the following matrix emerged.

Reference is made to table 1 for a description of the severity and likelihood categories.

RISK MATRIX SAMPLE			SEVERITY				
			1	2	3	4	5
			Negligible	Minor	Moderate	Major	Cata-strophic
LIKELIHOOD (/YEAR)	7	>1					
	6	10^{-1} - 1					
	5	10^{-2} - 10^{-1}					
	4	10^{-3} - 10^{-2}					
	3	10^{-4} - 10^{-3}					
	2	10^{-5} - 10^{-4}					
	1	10^{-6} - 10^{-5}					
				TOLERABLE		ALARP	NOT TOLERABLE

Figure 8: Analyzed and averaged company risks matrices

From figure 8 it can be observed that the ALARP region does not follow a linear pattern. Companies tend to mitigate risks of severe events even when their likelihood is extremely low.

BEST PRACTICE RISK MATRIX

10 WHAT IS AN EXAMPLE OF A BEST PRACTICE RISK MATRIX?

Based on the findings under section 9 combined with experience of the SIL platform members, the following best practices are advised to take into account when it comes to defining company risk matrices:

1. Clearly indicate which risks (combinations of severity & likelihood) are considered to be :
   - Not acceptable -> Risk must be reduced.
   - Tolerable -> Risk is considered to be sufficiently low or mitigated.
   - ALARP -> Risk needs to be shown to comply with the ALARP definition.

2. Limit the RAM matrix in terms of number of rows and columns in order to keep it practical and understandable for its users. More rows/columns take more time for its users to align on the position of risks, whereas the (human) ability to increase its accuracy of estimating risks is often limited.

3. Ensure the use of descriptions of severity and likelihood is unambiguous.

4. Ensure likelihood categories use both colloquial language as well as ordinal scales. Use steps of 10 for likelihood rows to align with SIL categories. This especially facilitates the use of the matrix during a LOPA.

Severity Category	TMEL (/year)
1 Negligible	10^{-2}
2 Minor	10^{-3}
3 Moderate	10^{-4}
4 Major	10^{-5} (note 1) / 10^{-6} (note 2)
5 Catastrophic	10^{-6}

Table 6: TMEL for Best Practice Risk Assessment Matrix

As described in section 2, we follow the guidance from the HSE UK to maintain a wide enough ALARP "buffer" between broadly acceptable and intolerable risks as in Figure 1. The resulting best practice Risk Assessment Matrix is presented in figure 9.

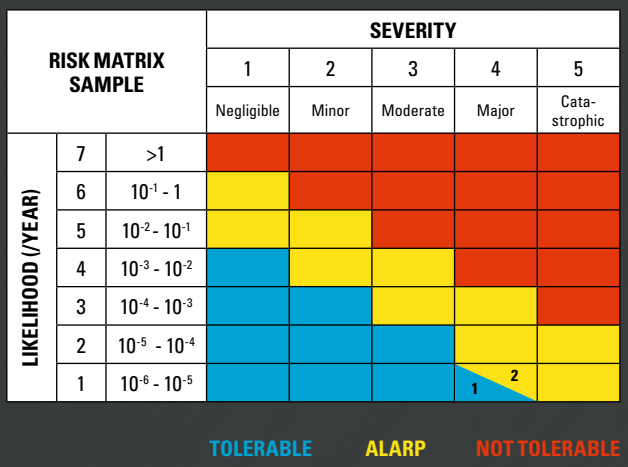


Figure 9 Best Practice Risk Assessment Matrix

Notes to figure 9:

1 Tolerable according to document [6]

2 ALARP according to SIL Platform applying a more conservative approach for severity category 4

11

Using the obtained reference scales, a typical calibrated risk matrix with SIL indication was developed. This was done for the best practice risk assessment matrix.

TYPICAL CALIBRATED RISK MATRIX WITH SIL INDICATION

Figure 10 is based on the results of figure 9. As the term SIL is strictly speaking only reserved for Safety Instrumented Functions (SIF), when a SIL rating is indicated in the above matrix it has the following meaning: assuming no other validated safeguards are in place, the risk can be reduced to TMEL levels by providing a SIF with a SIL rating as per figure 10.

In practice, the risk level of many scenarios can be and are reduced by validated non-SIF safeguards for example in the form of MSP or PSP. Then any residual RRF can still be covered by a SIF with usually a lower SIL level. The risk can be reduced to TMEL levels by providing a SIF with a SIL rating as per figure 10. The exact PFD required for each SIF is determined by the LOPA taking into account validated PFD's for all IPL's.

