Extension to Chapter 2.
SIL Allocation and Allocation Methods

Mary Ann Lundteigen   Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

- Become familiar with what is meant by SIL allocation
- Understand how SIL allocation is linked to risk analysis
- Become familiar with the SIL allocation methods:
  - Risk graph
  - Layers of protection analysis (LOPA)
  - Minimum SIL (as defined in the Norwegian Oil and Gas Guideline 070[1])
- Be able to identify pros and cons related to each allocation method

The slides provide additional information on some selected topics in Chapter 2 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

[1] https://www.norskoljeoggass.no/en/working-conditions/retningslinjer/

Outline of Presentation

1. Introduction
2. Allocation and Risk Reduction
3. Allocation Methods
4. Risk Graph
5. LOPA
6. NOG 070 & Minimum SIL

Purpose of Allocation

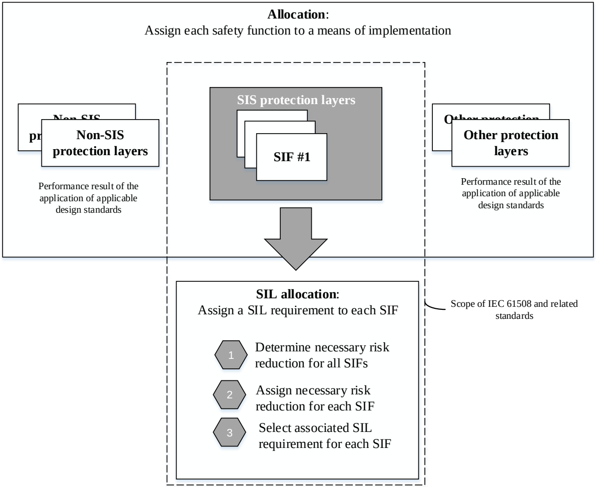
Allocation is the process that decides which safety functions to implement as SIFs and their associated SIL requirements.

The allocation process includes to:

- Allocate safety functions to different protection layers
- Decide which safety functions that are to be implemented as SIFs
- Determine the maximum PFD or PFH, and the associated SIL requirements, that follow from the need for risk reduction

Allocation is sometimes referred to as SIL allocation in this context, or SIL classification and SIL targeting.

Allocation Process


Allocation:
Assign each safety function to a means of implementation
Non-SIS protection layers
Performance result of the application of applicable design standards
SIS protection layers
SIF #1
Other protection layers
Performance result of the application of applicable design standards
SIL allocation:
Assign a SIL requirement to each SIF
1
Determine necessary risk reduction for all SIFs
2
Assign necessary risk reduction for each SIF
3
Select associated SIL requirement for each SIF
Scope of IEC 61508 and related standards

SIL Allocation in Functional Safety Standards

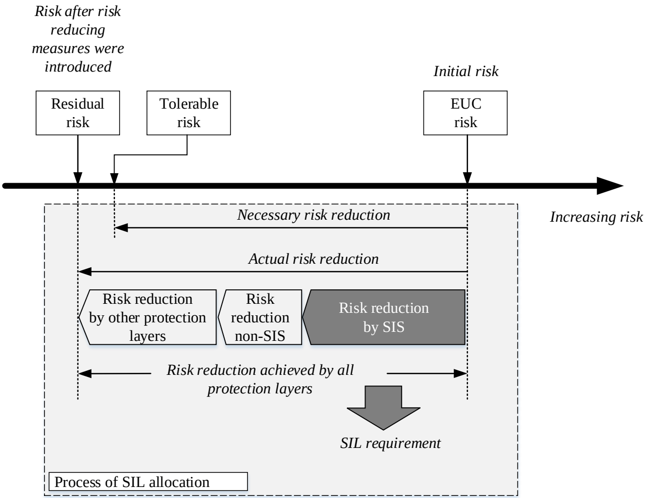
Some key points about SIL allocation:

