Universitetet
i Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme/specialisation: MSc Risk Management / Risk Assessment and Management	Spring /~~Autumn~~ semester, 2019 Open/~~Confidential~~
Author: Anna Kvæven	anna Kvæven (signature of author)
Faculty supervisor: Eirik B. Abrahamsen (UiS) External Supervisor: Kjell Sandve (ConocoPhillips Norway)	
Title of master's thesis: Optimisation of Test Intervals for Well Barriers	
Credits: 30	
Keywords: Well Barriers, Safety Instrumented Systems, Risk Management, Barrier Management, Functional Safety, Reliability, SIL, Uncertainty, Strength of Knowledge, NORSOK D-010, NOG 070, Decision making under uncertainty	Number of pages: 130 + supplemental material/other: 2 Stavanger, June 13th 2019 date/year

Title page for Master's Thesis
Faculty of Science and Technology

ACKNOWLEDGEMENTS

This thesis is submitted as the conclusive work of my master's degree in Risk Management at the University of Stavanger during the spring semester 2019. It was written in the offices of ConocoPhillips Norway in Tananger.

Writing this thesis has been an interesting, but highly demanding project. There are a few persons whose support I could not have completed this project without.

First of all, I would like to thank my supervisors Eirik B. Abrahamsen (UiS) and Kjell Sandve (ConocoPhillips Norway) for believing in me and agreeing to take on this project on such short notice. A special thank you to Jahon Khorsandi at ConocoPhillips Norway, for interesting discussions and always being available to answer my questions along the way. Last but not least, thank you Øystein for always having my back and cheering me on.

ABSTRACT

The common approach among operators on the Norwegian Continental Shelf to verify the functional integrity of well barriers, including the safety instrumented systems in wells, is to schedule proof tests according to the time – based requirements for well barrier components in the NORSOK D – 010 standard for well integrity. Due to observed indications of high component reliabilities by operators, it is believed that changing the maintenance strategy for well barrier components to a reliability performance – based approach where proof tests are scheduled according to demonstrated safety integrity level (SIL) in operation can yield substantial annual cost savings. However, todays recommended procedures for SIL verification and associated updating of component test intervals for well barrier components are associated with uncertainty.

In this thesis, a new and integrated approach for SIL verification and optimisation of component test intervals with added weight to uncertainties is suggested to identify optimum test intervals for well barrier components. To demonstrate the use of the suggested approach, a reliability/availability case analysis of the safety instrumented function "Isolation of production bore in one topside well from the production manifold/flowline (ESD)" in offshore production wells is performed based on historical component data provided by ConocoPhillips Norway. A checklist and decision framework to identify and communicate the uncertainties of the reliability analysis is developed to provide broad decision support in optimisation of test intervals.

The case analysis identified that the reliability of the PMV and PWV is significantly better than the DHSV. The uncertainty in the analysis results is identified as medium. The main sources of uncertainty are identified as differing operating environments between wells, and the applicability of the exponential lifetime distribution to model component lifetimes. Taking the uncertainties of the analysis into account, optimum component test intervals were identified as 6 months for the PMV/PWV, and 3 months for the DHSV, with a possibility for further extension if wells included in the data are filtered on operating environment. The documented historical reliability performance of well barrier components in this thesis shows that it can be justified to extend component test intervals beyond the requirements in NORSOK D-010, in order to keep the risk of the activities as low as reasonably practicable.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ALARP – As low as reasonably practicable

CCF – Common cause failure

CDF – Cumulative density function

COPNO – ConocoPhillips Norway

DD – Dangerous detected

DHSV – Downhole safety valve

DU – Dangerous undetected

E/E/PE - Electrical, electronic and/or programmable electronic components

ESD – Emergency shut down

EUC – Equipment under control

FF – Failure fraction

GEA – Greater Ekofisk Area

NCS – Norwegian Continental Shelf

NOG 070 – Norwegian Oil and Gas Guideline 070

P&T – Pressure and temperature

PDF – Probability density function

PFDavg – Average probability of failure on demand

PM programme – Preventive maintenance programme

PMV – Production master valve

PSA – The Petroleum Safety Authorities Norway

PWV – Production wing valve

RBD – Reliability block diagram

SD – Safe detected

SIF(s) – Safety instrumented function(s)

SIL – Safety integrity level

SIS(s) – Safety instrumented system(s)

SoK – Strength of knowledge

SU – Safe undetected

1 INTRODUCTION

1.1 Background

Barriers are all technical, operational and organizational measures implemented to reduce the risk of failure and accident situations. According to the Petroleum Safety Authority Norway (PSAN) [1] it is the responsibility of the operator of an offshore facility to stipulate maintenance strategies and principles so that the barrier functions are safeguarded throughout the facility's lifetime. For technical well barrier elements such as the safety instrumented systems, this includes regular proof testing and condition monitoring to verify that the functional integrity of the well barrier is maintained. [2]

For safety instrumented systems, the PSAN specifically recommend the standards IEC 61508 [3] and IEC 61511 [4], as well as the Norwegian Oil and Gas Guideline 070 (NOG 070) [5], to be used as a basis to achieve this requirement. [1] The NOG 070 guideline specifies minimum performance requirements (minimum SIL requirements) to the reliability of selected safety instrumented functions in wells that are required by national and international standards adopted in the Norwegian Petroleum sector. In the operational phase of the facility, it must be verified through maintenance and condition monitoring that the observed SIL of the safety instrumented functions meets the SIL requirement. The demonstrated reliability in operation relative to the SIL requirement shall form the basis for how frequently proof tests are scheduled in the maintenance programme.

However, the common approach among operators on the Norwegian Continental Shelf (NCS) to verify the functional integrity of well barriers, including safety instrumented functions in wells, is to schedule proof tests according to the time – based requirements for well barrier components prescribed in the NORSOK D – 010 standard for well integrity. [6] For example, following the NORSOK D-010 standard, the downhole safety valve (DHSV) should be tested every month until three consecutive tests have been successfully run, thereafter every third month until three successful tests have been run, and thereafter every six months.

For operators, the prescriptive approach to well barrier proof testing presented in NORSOK D-010 can result in as much as three days lost production per test, corresponding to an annual cost of 10M USD per asset. Due to observed indications of high component reliabilities by operators, it is believed that changing the maintenance strategy for well barrier components belonging to the safety instrumented systems from following the prescriptive approach in NORSOK D-010 to a reliability performance – based approach can yield substantial annual cost savings. [7]

This hypothesis formed the motivation of this thesis, which aims to identify optimum test intervals for well barrier components belonging to the ESD safety instrumented system in offshore production wells based on their demonstrated reliability in operation. The starting point of the study is the NOG 070 guideline. For a procedure on how to update component test intervals, NOG 070 refers to the work by Lundteigen and Hauge (SINTEF). [8]

Although the requirements and methods to adopt the reliability performance – based maintenance strategy for safety instrumented functions in wells are readily available in NOG 070, it has yet to be applied in practice by ConocoPhillips Norway (COPNO) and presumably other operators on the NCS. Changing the maintenance strategy and proof test intervals for well barrier components is a major decision that should not be made without due consideration, and the recommended procedures for SIL verification and updating component test intervals has been accused for not giving sufficient weight to uncertainties in the reliability analysis. [9-11] Some contributions have been made within academia on this matter, see for example [10-12]. However, transferring theoretical contributions into practical applications using real operational data can sometimes be a challenge.

In this thesis, a modified approach of the recommended methods in NOG 070 and Lundteigen and Hauge (SINTEF) [8] is developed for integrated SIL verification and optimisation of component test intervals for safety instrumented functions in wells, with added weight to uncertainties in the reliability analysis. In reliability analyses, uncertainty expresses our degree of knowledge about the system. A novel checklist is developed to evaluate the strength of knowledge underbuilding the reliability analysis. A semi – quantitative framework for assessment of uncertainties in the identified component test intervals is developed to provide broad decision support in determining optimum test intervals for well barrier components.

A case analysis using the suggested approach was performed based on operational data provided by COPNO. By the experience gained from performing the analysis, it is believed that the method presented in this thesis is a more practical approach to determine optimal test intervals for well barrier components while also giving added weight to the analysis uncertainties and communicating them to the decision maker in a meaningful way.

1.2 Objective and Limitations

OBJECTIVE

The objective of this thesis is to optimize the maintenance strategy for well barriers, by determining optimum test intervals for well barrier components with added weight to uncertainties. To achieve this objective, a reliability/availability case analysis of a safety instrumented function in offshore production wells will be performed using historical data from the Greater Ekofisk Area provided by ConocoPhillips Norway. Key research challenges and outputs include:

- Estimate updated component failure rates based on operational experience
- Can any performance influencing factors be identified that will affect the failure rates and hence the required test intervals between wells?
- Identify optimum component test intervals based on historical reliability performance
- Assess the validity of the recommended reliability model by identifying the lifetime distribution model that best fits historical component lifetime data
- Identify and assess sources of uncertainty in reliability analyses of safety instrumented functions in wells
- Can it be justified to extend component test intervals beyond the requirements in NORSOK D-010?
- Can it be recommended to change to a performance – based rather than prescribed test frequency for safety instrumented functions in wells?

LIMITATIONS

The identified failure rates, performance influencing factors, component reliabilities, uncertainties and optimum component test intervals in this study are limited to the component types included in the case analysis, based on currently available operational data. However, the developed analysis methods, discussions and recommendations are general.

There are several methods and tools that can be applied to increase the sophistication of reliability analyses and assessments of uncertainty. The choice of methods used in the current study is influenced by the available time and competence resources of the analyst (author).

1.3 Structure of the Report

The thesis report is structured as follows;

- ***Chapter 2*** introduces general theory and regulations to operators on the Norwegian Continental Shelf for risk management, well barriers and safety instrumented systems. The role of safety instrumented systems as a well barrier element is clarified, and basic concepts of system reliability is presented.
- ***Chapter 3*** presents sources of uncertainty and methods to assess uncertainty in reliability analyses.
- ***Chapter 4*** presents the safety instrumented function to be analysed in the case analysis, and its operating environment
- ***Chapter 5*** presents the relevant integrity performance requirements and verification methods for the safety instrumented functions' components according to NORSOK D-010 and NOG 070. The two approaches are compared and discussed.
- ***Chapter 6*** presents a new approach developed in this thesis study for an integrated and dynamic process of SIL verification and optimisation of component test intervals, with added weight to uncertainty
- ***Chapter 7*** demonstrates the use of the suggested approach by applying it to a case analysis of the safety instrumented function "Isolation of production bore in one topside well from the production manifold/flowline (ESD)" using historical component data from the Greater Ekofisk Area. A new checklist and decision framework for assessment of uncertainties in reliability analyses of safety instrumented functions in wells is presented and used to identify optimum component test intervals. The case analysis results are presented and discussed.
- ***Chapter 8*** discusses the practical applicability of the suggested approach for optimisation of component test intervals, and some implications of the results of the case analysis
- ***Chapter 9*** presents the conclusion of the study performed in this thesis, and answers to research challenges identified in the objective.
- ***Chapter 10*** makes recommendations for future research based on identified challenges and sources of uncertainty in the current study

2 THEORETICAL BACKGROUND

2.1 Regulations to the Petroleum Activities on the Norwegian Continental Shelf

For the design and operation of oil and gas facilities, there are typically several hierarchical layers of documentation that should be used in order to comply with local acts and regulations *(Figure 2.1)*, as will become apparent in the following sections of this thesis. [8] This chapter will therefore begin with a brief presentation of the regulatory hierarchy to be followed by operators on the Norwegian Continental Shelf (NCS).

For installations on the NCS, the acts and regulations provided by the Petroleum Safety Authority Norway (PSAN) are governing at the highest level. The regulations are *functional* and provides general guidance rather than strict criteria. To help operators and responsible parties of oil and gas facilities on the NCS to comply with the functional acts and regulations, the guidelines following the regulations often refer to recognized industry standards; such as the NORSOK and ISO standards.

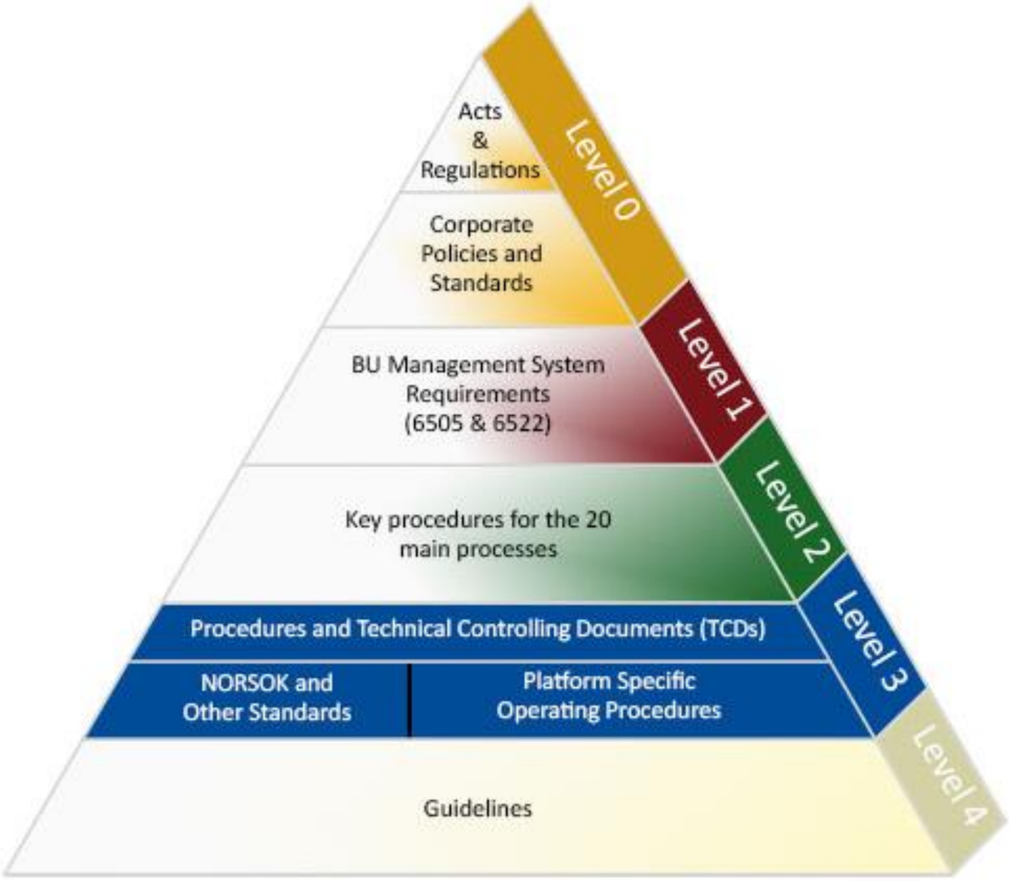


Figure 2.1: Documentation hierarchy for operators on the NCS. Courtesy of COPNO

Based on these regulations and standards, guidelines and company specific procedures have been developed as a more user – friendly method to comply with the regulations at the highest level. It can be understood that If such recognized standards, and thus the guidelines and procedures that are based on these standards, are followed, the requirements provided in the regulations are fulfilled. However, it is possible for operators and responsible parties to choose other solutions provided they are based on *sufficient documentation*. [13]

2.2 Risk Management

There is no doubt that the petroleum activities on the Norwegian Continental Shelf (NCS) has offered tremendous value creation and opportunities for the Norwegian society. However, historical events like the Piper Alpha and Macondo major accidents serve as strong reminders of how severe the consequences can be following a loss of control of the great amounts of energy that are handled at offshore oil and gas facilities.

The Petroleum Safety Authority Norway defines risk[1] as [15]:

> *"The consequences of the activity, with associated uncertainty"*

Where the term *consequences* is used collectively to cover both the final consequences of the activity; e.g. harm to, or loss of, human lives, health, financial assets and the environment, as well as the conditions and incidents that may lead to or result in these consequences. The term *associated uncertainty* refers to the uncertainty about what the consequences of the activities will be in terms of which incidents can occur, their frequency and which detriment or loss of values they can lead to. [15]

The objective of risk management is to strike the right balance between avoiding failure, hazard and accident situations on the one hand, while exploring opportunities on the other. [16] Through a sound risk management practice, the responsible party of petroleum activities on the NCS shall keep the risk of the activities as low as reasonably practicable (ALARP), as required by the PSAN Framework Regulations §11 [15].

