



**NTNU – Trondheim**  
Norwegian University of  
Science and Technology

# Management of the integrity of safety instrumented systems

**Martin Brataas**

Reliability, Availability, Maintainability and Safety (RAMS)

Submission date: June 2014

Supervisor: Mary Ann Lundteigen, IPK

Norwegian University of Science and Technology  
Department of Production and Quality Engineering





**NTNU – Trondheim**  
Norwegian University of  
Science and Technology

# Management of the integrity of safety instrumented systems

**Martin Brataas**

Reliability, Availability, Maintainability and Safety (RAMS)

Submission date: June 2014

Supervisor: Mary Ann Lundteigen, IPK

Norwegian University of Science and Technology  
Department of Production and Quality Engineering

This page is intentionally blank.

**MASTER THESIS**  
**Spring 2014**  
**for stud. techn. Martin Brataas**

**Management of the integrity of safety instrumented systems**  
**(Styring av integritet for instrumenterte sikkerhetssystemer)**

Many safety barriers in the oil and gas industry are realized by safety instrumented systems (SISs). The integrity, in terms of reliability and availability, is partly influenced by the SIS design and partly from how it is operated and maintained. 100% integrity may never be achieved, but it is necessary to demonstrate that the integrity is sufficient in light of risk criteria formulated for the installations. The Petroleum Safety Authority refers to two important standards for managing integrity for SIS, namely IEC 61508 which is an international standard and guideline 070 which is published by Norsk Olje og Gass. These standards use the concept of *safety integrity* and *safety integrity level* (SIL), and outline a process for managing SIL over the whole life cycle of the SIS. The Petroleum Safety Authority has conducted a number of investigations and audits, and many of them points at deviations and non-compliance in the management of integrity management of SISs. Some studies have also been carried out through e.g., the PDS forum in Norway, where also integrity issues have been discussed.

The main purpose of this master thesis is to suggest how the management of integrity may be improved for SISs in the oil and gas industry, with basis in a literature review. The improvements may be linked with the safety lifecycle, as a supplement to requirements defined for these phases in standards like IEC 61508 and IEC 61511.

To achieve this objective, the following tasks are suggested:

1. Define and explain the difference between a SIS and a SIF, and illustrate the difference using practical examples from the oil and gas industry.
2. Define what we mean by integrity in general and safety integrity in particular, in light of PSA regulations and standards such as NORSOK S-001, Norsk Olje og Gass guideline 070, IEC 61508 and IEC 61511.
3. Explain typical steps involved in the management of integrity of a SIS, with basis in the safety lifecycle in IEC 61508 or IEC 61511.

4. Define and discuss what we mean by SIL-follow-up in light of *Norsk Olje og Gas guideline 070* (appendix F) and "*Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase*" (SINTEF report A8788).
5. Outline and discuss factors influencing the SIL performance of a SIF in the operational phase.
6. Review reports, investigations and audits that have been published by the Norwegian Petroleum Authority and relevant for a like e.g., the PDS forum, and discuss the findings in light of influencing factors identified in task 4.
7. Suggest means to improve SIS follow-up in light of the task 6 in order to maintain, or even improve, the integrity of such systems.

The assignment solution must be based on any standards and practical guidelines that already exist and are recommended. This should be done in close cooperation with supervisors and any other responsibilities involved in the assignment. In addition it has to be an active interaction between all parties.

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 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: 10 June 2014.

Two bound copies of the final report and one electronic (pdf-format) version are required according to the routines given in DAIM. Please see <http://www.ntnu.edu/ivt/master-s-thesis-regulations> regarding master thesis regulations and practical information, inclusive how to use DAIM.

Responsible supervisor: Professor Mary Ann Lundteigen  
E-mail: mary.a.lundteigen@ntnu.no  
Telephone: +47 930 59 365

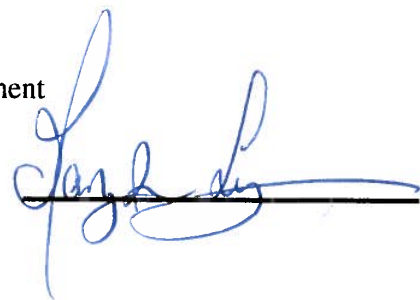
Supervisor(s) at NTNU: Professor Mary Ann Lundteigen  
E-mail: mary.a.lundteigen@ntnu.no  
Telephone: +47 930 59 365

**DEPARTMENT OF PRODUCTION  
AND QUALITY ENGINEERING**



Per Schjølberg

Associate Professor/Head of Department



Responsible Supervisor

## **Preface**

The thesis is written at Department of Production and Quality Engineering at NTNU, during spring of 2014. The thesis is work of the Master of Science program in Reliability, Availability, Maintainability and Safety (RAMS). The title of the assignment is Management of the integrity of safety instrumented systems (SIS). The main purpose of this master thesis is to suggest how the management of integrity may be improved for SIS in the oil and gas industry.

Trondheim, 2014-6-15

Martin Brataas

Signature



## **Acknowledgment**

I would like to thank Mary Ann Lundteigen for superb guidance. I have learned alot from her this spring semester, and i am grateful for the knowledge I gained from her.

M.B.

## **Executive summary**

The thesis consider management of safety instrumented systems/functions during the operational lifetime of the system/function. The location consider installations on the Norwegian continental shelf.

The thesis suggest a framework for monitoring the variability of safety performance when maintenance is performed. The thesis identified the need to monitor this variability by performing a review on investigations performed by Petroleum Safety Authority Norway. The framework that was presented, if applied correctly would suggest, not to performing the specific maintenance activities, that resulted in lack of redundancy within the system, hence the accident may have been avoided.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Objectives . . . . .	3
1.2	Approach . . . . .	4
1.3	Structure of the thesis . . . . .	4
1.4	Delimitations . . . . .	5
<b>2</b>	<b>SIS related concepts</b>	<b>6</b>
2.1	Equipment Under Control . . . . .	6
2.2	Introducing the concepts: SIS, SIF & SIL . . . . .	7
2.3	Safety Integrity . . . . .	9
2.4	Introducing: IEC 61508 & OLF 070 . . . . .	10
2.5	SIS requirements . . . . .	11
2.5.1	Functional Safety Requirement & Safety Integrity Requirements . . . . .	11
2.5.2	Safety Integrity Requirements . . . . .	11
2.5.3	Functional Safety Requirements . . . . .	12
2.6	Failure definitions . . . . .	13
2.6.1	Failure modes . . . . .	13
2.6.2	Random hardware or systematic failure? . . . . .	14
2.6.3	Independent or common cause failure? . . . . .	14
<b>3</b>	<b>SIS management</b>	<b>16</b>
3.1	Managing the integrity of the SIS . . . . .	16
3.2	SIS follow-up . . . . .	19

<i>CONTENTS</i>	1
3.2.1 SIS follow-up: Normal operation, maintenance and modification . . . . .	20
3.2.2 SIS follow-up: Monitoring performance and verification . . . . .	23
3.2.3 Short perspective follow-up: Deciding which components to maintain whilst ensuring safety . . . . .	23
3.2.4 Long perspective follow-up: Update failure rates and test intervals . . . . .	30
3.3 Factors influencing the SIL performance of a SIF . . . . .	34
3.3.1 Quantify loss of safety . . . . .	34
3.3.2 A general discussion on measuring loss of safety . . . . .	35
3.4 Architectural constraints . . . . .	37
<b>4 A review on SIS/SIL performance in the Norwegian continental shelf</b>	<b>39</b>
4.0.1 Discussion and Goal for the study . . . . .	39
4.1 Findings . . . . .	40
<b>5 Conclusions and further work</b>	<b>42</b>
5.1 Summary and conclusion . . . . .	42
5.1.1 Short perspective follow-up . . . . .	42
5.1.2 Conclusion: Short perspective follow-up . . . . .	43
5.1.3 Long perspective follow-up . . . . .	43
5.2 Discussion . . . . .	43
5.3 Further work . . . . .	44
<b>A Acronyms</b>	<b>46</b>
<b>B Naming parameters applied in the thesis</b>	<b>48</b>
B.1 Parameters affecting PFD . . . . .	48
<b>Bibliography</b>	<b>50</b>

# Chapter 1

## Introduction

This thesis consider safety (i.e. freedom from unacceptable risk), when the safety is maintained by safety instrumented functions (SIF), such as an emergency shut down valve. The location consider offshore installations on the Norwegian continental shelf.

It is not possible to guarantee success of a SIF, if a demand for it occur. Further, the probability that the SIF will fail to perform on a demand, increases over time if the present failure is hidden. The ability of a SIF to perform its required function when a demand occur (e.g. detect fire, given fire), will be dependent on how the SIF is designed, under which conditions it is operating, and how it is maintained. During design, the SIF is allocated a required integrity level (that reflect factors such as availability and reliability) in which it has to comply with during the operational phase of the installation. Follow-up activities during the operational phase of a SIF, are intended to measure if the SIF comply with safety integrity requirements. This thesis distinguish between short perspective follow-up and long perspective follow-up. The difference between the two categories may be that long perspective follow-up consider activities that may not be performed more than once a year, while short perspective follow-up consider activities related to daily/frequently management of safety-variability due to bypassing of SIF components, that are subjected to maintenance.

Regarding **short** perspective follow-up:

Different issues arise when SIF components are subjected to maintenance. This paper sug-

gest an approach that may be applied in order to decide; which SIF components/sub-functions are allowed to be maintained simultaneously (as the components are not able to perform its required function when they are subjected to maintenance), and; which precautions and countermeasures have to be implemented in order to approve a given maintenance configuration.

Regarding **long** perspective follow-up:

During design, different assumptions are made about the environment in which the SIF will operate, and about the performance of the SIF itself. Such assumptions consider the integrity of the SIF in terms of; *how often is it expected that the SIF will have a hidden failure, that interfere with the SIFs ability to maintain safety, that is only detectable by functional testing.* Such a failure rate is allocated to SIFs during design. The value of the "integrity-parameter" is considered an estimate, thus the parameter have to be verified in order to justify allocated integrity to SIF. As new "experienced/measured" data seldom arise, updating of the failure rates may only be performed once a year. The updating-activity is important in order to justify inspection/maintenance intervals that is applied, since if the failure rate was higher than expected/allocated for the SIF, the "at-this-moment-too-short" test interval may no longer be acceptable, as the probability that the SIF will fail to perform on a demand increase with a "greater" ratio as the failure rate becomes "higher".

## 1.1 Objectives

For a more detailed explanation of the objectives, refer to printout on page ??.

The objective is to perform a literature study in order to give basis for evaluating safety performance of safety instrumented functions (SIF) on the Norwegian continental shelf. The aim is to suggest any means that may contribute to increased safety integrity of the SIFs through the operational lifetime of a SIF.

## 1.2 Approach

In order to suggest improvements regarding managing of safety integrity for SIFs through their operational lifetime. The **literature study** must consider the following: (1) How is safety integrity of a SIF defined and measured? (2) What do relevant standards and guidelines say about how to ensure that safety integrity requirements are met during the life time of a SIF. (3) What factors may cause a SIF to fail? (4) How may safety integrity of a SIF fluctuate regarding; short perspective (i.e. during maintenance/inspection?), or; long perspective (increase in probability of failure on demand?) After the literature study is performed, a **review on investigations and audits** published by the Norwegian Petroleum Safety Authority is performed, in order to identify any weaknesses that may be avoided if the suggested means/approach would be implemented. A reference is made to chapter 4, in order to present how the "review on investigation and audits" was prepared.

The questions as presented above are not explicitly applied in this thesis, however what the questions consider are addressed within this thesis.