- IEC 61508 and related standards give a thorough description of **SIL allocation methods**
- SIL allocation is an **iterative process** in order to optimize the design so that the necessary risk reduction is achieved
- SIL allocation methods may be **qualitative, quantitative, or semi-quantitative**

Examples of methods included in functional safety standards are:

- Risk matrix
- Risk graph
- Layers of protection analysis (LOPA)
- Event tree analysis

From Risk Reduction to Allocation


Risk after risk reducing measures were introduced
Initial risk
Residual risk
Tolerable risk
EUC risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Risk reduction by other protection layers
Risk reduction non-SIS
Risk reduction by SIS
Risk reduction achieved by all protection layers
SIL requirement
Process of SIL allocation

EUC Risk: The Risk When Not Protected

☞ EUC risk: The risk arising from the EUC or its interaction with the EUC control system [IEC 61508].

Some remarks about the EUC risk:

- Industries may use different names for EUC risk. For example, process industry uses the term “process risk”
- EUC risk is often characterized as an event with an associated frequency (per hour or per year)

EUC risk may be determined on the basis of:

- Hazards and operability study (HAZOP)
- Preliminary Hazards identification (PHA)
- A review of past experience and data
- Expert judgments
- Information in databases and data handbooks

Tolerable risk: The Limit of what is Accepted

☞ Tolerable risk: Level of risk which is accepted in a given context based on the current values of society [IEC 61511].

Important factors that impact the definition of tolerable risk are:

- Guidelines from the appropriate regulatory authorities
- Discussions and agreements with the different parties involved int he application
- Industry standards and guidelines
- Industry, expert and scientific advice
- Legal and regulatory requirements, both general and of relevance to the specific application

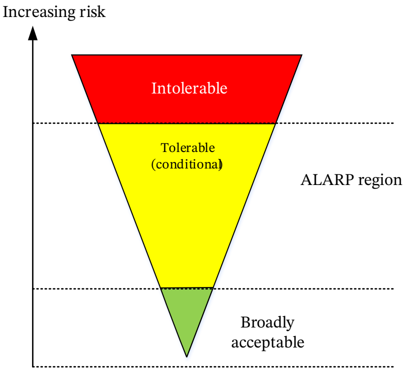
Residual Risk: The Risk after Risk Reduction

☞ Residual risk: Risk remaining after protective measures have been taken [IEC 61508].

Residual risk can end up in the ALARP region, or in the broadly acceptable region.

ALARP: Principle of Risk Reduction

ALARP is approach to risk reduction that is As Low As Reasonable Practically.



ALARP is explained in detail in e.g. UK HSE report “Reducing Risk, Protecting People, `http://www.hse.gov.uk/risk/theory/r2p2.pdf`

Risk Reduction: What is Required or Achieved

☞ Necessary risk reduction: Risk reduction to be achieved by the E/E/PE safety-related systems and/or other risk reduction measures in order to ensure that the tolerable risk is not exceeded. [IEC 61508]

The necessary risk reduction represents the *minimum* of what needs to be provided in light of the risk acceptance criteria.

☞ Actual risk reduction: Risk reduction that is achieved with all the implemented protection layers included.

The actual risk reduction determines the residual risk.

Risk Reducing Measures

Risk reduction measures cover all types of protection layers.

Examples include:

- EUC control system
- Human tasks according to formal procedures (e.g. operational procedures, evacuation procedures, emergency response procedures)
- Mechanical protection systems ("non-SIS', such as mechanical pressure relief valve')
- SIS (can be one or more systems)
- Passive systems (e.g. dikes, containment, firewalls, layout, etc)

SIL Allocation Methods

Commonly used methods for SIL allocation are:

Method	Type
Event tree analysis	Semi-quantitative
Risk graph	Qualitative or semi-quantitative
Layers of protection analysis (LOPA)	Semi-quantitative
Safety layer matrix	Qualitative or semi-quantitative
Minimum SIL	Semi-quantitative

Remark: Minimum SIL is an approach suggested in the Norwegian Oil and Gass Association guideline 070 on the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Sector. The approach is possible to adapt also in other sectors.