[1] Several definitions and interpretations of *risk* are commonly used, the reader is referred to [14]

In general, risk management can be divided into two central activities; risk assessment and risk treatment [16]. To be able to manage risk, we need metrics and descriptions of risk. The objective of risk assessments is to provide an informative risk description of failure, hazard and accident situations to the decision makers. The key components of risk are the consequences of the activity, and the uncertainty about what these will be. Uncertainty can be categorized as being either [14, 17]:

- **Aleatory (Stochastic):** Variation of quantities within a population of units
- **Epistemic:** A general lack of knowledge about the *true value* of a quantity, phenomenon or consequence

Probabilities are a good tool to model aleatory uncertainty, and the most common method used to describe risk in risk assessments is the combination of the selected set of consequences, and its associated probability of occurrence. [18]

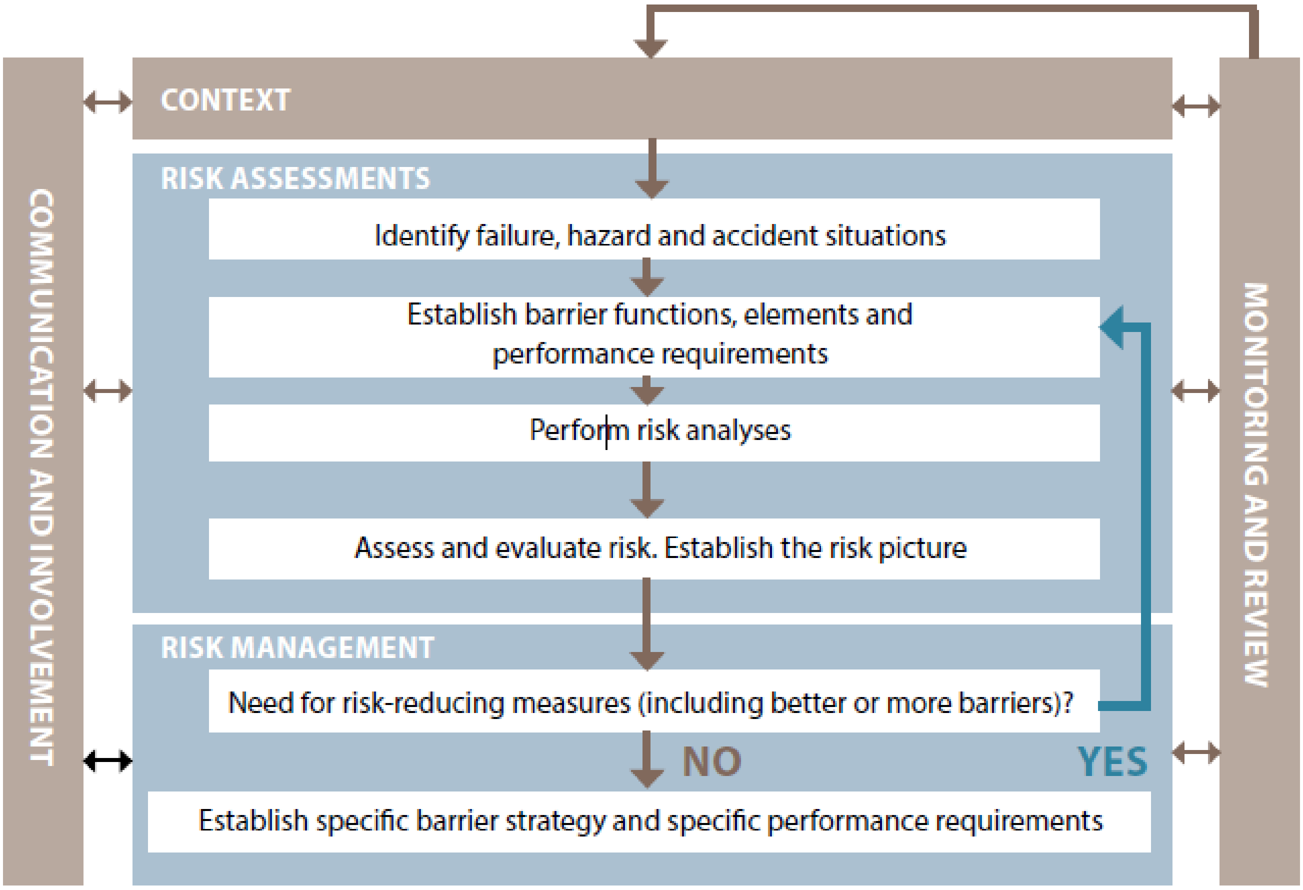

CONTEXT
RISK ASSESSMENTS
Identify failure, hazard and accident situations
Establish barrier functions, elements and performance requirements
Perform risk analyses
Assess and evaluate risk. Establish the risk picture
RISK MANAGEMENT
Need for risk-reducing measures (including better or more barriers)?
NO
YES
Establish specific barrier strategy and specific performance requirements
COMMUNICATION AND INVOLVEMENT
MONITORING AND REVIEW

Figure 2.2: The risk management processincluding the establishment of risk reducing measures (barriers) [2]

The results of the risk assessment are evaluated to assess whether the risk is acceptable or not, and whether there is a need to implement risk reducing measures. The evaluation is followed up by risk treatment, which represents the process of implementing risk reducing measures *(Figure 2.2)*. [16] This includes the establishment and follow – up of barriers, as of the PSAN Management regulations §4 [19]:

> *"In reducing risk as mentioned in §11 of the Framework* Regulations*, the responsible party shall select the technical, operational and organisational solutions that reduce the likelihood that harm, errors and hazard and accident situations occur… Furthermore, barriers as mentioned in §5 shall be established"*

2.3 Well Barriers

Barriers are measures whose function is to identify conditions that may lead to failure, hazard and accident situations, prevent an actual sequence of events from occurring and developing, and limit the harm and inconveniences should an accidental event occur *(Figure 2.3)*. [2]

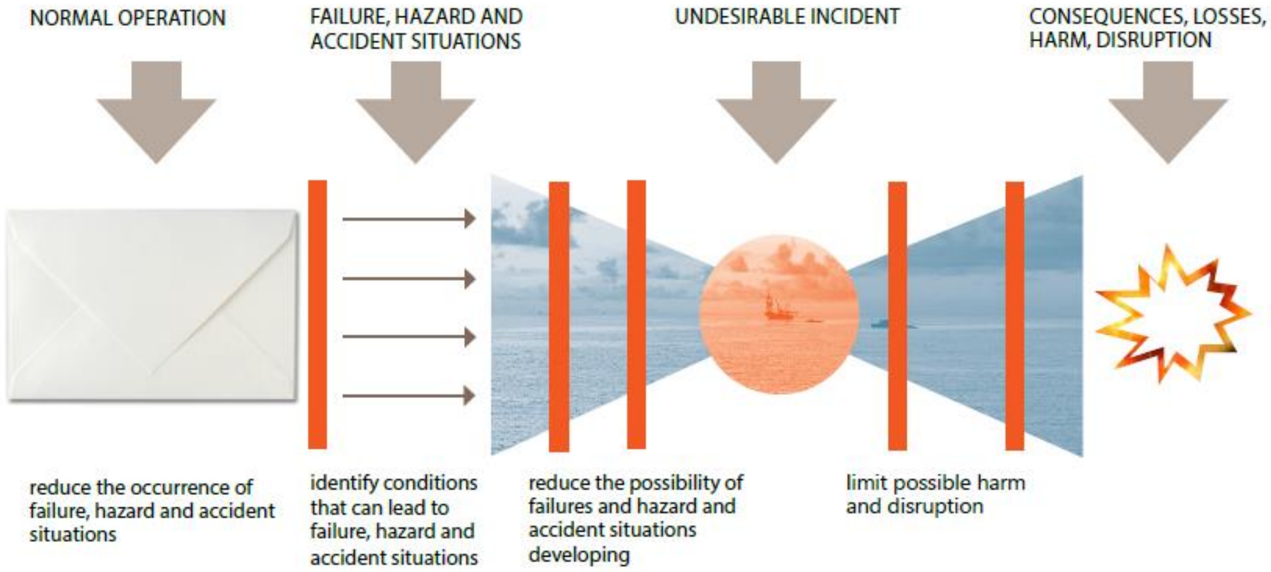

NORMAL OPERATION
FAILURE, HAZARD AND ACCIDENT SITUATIONS
UNDESIRABLE INCIDENT
CONSEQUENCES, LOSSES, HARM, DISRUPTION
reduce the occurrence of failure, hazard and accident situations
identify conditions that can lead to failure, hazard and accident situations
reduce the possibility of failures and hazard and accident situations developing
limit possible harm and disruption

Figure 2.3: The role of barriers in a risk management context. Normal operation: Risk reduction, safe and robust solutions. Failure, hazard and accident situations: Barriers. [2]

2.3.1 Key Concepts and Definitions

It is separated between the barrier function, its system and elements. Further, it is also important to be aware of its performance requirements, and performance influencing factors that may affect them.

- **Barrier function:** The role or task of a barrier. The barrier function may be realised through several barrier sub – functions. [2]
- **Barrier system:** System designed and implemented to perform one or more barrier functions [20]
- **Barrier element:** Technical, operational and organizational measures or solutions involved in the realization of a barrier function. [2]

- **Barrier performance:** The properties of the barrier with respect to its capacity, efficiency, reliability, accessibility, integrity, robustness and ability to withstand loads. [1]
- **Performance requirements:** Verifiable requirements for the properties of the barrier (elements) in order to ensure that the barrier is effective. [2]
- **Performance influencing factors:** Factors identified as having significance for barrier functions and the ability of barrier elements to function as intended [2]

At oil and gas facilities, a critical hazard that shall always be evaluated is the event of blowout and well releases [20] To prevent, control and mitigate these events, well barriers play a critical role. Well barriers are defined according to NORSOK D – 010 [6]:

- **Well barrier:** An envelope of one or several well barrier elements preventing fluids from flowing unintentionally from the formation into the wellbore, into another formation or to the external environment.

In the context of drilling and wells, the terms *barrier* and *well barrier* are both used somewhat interchangeably with reference to the technical barriers or technical barrier elements in the well. [2] Consequently, in this work, both terms can be understood in a similar manner, with reference to the above definitions.

2.3.2 Governing Regulations and Documents

Well barriers are regulated according to the following regulations and associated guidelines:

- **The framework regulations §11 (Risk reduction principles)** [15]
- **The management regulations §4 (Risk reduction)** [19]
- **The management regulations §5 (Barriers)** [1]
- **The facilities regulation §48 (Well Barriers)** [21]
- **The facilities regulations §8 (Safety functions)** [22]
- **The activities regulations §47 (Maintenance programme)** [23]

According to The management regulations §5;

> *“The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers’ function is safeguarded throughout the offshore or onshore facility’s life”*

In particular regarding well barriers; The facilities regulations §48 state that:

> *“Well barriers shall be designed such that well integrity is ensured, and the barrier functions are safeguarded during the well’s lifetime”*

To achieve the requirements to well barriers, the regulation guidelines recommend the standard NORSOK D-010 Chapters 4, 5, 6 and 15 to be used in the matters of HSE. Maintenance includes activities such as inspection, trial, testing, repair and monitoring. [24] After The activities regulations §47;

> *“Failure modes that may constitute a health, safety or environment risk shall be systematically prevented through a maintenance programme… The programme shall include activities for monitoring performance and technical conditions… “*

According to The activities regulations §47 regulation guidelines, the maintenance programme can include sub-programs for testing and preventive maintenance. For well control, well intervention equipment, subsurface safety valves and Christmas trees, the NORSOK D-010 standard should be used as a basis for maintenance activities.

2.3.3 Barrier Management

Barrier management comprise the coordinated activities for establishing and maintaining barriers so that they are available to fulfil their functions at all times. An overview of the barrier management process is illustrated below in *Figure 2.4*. [2]

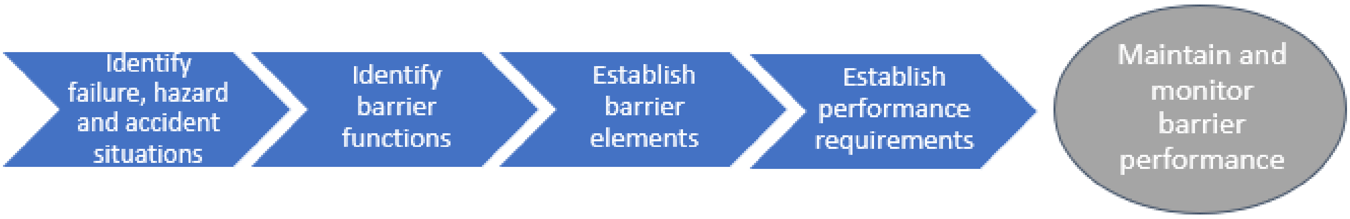

Identify failure, hazard and accident situations
Identify barrier functions
Establish barrier elements
Establish performance requirements
Maintain and monitor barrier performance

Figure 2.4: The barrier management process. Adapted from [2]

Through these activities, barrier management shall ensure that the necessary risk reduction is achieved to maintain safe operations. Barrier management is therefore an integrated part of risk management. [5]

2.3.4 Performance Requirements and Verification

An important aspect of barrier management is to establish performance requirements and maintain barrier performance throughout the facility's lifetime, as can be seen from *Figure 2.4* above. In accordance with the definitions in *Chapter 2.3.1* and the PSA Management Regulations §5 [1], verifiable performance requirements shall be identified and maintained by the operator or the party responsible for the oil and gas facility with respect to the functionality, integrity and survivability of barriers, as illustrated in *Figure 2.5* below; see also [25].

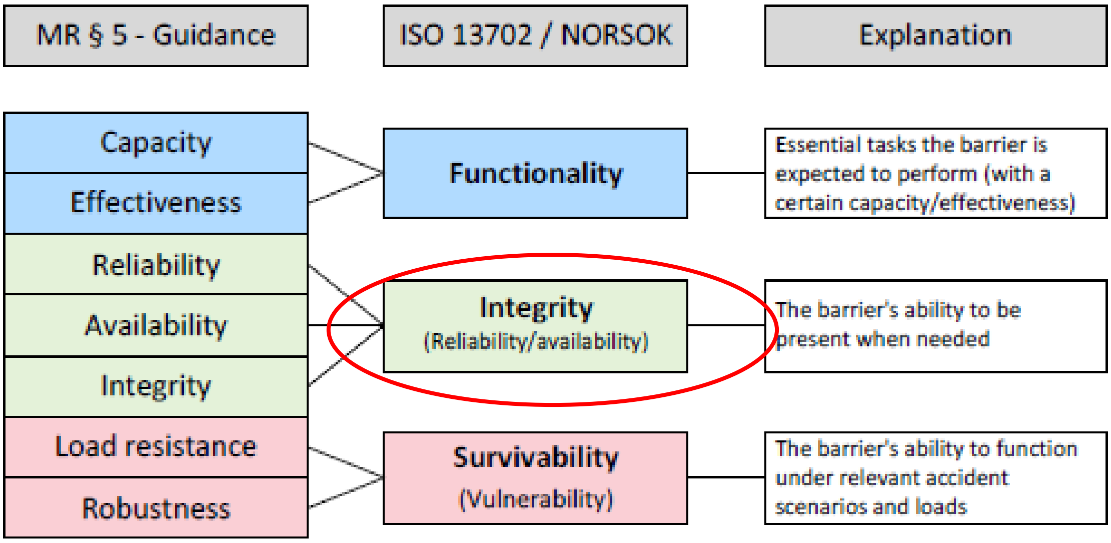

MR § 5 - Guidance
ISO 13702 / NORSOK
Explanation
Capacity
Effectiveness
Reliability
Availability
Integrity
Load resistance
Robustness
Functionality
Integrity
(Reliability/availability)
Survivability
(Vulnerability)
Essential tasks the barrier is expected to perform (with a certain capacity/effectiveness)
The barrier's ability to be present when needed
The barrier's ability to function under relevant accident scenarios and loads

Figure 2.5: The properties of barriers subject to performance requirements and verification [25]

Of special interest to the objective of this thesis, is the establishment and verification of performance requirements with respect to the *integrity* (reliability/availability) of well barriers. In this context, it is distinguished between *well integrity* and *well barrier integrity*:

- **Well integrity:** The application of technical, operational and organizational solutions to reduce the risk of uncontrolled release of formation fluids and well fluids throughout the life cycle of a well [6]

- **Well barrier integrity:** The availability, reliability and integrity of the well barrier, where *integrity* is understood as the ability and potential of the well barrier to be in place and intact at all times [2]

Hence, the integrity of the well barrier must be maintained, so that no uncontrolled release of fluids from the well to the surface occurs throughout the lifetime of the well. To achieve this, performance requirements are set to the well barrier integrity in terms of its reliability/availability, which must be verified through regular testing and inspections in line with the operators' maintenance strategy.