## 1.3 Structure of the thesis

The thesis is divided in chapters, where chapter 2 consider the basics for SIS related concepts. Some of the topics covered in chapter 2 consider; how safety integrity of a SIF is defined; standards and guidelines that give functional and safety integrity requirements to SIFs, and; factors that may cause a SIF to fail. Chapter 3 consider SIS management. Some of the topics covered in chapter 3 consider; the process of defining and ensuring that safety integrity requirements are designed and met; how safety integrity for a SIF may fluctuate during operation, short perspective follow-up and long-perspective follow-up is introduced in order to differ between loss in safety due to component subjected to maintenance, and the process off updating the probability of failure on demand. Further, chapter 3 consider a deeper discussion on factors that affect the probability of a SIF to fail on demand, and how these factors may be measured. Chapter 4 consider performing a review on SIS/SIL performance in the Norwegian continental shelf, while chapter 5 discuss and conclude the findings presented in chapter 4.

## 1.4 Delimitations

The main focus is SIS applications in the oil and gas industry on the Norwegian continental shelf. The main phase to focus on is the operational phase, rather than design phase. It is assumed that the SIS is operating on low demand (i.e. the SIF is seldom required to maintain safety), rather than continuously or high demand. Further, elements outside the scope of the thesis are as follows:

- Elaborate on similarities and differences between standards and practical guidelines (e.g. elaborate on how different methods conduct classification)
- The focus will be set on IEC 61508 (not IEC 61511) when addressing activities related to the life-cycle of a SIS.



# Chapter 2

## SIS related concepts

### 2.1 Equipment Under Control

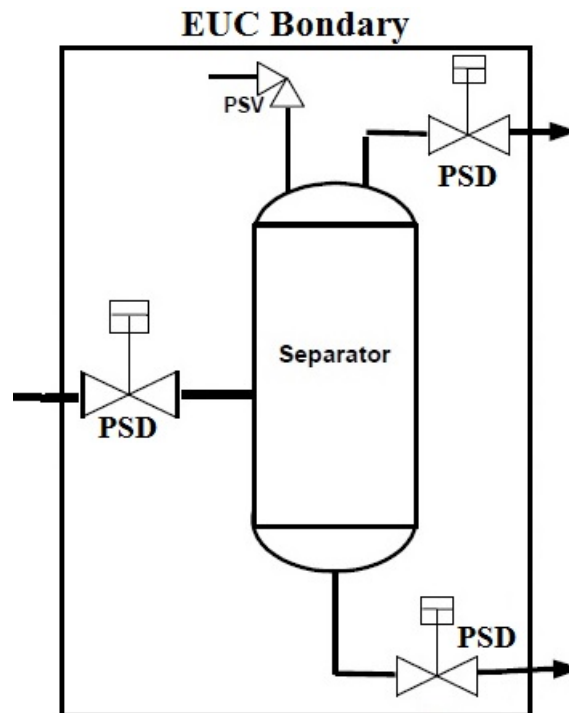
This section is based on OLF 070 (OLF, 2004), if not else specified.

The term Equipment Under Control (EUC) may consider; equipment/machinery that is protected by local safety functions (e.g. close valve), or; an area within an installation that is protected by global safety function (e.g. suppress fire in area). An EUC may be a separator that release pressurized fluid if the equipment is not controlled correctly. The local safety functions that are intended to "control" the separator may perform functional safety by e.g. closing pressure safety valve (PSV) and process shut down (PSD) valves, when a demand occur. When calculating risk related to different assessments (e.g. local area or global area), the term EUC boundary may be applied in order to limit the risk assessment to consider components that is relevant for the area. When calculating "local risk" it may not be relevant to consider the risk reduction provided by the fire suppression system. Hence the EUC boundaries may only consider components that are designed to "control" the separator. Example of such a boundary is given in figure 2.1, where PSV and PSD are considered within the boundaries since the components have its main function to "control" the separator.

Regarding global safety function, the EUC boundaries may be defined in a similar manner. Lets say we have an area subjected to fire and explosion. A global safety function may in this

case be "suppress fire in area", and the boundaries for such an EUC may be given by firewalls, since when assessing risk related to fire and explosion, it is reasonable to consider people inside the fire area that are exposed to the hazard, rather than people outside the fire area. A motivation for defining a fire area as a EUC, is to ensure that acceptable EUC risk (as required by IEC 61508/61511) is presented in a logical manner.

Figure 2.1: Boundaries for EUC, modified figure from OLF (2004)



## 2.2 Introducing the concepts: SIS, SIF & SIL

A **Safety Instrumented System** (SIS) is a system having its main function to provide functional safety<sup>1</sup> to local equipment or global areas, by maintaining a safe state if premises for safety are violated. A SIS system may represent; emergency shutdown system (ESD); process shutdown system (PSD); high integrity pressure protection system (HIPPS), and; fire and gas (F&G) detection system (Lundteigen, 2009). A SIS may be split into three parts, consisting of: (1) The input

<sup>1</sup>When safety depends on system or equipment to be operating correctly (excluding passive barriers), it is called functional safety. (ref. IEC:2008 61508-0)

elements are measuring the conditions on safety, such conditions may be level of pressure in pipes, distance between vessel and platform, concentration of gas particles in the air etc. (2) The indicators on safety given by the input elements are further processed by a logic subsystem (that consist of e.g. Programmable logic controller (PLC)). If the logical subsystem consider premises for safety to be violated, a signal will be sent in order to trigger the final element(s). (3) The final element may be; a vessel propeller that maintain safe distance between vessel and platform; a fire alarm that ensure awareness, or; an emergency shut down valve.

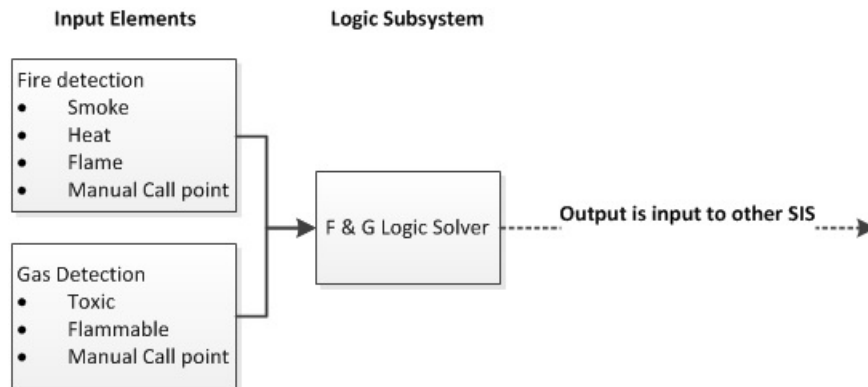
A **Safety Instrumented Function** (SIF) may be defined as a combination of input elements, logic subsystem(s) and final elements, that together maintain functional safety by "performing" a specific function (e.g close one valve). A SIS may perform one or more SIFs. In the case of process shutdown system (PSD), the system may consist of multiple shut-down valves, where each valve is dependent on a specific set of input elements, and often sharing the same logical solver. One SIF within PSD may may be "close valve  $x$ ", while another SIF may be "close valve  $y$ ". If the SIS in consideration is a fire detection system, the system may consist of several smoke/heat/flame detectors that together share a fire and gas (F&G) logic solver (OLF, 2004). The different SIFs within the fire detection system may be smoke detection, heat detection, and flame detection. Each SIF may consist of two elements/components that depend on each other for the SIF to be performing on demand (i.e. serial relationship). The two elements/components may be generalized to consist of component 1;the individual detector<sup>2</sup> (smoke/heat/flame), and component 2; F&G logic solver. The fire detection system may be connected to other systems such as; fire suppression systems, and; heating, ventilation, and air condition system (HVAC). An illustration of a fire detection system is given in figure 2.2.

For each SIF, a **Safety Integrity Level** (SIL) is specified. SIL describes the integrity (i.e. reliability and availability properties) of a SIF through four discrete levels of integrity, in which SIL 4 represents the highest level of integrity and SIL 1 represents the lowest level of integrity. When considering low demand mode, a specific SIL may express our confidence whether the SIF will perform as required when called upon. More precisely, the probability of a SIF performing the required function (e.g. close valve) when there is a demand for the safety function, under all

---

<sup>2</sup>It should be noted that one detector may incorporate multiple input elements that act on different final elements, such input elements may be smoke/heat/flame detection

Figure 2.2: Elements of a F&amp;G detection system, figure adapted from Honeywell (2009)



stated condition within a stated period of time (Pepperl+Fuchs). The probability as such do reflect more than the probabilistic failure data, other factors that may affect the probability of failure on demand are introduced later on.

## 2.3 Safety Integrity

**Integrity** may reflect availability and reliability properties for a particular function (Z-008, 2011). **Availability** is a measure of the % of time an item or system is able to perform a given function, while **Reliability** is a measure on for how long time the item or system is able to perform the function. Both availability and reliability affect the probability whether a function will work or not at a given time. **Safety** may be defined as freedom from unacceptable risk to assets, hence the phenomenon of consequence is introduced in the discussion. **Safety integrity** may then imply the probability that a function is able to maintain freedom from unacceptable risk at a given time. In IEC 61508-4 (2nd edition, 2010), safety integrity is defined as the "*probability of a SIS satisfactorily performing the specified safety functions under all stated conditions within a stated period of time*". It may be argued that if all possible conditions are considered (such conditions will have to reflect execution failure, e.g. fail to reset parameter after maintenance, and extreme weather), we may assume that the system is free from unacceptable risk, given that the function will perform on demand. However it may never be possible to count for all emerging risks. If safety is defined as freedom from unacceptable risk, applying the term safety may impose dif-

ferent management tasks in order to achieve freedom from unacceptable risk on a daily basis. Safety may have to be achieved on a daily basis through e.g. hazard analysis or risk assessment (ref. IEC:2005 61508-0): An hazard analysis identifies what has to be done to avoid the hazard present at the EUC, in other words; how may the EUC and safety-related systems be designed in order to reduce risk. Whilst risk assessment gives requirements to safety integrity.

When applying the term safety integrity, as in safety integrity level (SIL), we may state a probability that there is freedom from unacceptable risk present within a given period of time. If we were to do so, the calculations would have to consider functional safety in combinations with other safety-related systems in order to account for emerging risks.

## 2.4 Introducing: IEC 61508 & OLF 070

This section is based on IEC 61508 and OLF 070, if not else specified. The section intends to present a brief overview of the standard and guidelines. Theory presented here are further discussed in other chapters, hence the terms are not defined hereunder.

Petroleum Safety Authority (PSA) refers to IEC 61508 as a basis for sis design and follow-up of SIS/SIL, and suggests the OLF 070 as one out of several means to achieve compliance with this standard [Stein Hauge \(2008\)](#).

IEC 61508 is a international standard titled functional safety of E/E/PE (Electrical/ Electronic/ Programmable Electronic) safety-related systems (i.e. SIS), and the standard is applied in Norwegian petroleum industry. IEC 61508 require that hazard and risk assessment is performed in order to identify hazardous events that may occur due to risk related to machinery and process equipment. Safety (i.e. freedom from unadaptable risk/hazard) is ensured by functional safety and other safety-related systems. The standard covers the complete life cycle of a SIS, where different SIS-requirements are introduced in order to ensure that functional safety is maintained throughout the lifetime of the installation. The standard propose a quantitative and qualitative approach to assess the safety integrity a SIF may take or is required to conform with. SIL is introduced in order to simplify the process of specifying integrity performance of a SIF. OLF-070 is a guideline on applying the IEC 61508 standard. OLF-070 introduce minimum SIL that may

be applied for the most common safety functions. "Minimum SIL requirements are based on experience with a design practice that has resulted in safety level considered adequate" (OLF, 2004). Applying minimum SIL requirements for common safety functions will reduce the time-consuming processes of specifying a SIL for a basic SIF. Whenever deviation from minimum SIL requirements occur (i.e. component do not clame required SIL level), the deviations need to be treated according to IEC 61508, i.e. SIL level should be based on a fully qualitative or quantitative risk based approach.

## 2.5 SIS requirements

### 2.5.1 Functional Safety Requirement & Safety Integrity Requirements

The required SIS performance is given in the Safety Requirement Specification (SRS). SRS consider functional safety requirements and safety integrity requirements (Lundteigen, 2009): **Functional safety requirements**, stating *what and how* the SIS shall perform upon a process demand. While **safety integrity requirements**, stating *how well* the SIS is required to perform, that is the reliability/availability target and SIL level for the SIF. The terms are further discussed in following sub chapters.