Choice of Methods

What method to select depends on a number of factors:

- How detailed we are able to model the effect of each protection layer
- Experience and skills of personnel to undertake the work
- Information available about parameters of relevance for the methods in question. Some methods are more suited when many details about the design are in place, while some can be used for more early design evaluation
- Instructions or recommendations from company

Documentation

It is important to document the results, and its underlying assumptions, including

- Values used for parameters of the allocation method
- Drawings and revision number of all documents used
- References to failures that lead to demands
- Reference to data sources used to determine demand rates and the risk reduction suggested for protection layers

Risk Graph

Some key “words” about risk graph:

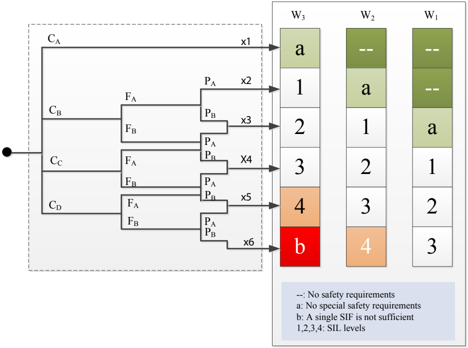
- Qualitative or semi-quantitative method
- First introduced in the German standard DIN V 19250
- An extension of risk matrix that addresses occupancy and ability to escape
- Initially used for machinery (and it is sometimes argued that this is the most suitable application)
- The approach has been adopted by the process industry, through standards like IEC 61508 and IEC 61511.

Risk Graph Parameters

Parameter	Description
Starting point:	The hazardous event, that if not handled, may develop into an accident. Corresponds to what we have introduced as a demand.
Consequence (C):	Consequence of hazardous event. Four categories, C_A which is the least severe one and C_D which is the most severe
Frequency (F):	Frequency and exposure time risk. Two categories, F_A which denotes rare to more often exposure in the hazardous zone, and F_B which denotes frequent to permanent exposure in the this zone
Possibility (P):	Possibility of avoiding the hazardous event. Two categories, P_A denotes that it is possible under certain (given) conditions, and P_B denotes that it almost impossible.
Frequency hazardous event (W):	Frequency of hazardous event (W), or demand rate. Three categories, W_1 which denotes a very slight probability of occurrence, W_2 denotes a probable occurrence, and W_3 denotes a high probability of occurrence.

Risk Graph Model

- Risk graph has a graph layout
- The starting point is a specific hazardous event, and its potential consequences and impact, is evaluated.
- The question to answer is if a new SIF is required and what is the SIL requirement.
- An entry point X*i* after judging the values of parameters C, F and P
- The frequency range (W*i*) of the hazardous event is identified
- The corresponding SIL requirement is identified.



	W_3	W_2	W_1
x1	a	--	--
x2	1	a	--
x3	2	1	a
X4	3	2	1
x5	4	3	2
x6	b	4	3

--: No safety requirements
a: No special safety requirements
b: A single SIF is not sufficient
1,2,3,4: SIL levels

Risk graph parameters - process industry example

This table is based on an example in IEC 61511, part 3, with some freedom used in the wording.

Parameter	**Description**
Starting point:	A type of demand that requires a response by a SIF
Consequence (C):	C_A is minor injury, C_B has the range 0.01 to 0.1 fatalites, C_C i has the range 0.1 to 1 fatalities, and C_D is greater than 1 fatality[2]
Frequency (F):	F_A less than 10% of the time. F_B more than 10%
Possibility (P):	P_A if provisions for altering the personnel, for avoiding , for shutting down and thereby giving personnel in the area more time and chance to escape, and that there is sufficient time to act (i.e. evaculate) before the situation escalates. P_B if criteria for A is not fulfilled. P_A may be set to a value, e.g. 30%
Frequency hazardeous event (W):	W_1 less than 0.1D per year, where D is a caliabration parameter[3], W_2 is between 0.1D per year and 1D per year, and W_3 is from 1D to 10D per year. Note that W is the frequency of the hazardous event where a response by a new SIF may be required, and not the frequency of worst case consequence.