2.4 Safety Instrumented Systems

Safety instrumented systems (SISs) constitute a group of safety systems that utilize electrical, electronic and/or programmable electronic components (E/E/PE) interacting with mechanical, pneumatic and hydraulic systems to detect, react and avert a hazardous situation so that the equipment it is protecting (equipment under control; EUC) is returned to a safe state.

SISs are frequently used in the process, automobile, nuclear and aviation industries to detect hazardous events and avoid harm to humans and the environment. [9, 26] At oil and gas installations, SISs are among others implemented in wells, where they play an important role in upholding well integrity.

Note that by being a technical system in the well whose role is to mitigate hazardous events and return the EUC (the well) to a safe state, the SIS is according to the definitions in *Chapter 2.2.1* also a technical well barrier system/element.

2.4.1 Key Concepts and Definitions

Safety instrumented systems are commonly subdivided into three main subsystems that must act together for the system to be able to perform its intended function; to *detect*, *react* and *avert* a hazardous situation [9, 26]:

- **Input element (sensor) - *detect*:** The Input element detects a deviation (potential hazard) and in response produces an appropriate electrical signal that is sent to the logic solver.

- **Logic solver – *react*:** The logic solver reacts to an electrical input signal from the sensor that exceeds a given threshold and sends an output signal to the final elements.

- **Final element – *avert:*** The final element performs the safety function and averts the hazard on signal from the logic solver.

A simple example of a typical SIS configuration can be seen in *Figure 2.6* below.

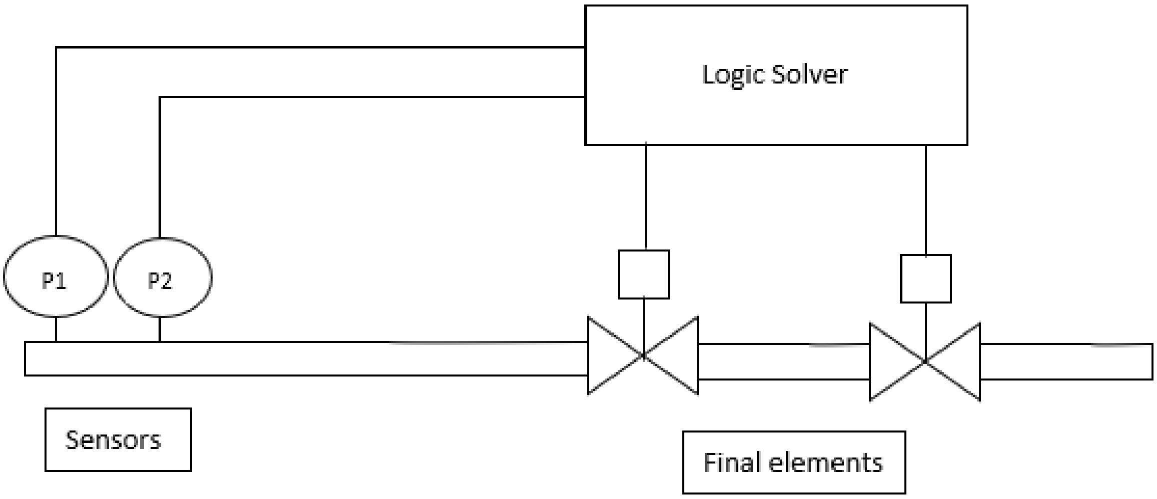


Figure 2.6: Example of a typical SIS: pressure protection system in pipeline comprised of sensors (pressure transmitters), logic solver and final elements (valves). Adapted from [26]

In this example, the EUC is a pipeline. A hazardous event that is detected and averted by the SIS may be that the pressure in the pipeline is too high. The pressure is registered by the sensors P1 and P2, which sends a signal to the logic solver. The CPU in the logic solver reacts to the pressure being too high and sends a signal to the final element valves to close.

VOTING

Whether the logic solver decides to react on the input signals from the pressure transmitters P1 and P2 depends on how the input signals are *voted*. If the input signals are voted *k*-out-of-*n (koon)*, the logic solver will react and signal the valves to close if *k*-out-of-*n* sensors raise an alarm. For example, for a 1oo2 voting in *Figure 2.6* above, the logic solver will signal the valves to close if one-out-of-two (1oo2) of the pressure transmitters detects a pressure deviation.

The voting of the final elements will generally depend on the physical installation. For the SIS in *Figure 2.6*, where two final elements (valves) are installed, only one of the two valves need to function for the pipeline to be shut in. Hence, the valves are voted 1oo2. Similar configurations including more than one final element is commonly used for *redundancy* if a high level of safety is sought. [9]

REDUNDANCY (FAULT TOLERANCE)

If a SIS subsystem has two or more components installed to perform the same function, such that if one component fails the system will still be able to function by using the other component, the system is said to be *redundant*, or *fault tolerant*. Redundancy can be further categorized as hardware redundancy (HFT) and software redundancy [26]:

- **Hardware redundancy/Hardware fault tolerance (HFT):** Hardware redundancy is achieved by installing one or more components in the SIS that can perform the same function. IEC 61508 [3] refers to this concept as *hardware fault tolerance*, which describes the ability of a hardware subsystem to continue performing its required function despite a faulty component. The HFT of a subsystem is given a digit to indicate how many faults the subsystem can handle before functionality is lost. For example, the HFT of the input elements and final elements in *Figure 2.6* that are voted 1oo2 is denoted by a HFT = 1. This is because the subsystems can tolerate one (1) hardware fault (one component failure) and still function as intended. Similarly, a 1oo1 subsystem has a HFT = 0, and a 2oo4 subsystem has a HFT = 2.

- **Software redundancy:** Software redundancy is achieved by having at least two software routines, where each software routine is written by an independent coding team.

2.4.2 Safety Instrumented Functions

A safety instrumented function (SIF) is a function performed by the SIS that has been designed intentionally to protect the EUC against a specific hazard, or *demand*. [26] As an example, the SIS that was presented in *Figure 2.6* performs the SIF “shut in of pipeline” upon the demand that the pressure in the pipeline becomes too high.

The relation between a SIS and a SIF is further illustrated in *Figure 2.7* below.

Here, the SIS consists of several input elements, one logic solver and several final elements, where the highlighted SIF only utilize some of these components. This illustrates that a SIF is one specified function performed by the SIS, but one SIS can perform several SIFs.[9].

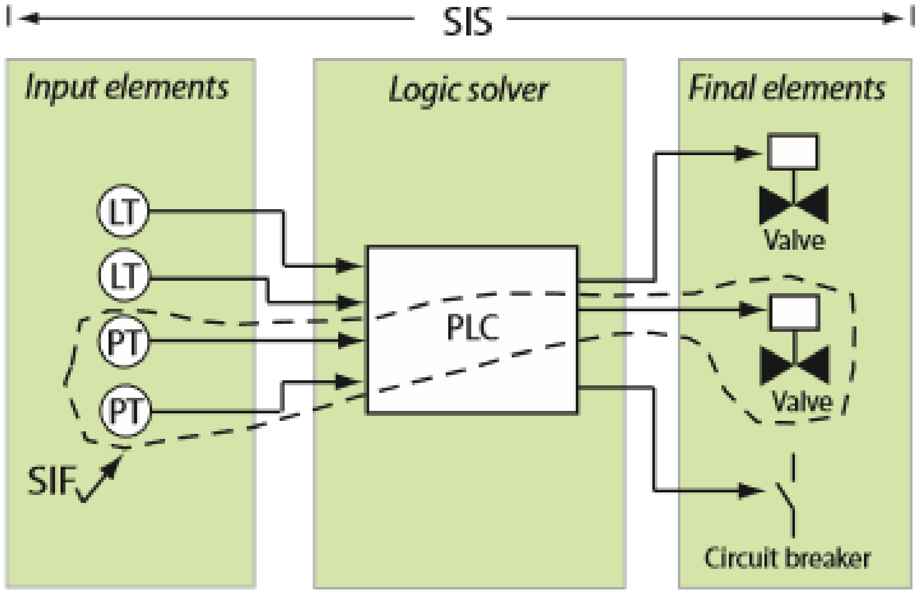


Figure 2.7: A SIS performing several SIFs [9]

If the EUC is a large system, it may be protected by several SISs. In such a case, the SISs are commonly given different names in relation to their main functions. At oil and gas installations, SISs include the emergency shutdown systems (ESD), process shutdown systems (PSD), fire and gas (F&G) detection systems and high-pressure protection systems (HIPPS). Each of these SISs in turn performs several SIFs. [9]

DEMAND AND DEMAND MODES

Because each SIF shall protect the EUC against a specific demand, it is necessary to specify what a demand is, and different demand modes (operating modes) of SIFs. Modes of operation are defined somewhat differently in IEC 61508 [3] and IEC 61511 [4]. [26] In the NOG 070 guideline [5], it is separated between *"on - demand mode"* and *"continuous/high - demand mode"*, and these terms will therefore be used for SIF demand modes in this thesis.

- **Demand:** An event or condition that requires the SIF to be activated to prevent a hazardous event from occurring or mitigate the consequences of a hazardous event. [26]

- **Continuous / high – demand mode:** The SIF is active during normal operation. A dangerous failure of the SIF may lead to an immediate hazardous event. [9]

- **On - demand mode:** The SIF is inactive during normal operation but will be activated upon *demand.*

FAILURE AND FAILURE CLASSIFICATIONS

When a component of a SIS is no longer able to perform its intended function, it is said to be *failed*. Unless the component is repaired, it will be in a *failed state* after the failure has occurred. [26] An important aspect of the design, installation and operation of SISs is to avoid introducing failures, reveal failures that have occurred, and to correct these failures. In this regard, failure classifications can provide valuable information about what cause components to fail, and the potential effects of component failure. [9]

Several failure classification systems are used for SISs, some examples are provided in [9, 26]. In accordance with the classification systems adopted in IEC 61508 [3] and IEC 61511 [4], the NOG 070 guideline [5] classifies failures based on their consequence and detectability. Consequently, this form of failure classification will also be used in the current work. According to this classification system, component failures can be classified in two main failure categories [5]:

- **Random hardware failures:** Failures resulting from the natural degradation mechanisms of components

- **Systematic failures:** Failures that are related to a particular cause other than natural degradation; e.g. errors made during specification, design, operation and maintenance

Due to their nature, systematic failures can in theory be eliminated by an appropriate modification, either in the design – or manufacturing process, operational and maintenance procedures, or training of personnel and work procedures. Random hardware failures however, cannot, but their occurrence can be predicted by probability distribution models, as will be further discussed in *Chapter 2.6.*

Both random hardware failures and systematic failures can be classified by *consequence* as being either dangerous or safe failures [5]:

- **Dangerous failure:** A failure that impedes or disables a given safety action
- **Safe failure:** A failure which favours a given safety action

Further, dangerous and safe failures can be classified by *detectability* as being either detected or undetected failures [5]:

- **Detected failure:** A failure that is detected by an automatic diagnostic test
- **Undetected failure:** A Failure that is not detected by an automatic diagnostic test

Whereas detected failures are revealed during normal operating procedures, undetected failures are not revealed until a proof test is performed on the component, or it fails to function in a demand mode, which is a critical situation. [9]

In addition, it is differentiated between independent or common cause failures (CCFs). Whereas independent component failures are, as indicated, failure of an independent component, CCFs are “simultaneous” failure of several components due to a shared cause. A drawback of redundancy, is that it increases the likelihood of CCFs. [5]

Based on the classification categories presented above, failures can be classified as dangerous detected (DD), dangerous undetected (DU), safe detected (SD) or safe undetected (SU).

A summary of the different failure classification categories is illustrated below in *Figure 2.8* [9].

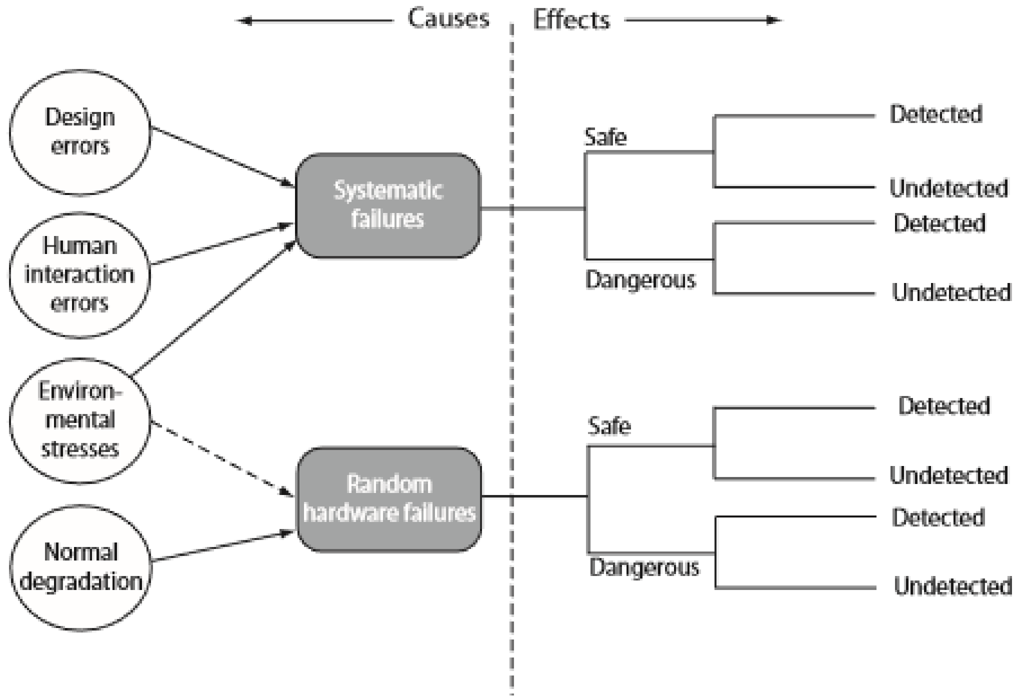


Figure 2.8: Failure classification categories for SISs [9]

THE FAIL-SAFE PRINCIPLE

An important property of SISs is the so-called fail – safe principle. This implies that in case of a specified failure, such as loss of power, SIS subsystem components shall fail to a safe position so that the safe state of the EUC is achieved. [9, 26]

TESTING

It is crucial that a SIF is able to perform its intended function in a situation of demand. Again, referring to the SIS example in *Figure 2.6*, if the pressure in the pipeline becomes too high, it is essential that the final elements (valves) function as intended and closes. To verify that a SIF or SIF subsystem performs its intended function, proof tests are performed regularly on the system according to predefined test intervals scheduled in the preventive maintenance programme.

It can be differentiated between three types of tests [26]:

- **Proof test:** Scheduled periodic test designed to reveal all DU failures. The time between two consecutive proof tests is the proof test interval (test interval), denoted τ.

- **Partial proof test:** Planned test designed to reveal some specific type of DU failure without significantly disturbing the EUC, sometimes carried out between (full) proof tests.