### 2.5.2 Safety Integrity Requirements

This section is based on IEC 61508-1 (edition 2, 2010), if not else specified.

For each safety function, a target failure measure shall be specified in terms of **probability of failure on demand (PFD)** for low demand mode<sup>3</sup> and **Probability of Failure per Hour (PFH)** for high/continuous demand mode. The specification may be based on quantitative or qualitative judgment. If a qualitative approach is utilized, the target failure measure is derived from table 2.1. Table 2.1 presents four discrete levels of acceptable loss of safety that a given SIF may be required to comply with. Further the specification shall contain (in addition to data present in table 2.1); the electromagnetic immunity limit that ere required; and limiting constraints due to

---

<sup>3</sup>Demand mode reflect how frequently a demand for a given SIS may occur.

Table 2.1: SIL for SIF operating on demand or in a continuous demand mode, from IEC 61508-1

SIL	On Demand	Continuous / High Demand
	Average probability of dangerous failure on demand ( $PFD_{avg}$ )	Average frequency of a dangerous-failure ( $h^{-1}$ ) ( $PFH$ )
4	$10^{-5} \rightarrow < 10^{-4}$	$10^{-9} \rightarrow < 10^{-8}$
3	$10^{-4} \rightarrow < 10^{-3}$	$10^{-8} \rightarrow < 10^{-7}$
2	$10^{-3} \rightarrow < 10^{-2}$	$10^{-7} \rightarrow < 10^{-6}$
1	$10^{-2} \rightarrow < 10^{-1}$	$10^{-6} \rightarrow < 10^{-5}$

common cause failure. Since the estimated "target" failure probability will be derived based on a set of assumptions, such assumptions is to be addressed in the specification. The assumptions may consider extreme environmental conditions (including electromagnetic environment) that are likely to occur during the SIS lifespan.

### A discussion on demand modes

The idea behind distinguishing between low and high/continuous demand modes, may be because when in high/continuous demand mode (i.e. frequently demand for SIF), it is expected that when a dangerous SIF failure occur, harm is expected to occur within a short period of time. For low demand mode (i.e. rarely demand for SIF), if a dangerous failure occurs, harm may occur if the failure is hidden during normal operation and not detected during scheduled inspection.

### 2.5.3 Functional Safety Requirements

This section is based on IEC 61508-1 (edition 2, 2010), if not else specified.

The functional safety requirement shall be specified for all SIFs. The specification describe the logics behind the SIS, that is on which level the input elements shall act upon (e.g. maximum allowable pressure in tank), and how the final elements are intended to achieve or maintain functional safety (e.g. maximum allowable time it takes to close an emergency valve), under relevant modes of EUC operation (considering EUC; ,startup, maintenance, steady state operations, and abnormal conditions). Further, the specification is to describe how the SIS is expected to perform when different SIS failure occur. In order to consider such, the specification describes how

the SIF is dependent upon or interacting with other safety-related systems ( including operator-SIS interface) either within or outside the EUC.

## 2.6 Failure definitions

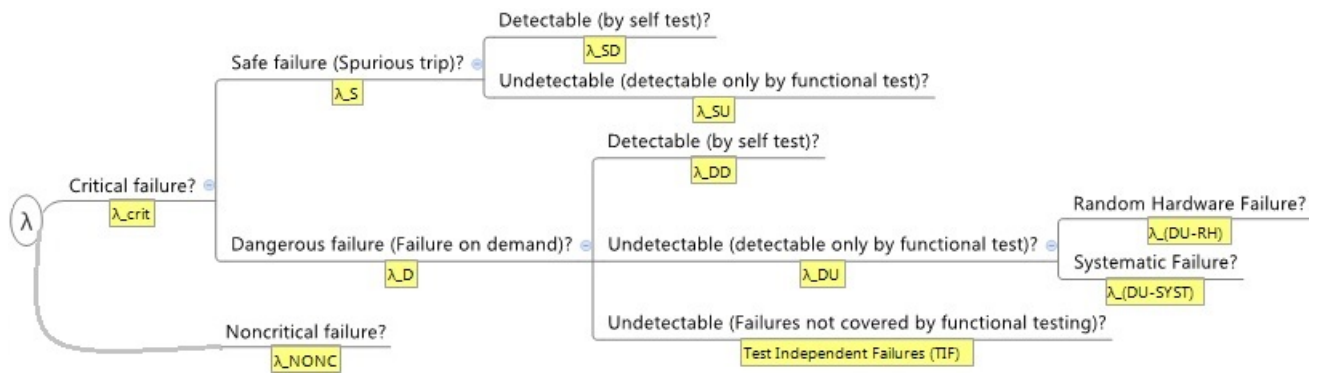
This section is based on [pds \(2010\)](#) if not else specified. For a brief discussion on PDS method in relation to IEC 61508, refer to section [3.3](#).

### 2.6.1 Failure modes

The PDS method consider three different failure modes; dangerous; safe, (spurious trip) and noncritical failures, ref. figure [2.3](#). A **dangerous failure** is present if the required safety function is not able to perform on demand (e.g. valve not close on demand). A dangerous failure may be detectable, undetectable or test-independent. Dangerous undetected (DU) failure consider a failure that is not detected by automatic self test as the failure may only be identified during functional testing, while dangerous detected (DD) failure are failures detected by automatic self-tests. Dangerous failures that are not revealed during functional testing, may be named *test independent failures* (TIF). A TIF may occur if a gas detector at an offshore installation is tested with test gas rather than hydrocarbon gas. The test gas is provided to the detector trough a hose going into the detector head. Such a test is not able to reveal whether the detector is on a wrong location, or if the detector is covered with dust ([Per Hokstad, 2009](#)), hence a TIF may occur. **Safe failures** is as a failure that have the potential to cause a spurious trip (i.e. a failure where the safety function is activated without a demand). A safe failure may be detectable by any means. If the failure is considered safe detectable (SD), an actual spurious trip may be avoided, regarding safe undetectable (SU) failure, such a failure may not be avoided, hence a spurious trip may occur. All other failures are named **noncritical failure**, as such failures do not affect the main function of a SIS.



Figure 2.3: Failure categories



### 2.6.2 Random hardware or systematic failure?

According to PDS method, dangerous undetected (DU) failures may be divided into random hardware failure and systematic failure. **Random hardware failure** occur due to natural degradation of the component, that is failures that occur within assumed operating conditions. **Systematic failures** are defined as "a particular cause other than natural degradation and foreseen stressors", (pds, 2010). Systematic failures may be introduced during different life cycle phases of the SIS, and the failures may be caused by e.g. "fail to reset parameter after maintenance", or "fail to perform checklist after maintenance". A fully reparation of a systematic failure, may also ensure that the failure do not re-occur. This may be the case if fire alarms are relocated from a "defect-location" to a location directly above the potential hazard.

### 2.6.3 Independent or common cause failure?

A common cause failure (CCF) consider multiple components which are unable to perform as required due to a common cause. While an independent cause may trigger a single component to fail, a common cause may cause multiple identical components to fail within the same period of time. In the context of SIS, we consider failure of a single or several SIFs, and the failures are to occur within the same inspection or functional test interval. Maryam Rahimi (2012). Common cause failures are of particular importance in redundant systems. Given that two smoke detectors have equal probability of failing to perform on demand, having redundant components

placed at the same location may be seen as an effort that increase the probability to detect a fire. However if both detectors are placed on a location were they are not able to detect if smoke is present, both detector may be considered to "carry" a failure that is caused by a common cause (i.e. inappropriate location of detectors).

Common cause failures may happen due to the following<sup>4</sup>:

- A common **design** that does not fit into the assumed state/condition of the system.
- A common **installation** error
- A common **human action** error. Human action represents all human interaction with the system during operation. It may be expected that an operator perform insufficient maintenance for multiple components, given that the operator has lack of experience about the system. The common cause may be identified as lack of experience.
- A common **abnormal stress** (e.g. harsh environment) that the components was not designed to withstand.

A SIF may be treated independent if it does not share parameters as listed above with other SIFs. This may imply; diverse technology; SIF do not share components (e.g. power supply); SIFs do not share common operational, maintenance or test procedures, or; SIF are not subjected to similar environment.

---

<sup>4</sup>The categories and their definitions are based on [Rausand \(2011\)](#) and [Maryam Rahimi \(2012\)](#)

# Chapter 3

## SIS management

### 3.1 Managing the integrity of the SIS

This section is based on IEC 61508-1 (edition 2, 2010), if not else specified.

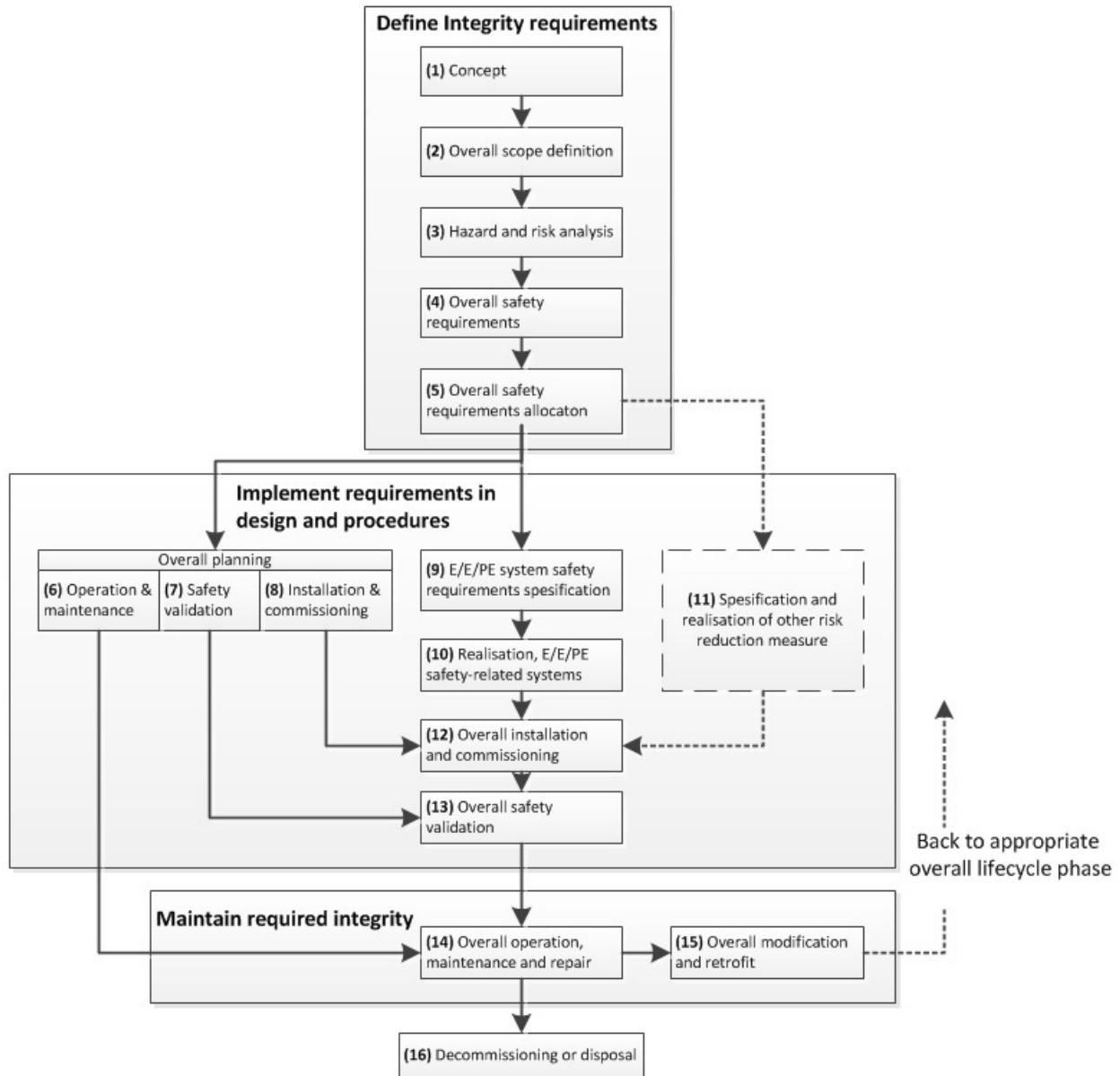
The IEC 61508 standard present different objectives and requirements, that the relevant stakeholders have to comply with in order to ensure conformance with different standards and regulations. The objectives and requirements are coupled to different phases of the Safety Life Cycle (SLC). The SLC may be considered a tool that guide the process of defining and ensuring that safety integrity requirements are designed and met. SLC according to IEC 61508 is presented in figure 3.1, and the different life cycle phases may be divided into three distinct categories, where step 1 to 5 consider defining integrity requirements for the SIS. The following phases from step 6 to 13 consider implementing the requirements into actual design and procedures, while step 14 to 15 consider activities that maintain required integrity. From this point onwards, a more detailed presentation of the different steps in figure 3.1 will be given.