[2] The number of persons exposed to the hazards multiplied by the vulnerability (i.e. likelihood of being killed if exposed).

[3] Here, we assume that D is 1.

Calibration of Risk Graph

Using the “default” setup of the risk graph in e.g. IEC 61508 or IEC 61511 does not necessarily give the correct SIL-requirements.

☞ Calibration: Adjust layout of risk graph and parameter values with risk acceptance criteria.

- The underlying assumption of the default set-up in IEC standards (e.g. IEC 61508 part 5 and IEC 61511 part 3).
- This may not correspond to risk acceptance criteria defined by a specific company or regulatory body.

Calibration of the risk graph may be required to allign with *your* criteria.

Calibration Procedure

The calibration can be carried out by the following steps:

1. Identify the tolerable frequency for each of the consequence categories. A plant owner may provide this in a risk matrix format.
2. Define applicable values for $\mathrm{F_A}$, $\mathrm{F_B}$, $\mathrm{P_A}$, $\mathrm{P_B}$ for the plant or equipment where risk graph is to be used.
3. Decide on suitable ranges for W_i in light of the application. Choose the highest value of each range for the calibration.
4. Calculate the maximum PFD for each cell using the following formula:

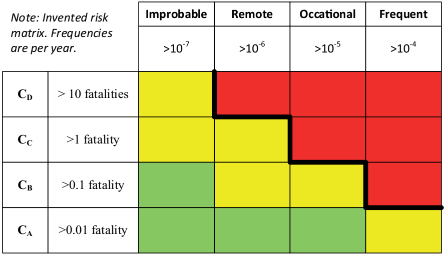
   $$\mathrm{PFD}_{\mathrm{req,i}} = f_{\mathrm{tol,Cj}}/(F_{\mathrm{k}} \cdot P_{\mathrm{m}} \cdot W_i)$$

   by changing the value of indexes so that each path in the risk graph is investigated.
5. Insert the corresponding SIL requirements in each cell, based on the calculated PFD.

There are several challenges reported when calibrated the risk graph, see e.g. in Chapter 6.2 in de Sallis, C. Using Risk Graphs for SIL Assessment (IChemE, 2011).

Identifying Tolerable Frequencies

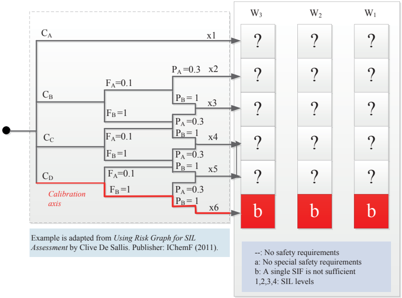
- A risk matrix may be used as basis for selecting tolerable frequencies, and one example is shown below.
- In this matrix, we note that the tolerable frequency for:
    - C_A is $\leq 10^{-3}$ per year
    - C_D is $\leq 10^{-6}$ per year



Note: Invented risk matrix. Frequencies are per year.		Improbable	Remote	Occational	Frequent
		$>10^{-7}$	$>10^{-6}$	$>10^{-5}$	$>10^{-4}$
C_D	> 10 fatalities	🟨	🟥	🟥	🟥
C_C	>1 fatality	🟨	🟨	🟥	🟥
C_B	>0.1 fatality	🟩	🟨	🟨	🟥
C_A	>0.01 fatality	🟩	🟩	🟩	🟨

Practical Example

1. Select the calibration axis for C_D. We know from the risk graph that $f_{tol} < 10^{-6}/year$
2. Calculate the probability at entry point X6 for given values of F_B and P_B. The result is “1”.
3. Determine the range of each W_i-category. We select for this example only cell for W_2. We assume the maximum value of this range is 0.1/year.
4. Calculate maximum PFD for the corresponding cell. The result in our example is PFD_{req} as 10^{-5}, which is outside the range of SIL table (beyond SIL 4). Corresponding cell is then marked “b” according to risk graph rules.
5. Repeat the process for the other cells.