- **Diagnostic self – test:** Automatic partial – test where built-in self-test features are able to detect faults (DD or SD failure).

If a DU failure is present in a moment of demand, the SIF may be impaired from performing its intended function. SIFs and its associated components shall therefore be proof tested regularly

2.4.3 Governing Regulations and Documents

Safety instrumented systems at oil and gas installations on the NCS are regulated according to:

- **The framework regulations §11 (Risk reduction principles)** [15]
- **The management regulations §4 (Risk reduction)** [19]
- **The management regulations §5 (Barriers)** [1]
- **The facilities regulations §8 (Safety functions)** [22]
- **The activities regulations §47 (Maintenance programme)** [23]

According to the management regulations §5 (Barriers) guidelines; standards such as IEC 61508 [3] and IEC 61511 [4] in addition to the NOG 070 guideline [5] should be used as a basis for SISs in offshore petroleum activities. The facilities regulations §8 guidelines further recommend IEC 61508 and the NOG 070 guideline to be used when stipulating performance requirements to SIFs. The activities regulations §47 guidelines state that for safety systems, the activities in the maintenance programme, including performance monitoring activities, shall be based on NOG 070.

THE IEC STANDARDS AND NOG 070 GUIDELINE

The international standards IEC 61508 [3] and IEC 61511 [4] are widely recognized as the basis for specification, design and operation of SISs. IEC 61508 is “the manufacturers guideline” and covers in-depth requirements and constraints to design of SIS hardware and software, whereas IEC 61511 is the “system integrators and end users’ standard” and was developed by the process industry to adapt the application of IEC 61508 to SISs in process facilities. [5]

The Norwegian Oil and Gas Guideline 070 “Application of IEC 61508 and IEC61511 in the Norwegian Petroleum Industry (Recommended SIL Requirements)” (NOG 070) [5] offers a simplified method to apply the IEC 61508 and IEC 61511 standards specifically to installations in the Norwegian Petroleum Industry, either in the design and engineering phase of the installation, or in the operational phase by demonstrating compliance with the requirements in IEC 61508/IEC61511/NOG 070.

Note that in later sections of this thesis, it is referred to the respective IEC standards and NOG 070 guideline on numerous occasions. It is then with reference to the above sources.

2.4.4 Management of Functional Safety

Management of functional safety comprise the coordinated activities to ensure that performance requirements to SISs/SIFs are identified, designed and maintained during the entire lifecycle of the systems. [5]

A simplified illustration of the functional safety management process is presented in *Figure 2.9* below.

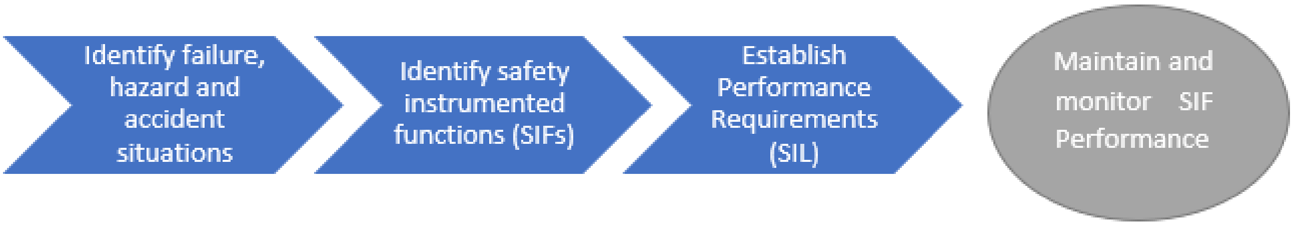

Identify failure, hazard and accident situations
Identify safety instrumented functions (SIFs)
Establish Performance Requirements (SIL)
Maintain and monitor SIF Performance

Figure 2.9: Key activities in management of functional safety

2.4.5 Performance Requirements and Verification (Minimum SIL Requirements)

After the necessary SIFs have been identified according to *Figure 2.9* above, performance requirements are allocated to the identified SIFs in terms of minimum *safety integrity level (SIL)*. [5] In short, safety integrity is a measure of how well the SIF is required to perform in order to achieve a specified level of risk reduction. It is distinguished between four safety integrity levels; SIL 1-4, where SIL 1 is the lowest (least reliable) and SIL 4 is the highest (most reliable) safety integrity level. The highest level of risk reduction is achieved at SIL 4. [9]

NOG 070 presents predefined minimum SIL requirements for selected SIFs that are already required by standards adopted in the Norwegian Petroleum Sector. The required SIL shall be realised for each SIF during SIS design and engineering. [8] Throughout the operational lifetime of the facility, it shall be verified through the operators' maintenance and monitoring activities *(Figure 2.10)* that the SIF complies with the SIL requirement laid down in design, so that the SIF is safeguarded throughout the facility's lifetime in accordance with PSAN regulations.

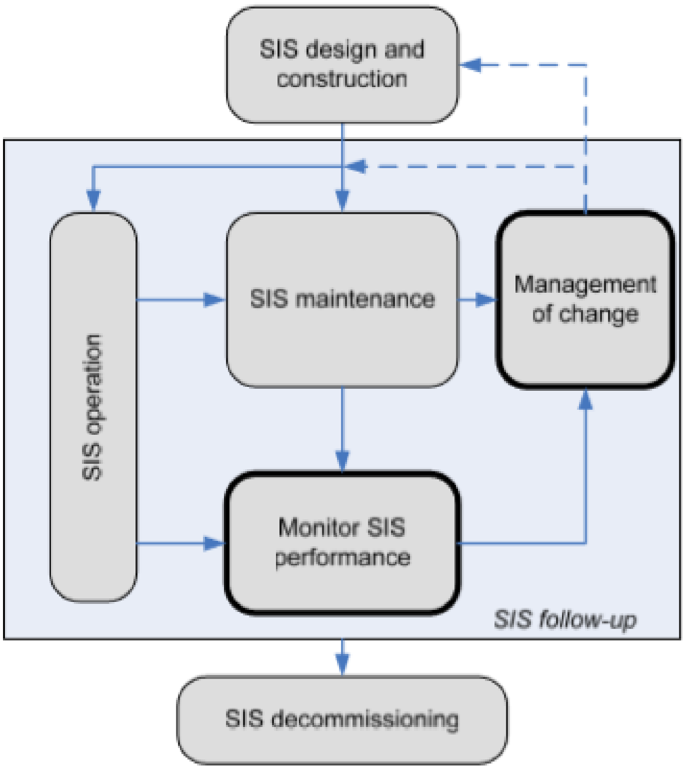


Figure 2.10: Follow up of SIFs in the operational phase of the facility. [8]

2.5 Well Barriers, Safety Instrumented Systems and Risk

Operators shall select technical, operational and organisational measures that reduce the risk of the activities. This implies the establishment of a wide combination of technical, operational and organisational barriers, of which safety instrumented systems (e.g. ESD, PSD, F&G) only play a part. Together, the barriers shall reduce risk to an acceptable level at the facility *(Figure 2.11)*.

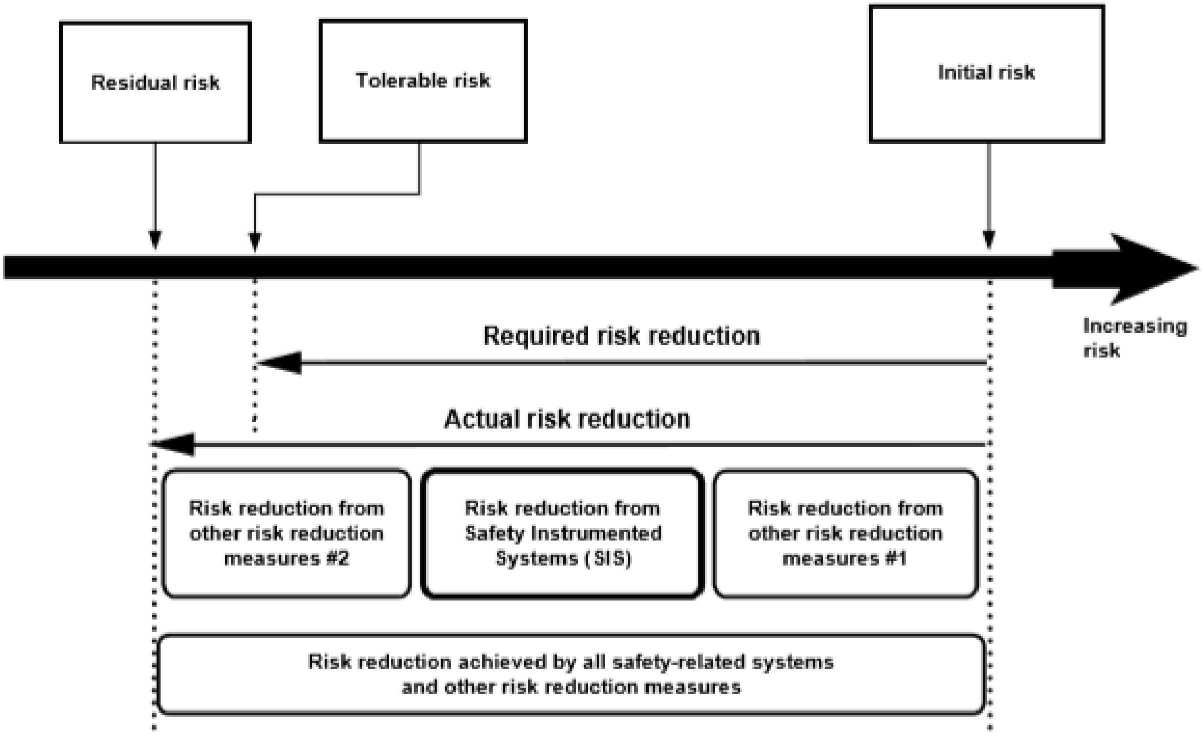

Residual risk
Tolerable risk
Initial risk
Increasing risk
Required risk reduction
Actual risk reduction
Risk reduction from other risk reduction measures #2
Risk reduction from Safety Instrumented Systems (SIS)
Risk reduction from other risk reduction measures #1
Risk reduction achieved by all safety-related systems and other risk reduction measures

Figure 2.11: Framework for risk reduction [5]

Hence, management of functional safety can be considered a subset of barrier management. [5] To comply with PSAN regulations it is clear that it should, however, be differentiated between the follow – up of well barrier elements realised by safety instrumented systems, and other technical, human and organisational well barrier elements.

2.6 Reliability

2.6.1 Reliability/Availability

Reliability is an expression (measure) of the ability of a *non-repairable* component, system or other item considered as an entity, to perform its intended function within a specified period of time. [18] In mathematical terms, the item can either be functioning, or not functioning, and the reliability of an item can be expressed in its most basic form by the *survival function* as the probability that the item is in the functional state within the specified time period. [27] Other common measures of reliability include [27, 28]:

- The probability of item failure in the time interval (0, t] (failure function)
- The frequency of item failures at time t (probability density function)
- The number of item failures per time unit (failure rate)

MEASURES OF RELIABILITY/AVAILABILITY

The state of an item at a given time *(t)* can be expressed by the discrete random state variable *X(t) [28]*:

$$X(t) = \begin{cases} 1 & if\ the\ item\ is\ functioning\ at\ time\ t \\ 0 & if\ the\ item\ is\ in\ the\ failed\ state\ at\ time\ t \end{cases}$$

In reliability analyses, the time period of interest is usually the *time to failure (T)*; that is, the elapsed time from the item is set in operation at *t = 0*, until the item enters the failed state. After the item has failed, it may be repaired, or it may in fact be *non-repairable*, and discarded or replaced by another item. The relation between the state of an item and time to failure can be seen below in *Figure 2.12*.

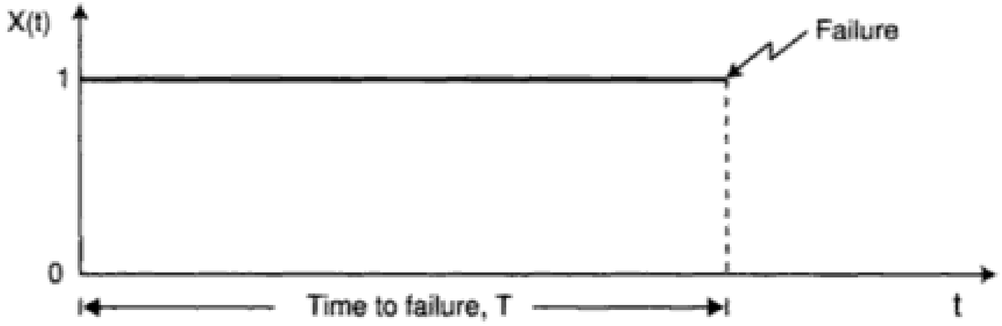


Figure 2.12: The relation between the state of an item and the time to failure [28]

The Failure Function (Item Unreliability)

What the time to failure, T, will be, is unknown and subject to chance variations. However, by the approximation that the discrete random variable T can be modelled as a continuous random variable with probability density function *f(t)*, the probability that the item fails within the time interval (0, t] can be estimated by the cumulative distribution function *F(t)*, called the *failure function* or *unreliability* of the item [26, 28]:

$$F(t) = P(T \leq t) = \int_0^t f(u)du \quad , \quad for\, t > 0 \quad (\mathbf{2.1})$$

Where the probability density function f(t) is the derivative of F(t), and shows the frequency of failures (number of failures per unit time at time t) [28]:

$$f(t) = \frac{dF(t)}{dt} = \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} = \lim_{\Delta t \to 0} \frac{P(t < T \leq t + \Delta t)}{\Delta t} \quad (\mathbf{2.2})$$

When Δt is small, we have that:

$$P(t < T \leq t + \Delta t) \approx f(t) \cdot \Delta t \quad (\mathbf{2.3})$$

Which implies that when the value of f(t) is small, the probability that the item fails in the interval (t, t + Δt) is low, and when the value of f(t) is high, the probability that the item fails in the interval (t, t + Δt) is high. Thus, the function f(t) will indicate at what time failure of the item is most likely to occur and is therefore called the probability density function (pdf). [28]

The Survival Function (Item Reliability)

The survival function estimates the probability that the item does *not* fail within the specified time interval (t, t + Δt), in other words, that the item survives the specified time interval.

The survival function is defined by [26]:

$$R(t) = P(T > t) = 1 - F(t)\,, \qquad for\; t\; > 0 \quad (\mathbf{2.4})$$

The mathematical relation between the survival function, failure function and probability density functions can be seen below *Figure 2.13*.