**Step 1 to 3** consider developing a level of understanding and criteria about EUC and the associated risk. A hazard and risk analysis is to be performed in order to derive hazardous events<sup>1</sup> that may occur. In **step 4**, an overall safety function is created for each hazardous event, such a safety function may be defined as "prevent distance between supply-vessel and installation to be be-

---

<sup>1</sup>Hazardous event may be defined as "the point at witch control of the hazard is lost, this is the point from witch further barriers can only mitigate the consequence of the event". [Rausand \(2011\)](#)

Figure 3.1: Life cycle of a SIS, figure adapted from IEC 61508-1 (2010 edition 2).



low one meter". Each requirement (e.g. minimum one meter etc.) may be determined quantitatively and/or qualitatively. Such an overall safety function will not be specified in technology-specific terms, since the specific method to be implemented is introduced in step 5. The output from step 4 is a specification that reflects required safety integrity regarding the overall safety function. The target is not to be specified in terms of SIL at this point, as SIL is introduced in step 5. However the target may be defined as required risk reduction or tolerable rate of hazardous events for given failure modes (e.g. number of failures per hour regarding supply-vessel to close or to far away from installation). **Step 5** consider allocating overall safety functions (that was identified in step 4) to designated E/E/PE safety-related systems or other risk reducing measures, such as a SIS may be a dynamic positioning system (DP) that is intended to maintain a vessel position by using propellers and thrusters as final elements. The allocation is an iterative process, if the tolerable risk can not be achieved, then the specification for the EUC (SIS not included in this EUC), E/E/EP system (i.e. SIS) or other risk reducing measures, may be modified. Further a target SIL is allocated to each overall safety function (i.e. SIF), and as mentioned in section 2.5.2, when applying the SIL table, one has to consider limitations due to common cause failure and other hardware and regulatory constraints. **Step 9** consider deriving safety requirement specification (SRS) (ref. chapter 2.5) from safety integrity requirements and functional safety requirements, having step 1 to 5 as the basis. Considerations related to constructing SRS were identified in sections 2.5.2 and 2.5.3. In **step 10**, the objective is to create/realize a SIS that conforms with the SRS, and **step 11** consider specification and realization of other risk reduction measures. Considerations related to step 11 are not discussed in the thesis, as the IEC 61508 standard do not cover those subjects. Step 6 to 8 Consider developing a plan in order to prepare for tasks such as; installation and commissioning; operation and maintenance, and; safety validation. Regarding **step 6** (planning for operation & maintenance) the objective is to ensure that functional safety is maintained by designing documentation and procedures that guide how activities in step 14 (overall maintenance and repair) is performed, as well as ensuring that the status on safety/hazardous-events/incidents is updated. The plans shall specify; routine actions that compensate for reduced safety due to SIF is by-passed; procedures applied when bypassing/during-bypass/returning the SIF to normal operation, and; procedures that will determine if normal operation is present. Further a systematic analysis is performed in or-

der to schedule routine maintenance activities carried out to detect DU failures. In **step 7** the objective is to develop a plan for the overall safety validation that is performed in step 13. The planning activity is introduced in order to construct measures, techniques and procedures that will identify whether the allocated safety functions conforms with the safety requirement specification (ref section 2.5). The plans should reflect; the specification of the SIS (and EUC) to be validated and for which modes of operations; who should perform the validation; necessary calibration tools and equipment to be applied and; type of validation strategy (e.g. analytical methods, statistical tests etc.). The objective in **step 8** is to develop a plan for installation and commissioning to assure that functional safety is achieved. Regarding installation, factors that may ensure functional safety are; allocation of responsibilities; having defined schedule and procedures; the sequence in which elements are integrated, and; declaring parts ready for installation and when the installation activities are complete. Regarding commissioning, factors that may ensure functional safety are; allocation of responsibilities, and; having defined schedule and procedures that is coherent regarding installation and validation. **Step 12, 13 and 14** consider performing overall installation, commissioning, safety validation, operation, maintenance and repair according to prescribed plans (refer to step 6, 7 and 8). In **step 15 and 16**, the objective is to ensure functional safety during and after modification, retrofit, decommissioning or disposal. The different tasks may happen due to safety performance is below target or the EUC is to be modified. The tasks shall only be initiated by authorization that manage functional safety, and the decision whether to perform the tasks are based on a impact analysis (e.g. hazard and risk assessment) that reflect the change in functional safety. If a hardware or software modification were to be implemented (step 15 is here considered), it might be necessary to return to the appropriate life cycle phase, in order to e.g. specify new functional or safety integrity requirements that reflect new hazards and risks.

## 3.2 SIS follow-up

This section is based on [Stein Hauge \(2008\)](#), if not else specified.

This section apply a fire and gas (F&G) detection and suppression system (ref. figure 3.3). In

reality such a system may not be named F&G detection and suppression system, and the system as presented may incorporate components that belong to other SISs. This chapter assume the elements/components in figure 3.3 to be a part of a F&G detection and suppression system in order to simplify the discussion.

SIS follow-up depends primarily on tasks performed in preparation of; operation and maintenance, and; safety validation (ref. fig 3.1, step 6 and 7), and is executed during the operational phase of the installation. As mentioned in section 3.1, one objective in "preparation phase" is to ensure that functional safety is maintained by designing documentation and procedures. Regarding SIS follow-up procedures, the main activities are illustrated in figure 3.2. During operation, SIS follow-up may be split in two categories, having activities related to; (1) normal operation, maintenance, modification, and; (2) monitoring and verification (ref. figure 3.2, maintain and monitor). The categories are discussed in following subsections.

### **3.2.1 SIS follow-up: Normal operation, maintenance and modification**

This section refer to figure 3.2, *Maintain*.

The F&G detection and suppression system consist of multiple parts, such as; F&G detectors and manual call points; F&G logic solver that may rely on battery backup; sounder/beacons intended to actuate on emergency, and; a F&G suppression system that suppress fire and gas (e.g. ventilating gas, provide water etc.). Some of the components may have a property that alert if a failure is present (alerting if battery bacup is considered in a failed state, i.e. DD failure), some of the components may have test independent failures (i.e. failure not identified through functional testing), and some may have strong aging parameter. Hence different maintenance strategies are present for different components. Choice of maintenance tasks for given component is described in the SRS and maintenance system.

The first steps when performing maintenance is to plan for and execute preventative maintenance (PM) and functional testing, PM may here represent scheduled overhaul and replacement. Functional testing and PM may never guarantee that all relevant factors that functional safety rely on, are sufficiently present until next inspection/maintenance. Regarding functional

Figure 3.2: Illustration of SIS follow-up activities Stein Hauge (2008)

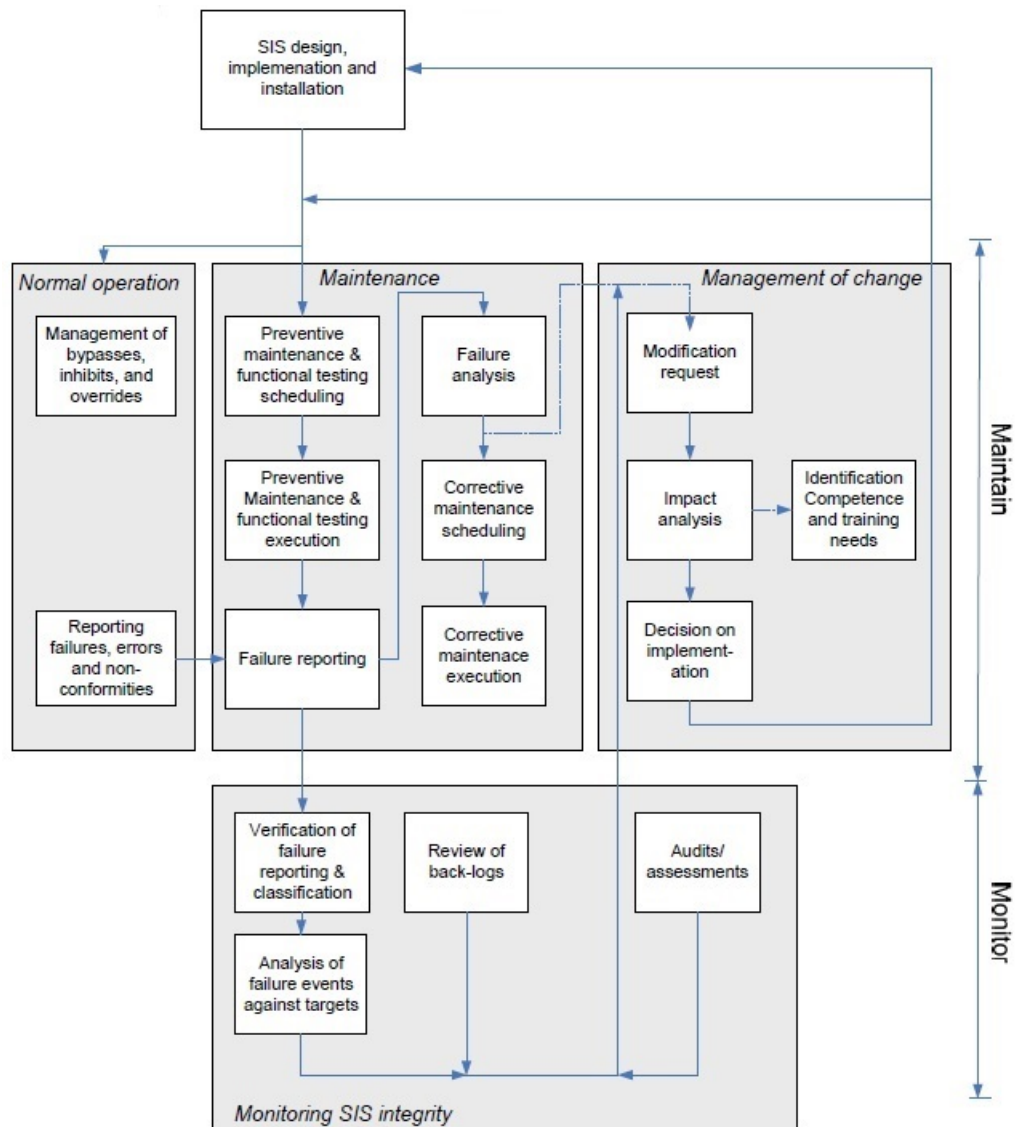
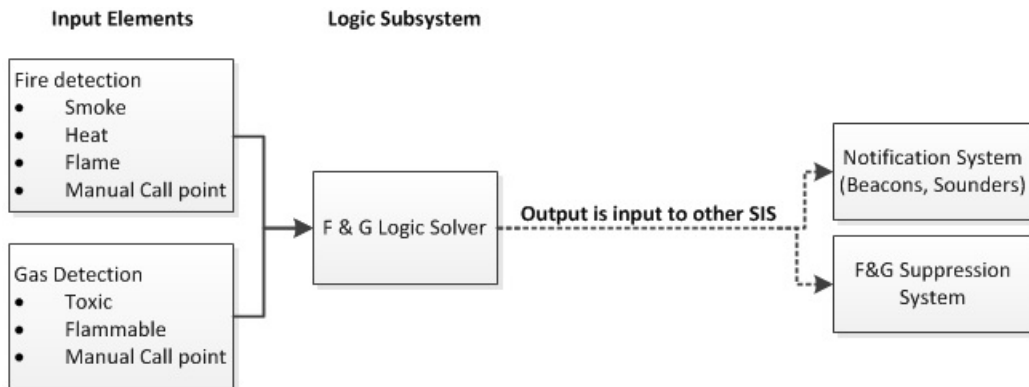