Example is adapted from *Using Risk Graph for SIL Assessment* by Clive De Sallis. Publisher: IChemF (2011).

--: No safety requirements
a: No special safety requirements
b: A single SIF is not sufficient
1,2,3,4: SIL levels

An inconsistency problem?

The book "Using Risk Graphs for SIL Assessment (IChemE, 2011)," Chapter 6.2 and 6.3, discusses some inconsistency problems in the risk graph approach. Among these are:

- Risk graph is not a precisely mathematical tool
- Not always a linear increase in levels (a,1,2,3,b) in each column of the risk graph
- One entry point, e.g., entry point x5 may represent a less severe event than entry point x3

These inconsistencies have been identified after having multiplied the values assigned to a consequence category (e.g., C_D is 10 fatalities, C_C is 1 fatality, etc) with the values assigned to F_A, F_B, P_A, P_B (depending on the path taken).

Layers of Protection Analysis (LOPA)

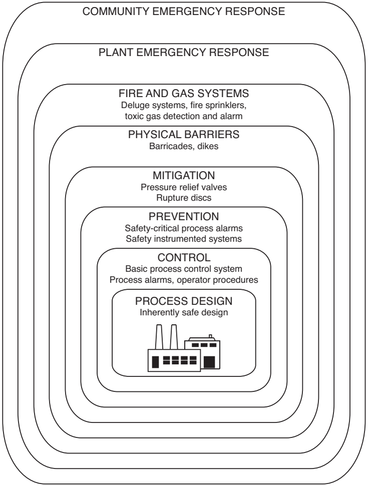
LOPA was developed for the process industry by the Center for Chemical Process Safety (CCPS) as a method for determining the necessary risk reduction new SIFs.

☞ Layer of protection analysis (LOPA): Approach that lists and quantifies the joint effects of existing *independent* protection layers, and that identifies the necessary risk reduction of additional SIFs, if needed.

- See e.g., *Layers of Protection Analysis: Simplified Process Risk Assessment.* Published by CCPS in 2001
- Adopted by IEC 61508 and IEC 61511
- Builds on the results from a hazards and operability study (HAZOP)
- Applicable to determine SIL requirements of low-demand systems
- A semi-quantitative approach, using a table setup.

Examples of Protection Layers

- Layers of protection ("the onion") is a concept often used in industries where risk reduction is distributed to several barriers, rather than a one or very few.
- This approach indicates that protection layers are organized according to their efficiency and closeness to the source of demand.
- A similar concept to layers of protection is defense-in-depth.

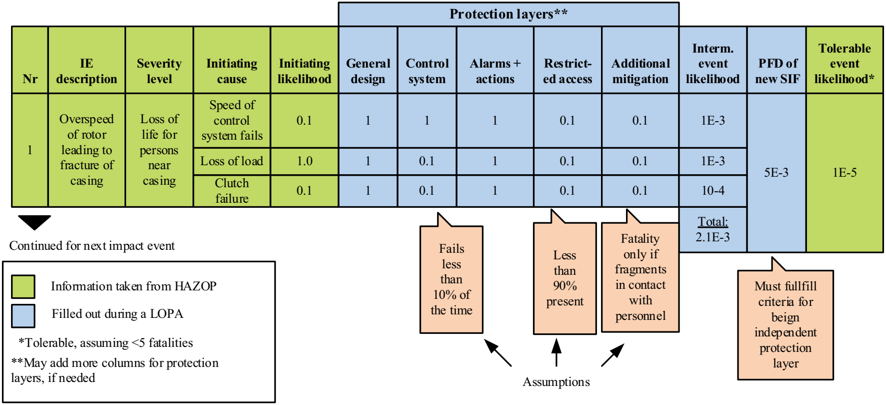

COMMUNITY EMERGENCY RESPONSE
PLANT EMERGENCY RESPONSE
FIRE AND GAS SYSTEMS
Deluge systems, fire sprinklers, toxic gas detection and alarm
PHYSICAL BARRIERS
Barricades, dikes
MITIGATION
Pressure relief valves
Rupture discs
PREVENTION
Safety-critical process alarms
Safety instrumented systems
CONTROL
Basic process control system
Process alarms, operator procedures
PROCESS DESIGN
Inherently safe design