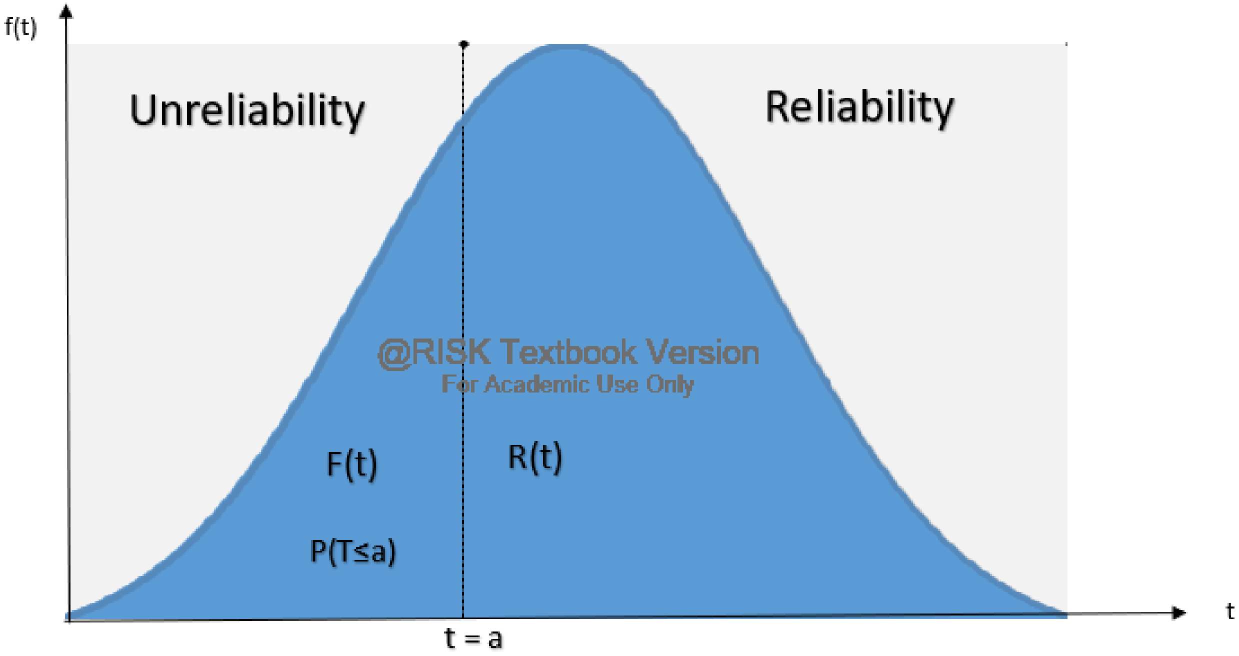


Figure 2.13: The relation between the probability density function f(t), item reliability R(t) and item unreliability F(t)

The Failure Rate

Another important measure of reliability is the failure rate function, which describes the probability that an item will fail in the time interval (t, t + Δt) given that it has already survived until time t. The failure rate function is mathematically defined as [18]:

$$z(t) = \frac{f(t)}{R(t)} \quad (\mathbf{2.5})$$

When a large population of items is put into operation at t = 0, we will have that [18]:

$$z(t) \cdot \Delta t \approx \frac{number\ of\ components\ that\ fail\ in\ the\ interval\ (t, t + \Delta t)}{number\ of\ components\ that\ function\ at\ time = t} \quad (\mathbf{2.6})$$

$$z(t) \approx \frac{number\ of\ components\ that\ fail\ in\ the\ interval\ (t, t + \Delta t)}{(number\ of\ components\ that\ function\ at\ time = t) \cdot\ \Delta t} \quad (\mathbf{2.7})$$

Hence, the practical interpretation of the failure rate is the number of registered failures in a population of items during the aggregated observation time.

For a large population of components, the change in failure rate with time tends to approximate what is called a *“reliability bathtub curve”* indicating the lifetime characteristics of the units. [18, 27] The reliability bathtub curve *(Figure 2.14)* is characterised by its three phases showing (I) a decreasing failure rate (DFR) in the *burn – in period*, (II) a constant failure rate (CFR) in the *useful life phase*, and an increasing failure rate (IFR) due to degradation of components in the *wear – out phase*. [27]

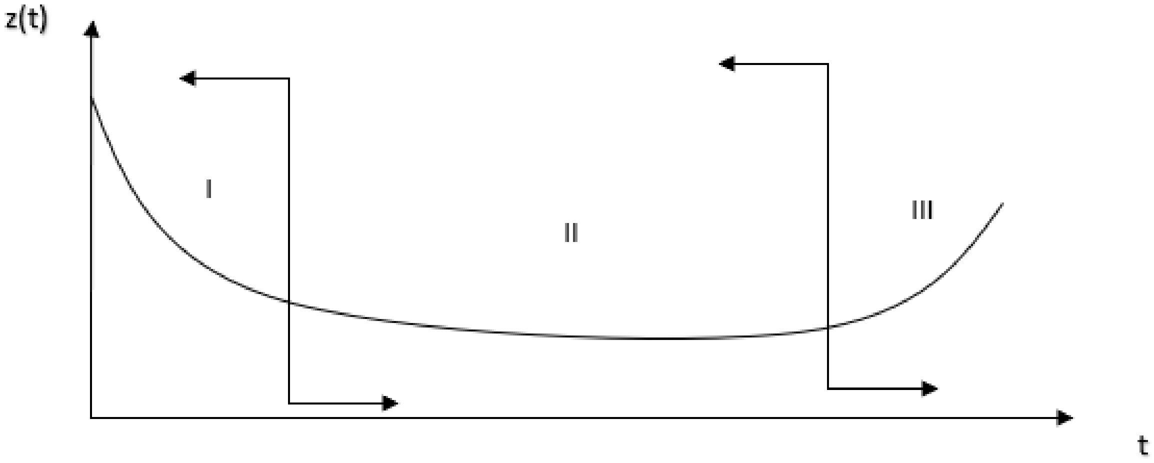


Figure 2.14: The reliability bathtub curve showing a decreasing failure rate, DFR (I); constant failure rate, CFR (II) and increasing failure rate, IFR (III).

The tendency of components to show an initially high failure rate in the burn – in phase is generally related to "children's diseases" such as construction – or material failures. However, because components are often tested at the manufacturer before they are distributed to the end users, and again before they are put into operation, components carrying "children's diseases" are often weed out from the population of units that is actually put in operation at an end user.

Hence, components that survive the burn – in phase and is put into operation have usually reached their useful life phase, and tend to show an approximately constant failure rate, until they reach the wear out phase where the effects of wear and tear of the aging components become dominant and an IFR is typically observed. [18]

Availability

For repairable items, the reliability is commonly measured in terms of the *availability* of the item at time t [26]:

$$A(t) = P(X(t) = 1) = P(the\ item\ is\ able\ to\ function\ at\ time\ t) \quad \mathbf{(2.8)}$$

That is, the availability is the probability that the item is in the functional state at time *t*. The exact opposite outcome, the probability that the item is *not* in the functional state at time t, may also be of interest in a reliability analysis. This is termed the *unavailability* of the item, and expressed as [26]:

$$\bar{A} = P(X(t) = 0) = P(the\ item\ is\ not\ able\ to\ function\ at\ time\ t) = 1 - A(t) \quad (\mathbf{2.9})$$

In other cases, it is the unavailability within a time interval rather than a specified point in time that is of interest. This can be expressed as the average unavailability over the time interval *(t_1, t_2)*. A common measure of average unavailability for systems that operate in the on – demand mode, is the average probability of failure on demand (PFD$_{avg}$), mathematically expressed as [29]:

$$PFDavg = \frac{\int_0^\tau F(t)dt}{\tau} \quad (\mathbf{2.10})$$

The PFD$_{avg}$ is based on the assumptions:

- The components are put in operation at time t = 0
- The state of the system can only be known by performing a proof test
- The system is tested at regular time intervals of length τ, and repaired if necessary
- After a test (repair), the system is assumed as good as new
- The test and repair times are considered negligible

The PFD$_{avg}$ *(Figure 2.15)* can be understood such that if a demand occurs at a random time in the future, the PFD$_{avg}$ is the averaged probability that the component/system is not able to perform its intended function on demand. [26]

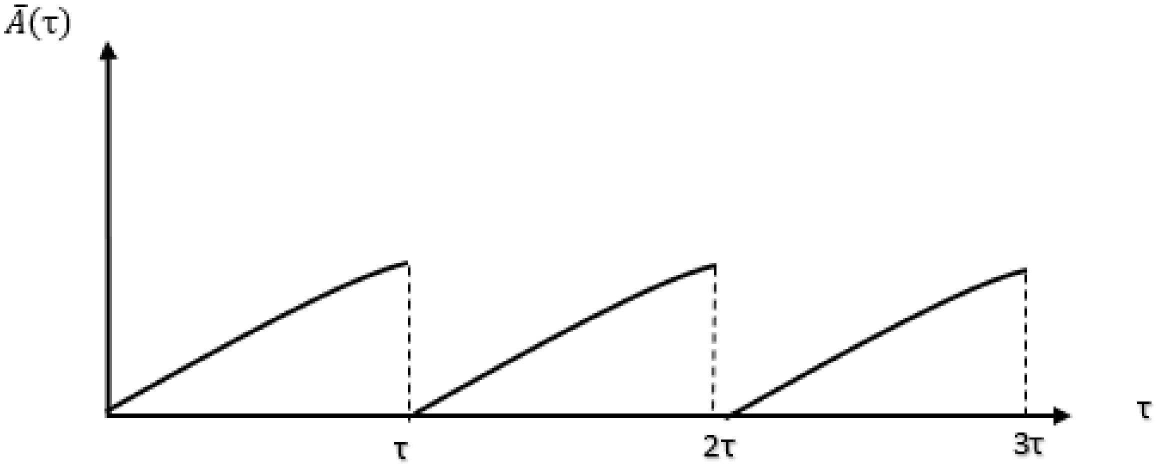


Figure 2.15: The average unavailability (PFD$_{avg}$) of a periodically proof – tested item

LIFETIME DISTRIBUTIONS

The *expected lifetime* of units can be modelled by different probability distributions, fully described by its pdf. From the inherent pdf, both F(t), R(t), z(t) and A(t) can be derived.

Several probability distribution models exist. The distributions have typically been derived by mathematicians, statisticians and engineers to model certain behaviour, and different distributions are therefore better suited to represent certain types of data than others. Some probability distributions have proven particularly useful to model lifetime data and are therefore commonly referred to as *lifetime distributions.* [30]

Two lifetime distributions that are used extensively within the field of reliability to model component lifetimes, are the exponential and Weibull distributions. [27] These lifetime distributions will therefore be shortly discussed in the following.

The Exponential Distribution

A component that has an exponentially distributed lifetime with parameter λ is characterised by:

$$f(t) = \lambda e^{-\lambda t} \quad (\mathbf{2.11})$$

$$F(t) = 1 - e^{-\lambda t} \quad (\mathbf{2.12})$$

$$z(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda \quad (\mathbf{2.13})$$

For $t > 0$, $\lambda > 0$

From the above, it follows that components with exponentially distributed lifetimes are characterised by a constant failure rate function, with failure rate λ. Because the failure rate is constant with time, the likelihood of a failure occurring is the same independently of how long the component has been in operation. [27] This is referred to as the “memoryless” property of the exponential distribution, a property which greatly simplifies the mathematics of the analysis for components with exponentially distributed lifetimes. The exponential distribution is therefore frequently used in applied reliability analyses.

The assumption that the failure rate of components is constant with time might seem unrealistic for practical applications. However, for components that are in their useful lifetime within the period of time that is studied in the reliability analysis, this is a reasonable assumption. [18] Thus, the exponential distribution is known to generally provide good descriptions of electric and electronic component lifetimes and might also be applicable to model the lifetime of units composed of several mechanical components that have been in operation for some time. [18]

However, the exponential lifetime distribution should be used with caution. Due to its simplicity there is a danger that it is sometimes used in situations where it is not appropriate, e.g. to model the lifetime of components and systems where the likelihood of failure is significantly affected by age (wear and tear), causing the units to enter the wear – out phase early. [30]

The Weibull Distribution

A component that has a Weibull distributed lifetime with shape parameter α and scale parameter β is characterised by [31]:

$$f(t) = \frac{\alpha t^{\alpha-1}}{\beta^{\alpha}} e^{-(\frac{t}{\beta})^{\alpha}} \quad \mathbf{(2.14)}$$

$$F(t) = 1 - \ e^{-\left(\frac{t}{\beta}\right)^{\alpha}} \quad \mathbf{(2.15)}$$

$$z(t) = \frac{f(t)}{R(t)} = \frac{\frac{\alpha t^{\alpha-1}}{\beta^{\alpha}} e^{-(\frac{t}{\beta})^{\alpha}}}{e^{-(\frac{t}{\beta})^{\alpha}}} = \frac{\alpha t^{\alpha-1}}{\beta^{\alpha}} \quad \mathbf{(2.16)}$$

For α > 0, β > 0, t > 0

The shape parameter α controls the shape of the failure rate function. Holding β constant and noting the relation that β = $\frac{1}{\lambda}$, as seen for example in [26], we have that:

- α < 1: the failure rate function is decreasing (DFR)
- α > 1: the failure rate function is increasing (IFR)
- α = 1: the failure rate function is reduced to z(t) = λt (the exponential function) with constant failure rate λ = $\frac{1}{\beta}$

Hence, by varying the shape parameter, the Weibull lifetime distribution can be used to model the lifetimes of components both in the burn in phase, useful lifetime phase and wear out phase. The flexibility of the Weibull function by varying the parameters α and β makes it very useful, and it is perhaps the most widely used model in reliability analyses. [27]

The Weibull distribution was developed by Waloddi Weibull to model the strength of materials and is therefore particularly well suited to model the lifetimes of electronic and mechanical components, equipment and systems in all life phases. [27, 30]

2.6.2 Quantification of System Reliability

Several methods can be used to quantify system reliability. A helpful tool that is commonly used to calculate the reliability of a system comprised of several items (components), is the use of reliability block diagrams. A reliability block diagram (RBD) is a graphical representation of the system that shows the logical connections needed for the system to perform its intended function.

The diagram consists of functional blocks connected by lines from two endpoints a and b, representing the endpoints of the system. Each functional block represents an item or a specific function of an item within the system, and the reliability block diagram shows the information (reliability) flow through the system. The logic is such that if an item is functional, it is possible for information to flow through the functional block. If enough items are functional so that it is possible to pass information through the system from a to b, the system is functional. [26, 27]

Two basic RBDs that are used in reliability quantification of SIFs are series system and parallel system RBDs *(Figure 2.16)*, and combinations of the two *(Figure 2.17)*.

SERIES SYSTEM

A series system is a system that functions if and only if *all* of its *n* items is in the functional state. Series systems are therefore voted *noon*. In *Figure 2.16* below, the series system (left) will only function if Component A is functioning.

PARALLELL SYSTEM

A parallel system is functioning if *at least* one of its *n* items are functioning. In *Figure 2.16* below, the parallel system (right) is voted 1oo2, and will function if at least one of its two components are functioning.

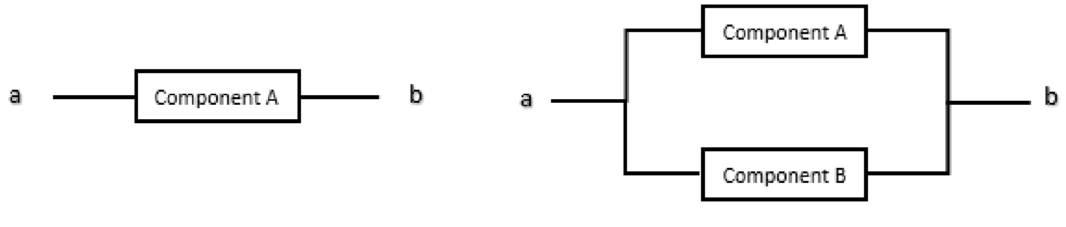


Figure 2.16: Reliability block diagram of a series system (left) having 1oo1 configuration and parallel system (right) having 1oo2 configuration.

The graphical illustration of information (reliability) flow through the system represented by the RBDs are used to deduct the equation for system reliability (unreliability) of SIFs, as will be performed in later chapters of this thesis.

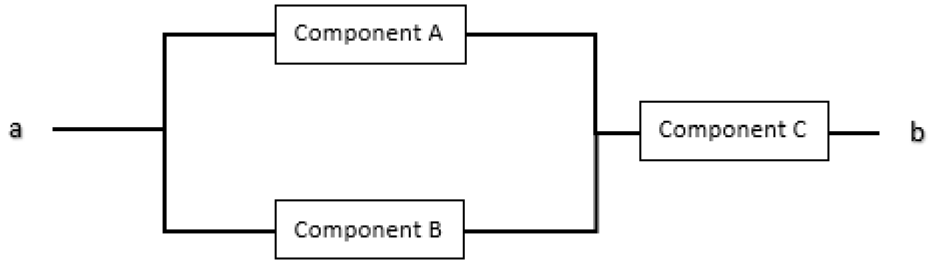


Figure 2.17: Series – parallel reliability block diagram with voted components: A and B: 1oo2, C: 1oo1

The information is combined logically using AND/OR logic gates to quantify the unreliability or reliability of the system. As an example, the RBD in *Figure 2.17* yields the logic diagram (fault tree) of the system seen in *Figure 2.18*.