Figure 3.3: Illustration of the F&amp;G detection and suppression system



testing, the best solution would be to perform a real demand, but testing with real gas may not be suitable. In such a case it may be relevant to apply a non toxic test gas if applicable. Bypasses, inhibits, and overrides are introduced if the test do not reflect real demand, or the process is not to be disturbed. Such bypasses are subjected to systematic failures, it may be because improper setting or resetting of e.g. fire suppression system, in addition a real fire may occur while the fire suppression elements are bypassed. Hence strict procedures should be established that enforce safe interaction. The procedures may reflect; provision of use; instructions for performing bypasses; precautions that may decrease probability of introducing systematic failures, and; logging of bypass in combination with routines that ensure such information to flow between shifts. Components included in functional testing are the only one to be credited as tested, while omitted components have to be covered on a separate test. Functional testing and other relevant inspection/monitoring actions (e.g. self diagnostics, spurious trips and real demand) may result in updated knowledge on failures, errors and nonconformities. Such failures are recorded through the maintenance system. When documenting such failures it is important to classify failure according to severity (e.g. safety critical failure, DD or DU) in order to ensure appropriate analysis and repair actions. Hence the PM and functional testing procedures or relevant documentation should enforce the operator to consider factors such as failure cause and effect (e.g. is the failure safety critical?). If a failure were to occur, compensating measures is to be evaluated and implemented until the failure is repaired. Regarding safety critical failure, the Norwegian petroleum safety authority (PSA) state that the failure have to be treated immediately. If the task

is delayed, compensating measures have to be introduced in order to ensure safety.

Handling of SIS modification is sometimes referred to as management of change (MoC) (ref. figure 3.2). Modification may be initiated if deviation from SRS occur, those deviations may reflect operation outside assumed/expected conditions, high number of false fire alarms or expansion of the process plant. More generally, the demand for modification may come from results from failure analysis that was based on experienced performance. As previously stated (ref. 3.1, step 15), a modification request is then initiated by authorization that manage functional safety, and the decision whether to perform the tasks are based on a impact analysis. If hardware or software modification were implemented, appropriate life cycle phase have to be initiated and necessary competence/training needs have to be addressed. For a further discussion on the topic, refer to section 3.1, step 15.

### **3.2.2 SIS follow-up: Monitoring performance and verification**

This section refer to figure 3.2, *Monitor*.

Monitoring SIS performance considers comparing recorded SIS performance with target values specified in SRS, the targets may reflect the "safety-performance" and/or "failure-performance" of a SIS. Further every assumption made about; the SIS; the state it is operating within, and; how it is maintained, have to be verified during operation. Procedures and work practices have to be evaluated in order to address whether they are effective in terms of their ability to avoid and control the occurrence of systematic failures. Such tasks may be incorporated in already defined procedures for verification and audit activities (ref. section 3.1, step 13).

### **3.2.3 Short perspective follow-up: Deciding which components to maintain whilst ensuring safety**

This section is based on [Erin](#), if not else specified.

This section aims to propose an approach/framework for evaluating different maintenance/inspection configurations. The approach consider deciding which components to be maintained/bypassed

simultaneously. The approach is based on how a selection of organizations within the United States nuclear industry perform evaluation of maintenance configurations, however identifying how "evaluating the performance of a SIS subjected to maintenance" may give rise to decisions, are some of the findings identified within this thesis, however all methods applied are of common knowledge.

### **Introduction**

A selection of organizations within the United States nuclear industry applies risk monitoring software, as a tool to evaluate different maintenance configurations that may be applied in the nearest future. The software considers a Probabilistic Risk Assessment (PRA) framework. The inputs to the assessment are mainly the states that the components will take when they are subjected to inspection/maintenance. If the components are being maintained or bypassed, they are considered unavailable, and marked as such in the PRA software. The output of PRA is mainly the risk picture that reflect whether the risk that follows a given maintenance configuration is tolerable or not.

### **Introducing the PRA approach**

Probabilistic Risk Assessment (PRA), is an approach that applies quantitative values on frequency/ probability in combination with severity in order to assess risk. Risk may be explained as a combination of; likelihood of different accident scenarios to occur, and; the consequences that may happen given the different accident-scenarios have occurred. Accident-scenarios are uniquely defined chain of events confined by initiating event and a corresponding end state of relevance [Johansen \(2010\)](#). An initiating event may be defined as the first deviation from normal operation, that may cause a chain of events that may or may not lead to harm on assets. An initiating event may be e.g.; fail to reset parameters after maintenance on water pump, or; an explosion that require the start of the F&G detection and suppression system. Following, the end state of relevance may consider uncontrolled fire, controlled fire, or; damage to people or assets. The accident scenarios between initiating event and end state may be modeled with an event tree. The event tree models what may occur if; physical systems (e.g. sprinkler system or fire alarms), or; human intervention, interrupt or fail to interrupt the accident sequence (ref.

figure 3.7 on page 30). When the events within the event tree reflect different final elements that perform (or fail to perform) functional safety (e.g. provide water or notify on fire), the different events may then be modeled through a Reliability Block Diagram (RBD)<sup>2</sup>. Where different blocks in the diagram may represent components or functions.

If the RBD did consider components within a SIF, the different blocks in the diagram may then represent; input elements (e.g. automatic fire detector and manual call point); F&G logic subsystem (e.g. main power supply, battery backup, F&G logic solver 1 and 2), and; final elements (e.g. water pump A and B, sprinkler and fire alarm) (ref. figure 3.8 on page 30). If the RBD should consider functions, each block may then represent a specific function such as; smoke detection; heat detection, or; flame detection, note that all functions may be placed in the same "detector component". It may be preferable to let the RBD consider functions, since PFD values for given safety functions may already be available in the SRS, or easily be collected for the most basic safety function (ref. OLF-070, application of minimum SIL requirement for common safety functions). However, if a redundant component within the SIF is subjected to maintenance, the RBD, regarding the SIF, may preferably be represented by components in order to credit the fact that the SIF is able to perform on demand due to a redundant component being maintained. Anyhow, the reliability-values presented in the RBD may reflect PFD if low demand mode of operation are considered. How the  $PFD_{system}$  may be calculated are discussed further on.

**Remark** It may be difficult to model input element "manual call point" as a single block in the RBD, as the reliability given to this block may represent the probability for a manual call point being triggered by an operator at the time a fire is present, and the probability that the manual call point will transmit the signal when triggered. The US nuclear PRA model adapted to this situation (or similar) by assuming that the action "applying manual call point" will always fail (i.e. non credit given) if the task is not presented in any procedure, however it is expected that the "manual call point procedures" are well known, hence the action will be credited. The "reliability value" given to the manual call point may vary between dif-

---

<sup>2</sup>A Reliability Block Diagram (RBD), consists of blocks that represent different components and their dependence needed for the system to be operating (i.e. perform functional safety). The blocks that represent the system are given a reliability value, and by applying a structure function on the blocks/reliability values, it is easy to calculate the system reliability.

ferent maintenance configurations. This variation is expected to occur, since the essence in performing the presented PRA approach, is to increase reliability for "other reliability blocks" that is not subjected to maintenance. This may be conducted by e.g. introduce procedures/precautions that may ensure "a newly tested physical-redundant" manual call point being triggered if an explosion would occur. Other means that may be applied in order to reduce the risk picture are discussed later on.

### **Performing PRA, to decide maintenance configuration**

As previously stated, the output of PRA is mainly the risk picture that reflect whether the risk that follows a given maintenance configuration is tolerable or not in comparison with no maintenance performed. The risk that reflect "no maintenance is performed" may be named base-risk. Further, the base-risk is a combination of base-probability and base-severity (ref. figure 3.5). In figure 3.5, the different magnitude of risk are given different colors; red (high risk), yellow (medium risk), and green (low risk). Lets say that four different maintenance configurations were evaluated (ref. figure 3.6), where the end states "frequency (per year) of uncontrolled fire with no alarm" were applied as the indicator on safety performance<sup>3</sup>. The frequency of this consequence were previously (during e.g. design-phase) identified to be  $8.0 \times 10^{-8}$  per year, and reflect normal operation when no maintenance is performed (this maintenance configuration is given number 0, ref. figure 3.6). The frequency were calculated applying the event tree in figure 3.7. The frequency will vary according to how the sprinkler system and fire alarm system will perform on demand, and how often explosion is estimated occur. The probability for the sprinkler system to fail on demand is in figure 3.7 given to be 0.01. The PFD value of 0.01 is calculated applying a RBD as presented in figure 3.8, and the value may be named base- $PFD_{system}$ , since it reflect normal operation, and all blocks within the RBD ("fire alarm" not included) are given credit<sup>4</sup>. When a specific maintenance configuration is assessed, different rules may be applied in order to give credit to blocks/components in the RBD. The rules may be based on regulations

<sup>3</sup>Risk picture (ref. fig 3.6) may be evaluated for all consequences in figure 3.7 in order to assess overall risk for maintenance configuration, however only consequence number 1 (ref. figure 3.7) is applied here due to simplifying the discussion.

<sup>4</sup>In order to simplify the discussion, the "sprinkler system" and "fire alarm system" is assumed to be independent, this assumption may be true if separate input elements and logic subsystem is applied for the systems. The assumption of independence between the systems, may not be reflected in figure 3.8, however figure 3.8 is meant to illustrate functions/components that the final elements are dependent on.

or constraints, such as "safety may only be ensured if  $K$  out of  $N$  subsystems/water pumps perform according to requirements". Hence if 2 out of 3 water pumps are needed to ensure safety, and two water pumps are subjected to maintenance, the last water pump may not be credited. Given that the "sprinkler system" are given following constraints (ref. figure 3.8):

- Automatic Detector (AD) & Manual Call Point (MP): 1oo2
- Main Power Supply (MS) & Battery Backup (BB): 1oo2
- F&G Logic Solver 1 (1) & F&G Logic Solver 2 (2): 1oo2
- Water Pump A (A) & Water Pump B (B): 1oo2
- Sprinkler (S): 1oo1

And it is assumed that the different KooN elements are in a serial relationship (ref. figure 3.8), the PFD given to the "sprinkler system" may be calculated as such:

**Remark** We consider short perspective risk, i.e. increased risk during maintenance, hence the PFD value for the component or function that is subjected to maintenance (ref. equation 3.1) will not be credited, i.e.  $PFD = 0$ .

$$PFD_{system} = PFD_{AD\&MP} + PFD_{MS\&BB} + PFD_{1\&2} + PFD_{A\&B} + PFD_S \quad (3.1)$$

Each PFD may be calculated applying the formula  $PFD = \frac{E(Downtime)}{\tau}$ . In a SIS context, the formula may be understood as the average percentage of time interval ( $0 \rightarrow \tau$  or  $\tau \rightarrow 2\tau$ ) where the component is not able to performing required functional safety due to a DU failure. The value  $\tau$  will reflect the time since last inspection/maintenance. If  $\lambda_{DU} \times \tau$  is a "small" number for all components, the PFD value may be approximated as given in figure 3.4. Hence equation 3.1 may now be calculated applying the following formula:

$$PFD_{system} = \frac{(\lambda_{DU_{AD\&MP}} \tau_{AD\&MP})^2}{3} + \frac{(\lambda_{DU_{MS\&BB}} \tau_{MS\&BB})^2}{3} + \frac{(\lambda_{DU_{1\&2}} \tau_{1\&2})^2}{3} + \frac{(\lambda_{DU_{A\&B}} \tau_{A\&B})^2}{3} + \frac{\lambda_{DU_S} \tau_S}{2}$$