LOPA Parameters

Key parameters in LOPA are:

Parameter	Description
Impact event:	The starting point of a LOPA analysis. Corresponds to the unwanted consequences identified during a HAZOP study
Initiating cause	Initiating event(s) or causes identified in a HAZOP study that may lead to the unwanted consequences
Initiation likelihood, f_{IE}:	The inintiating event likelihood. Often selected on the basis of experience data or generic data set provided by the operator
Independent protection layers (IPLs):	Functions, actions, or conditions that may prevent, or reduce signifcantly the likelihood of having the impact event
Intermediate event likelihood:	The likelihood (e.g., frequency) of having the impact event, given the existence of the identified IPLs
Tolerable mitigated event likelihood:	The tolerable likelihood (e.g., frequency) of impact event
$\mathrm{PFD}_{\mathrm{avg}}$ required	The required $\mathrm{PFD}_{\mathrm{avg}}$ of a new SIF. The $\mathrm{PFD}_{\mathrm{avg}}$ may be allocated to more than one SIF, if necessary

LOPA Table



					Protection layers**							
Nr	IE description	Severity level	Initiating cause	Initiating likelihood	General design	Control system	Alarms + actions	Restricted access	Additional mitigation	Interm. event likelihood	PFD of new SIF	Tolerable event likelihood*
1	Overspeed of rotor leading to fracture of casing	Loss of life for persons near casing	Speed of control system fails	0.1	1	1	1	0.1	0.1	1E-3	5E-3	1E-5
			Loss of load	1.0	1	0.1	1	0.1	0.1	1E-3		
			Clutch failure	0.1	1	0.1	1	0.1	0.1	10-4		
										Total: 2.1E-3		

Continued for next impact event

Fails less than 10% of the time

Less than 90% present

Fatality only if fragments in contact with personnel

Assumptions

Must fullfill criteria for beign independent protection layer

🟩 Information taken from HAZOP

🟦 Filled out during a LOPA

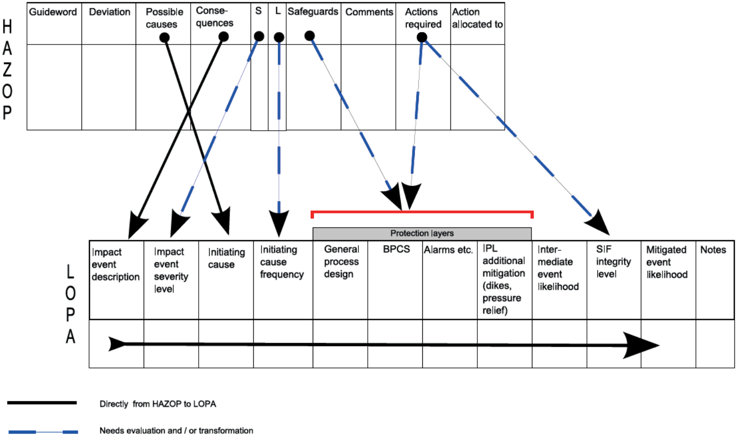
*Tolerable, assuming <5 fatalities

**May add more columns for protection layers, if needed

A “1” is assigned if a barrier is not relevant for the particular initiating cause in question.