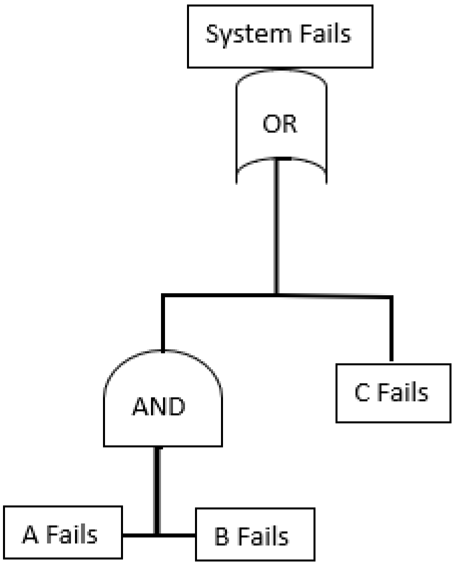


Figure 2.18: Logic diagram (fault tree) of the series – parallel system RBD

It can be seen that the system will fail if component A AND component B fails, OR component C fails. From this, the probability of system failure (system unreliability) and the system reliability can easily be deduced using basic probabilities [27]:

$$System\ unreliability = \ P(system\ failure)$$

$$= [P(A\ Fails) \cdot P(B\ fails)] + P(C\ fails)\ \ (\mathbf{2.17})$$

$$System\ reliability = 1 - P(system\ failure)\ \ (\mathbf{2.18})$$

Where system reliability is mathematically expressed as R(t) or A(t), and the probability of component failure and system failure is expressed by F(t) or $\bar{A}(t)$, in reference to *Chapter 2.6.1*.

Hence, to estimate the reliability (unreliability) of the system, the reliability (unreliability) or availability(unavailability) at component level must first be estimated by the analyst.

2.6.3 Analysis of Lifetime Data

From the discussions in *Chapter 2.6.2* on quantification of system reliability, it is evident that before the analyst can perform a mathematical reliability analysis of the system, the analyst must determine:

- The probability of component failures, expressed by F(t) or $\bar{A}(t)$
- Which lifetime distribution that best models the component lifetimes, and should be used to estimate F(t) or $\bar{A}(t)$
- The input parameters needed to express F(t) or $\bar{A}(t)$ depending on the choice of lifetime distribution, e.g. the failure rate (λ) for the exponential distribution, and the shape and scale parameters (α, β) for the Weibull distribution

The primary and perhaps most challenging part of the above tasks is to identify which lifetime distribution and parameters that best models the component lifetimes.

In general, this can be determined in two ways;

- By a qualitative assessment of the experienced analyst and engineers based on knowledge of e.g. component behaviour, the system, and environmental or other factors affecting them, as well as the suitability of different lifetime distributions to model certain types of units and behaviour

- By a quantitative analysis of collected operational data of component lifetimes using methods such as hazard plotting and goodness of fit – tests.

The latter method will be further discussed throughout this chapter. The basis of the lifetime analysis is collected operational data of a population of comparable units (components), where the quantity of interest is the time – to – failure of the components. A typical challenge with such collected operational data, is that the data set is censored.

COMPLETE AND CENSORED DATA

In life data analysis, it is differentiated between complete and censored data. In a complete data set, all units have failed when the trial (data collection) is terminated. In a censored (incomplete) data set, some of the units in the data set has not yet failed when the data collection is terminated. In practice, it is common that most of the observed lifetimes in the collected data are censored. [27]

It is common to separate between three main types of censored data [27]:

- **Left censored data:** The units have been in operation for some time before the observation period begins

- **Right censored data:** The units are observed until whatever comes first of the end of the observation time, or *k* out of *n* components have failed.

- **Multiple censored data:** Some items are withdrawn from the trial for other reasons than the defined “failure mode” of the analysis, in addition to both right and left censoring.

Whether the data set is complete or censored is an important characteristic that should be incorporated in the further analysis of the underlying lifetime distribution.

DISTRIBUTION FITTING (GOODNESS OF FIT – TESTS)

Sometimes, the analyst may have an assumption about which lifetime distribution that best models the data based on experience, engineering judgement and/or historical data. A logical starting point is therefore to assess whether the distribution is indeed a good fit to model the observed lifetime (failure) behaviour of the units. Other times, the analyst might identify several lifetime distributions as potentially good candidates to model the unit lifetimes, and the question then becomes which distribution that models the dataset *best*.

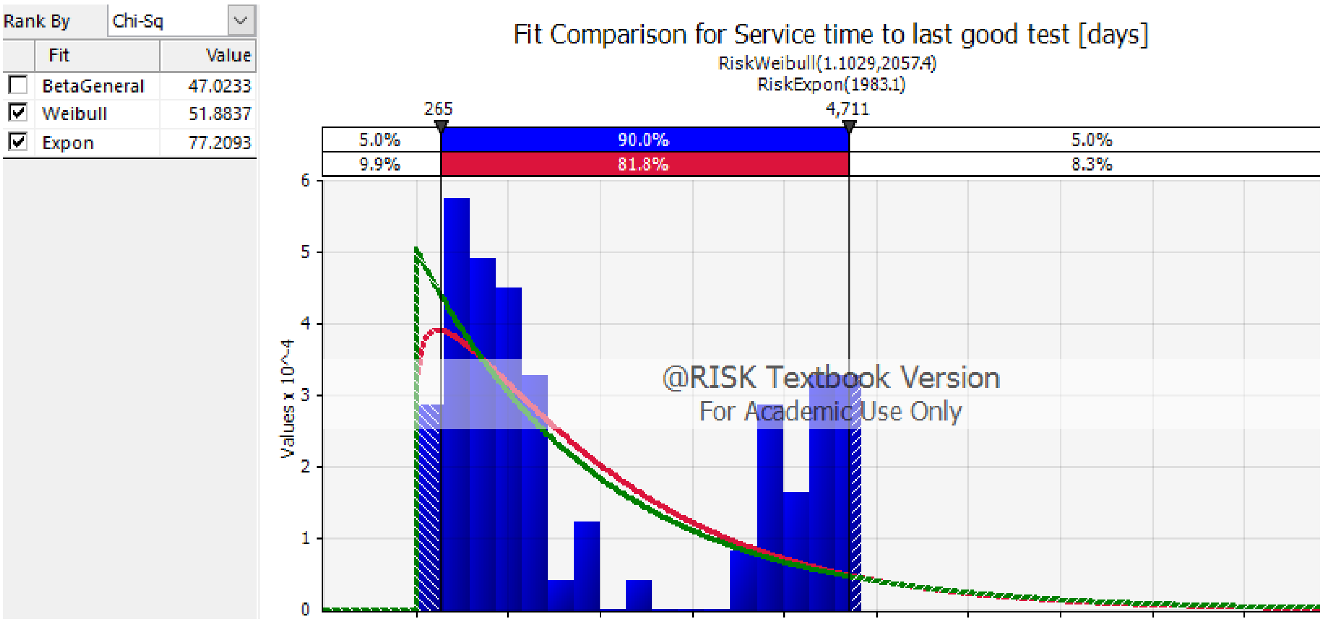
In these circumstances, a good solution is to fit different lifetime distribution models to the data and perform a *goodness of fit – test*. A goodness of fit - test is a test that assesses how well a statistical model fits a set of observations. Different goodness of fit – tests can be used but their appropriateness is dependent on the available volume of data. For large sample sizes (e.g. ≥ 20), the χ^2 goodness of fit – test is recommended. The procedure for carrying out a χ^2 goodness of fit – test is as follows [27]:

1) Assume a lifetime distribution and estimate the parameters from the observed data
2) Divide the failure timescale into a number of intervals with at least five failure times per interval (the interval widths need not be equal)
3) Calculate the theoretical number of failures per interval (calculate the probability of failure at the beginning and end of each interval and multiply the difference by sample size)
4) Calculate the χ^2 statistic from the formula:

$$\chi 2 = \sum_{1}^{K} \frac{(f_i - F_i)^2}{F_i} \quad (\mathbf{2.19})$$

Where K is the number of intervals, f_i is the observed frequency in interval i and F_i is the theoretical frequency in interval i. If the calculated $\chi 2$ value is less than the value provided in $\chi 2$ tables for the given degrees of freedom *((K-1) - #of parameters),* the distribution is a good fit. [27] When comparing the best fit between different distributions, the smaller the $\chi 2$ – value, the better the fit. [31]

Alternatively, distribution fitting and goodness of fit – tests can be performed “automatically” by different statistical software tools, such as Palisade @risk. An example of distribution fitting and goodness of fit – comparison between the exponential and Weibull distribution to model component lifetime data using Palisade @risk can be seen below in *Figure 2.19*. Using Palisade@risk, the software will also estimate the distribution parameters based on maximum likelihood estimation of the input sample data (collected lifetime data). [31]



Rank By: Chi-Sq

	Fit	Value
□	BetaGeneral	47.0233
☑	Weibull	51.8837
☑	Expon	77.2093

Figure 2.19: Chi – Square Goodness of fit - comparison of the Exponential and Weibull distributions to model component lifetime data.

HAZARD PLOTTING

Another method that is frequently used in reliability analyses to identify the underlying lifetime distribution, is hazard plotting, also known as Nelson estimation. [18] This method can be used for both complete and censored data sets and is particularly useful for data sets where only a few failures (e.g. ≥ 3) are observed in the observation period, which can be a “problem” in the analysis of highly reliable units.

The method is based on the relation between the failure rate (hazard rate) z(s), the cumulative hazard rate Z(t) and the survival function R(t) [32]:

$$Z(t) = \int_{o}^{t} z(s)ds \quad (\mathbf{2.20})$$

$$R(t) = e^{-Z(t)} \quad (\mathbf{2.21})$$

A plot of the cumulative hazard rate Z(t) versus time, called a hazard plot, will indicate the shape of the failure (hazard) rate; whether it is DFR, CFR or IFR, and therefore the underlying lifetime distribution.

The reason is this; in reference to *Chapter 2.6.1*, the survival function for the exponential distribution is $R(t) = e^{-\lambda t}$; hence for the exponential distribution Z(t) = λt. Therefore, if a plot of Z(t) versus time is linear through origin with slope λ, the underlying distribution is exponential with failure rate λ.

However, if the plot of Z(t) versus time is NOT linear, it can easily be checked if the lifetimes are Weibull distributed. From *Chapter 2.6.1,* the survival function of the Weibull distribution is $R(t) = e^{-(\frac{t}{\beta})^{\alpha}}$; thus, for the Weibull distribution, Z(t) = $(\frac{t}{\beta})^{\alpha}$. Hence, taking the logarithm on both sides one obtains:

$$\ln\big(Z(t)\big) = \alpha \ln\left(\frac{1}{\beta}\right) + \alpha \ln(t) \quad (\mathbf{2.22})$$

Therefore, if a plot of ln Z(t) versus ln (t) is linear, the underlying distribution is Weibull, and approximate values of α and β can be found from the plot. [32]

2.6.4 Reliability of Safety Instrumented Functions (NOG 070/The PDS Method)

NOG 070 sets minimum performance requirements (SIL requirements) to the integrity of selected SIFs, measured as average (un)availability of the SIF. For on – demand SIFs, the average unavailability is calculated as the average probability of failure on demand ($\mathrm{PFD_{avg}}$). The derivation of the minimum SIL requirements in NOG 070, as well as the recommended method for end-users to re-calculate the updated PFD$_{avg}$ based on operational data for SIL verification, is based on The PDS method [33]. The PDS method is a widely recognized method for calculation of SIS reliability in the oil and gas industry. [5]

According to the PDS Method Handbook [33], §3.7.2 The PFD$_{avg}$ is the average probability that a SIS (SIF) is *unable* to perform its safety function upon demand. The PDS method quantifies the PFD$_{avg}$ as the loss of safety due to *DU failures* during the time period when it is unknown that the function is unavailable.

QUANTIFICATION OF PFD$_{AVG}$ - COMPONENT LEVEL

Assuming that data collection takes place during the useful lifetime of the components[2], with exponentially distributed component lifetimes with a constant rate of DU failures λ_{DU} and average time between proof tests τ/2 (where SIF unavailability will be unknown), the PFD$_{avg}$ for a single 1oo1 voted component can calculated by the simplified formula [5]:

$$PFDavg \approx \lambda_{DU} \cdot \frac{\tau}{2} \quad \mathbf{(2.23)}$$

Contributions from Independent and Common Cause Failures

For redundant systems, it is important to distinguish between DU failures that are due to independent and common cause component failures[3]. The common method to account for the failure contribution from CCFs to the PFD$_{avg}$ is the use of the β – factor model, in which a certain fraction (β) of DU component failures are attributed to a common cause that will lead redundant components to fail approximately simultaneously.

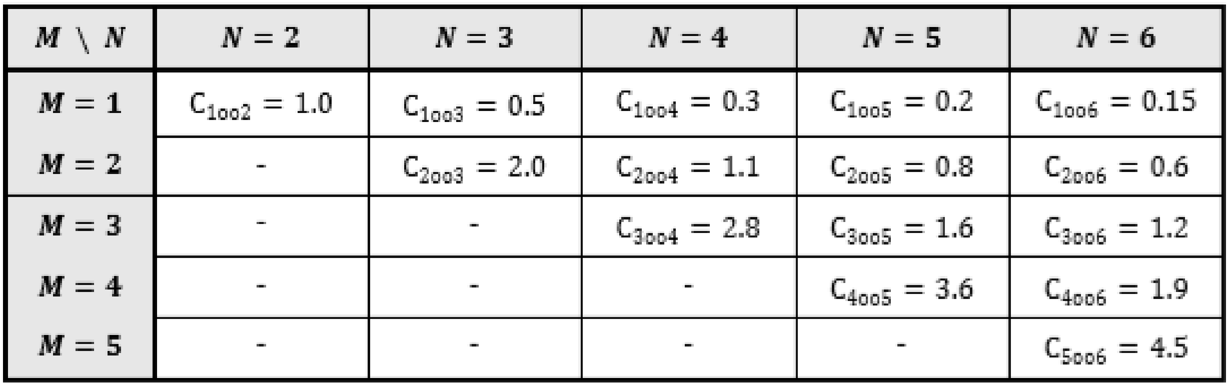
In the PDS method, an extended version of the β – factor model is adopted that differentiates between different voting configurations. Different rates of common cause failures are assumed dependent on the voting configuration. This is expressed by introducing a modification factor for different voting configurations (C$_{MooN}$). For example, a 2oo3 voted component configuration will have a component DU failure rate due to CCFs equal to $C_{2oo3} \cdot \beta \cdot \lambda_{DU}$. [5]

[2] Reference is made to NOG 070, *§ 8.5.3*

[3] For a discussion on failure classifications, reference is made to *Ch. 2.4.1* of the thesis

C_{MooN} values are provided by NOG 070/The PDS Method handbook for different voting configurations, as seen below in *Table 2.1*

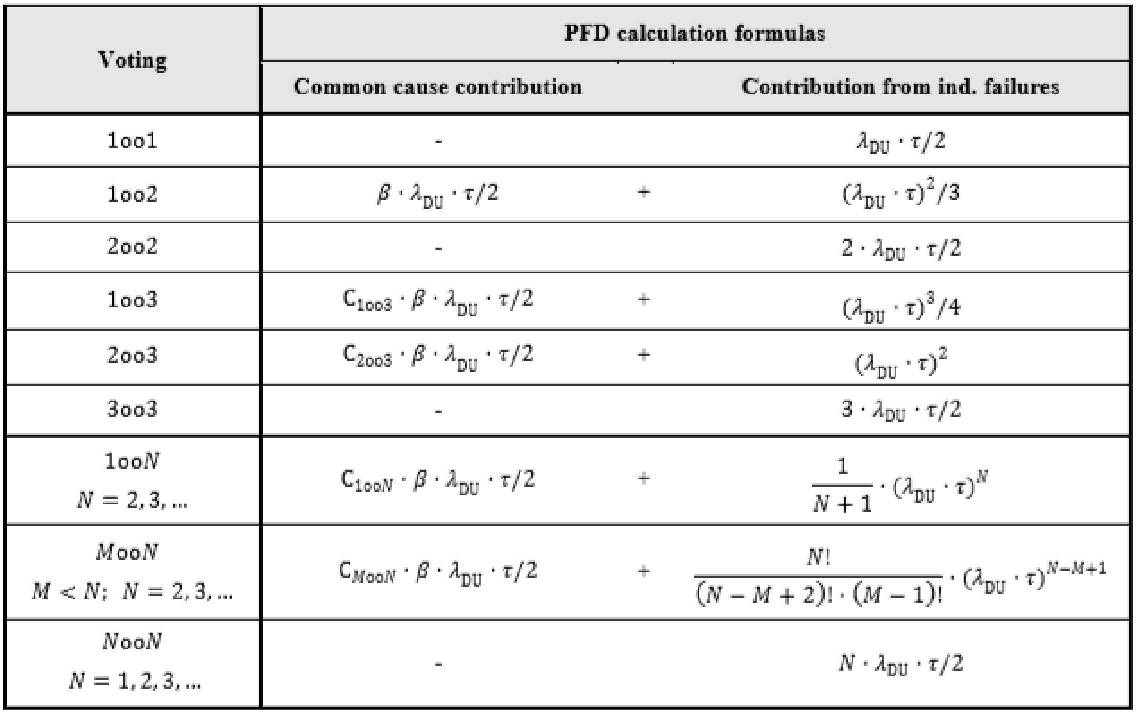
Table 2.1: C_{MooN} voting modification factors for redundant components [5]



$M \setminus N$	$N = 2$	$N = 3$	$N = 4$	$N = 5$	$N = 6$
$M = 1$	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.2$	$C_{1oo6} = 0.15$
$M = 2$	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.8$	$C_{2oo6} = 0.6$
$M = 3$	-	-	$C_{3oo4} = 2.8$	$C_{3oo5} = 1.6$	$C_{3oo6} = 1.2$
$M = 4$	-	-	-	$C_{4oo5} = 3.6$	$C_{4oo6} = 1.9$
$M = 5$	-	-	-	-	$C_{5oo6} = 4.5$

Hence, for redundant subsystems components, the expression for the PFD_{avg} at component level is comprised of an independent contribution and a common cause contribution where the mathematical expression depends on the voting configuration, as seen below in *Table 2.2*.