A fraction of the PFD may consider DU failures that come from common cause failures. Lets say that a system had a 1oo3 configuration, and one of the parallel components were subjected

---

<sup>5</sup>The equation assume equal  $\tau$  for redundant components

Figure 3.4: approximated PFD for different koon constraints,, Rausand (2011)

$k \setminus n$	1	2	3	4
1	$\frac{\lambda\tau}{2}$	$\frac{(\lambda\tau)^2}{3}$	$\frac{(\lambda\tau)^3}{4}$	$\frac{(\lambda\tau)^4}{5}$
2	-	$\lambda\tau$	$(\lambda\tau)^2$	$(\lambda\tau)^3$
3	-	-	$\frac{3\lambda\tau}{2}$	$2(\lambda\tau)^2$
4	-	-	-	$2\lambda\tau$

Series/Parallel

to maintenance. While maintenance is being performed, the components that are in a standby state (i.e. they may perform on demand) would be considered a 1oo2 configuration. The PFD for such a configuration would be calculated applying the flowing equation (Rausand, 2011):

$$PFD = PFD_{independent} + PDF_{commoncause} = \frac{((1 - \beta)\lambda_{DU} \times \tau)^2}{3} + \frac{\beta\lambda_{DU} \times \tau}{2}$$

In addition to evaluate plausible maintenance configuration, performing the PRA-approach as presented may give basis for communicating risk by visualizing the "risk of the day". Such an integrated tool may easily communicate that the fire area is subjected to medium (yellow) risk due to performing maintenance on "fire alarms". Such an assessment might end up with identifying necessary precautions that is communicated to the people subjected to the harm, hence the magnitude of the risk may be reduced and given maintenance configuration may be executed.

The approach presented here is identified as short perspective follow-up, since a given risk picture is only considered representative while the maintenance configuration is performed. It may be that a given configuration of components that are unavailable due to maintenance are running the next day, while "other" components are marked as unavailable the "next day" due to a different maintenance configuration being executed. Updating the failure data (PFD) may

not be performed after each session of inspection and maintenance, since data such as "time in service" and occurrence of incidents and failures may not be "changed" between sets. Thus the next section consider how failure data may be updated as new "experience" is gained.

Figure 3.5: Risk picture, the figure is not to be understood as a risk matrix, the figure illustrate how the color-coding in figure 3.6 should be interpreted.

Probability/Frequency (relative to base)	Severity (relative to base)	Risk Picture Should the maintenance configuration be accepted? (Relative to maintenance configuration: 0)
High increase from Base Probability	High increase from Base Severity	High risk introduced, maintenance configuration may not be performed.
Medium increase from Base Probability	Medium increase from Base Severity	Medium risk introduced, maintenance configuration may be performed under specific consideration. Such considerations reflect measures that are not counted for in the PRA-model, such considerations may be maintenance duration, or abstract factors such as risk awareness.
Equal or less than Base Probability	Equal or less than Base Severity	Acceptable risk introduced, i.e. same as or better than target. (target may be: Expected number of fatalities per year, when no maintenance is performed)

Figure 3.6: Risk picture on different maintenance configuration. Note that the risk picture for configuration 3 is green, since no fatalities occur due to people are evacuated from fire area.

Outcome [1]: Uncontrolled fire with no alarm (ref. event tree)	Probability /Frequency (Per year)	Severity (per outcome)	Risk Picture (including notes)
Maintenance configuration 0	$8.0 \cdot 10^{-8}$ (Base frequency)	Multiple fatalities (Base severity)	No maintenance performed (Base Risk)
Maintenance configuration 1	$8.0 \cdot 10^{-6}$	Multiple fatalities, same as base	Maintenance performed on water pump A and B
Maintenance configuration 2	$8.0 \cdot 10^{-7}$	Multiple fatalities, same as base	Maintenance performed on water pump A
Maintenance configuration 3	$9.0 \cdot 10^{-6}$	No fatalities, significant material loss, better than base	Maintenance performed on water pump A and B, and fire alarms are maintained, while people are being evacuated from the fire area.

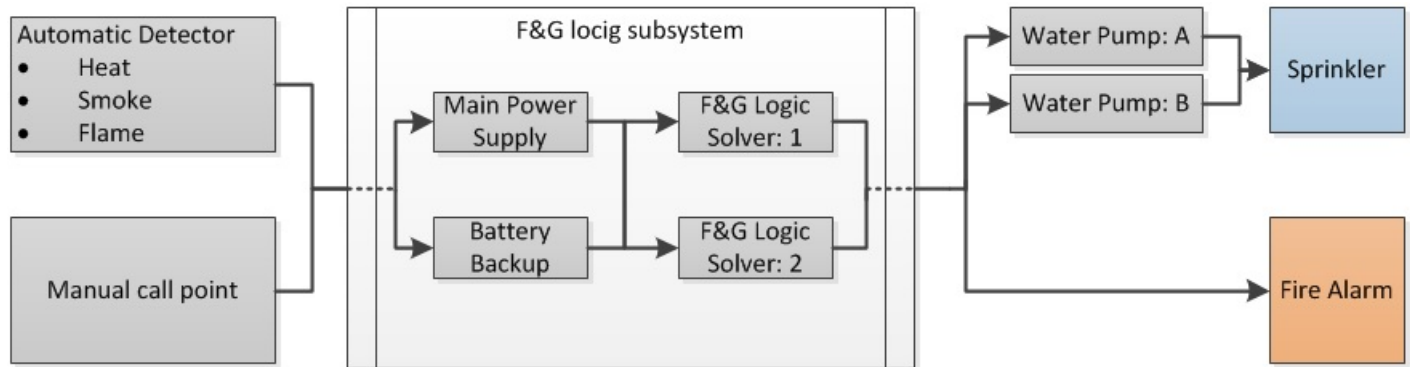


Figure 3.7: Event tree, regarding initiating event: Explosion [Rausand \(2011\)](#)

**Maintenance Configuration: 0**

Initiating Event	Start of fire	Sprinkler system do not function	Fire alarms is not activated	Outcomes	Frequency (Per year)	No.
Explosion $10^{-2}$ per year	True	True	True	Uncontrolled fire with no alarm	$8.0 \cdot 10^{-8}$	1
			False	Uncontrolled fire with alarm	$7.9 \cdot 10^{-5}$	2
		False	True	Controlled fire with no alarm	$8.0 \cdot 10^{-5}$	3
			False	Controlled fire with alarm	$7.9 \cdot 10^{-3}$	4
	False			No Fire	$2.0 \cdot 10^{-3}$	5

Figure 3.8: Reliability block diagram for functional safety systems: Sprinkler and Fire Alarm



### 3.2.4 Long perspective follow-up: Update failure rates and test intervals

A reference is here made to appendix [B](#)

During operation, verification is to be performed in order to verify that ongoing safety integrity correlate whit the premises for safety integrity that was laid down during design of the installation. The premises laid down during design constitute different uncertainties related to  $\lambda_{DU}$  and inspection/test interval  $\tau$ . The value of  $\tau$  that is given to a component subjected to mainte-

nance may be defined on the basis of an estimation of "true  $\lambda_{DU}$ "<sup>6</sup>, hence when new knowledge about the "true  $\lambda_{DU}$ " arise, the failure rates (regarding  $\lambda_{DU}$ ) and test intervals ( $\tau$ ) may be updated in order to implement more "effective" maintenance-intervals or introduce additional safety-related systems. If "long perspective follow-up" identified that  $\tau$  may be the double of what was previously stated, number of inspections/maintenance per year may than be half of what is previously applied, hence money saved.

### Introducing target and performance indicator

The ongoing safety performance are measured through a set of *performance indicators*, that may explain the different states a system may take. Target values are applied in order to measure safety performance against a threshold. In the context of SIS, the target may be given by a SIL that is allocated to a SIF during design. The SIL reflect a treshold-PFD that may be named  $PFD_{required}$ .  $PFD_{actual}$  is the experienced PFD that will be compared to  $PFD_{required}$ .

PFD values are calculated by parameters such as  $\lambda_{DU}$  and  $\tau$  (ref. figure 3.4). Regarding  $\lambda_{DU}$ , the parameter is countable (number of experienced dangerous undetected failure per hour) for a given SIF, hence it may act as the performance indicator. Regarding a specific SIF, the failure rates that is experienced may be summed for all components that belong to a SIF, hence the  $PFD_{required}$  value that correspond to the SIF will be applied as the target. If  $\lambda_{DU}$  is summed for individual/identical components within the SIF, a different target may be applied for the identical SIF-components in consideration. However the sum of  $\lambda_{DU}$  failures that are identified across the individual components of the SIF may not exceed the  $PFD_{required}$  threshold given to the SIF.

### Introducing the performance indicator (DU-failure) and target value (E(X))

Regarding SIS, the target may be given by expected number of DU failures ( $E(X)$ ), for  $n$  identical components, with assumed failure rate  $\lambda_{DU}$ , that are expected to be in service for  $t_n$  accumulated time in operation. The formula for calculating target  $E(X)$  is presented hereunder

---

<sup>6</sup>PFD for a single component may be calculated as:  $PFD = \frac{\lambda_{DU} \times \tau}{2}$ , from this equation it may be seen that if the PFD value is defined according to SIL requirement (i.e a treshold is given), and  $\lambda_{DU}$  is an estimate of "true  $\lambda_{DU}$ ", the  $\tau$  parameter is the only factor that may be adjusted in order to maintain required PFD

(Stein Hauge, 2008):

$$E(X) = n \times t \times \lambda_{DU} = t_n \times \lambda_{DU}$$

The performance indicator is than experienced number of DU failures, among the  $n$  identical components, that have been in service for  $t_n$  accumulated time.

### Rules to be applied, regarding target

Lets say that expected number of DU failures ( $E(X)$ ) were estimated to be 4 per year for a given number of fire detectors within the interval of one year. If all detectors had been subjected to at least one functional test or similar during one year, and number of experienced DU failures turned out to be less then, or equal the target value, the experienced safety integrity may then be considered acceptable. Further risk reduction may be applied according to ALARP<sup>7</sup> principle. IF  $E(X)$  were found to be larger than 4, the result is then to be considered worse than target. A consequence of such may result in required SIL level not being satisfied, and the response would be to apply more frequent tests, or improve functional safety by other safety-related means.

### Rules to be applied, regarding applying new and old failure rates

Given both new failure rate from operational data and original failure rate from design data are present. The decision on how to apply/combine those failure rates are based on how confident we are whether the new failure rate is true. The logic behind the decision is presented here: (1) If we are equally or more confident in the new failure rate compared to the original failure rate, we may decide to apply only the new failure rate. (2) If we lack confidence in the new failure rate (i.e. have insufficient accumulated time of components in operation), we need to combine the original failure rate from design, with the new failure rate from operational data.

### Updating failure rates with respect to: Operational Data

If we apply data from operation only, following formula may be applied:

$$\hat{\lambda}_{DU} = \frac{x}{t_n} \quad (3.2)$$

---

<sup>7</sup>ALARP: Risk is to be reduced to "as low as reasonable practicable", Rausand (2011).