LOPA vs HAZOP

There is a close relationship between HAZOP and LOPA:



Guideword	Deviation	Possible causes	Conse-quences	S	L	Safeguards	Comments	Actions required	Action allocated to

				Protection layers							
Impact event description	Impact event severity level	Initiating cause	Initiating cause frequency	General process design	BPCS	Alarms etc.	IPL additional mitigation (dikes, pressure relief)	Inter-mediate event likelihood	SIF integrity level	Mitigated event likelihood	Notes

H A Z O P
L O P A
Directly from HAZOP to LOPA
Needs evaluation and / or transformation

From: Masterthesis by Christopher A. Lassen (NTNU, 2008)

Do’s and Don’ts of LOPA

... with focus on don’ts:

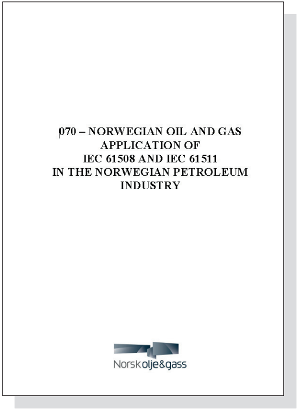
- Only relevant protection layers should be credited. A relevant protection layer is a safety barrier that is:
    - (i) able to prevent or alter the severity of the initiating cause, and (ii) is independent of the initiating cause
- Crediting too many barriers should be avoided, in particular if operator response is involved, as the operator may become overloaded with tasks in a critical situation
- Crediting too many barriers should also be avoided from a management perspective, and in particular if they are conditional for the situation.

Minimum SIL in NOG 070

NOG 070 defines *minimum SIL requirements* for commonly used SIFs in the Norwegian offshore oil and gas industry.

☞ Minimum SIL requirement: SIL requirement calculated for standard safety functions, using applicable field data.

The Norwegian Petroleum Safety regulations has accepted NOG 070 as an industry best practice, by giving reference to the standard.

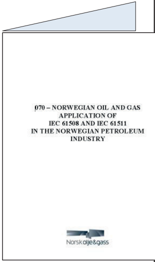


070 – NORWEGIAN OIL AND GAS
APPLICATION OF
IEC 61508 AND IEC 61511
IN THE NORWEGIAN PETROLEUM
INDUSTRY

Norskolje&gass

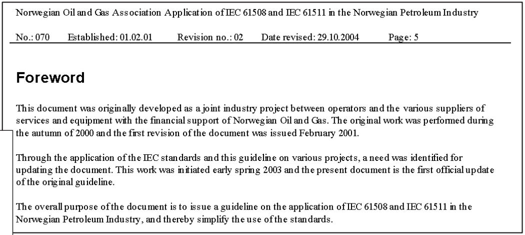
Available from `http://www.norskoljeoggass.no/no/Publikasjoner/Retningslinjer/`.

Background for NOG 070



070 – NORWEGIAN OIL AND GAS
APPLICATION OF
IEC 61508 AND IEC 61511
IN THE NORWEGIAN PETROLEUM
INDUSTRY

Norsk olje&gass



Norwegian Oil and Gas Association Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry

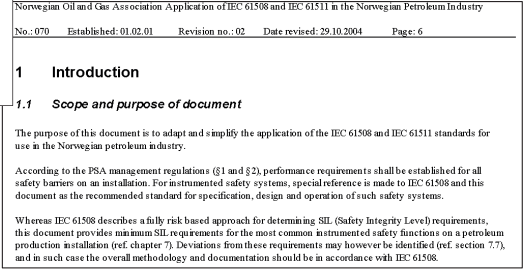
No.: 070 Established: 01.02.01 Revision no.: 02 Date revised: 29.10.2004 Page: 5

Foreword

This document was originally developed as a joint industry project between operators and the various suppliers of services and equipment with the financial support of Norwegian Oil and Gas. The original work was performed during the autumn of 2000 and the first revision of the document was issued February 2001.

Through the application of the IEC standards and this guideline on various projects, a need was identified for updating the document. This work was initiated early spring 2003 and the present document is the first official update of the original guideline.