Table 2.2: Summary of simplified formulas for the PFD_{avg}, as presented in [5]



Voting	PFD calculation formulas		
	Common cause contribution		Contribution from ind. failures
1oo1	-		$\lambda_{DU} \cdot \tau/2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau/2$	+	$(\lambda_{DU} \cdot \tau)^2/3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau/2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	+	$(\lambda_{DU} \cdot \tau)^3/4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	+	$(\lambda_{DU} \cdot \tau)^2$
3oo3	-		$3 \cdot \lambda_{DU} \cdot \tau/2$
1oo$N$ $N = 2, 3, \ldots$	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	+	$\frac{1}{N+1} \cdot (\lambda_{DU} \cdot \tau)^N$
Moo$N$ $M < N;\ N = 2, 3, \ldots$	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	+	$\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}$
Noo$N$ $N = 1, 2, 3, \ldots$	-		$N \cdot \lambda_{DU} \cdot \tau/2$

For example, a 1oo2 voted component will have an independent and CCF contribution to the PFD$_{avg}$ [5]:

$$PFDavg_{1oo2}{}^{ind.} \approx \frac{(\lambda_{DU} \cdot \tau)^2}{3} \quad (\mathbf{2.24})$$

$$PFDavg_{1oo2}{}^{CCF.} \approx \beta \cdot \left(\lambda_{DU} \cdot \frac{\tau}{2}\right) \quad (\mathbf{2.25})$$

And the total PFD$_{avg}$ for the component becomes:

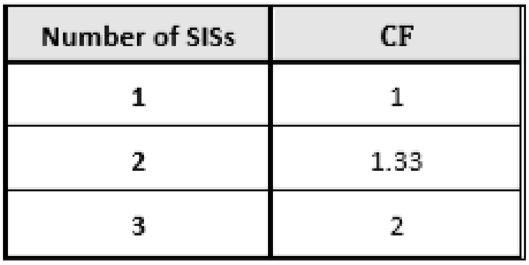
$$PFD_{avg} \approx \frac{(\lambda_{DU} \cdot \tau)^2}{3} + \beta \cdot (\lambda_{DU} \cdot \frac{\tau}{2}) \quad (\mathbf{2.26})$$

QUANTIFICATION OF PFD$_{avg}$ - TOTAL FOR SIF

For system unavailability quantification of the total SIF, the PFD$_{avg}$ of the SIF at function level is calculated by combining the PFD$_{avg}$ contributions from its subsystem components. The voting configurations of components and equation for system reliability quantification is determined from the SIFs RBD in line with the theory presented in *Chapter 2.6.2.*

Because dependencies exist between SIFs and SIF subsystem components due to factors such as close location, common utility sources and simultaneous proof testing, the combined independent PFD$_{avg}$ is not appropriate in practice. To model systemic component dependencies, the aggregated independent PFD$_{avg}$ is multiplied with a correction factor in accordance with *Table 2.3 [5]*.

Table 2.3: Correction factors for multiple SISs when the structure of each system/simultaneous proof testing is disregarded [5]



Number of SISs	CF
1	1
2	1.33
3	2

3 UNCERTAINTY IN RELIABILITY ANALYSES

Safety instrumented systems and other barriers are implemented to reduce the risk of failure and accident situations. For safety instrumented functions, the demonstrated SIL in operation is used as a measure of the achieved level of risk reduction provided by the SIF. Whether the SIF meets the quantitative SIL requirement is based on a reliability analysis of SIF components. In this regard, it is important to be aware that the quantification of reliability is associated with uncertainty.

3.1 What is Uncertainty

The concept of uncertainty was briefly introduced in *Chapter 2.2.* The definition and conceptualisation of *uncertainty* differs in different contexts and has been subject to debate[4]. In general, uncertainty arises due to imperfect or incomplete knowledge about a hypothesis, a quantity or the occurrence of an event. [14]

In reliability analyses, uncertainty expresses our degree of knowledge about the system. [9] Statistical models (lifetime distributions) are used to treat aleatory uncertainty, for example by estimating the *expected* lifetime of components and system reliability. However, a model is merely an idealized, simplified representation of the world. [28]. Epistemic uncertainty lies in a general lack of knowledge about how well these models are able to capture the true behaviour of the system. Hence, the results of the reliability analysis may provide more or less good predictions of future outcomes. [26]

The PDS Method Handbook [33] classifies uncertainty in reliability analysis as data uncertainty and model uncertainty. In the nuclear industry, uncertainty is classified as parameter uncertainty, model uncertainty and completeness uncertainty. [26] In later chapters of this work, a reliability analysis is performed on a SIF in offshore production wells. The analysis includes data collection and treatment, model selection, parameter estimation and quantification of SIF reliability. Uncertainty is introduced in all four stages. Consequently, data uncertainty, parameter uncertainty, model uncertainty and completeness uncertainty will all be regarded in this work.

[4] For an overview and discussion, the reader is referred to [17]

3.2 Data Uncertainty

Data uncertainty in a reliability analysis relates to the extent with which the collected data from a population of comparable units is relevant and able to represent future performance. In particular, uncertainty arises due to the facts that [33]:

- **Historical data is not the same as future performance:** Historical component performance demonstrated from operational data is often based on various samples with varying age and operating conditions. The data may not be representative for future performance of all components and operational environments

- **Incomplete data:** The collected data may be incomplete due to few samples, lack of censoring or the exclusion of certain types of failures

- **Poor reporting and interpretation:** Uncertainty arises in the data collection, failure reporting, failure classification and the interpretation of the collected data

3.3 Parameter Uncertainty

Parameter uncertainty relates to the uncertainty in the parameters (e.g. failure rates, shape – and scale factors) used in the reliability calculation. This class of uncertainty is closely related to data uncertainty, as the estimated parameters are based on the collected data, and the analyst's interpretation and treatment of the collected data. Some particular challenges that often introduce parameter uncertainty are [26]:

- **The no data – problem:** Because SIS components are generally designed to be highly reliable, few or even no failures can be expected to occur even during a long observation period. Few datapoints in the analysis makes the parameter estimations more uncertain.

- **Differing operational environments:** If parameters are estimated based on generic data from a large population of units in differing operational environments, the parameters may be inappropriate for units in other environments.

- **The effect of CCFs**: The method and factors used to include the contribution of CCFs to component failure rates are based on generic data that might not be appropriate for all SISs

- **Lack of operational experience**: Because the operational environment will affect the performance of system units, it is advised to use installation specific data (rather than generic data) to estimate parameters if sufficient operational experience is available to arrive at parameter estimates with a sufficient level of confidence. For failure rates, this will generally require at least $3 \cdot 10^6$ operating hours[5], which is often not available.

3.4 Model Uncertainty

Model uncertainty lie in the degree to which the model used in the reliability analysis is able to capture the most important phenomena of the components/system, in light of the operating conditions. [33] Component models should also represent issues relating to testing and maintenance, such as proof test and diagnostic test coverage, and the possibility of performing partial stroke tests of emergency shutdown valves. [26] The choice of model may more or less appropriately be based on, among others [9]:

- **Regulations, standards and guidelines**
- **Competence**
- **Time resources**
- **Available tools**

3.5 Completeness Uncertainty

Completeness uncertainty arise from factors that are not considered in the reliability analysis. Even if the data and models used in the analysis are of high quality, failing to include all relevant factors will still result in a more uncertain estimate of the reliability. It is separated between known and unknown completeness uncertainty [26]:

- **Known completeness uncertainty:** Uncertainty due to the deliberate exclusion of *known* factors from the analysis. This may be done for several reasons, such as lack of competence, limited time and monetary resources, lack of models or data to support said

[5] Reference is made to [8], p. 25

models. Known completeness uncertainty is reflected in the simplifications and assumptions made in the analysis, and the degree of exclusion can serve as an indicator of the degree of uncertainty in the reliability estimate.

- **Unknown completeness uncertainty:** Exclusion of factors that are not known or identified by the analysts, sometimes referred to as ignorance. Because these factors are unknown, their effect on uncertainty is difficult to account for or judge.

3.6 Assessments of Uncertainty in Reliability Analyses

Different tools are available to represent and assess uncertainty in reliability analyses. The ideal representation of uncertainty is subject to debate, see for example discussions by Aven [17], and the preferred choice of method to assess uncertainties in the reliability analysis will be dependent on several factors such as the nature of the system, available data, regulations and guidelines, competence, available time and resources etc.

However, the analyst should be aware and critical about what the implications, strengths and weaknesses are of the method of choice to decide whether the method is appropriate. Hence, rather than going into the details of different tools to assess uncertainty in reliability analyses, this subchapter will present some brief discussions about the underlying theories of the main categories of methods used to assess uncertainties in reliability analyses.

The methods for representing and assessing uncertainty can roughly be divided into three main categories;

- **Quantitative methods; using probabilities (frequentist or subjective)[6]**
- **Qualitative methods; e.g. using classification systems**
- **Semi – quantitative methods; combining quantitative and qualitative approaches**

In reliability analyses, variation of quantities such as component lifetimes and system availability due to inherent randomness is known as aleatory uncertainty. Although aleatory uncertainty can, in principle, not be reduced, statistical models such as the average probability

[6] For a proper discussion on the difference between frequentist and subjective probabilities, the reader is referred to [17]

of failure on demand can provide mathematical expressions of the variation in system reliability (availability). Hence, it is argued by some that although the aleatory uncertainty cannot in principle be reduced, it can always be quantified. [34]

In these contexts, probabilities interpreted in the sense of relative frequencies are commonly used. Building on the discussions by Flage and Aven [35]; for the case of probability of failure on demand, such an interpretation implies that the probability of the event "failure on demand" will be defined as the fraction of times this event would occur, if the trial (demand) was theoretically repeated an infinite number of times for an extended population of components/systems. Inherent variation and randomness in the extended population will cause the event "failure on demand" to occur some, but not all of the times the trial (demand) is repeated. This will generate a "true" PFD, which describes the aleatory uncertainty (variation) in the occurrence of a failure in a situation of demand. This is the "true" underlying quantity of the PFD, which the availability model tries to estimate.

However, the models and parameters used to express this uncertainty are based on a number of assumptions, simplifications and suppositions reflecting the analyst's belief about system behaviour. These are based on the analyst's current knowledge about system physics, processes, operating conditions and so on. Referring to the previous discussions in this chapter, this causes uncertainties to be hidden in the choice and treatment of data, parameters and models. Hence, the model outputs may provide more or less good predictions of future system availability, and surprises can occur relative to our beliefs. The analyst's current knowledge may be strong or weak, which will affect the "correctness" of the estimations. [36] This general lack of knowledge about the "true" value of the PFD is known as epistemic uncertainty.

Because epistemic uncertainty arises due to imperfect knowledge, it can be reduced by acquiring more information. For this reason, some authors advocate that it should be distinguished between aleatory and epistemic uncertainty in the reliability analysis, see for example [36, 37]. The idea is that since epistemic uncertainty can be reduced, knowing how large portion of the uncertainty that is epistemic uncertainty implies knowing how much of the uncertainty that is removable so that the model can be improved and yield better estimates of future system behaviour – or alternatively, how much trust should be put in the model estimates in a decision context. And, as advocated by O'Hagan and Oakley [37], for the assessment of uncertainties to be consistent, probabilities should be used also to describe the epistemic uncertainties in the analysis. This implies a purely quantitative assessment of uncertainties.

QUANTITATIVE ASSESSMENTS OF UNCERTAINTY

Different probabilistic methods are commonly used to quantitatively express the epistemic uncertainty of model input parameters (e.g. λ, α, β) and/or model output parameters (e.g. PFD_{avg}) in reliability analyses. Again, using the estimated average probability of failure on demand as an example, some common methods to assess the uncertainty in the estimate include to also provide [26]:

- A standard deviation for PFD_{avg}
- A confidence interval for PFD_{avg}, for example the 70% confidence interval;
  $P\ (PFD_{avg,L} \leq PFD_{avg} \leq PFD_{avg,U}) \geq 70\%$[7]
- A probability of meeting the target PFD_{avg};
  $P\ (PFD_{avg} \leq PFD_{avg,\ target}) \geq 70\%$
- By use of expert elicited, subjective probabilities

In addition, the propagation of epistemic uncertainties in the input values to the model output can be assessed using sampling methods such as Monte Carlo analysis, which is frequently used in reliability analyses to propagate epistemic parameter (e.g. failure rate) uncertainties to the model output. See for example [10, 36]

However, as argued by O'Hagan and Oakley [37], although probabilities are in theory "the perfect tool" to assess both aleatory and epistemic uncertainty, the distinction between aleatory and epistemic uncertainties can be blurry. And although using probabilities to express both types of uncertainty is a good method in theory, it is not necessarily an easy task in practice. For example, some of the (assumed aleatory) variability of the system could be reduced by changing the model conditions, and must therefore have been epistemic, not aleatory. In addition, there are several factors affecting the availability of the system, such as variation in operational environment within the population, human and organisational factors, that the probability model and quantitative assessments of uncertainty won't capture or model in a satisfying manner.

[7] The 70% confidence interval implies that there is a 70% confidence that the "true" PFD_{avg} will be within this interval. If the interval is wide, the epistemic uncertainty in the PFD_{avg} is large.

In these cases, expert elicited subjective probabilities that expresses the degree of belief of the expert (analyst) can be used to quantitatively express the uncertainty in the estimates. However, O'Hagan and Oakley acknowledge that oftentimes people find it difficult to express their knowledge and beliefs in probabilistic forms. Hence, in practice, expert elicitation of probabilities is far from a perfect process – probabilities are perfect, but we can't elicit them perfectly. [37]

In addition, as argued by Flage and Aven [35], the implications of the assigned probabilities and what they truly express may be difficult for the decision maker to fully comprehend, which causes difficulties in communicating what the results of the analysis really means. As reliability analyses should first and foremost provide decision support, and the objective is then partially lost. This might lead to weakened conclusions and inspires the use of alternative methods for assessment of uncertainties.