### Updating failure rates with respect to: Operational Data & Design Data

If we combine the original failure rate from design data with the new failure rate from operation data, we may state that; (1) we do not have sufficient confidence in the new failure rate, and (2) we may be able to adjust the original failure rate from design based on operational experience. We introduce uncertainty parameters  $\alpha$  and  $\gamma$  in combination with equation 3.2, in order to obtain the updated failure rate:

$$\ddot{\lambda}_{DU} = \frac{\gamma + x}{\alpha + t_n} \quad (3.3)$$

Further, the uncertainty parameters  $\alpha$  and  $\gamma$  are defined as:

$$\alpha = \frac{\lambda_{DU}}{(\lambda_{DU-CE} - \lambda_{DU})^2}$$

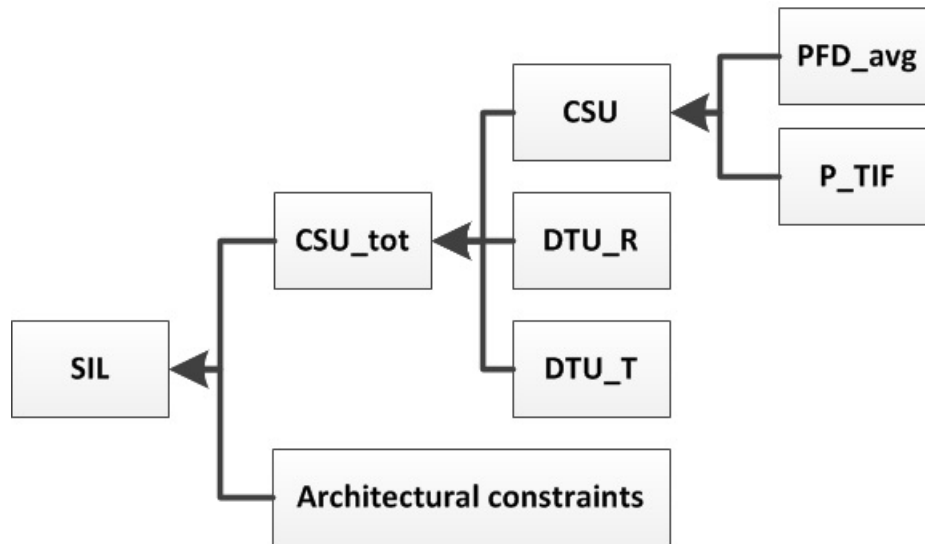
$$\gamma = \alpha \times \lambda_{DU}$$

To what extent we trust the original estimate of  $\lambda_{DU}$ , is defined by the conservative failure rate  $\lambda_{DU-CE}$ , and the parameter may be chosen according to logic:

$$\lambda_{DU-CE} = \max\{(\text{user specified value}), (2 \times \lambda_{DU}), (5 \times 10^{-7})\}$$

This rule implies that  $\lambda_{DU-CE}$  can either be specified according to user or take the value  $2 \times \lambda_{DU}$ . If either of the values are less than  $5 \times 10^{-7}$ , than  $5 \times 10^{-7}$  per hour is anyway taken in order to avoid that vary low estimates for  $\lambda_{DU-CE}$  totally outweighs the operational experience.

Figure 3.9: Overview of factors affecting the SIL performance of a SIF, according to PDS method



### 3.3 Factors influencing the SIL performance of a SIF

This section is based on (pds, 2010) if not else specified. The section presents factors important to consider when quantifying loss of safety.

Factors that affect what SIL a given component may claim, are illustrated in figure 3.9,. The factors are listed are relevant if the PDS method is applied. The different element in figure 3.9 are discussed hereunder.

#### 3.3.1 Quantify loss of safety

IEC 61508 apply  $PF_{D_{average}}$  in order to quantify loss of safety due to random hardware failure.  $PF_{D_{average}}$  is defined as the "average probability of failure on demand", that is the average probability that a SIF is unable to perform the required safety function on demand.

The PDS-method applies a different parameter in order to quantify loss of safety; total critical safety unavailability ( $CSU_{TOT}$ ) is defined as the "propability that the component/system will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event, (and it is not known that the safety system is available)". The  $CSU_{TOT}$  formula is given in

equation 3.4

$$CSU_{TOT} = PFD_{avg} + P_{TIF} + DTU \quad (3.4)$$

If DTU is excluded from equation 3.4, the term critical safety unavailability is then applied:

$$CSU = PFD_{avg} + P_{TIF} \quad (3.5)$$

In equation 3.4, the  $PFD_{avg}$  value reflects the average probability that a SIF is unable to perform the required safety function on demand due to a dangerous undetected failure (with rate  $\lambda_{DU}$ ), during the period when it is unknown that the function is available. Since the PFD value according to the PDS-method only considers time when it is unknown that the SIF is unavailable, the additional parameter downtime unavailability (DTU) is included (ref. equation 3.4) as a separate notation. DTU is the average time a given SIF is unavailable due to; ( $DTU_R$ ) SIF out for repair, and; ( $DTU_T$ ) SIF out for planned testing and maintenance (i.e.  $DTU = DTU_R + DTU_T$ ). The DTU value may be negligible if it has a relatively insignificant impact on  $CSU_{TOT}$ . A discussion on whether to include  $DTU$  in the assessment, and how this practically may be performed are not elaborated any further. However it may not be necessary to include  $DTU$  in the assessment, since risk related to "known" downtime unavailability, may be considered when "short perspective follow-up" is performed, refer to section 3.2.3.

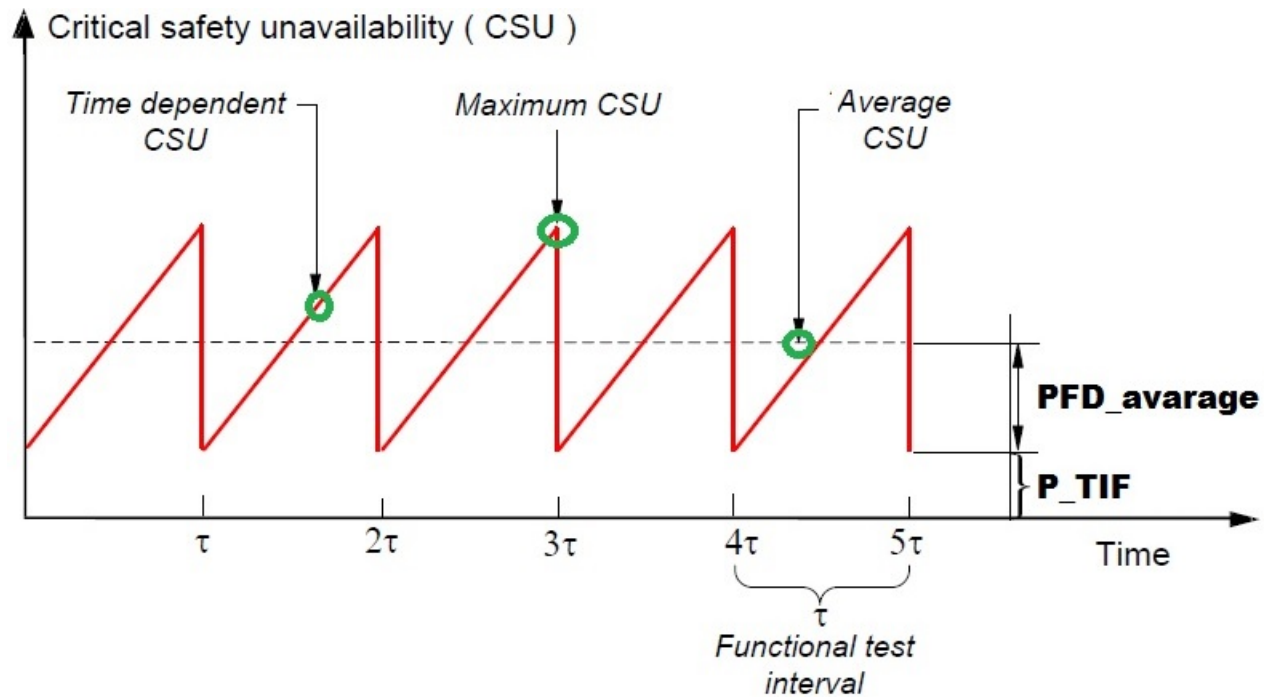
$P_{TIF}$  in equation 3.4 is defined as the probability of a test independent failure (TIF). Refer to section 2.6, for a discussion on TIF.

### 3.3.2 A general discussion on measuring loss of safety

In this section, the PFD is applied as the variable that reflects the probability that a SIF is unable to perform the required safety function on demand.

As illustrated in figure 3.10, the probability of failure on demand (PFD) varies between tests (the variation is illustrated by the red function). The PFD will increase until next scheduled maintenance and decrease if failures were identified and repaired during inspection/ maintenance. If all failures were identified and repaired during inspection and maintenance, the component may be considered "as good as new", a low PFD value will reflect such a condition.

Figure 3.10: How may CSU be calculated, ref. pds (2010).



$PFD_{avg}$  is the average PFD for a given interval. As illustrated in figure 3.10,  $PFD_{avg}$  is higher than time dependent PFD ( $PFD_t$ ) in the first half of a given interval, however in the second half of the interval, the  $PFD_t$  may be higher than  $PFD_{avg}$ . A consequence of such may be that the SIF in consideration does not conform with required PFD ( $PFD_{req}$ , that is given by allocated SIL) in half of the test interval, despite that the  $PFD_{avg}$  is below  $PFD_{req}$ .

### Test/diagnostic Coverage

This section follows the notation of IEC 61508, regarding TC and DC.

*Test Coverage* (TC) (as well as *Diagnostic Coverage* (DC)) is the fraction of *safety critical failures*<sup>8</sup> that are identified through testing. DC is applied when a component has built in automatic on-line diagnostic test, hence DC will reflect the fraction of safety critical failures that a "component" may reveal by self diagnostics. While TC reflect fraction of failures that are detected by

<sup>8</sup>A safety critical failure is a failure that if not detected will cause the safety function in consideration to not perform when a demand occur.

human during test or inspection. TC and DC reflect a property about the test-method in terms of "how capable is the test-method regarding identifying all possible dangerous failures." A TC value of 0.5 may be understood as the method/tools applied under testing is capable to reveal 50% of possible dangerous failure modes. Failures that are not identified during functional testing, may be named *test independent failures* (TIF), ref. section 2.6. TIF may always be counted for when quantifying loss of safety for a given inspection interval, since functional testing may never be considered to have a TC of equal 1, the same may be considered for DC.

### 3.4 Architectural constraints

This section is based on [pds \(2010\)](#), if not else specified.

IEC 61508 introduce the safe failure fraction in combination with hardware fault tolerance in order to allocate SIL. Further, type A and B components are introduced according to IEC 61508, 2nd edition 2010. In this section, safe failure fraction (SFF) is defined according to PDS method.

The highest SIL that can be claimed for a SIF is limited by architectural constraints. The constraints consider; hardware fault tolerance given to the SIF, safe failure fraction present at the SIF, and how much we know about and trust failure data given to the SIF.

**Safe Failure Fraction** (SFF) may be defined as the fraction of failures that are considered safe. Safe failures may be safe undetected failures ( $\lambda_{SU}$ ) (e.g. undetected spurious trip), dangerous detected failures ( $\lambda_{DD}$ ), or safe detected failures ( $\lambda_{SD}$ ), while dangerous undetected failure ( $\lambda_{DU}$ ) may be the failure type considered unsafe [pds \(2010\)](#). The SFF formula is given in equation 3.6.

$$SFF = 1 - \frac{\lambda_{DU}}{\lambda_{DU} + \lambda_{SU} + \lambda_{DD} + \lambda_{SD}} \quad (3.6)$$

A **hardware fault tolerance** (HFT) may imply how redundant the system is. A HFT of  $N = 1$ , suggest that one "redundant" component/block may be in a fault state, and functional safety may still be performed, while HFT of  $N = 0$ , suggest that if the component/block in consideration will be given a fault state, functional safety will not be performed [Pepperl+Fuchs](#).

How much we know about and trust failure data given to the SIF, is dependent on whether failure



modes for all components constituting the SIF are well known, whether we know how different SIF-subsystems may behave under fault conditions, and if there is sufficient dependable failure data from field experience regarding DU and DD failures [Pepperl+Fuchs](#). If we have sufficient data/knowledge, we may for a given SIF claim SIL according to "subsystem type A" (ref. fig 3.11), if not we may claim SIL according to "subsystems type B" (ref. fig 3.12). As illustrated in figure 3.11 and 3.12, the architectural constraints such as SFF and HFT may set a limit/cap on the SIL allocated to a SIF.