The overall purpose of the document is to issue a guideline on the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, and thereby simplify the use of the standards.



Norwegian Oil and Gas Association Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry

No.: 070 Established: 01.02.01 Revision no.: 02 Date revised: 29.10.2004 Page: 6

1 Introduction

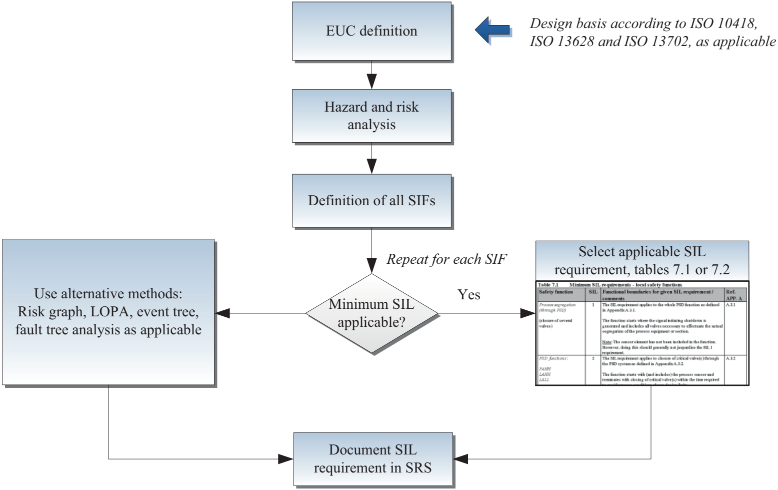
1.1 Scope and purpose of document

The purpose of this document is to adapt and simplify the application of the IEC 61508 and IEC 61511 standards for use in the Norwegian petroleum industry.

According to the PSA management regulations (§1 and §2), performance requirements shall be established for all safety barriers on an installation. For instrumented safety systems, special reference is made to IEC 61508 and this document as the recommended standard for specification, design and operation of such safety systems.

Whereas IEC 61508 describes a fully risk based approach for determining SIL (Safety Integrity Level) requirements, this document provides minimum SIL requirements for the most common instrumented safety functions on a petroleum production installation (ref. chapter 7). Deviations from these requirements may however be identified (ref. section 7.7), and in such case the overall methodology and documentation should be in accordance with IEC 61508.

NOG 070 Approach



EUC definition

Design basis according to ISO 10418, ISO 13628 and ISO 13702, as applicable

Hazard and risk analysis

Definition of all SIFs

Repeat for each SIF

Minimum SIL applicable?

Yes

Use alternative methods: Risk graph, LOPA, event tree, fault tree analysis as applicable

Select applicable SIL requirement, tables 7.1 or 7.2

Table 7.1 Minimum SIL requirements - local safety functions

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
Process segregation (through PSD) (closure of several valves)	1	The SIL requirement applies to the whole PSD function as defined in Appendix A.3.1. The function starts where the signal initiating shutdown is generated and includes all valves necessary to effectuate the actual segregation of the process equipment or section. Note: The sensor element has not been included in the function. However, doing this should generally not jeopardise the SIL 1 requirement.	A.3.1
PSD functions: *PAHH* *LAHH* *LALL*	2	The SIL requirement applies to closure of critical valve(s) through the PSD system as defined in Appendix A.3.2. The function starts with (and includes) the process sensor and terminates with closing of critical valve(s) within the time required	A.3.2

Document SIL requirement in SRS

Procss of Establishing Minimum SIL Requirements

NOT YET INCLUDED

Pros and Cons of NOG 070

NOG 070...

- ...may help avoiding unnecessary paperwork for defining "standard" SIFs used in relation to an offshore facility
- ...defines common (best practice) ways of defining standard SIFs, in relation to boundaries and typical level of redundancy.
- ...may result in non-conservative SIL requirements if too pessimistic data (too high failure rates) are used in the calculations, or very short test intervals

Remark

NOG 070 covers many other aspects than minimum SIL, but these are not mentioned here.