RISK MATRIX SAMPLE			SEVERITY				
			1	2	3	4	5
			Negligible	Minor	Moderate	Major	Catastrophic
LIKELIHOOD (/YEAR)	7	>1	SIL 3	Change Design (*)	Change Design (**)	Change Design (**)	Change Design (**)
	6	10^{-1} - 1	SIL 2	SIL 3	Change Design (*)	Change Design (**)	Change Design (**)
	5	10^{-2} - 10^{-1}	SIL 1	SIL 2	SIL 3	Change Design (*)	Change Design (**)
	4	10^{-3} - 10^{-2}	a	SIL 1	SIL 2	SIL 3 / Change design (*)	Change Design (*)
	3	10^{-4} - 10^{-3}	x	a	SIL 1	SIL 2/3	SIL 3
	2	10^{-5} - 10^{-4}	x	x	a	SIL 1/2	SIL 2
	1	10^{-6} - 10^{-5}	x	x	x	a / SIL 1	SIL 1

Figure 10: Best Practice Risk Assessment Matrix with SIL indication

Notes to figure 10:

a An alarm and operator action OR BPCS action can provide sufficient risk mitigation.

x No specific mitigating measures are required.

** If redesign is not feasible, in exceptional cases a SIF of SIL 4 quality could be considered.*

*** Redesign is the only acceptable solution.*

REFERENCE DATA

Per sector

Information was collected from the following operational sectors:

- Oil & Gas (including EPC's)
- Chemical
- Power
- Coating
- Pharmacy
- Waste treatment

Geographical

Information as collected from the Oil & Gas and Chemical sectors has an international character, while the information related to Pharma and Waste treatment was based on local information. (Netherlands)

AUTHORS

- Joep Coenen - Versatec Energy B.V.
- Elena Mauro - Yokogawa
- Anton Prins - NRG

The authors like to express a word of thanks to the following members of the SIL Platform for their thorough review and contributions:

- Andre Fijan - Fluor Corporation B.V.
- Gert Sloof - Bilfinger Tebodin Netherlands B.V.
- Gerard Wamelink - ConXP
- Leon Heemels - RMT Solutions N.V.
- Menno van der Bij - Technip Benelux B.V.
- Diederik Hebels - Teijin Aramid B.V.
- Willem van der Bijl - PRODUCA Communicatie BV

DISCLAIMER

"The views expressed in this paper are those of the individual SIL Platform members and do not reflect those of employer, or member companies."

REFERENCES

[1] AIChE - Center for Chemical Process Safety, Layer Of Protection Analysis - simplified process risk assessment, John Wiley & Sons, Inc., , 2011.

[2] CCPS, Guidelines for enabling conditions and conditional modifiers in Layer of Protection Analysis, CCPS, 2013.

[3] CCPS, Guidelines for initiating events and independent protection layers in layer of protection analysis, CCPS, 2015.

[4] International Electrotechnical Commission (IEC), IEC61511 Functional safety - Safety instrumented systems for the process industry sector, Geneva - Switserland: International Electrotechnical Commission (IEC), 2016.

[5] RIVM, An international comparison of four quantitative risk assessment approaches Benchmark study based on a fictitious LPG plant, Bilthoven: Ministerie van Welzijn, Volksgezondheid en Cultuur , 2011.

[6] Inspectie SZW, Werkdocument 233 - Een methode voor de beoordeling van het interne risico van inrichtingen met gevaarlijke stoffen., Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid, februari 2002.

[7] HSE, REDUCING RISKS, PROTECTING PEOPLE, HSE's decision-making process, ISBN 0 7176 2151 0: Health and Safety Executive, 2001.

[8] D. V. a. M. Koucky, „Selected overview of risk assessment techniques," Problemy Eksploatacji , vol. 4, pp. 19-32, 2009.

[9] IEC, „IEC 61882Hazard and operability studies (HAZOP studies) - Application guide," IEC, Geneva - Zwitserland, 2016.

[10] C. Timms, „ACHIEVING ALARP WITH SAFETY INSTRUMENTED SYSTEMS," in 1st IET International Conference on System Safety, 2006.

[11] „Meetschaal," Wikipedia, [Online]. Available: https://nl.wikipedia.org/wiki/Meetschaal. [Geopend 17 07 2018].

[12] HSE UK, „Offshore Installations (Safety Case) Regulations 2005 Regulation 12 Demonstrating compliance with the relevant statutory provisions," HSE UK, Abderdeen, 2006.

[13] CCPS, Guidelines for safe automation of chemical processes, New York: American Institute of Chemical Engineers , 1993.

[14] A. M. (. Dowell, „Layer of Protection Analysis: A New PHA Tool After Hazop, Before Fault Tree Analysis," in International Conference and Workshop on Risk Analysis in Process Safety, New York, 1997.

[15] International Electrotechnical Commission (IEC), IEC61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Geneva - Switserland: International Electrotechnical Commission, 2010.

SIL Platform