Figure 3.11: SIL limit for type A components, process ruled by architectural constraints (IEC 61508-2)

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % ... 90 %	SIL2	SIL3	SIL4
90 % ... 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Figure 3.12: SIL limit for type B components, process ruled by architectural constraints (IEC 61508-2)

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % ... 90 %	SIL1	SIL2	SIL3
90 % ... 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

# Chapter 4

## A review on SIS/SIL performance in the Norwegian continental shelf

This chapter consider monitoring SIS/SIL performance in the Norwegian continental shelf. The focus is set on the operational phase. The review is based on audits and accident investigations published by the Norwegian Petroleum Safety Authority (PSA).

### 4.0.1 Discussion and Goal for the study

The goal is to identify weakness according to factors discussed within this thesis. The research approach that is applied consider reviewing of different publications by petroleum safety authority Norway, in order to address weakness. An additional effort is made to connect any findings related to short term follow-up.

#### Factors to look for regarding short-term follow-up

Factors to look for are as follows:

1. Is acceptable risk / required safety within a given "EUC-area" met during maintenance?
2. Are maintenance activities that is performed at a given installation justified in documentation

Regarding [1 & 2]: Safety integrity requirements (for all SIFs subjected to maintenance) allocated to different safety-related systems within an "EUC-area" have to be fulfilled while maintenance

is performed in order to ensure acceptable risk. Following, the maintenance activities (regarding overrides, inhibits and bypasses of SIF components subjected to maintenance) may only be authorized if the responsible company are able to prove that safety requirements are met during maintenance. The authorization may have to be based on information given in the SRS, such information/data may be; (1) Safety integrity requirements that is allocated the different safety functions, that are subjected to maintenance, or included to mitigate the "risk picture"); (2) architectural constraints in terms of K-out-of-N-requirement, for when safety is expected for redundant components. If the company/organization is not able to proof that required (and documented) safety is maintained during maintenance, than short perspective follow-up may be considered.

### **General factors regarding SIS/SIL follow-up**

- Is SIL data presented in any spesification, such as SRS or maintenance management system?

### **Other factors of interest**

Hereunder are factors listed that did not get any additional effort.

- Are failures systematic or random?
- Regarding systematic failures: is the failure introduced during design or operation?
- Is the SRS updated, regarding the life-cycle of a SIS?

## **4.1 Findings**

References/activity number listed below refer to specific PSA publications that is applied. Different quotes are presented hereunder, the quotes are taken from the reference that is considered.

### **Audits by PSA**

**2014** Installation: Alvheim. Type: Audit. Reference: 015203027

SIL requirements are not referred to when allocating test intervals. **Quote:** "ikke samsvar mellom krav i SRS og testintervallet i vedlikeholdssystemet".

**2013** Installation: Stena Don. Type: Audit. Reference: 407003004

The company did not have sufficient knowledge about SIL requirement that was allocated to the control system of the blow out preventer.

**2012** Installation: Mærsk Inspirer. Type: Audit. Reference: 400006003

The test intervals presented in the maintenance management system are not justified according to SIL requirements. **Quote:** "Forutsetninger i SIL analyser om testintervaller er ikke implementert i vedlikeholdssystemet".

### **Investigations by PSA**

**2010** Installation: Island Gullfaks B. Type: Investigation. Reference: 001050014

**The case:** Hydrocarbons got released to the environment with a leak rate of 1.3 kg/s that occurred during one hour. The leak occurred over one hour due to the maintenance configuration that was applied excluded a "layer of protection" from the system. The removing of this "layer of protection" was not justified in any documentation. The maintenance configuration that was applied included bypassing a wing-valve (i.e. the layer of protection that was removed). Hence the maintenance configuration that was performed, utilized only the manual emergency shutdown valve as a "layer of protection", i.e: the manual emergency valve was closed manually, and this valve did not perform on demand, hence it leaked hydrocarbons into the environment. The operator "had" to bypass the wing-valve due to the tools that was intended to be applied was not available for the moment. Through interviews performed by Petroleum Safety Authority, it appears that the operators at the platform have "the freedom" to open "existing barriers", if new barriers are implemented. Further, the operators claimed that they did not need to perform functional testing on the newly added barrier (i.e. manual emergency valve in this context).

Additional deviations identified by PSA: (1) It is not established a clear and unambiguous acceptance criteria regarding when it is allowed to exclude main safety functions from operation. (2) The company did not have updated risk analysis that provides a complete and comprehensive picture of explosion-risk that was present at the area in consideration.

# Chapter 5

## Conclusions and further work

The chapter is divided into consider short perspective follow-up, and long perspective follow-up of SIS during the operational life time of a SIS/SIF.

### 5.1 Summary and conclusion

#### 5.1.1 Short perspective follow-up

The review on the Norwegian continental shelf, revealed that the operator(s) (i.e. maintenance personnel) had the "freedom" to open "existing barriers". They thought they were allowed to act according to their own judgment/knowledge, this may have occurred as a consequence of unacceptable safety management. They did not have sufficient knowledge about the importance to conform with SIL requirements, this resulted in a risk picture that was unacceptable. The hydrocarbon leakage may not have occurred if the management had implemented the PRA approach. The PRA approach consider deciding which component/function (i.e. manual emergency shut down valve (ESV), or wing-valve), is allowed to be subjected to maintenance (i.e. bypassed). The different events in the fault tree model (regarding SIF perform or fail to perform on demand) may in this context only be wing-valve, and ESV, though the ESV would be considered in the same way as the "manual call-point", as presented in chapter [3.2.3](#). Such an PRA approach would identify, that the risk of bypassing the ESV would not be acceptable (this may be illustrated in the model by having one "layer of protection" against release of hydrocarbons,

and the only "layer" /ESV may have a high PFD if the time since last maintenance is large. However performing the PRA assessment, may conclude that maintenance configuration "X", that include the following precaution; *inspect and test manual emergency valve before deactivation of wing-valve*, may be an acceptable maintenance configuration.

### **5.1.2 Conclusion: Short perspective follow-up**

The objective (ref. section 1.1) was to perform a literature study in order to give basis for evaluating safety performance of safety instrumented functions (SIF) on the Norwegian continental shelf. The aim was to suggest any means that may contribute to increased safety integrity of the SIFs through the operational lifetime of a SIF.

The thesis suggest a framework for monitoring the variability of safety performance when maintenance is performed. The thesis identified the need to monitor this variability by performing a review on investigations performed by Petroleum Safety Authority Norway. The framework that was presented, if applied correctly would suggest not to performing the specific maintenance activities, that resulted in lack of redundancy within the system, hence a gas leak may have been avoided.

### **5.1.3 Long perspective follow-up**

The review identified deviations in; documenting SIL requirements, and; test intervals was not justified by SIL requirements. In the absence of referring to SIL requirements (that was developed during design), the functional test interval that is applied, may not conform with the risk picture that SIL allocation was based on. Hence safety may no longer be justified.

## **5.2 Discussion**

### **Limitations**

I do not have sufficient knowledge about how SIL is allocated to a "complex" SIS. With this knowledge, I might be able to give an example of how different SILs may be distributed among

the "components/blocks" within the functional reliability block diagram.

The focus was set more towards short perspective follow-up, hence this thesis did not present any new approach regarding long perspective follow-up.

For other limitations, refer to section "future work"

### **Strengths**

This thesis pointed out the need to address short perspective follow-up of SIS, by performing a review of safety performance on the Norwegian continental shelf. An approach was presented, that if applied would give clear decisions to not "exclude" the SIF (i.e. wing-valve) from the system.

A benefit with performing the suggested PRA approach, may be to apply PFD time dependent in stead of PFD average when assessing the risk picture, since the time interval for the maintenance activity is relatively small, and the PFD time dependent parameter ( $PFD_t$ ) would reflect the time since last inspection/maintenance is performed (i.e. do not count for the total inspection interval). Applying  $PFD_t$  may result in "giving more credit" to components/functions that was maintained in the "nearest past", hence a maintenance activity performed on the redundant components may be allowed. Further, if a component/function is soon to be tested, applying  $PFD_t$  may result in concluding that this component/function have to be functional tested in order to perform the given maintenance configuration, since the  $PFD_t$  given to the function/component probably do not conform with SIL requirement (ref. figure 3.10).

## **5.3 Further work**

### **Short term**

- How may the blocks (i.e. SIF-components) within the reliability block diagram (RBD) reflect safety integrity; (1) in terms of SIL allocated to functional safety (i.e. functional

blocks), or; (2) should the individual components be given PFD values.

- Investigate further on accidents that have occurred during maintenance, in order to address the benefit of applying the suggested PRA approach.
- Should the different SIF-components/functions in the "functional reliability block diagram", (that is not subjected to maintenance i.e. operating), represent; average PFD ( $PFD_{avg}$ ), that is related to test-interval applied, or; PFD time dependent ( $PFD_t$ ), that is related to time since last performed inspection/maintenance. This question may be relevant, since the time interval of performing maintenance is relatively short, and  $PFD_t$  may on the later side of the inspection interval not conform with allocated SIL.



# Appendix A

## Acronyms

**BOP** Blowout Preventer

**CCF** Common Cause Failure

**CM** Corrective Maintenance

**DC** Diagnostic coverage

**DTU** Down time unavailability

**IM** Individual Risk

**Moc** Management of Change

**PM** Preventative Maintenance

**PRA** Probabilistic Risk Assessment

**PSA** Petroleum Safety Authority (PSA)

**PSD** Process Shut Down

**PSV** Pressure Safety Valve

**RBD** Reliability Block Diagram

**SFT** Scheduled Functional Test

**SLC** Safety Life Cycle

**SRS** Safety Requirement Specification

**TC** Test Coverage

**QRA** Quantitative Risk Analysis

# Appendix B

## Naming parameters applied in the thesis

### B.1 Parameters affecting PFD

$\tau$  = Test interval

$\beta$  = Beta factor (modeling common cause failure)

$\lambda$  = Failure rate

---

The parameters on failure rate as presented under, are defined beyond their definitions in the source, in order to explicitly refer to whether the parameters were applied in design or operation.

---

$\lambda_{DU}$  = Original DU failure rate, from design data

$\hat{\lambda}_{DU}$  = New DU failure rate from operational data

$\lambda_{DU-CE}$  = Conservative original DU failure rate. The parameter is correlating with our confidence in the original DU failure rate, when operational data is available.

$\ddot{\lambda}_{DU}$  = Updated failure rate based on design data and operational data

---

Other parameters of relevance

---

$n$  = number of components in the population of comparable components

$x$  = number of observed DU failures during observation period

$t$  = observation period

$t_n$  = total aggregated time for  $n$  components in operation (=  $t \times n$  if all components have been in operation)

# Bibliography

(2004). 070 - norwegian oil and gas application of iec 61508 and iec 61511 in the norwegian petroleum industry.

(2010). Pds data handbook.

(2010). Pds method handbook.

Erin. United states nuclear industry experience in dynamic risk assessment.

Honeywell (2009). Integrated fire and gas solution - improves plant safety and business performance.

Johansen, I. L. (2010). Foundations of risk assessment.

Lundteigen, M. A. (2009). *Safety instrumented systems in the oil and gas industry*. PhD thesis, NTNU.

Mary Ann Lundteigen, M. R. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing.

Maryam Rahimi, Marvin Rausand, M. A. L. (2012). Management of factors that influence common cause failures of safety instrumented system in the operational phase.

Pepperl+Fuchs. Manual, safety integrity level.

Per Hokstad, Solfrid Hobrekke, M. A. L. T. O. (2009). Use of pds method for railway applications.

Rausand, M. (2011). *Risk Assessment: Theory, MMethod, and Applications*. Wiley.

Stein Hauge, M. A. L. (2008). Guidelines for follow-up of sis in the operational phase.

Z-008 (2011). Risk based maintenance and consequence classification, edition 3.