SEMI – QUANTITATIVE AND QUALITATIVE ASSESSMENTS OF UNCERTAINTY

An alternative approach as suggested by Flage and Aven [35], is to interpret probabilities in a Bayesian perspective[8] as purely epistemic – based subjective expressions of uncertainty as seen by the assessor, based on the currently available background knowledge.

The background knowledge encompasses all system knowledge, historical performance data and assumptions and presuppositions made in the analysis. As the current knowledge (and lack thereof) is the backbone of the assigned probabilities, it is necessary to make some reflections on the strength of the knowledge supporting the probabilities in order to assess whether the uncertainty of the produced estimate is small or large. Hence, the appropriate assessment of uncertainties in this perspective is a semi-quantitative approach with the pair (P, SoK), where the quantitative uncertainty assessment (P) should be accompanied by a *qualitative* assessment of the uncertainty (e.g. classified as small, medium, large) in the estimate based on the strength of the background knowledge (SoK).

[8] The interested reader is referred to [17]

The following checklist is proposed by Flage and Aven [35] as a guideline to assess the SoK and associated uncertainties in the quantitative estimate, see also [17]

The knowledge is weak (uncertainty is large) if <u>one or more</u> of the following conditions are met:

- The phenomena involved are *not* well understood, the models are non-existent or known/believed to give poor predictions
- The assumptions made represent strong simplifications
- Data are not available, or are unreliable
- There is a lack of agreement among experts

The knowledge is strong (uncertainty is small) if <u>all</u> of the following conditions are met:

- The phenomena involved are well understood; the models used are known to give good predictions
- The assumptions made are seen as very reasonable
- Much reliable data are available
- There is a broad agreement among experts

The knowledge and uncertainty are medium if somewhere in between the above.

Purely qualitative assessments of uncertainty can also be performed, using similar checklists as the above. This can for example be useful as an addition to the results of a reliability analysis performed by other analysts to give added weight to the uncertainties of the analysis, see for example [11].

4 CASE PRESENTATION

In this thesis, a reliability/availability case analysis will be performed on a SIF that is part of the ESD SIS in offshore production wells to determine optimum test intervals for the SIFs final elements (well barrier components). To perform the analysis, operational reliability data of the components is collected from production wells at the Mike, Zulu and Sierra installations located in The Greater Ekofisk Area at the NCS, operated by ConocoPhillips Norway. A brief introduction of a standard production well will be presented prior to the case system (SIF) to be analysed, and its operating environment.

4.1 Production Wells

Production wells transport reservoir fluids (oil, gas, water) from the producing reservoir through the production tubing to the process facilities on the installation (platform). The *well* is comprised of the well completion, casing programme, wellhead and x-mas tree [38]:

- **Casing programme:** All casing and liner strings, including hangers and cement in the wellbore.

- **Well completion:** Assembly of tubing hanger, downhole tubular, safety valve, production packer, and other equipment placed inside the production casing.

- **Wellhead:** Surface or seabed termination of the wellbore, incorporating facilities for production tubing and installing the x-mas tree.

- **X-mas tree:** Assembly of valves, pressure gauges and chokes fitted to the wellhead to control well flow

On surface wells, the wellhead, x-mas tree and production control systems are positioned at the platform. A sketch of a typical production well can be seen below in *Figure 4.1*.

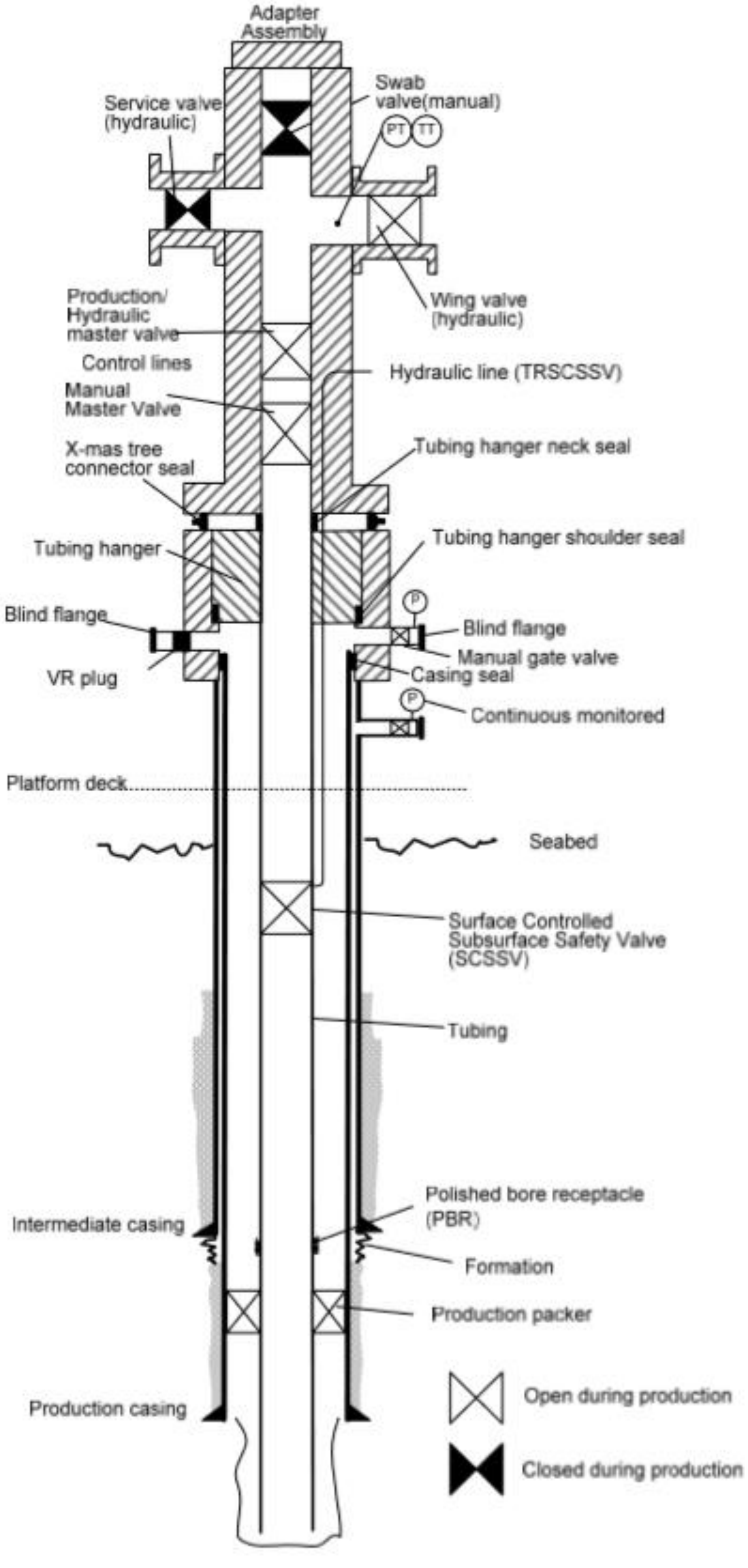


Figure 4.1: Standard surface production well [38]

The part of the well located above sea level is commonly referred to as the topside. A simplified schematic of a topside well can be seen below in *Figure 4.2*. Some important components integrated in the production tubing of the topside well are the downhole safety valve (DHSV), the production master valve (PMV) and the production wing valve (PWV).

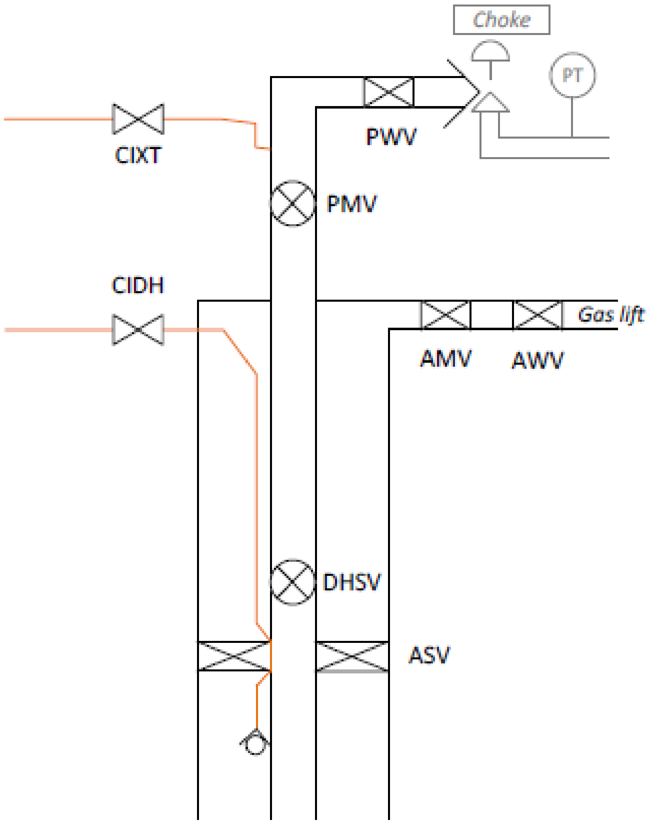


Figure 4.2: Well schematic of topside well. The DHSV, PMV and PWV are integrated in the production tubing. [5]

The DHSV is located down the wellbore and can thus shut in the entire topside well in closed position. The PMV is located on the x-mas tree and controls the flow from the wellbore. The PWV is located on the side of the x-mas tree and is used to control or isolate the production. [38]

4.2 System to be Analysed

4.2.1 Overview of the Case SIF

The system to be analysed in the case analysis in this thesis, is the SIF “Isolation of production bore in one topside well from the production manifold/flowline (ESD)” specified in the NOG 070 guideline *(Figure 4.3)*, hereby referred to as “the case SIF”.

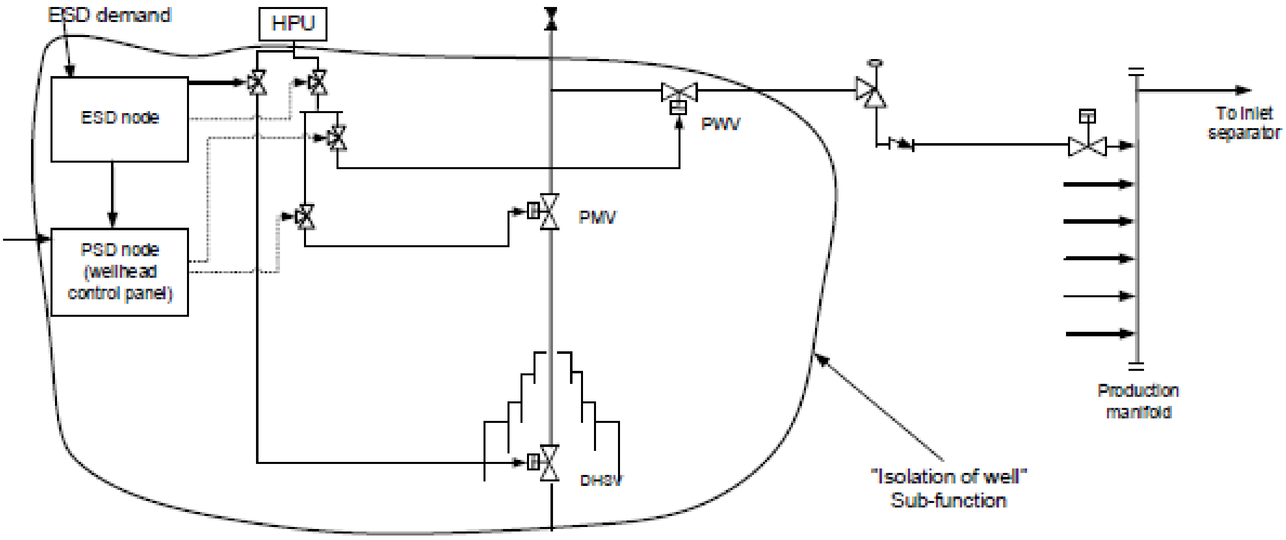
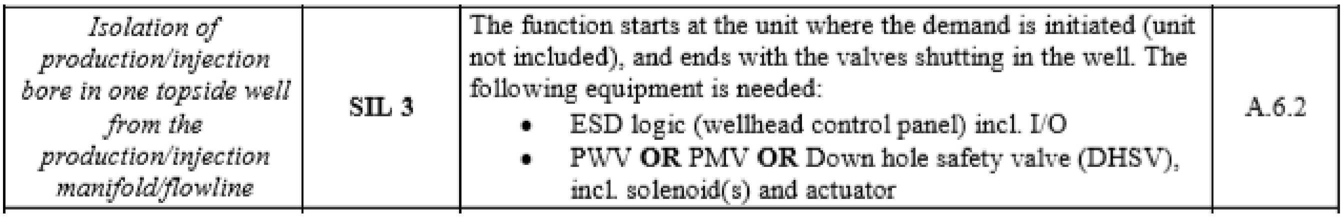


Figure 4.3: Definition of the SIF “Isolation of production bore in one topside well from the production manifold/flowline (ESD) [5],p. 89

The case SIF operates in an on – demand mode and has been given the minimum SIL requirement **SIL 3** (PFD$_{avg}$) in the NOG 070 guideline.

Table 4.1: Minimum SIL requirement to the SIF “Isolation of production bore in one topside well from the production manifold/flowline”



Isolation of production/injection bore in one topside well from the production/injection manifold/flowline	**SIL 3**	The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well. The following equipment is needed: • ESD logic (wellhead control panel) incl. I/O • PWV **OR** PMV **OR** Down hole safety valve (DHSV), incl. solenoid(s) and actuator	A.6.2

SIF FUNCTION:

As can be seen from *Table 4.1*, the function to be performed by the case SIF is to isolate the production bore in the topside well, starting at the unit where the demand is initiated and ending with the valves (PMV, PWV, DHSV) shutting in the well.

SIF SUBSYSTEMS:

The case SIF is comprised of the subsystems:

- **Logic solver:** ESD logic, with redundant I/O signal and redundant CPU
- **Final elements:** PMV, PWV and DHSV, including solenoids and actuators.

An overview of the subsystems' function, demand – and failure modes can be seen in *Table 4.2*

Table 4.2: Overview of subsystem functions, demand and failure modes.

Component	Location	Functionality	Demand Mode	Safe State[9]	Failed State
ESD Logic	Wellhead control panel	Shall limit energy supply by activating shut down functions. ESD logic **shall** provide correct output signal	On demand	Provides correct output signal	DU: Wrong input signal. DU: Logic not consistent with block logic drawings
DHSV	Wellbore	Prevent hydrocarbon or chemical flow up the production tubing. [6] **Shall** close within specified time. **Shall** keep tight and not leak according to specifications	On demand	Closed	DU: Fail to close on command or within specified time DU: Leakage in closed position above criteria SU: Fail to open SU: Spurious activation
PMV	X-mas tree	Shut in production tubing/annulus [39] **Shall** close within specified time. **Shall** keep tight and not leak according to specifications.	On demand	Closed	
PWV	X-mas tree	Control production/annulus flow [39] **Shall** close within specified time. **Shall** keep tight and not leak according to specifications.	On demand	Closed	

[9] All valves are hydraulically fail-safe, and will return to the safe state (closed position) upon a loss of hydraulic power [5]

The reason why the case SIF as specified in NOG 070 does not include an input element, is that there are several hazards (demands) that will cause the ESD to activate; that is, the ESD logic receives signals from several input elements on the installation *(Figure 4.4)*. Therefore, the specified case SIF begins with an activation of the ESD logic and ends with the valves shutting in the well.

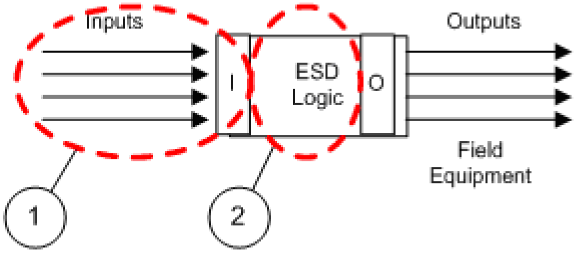


Figure 4.4: ESD logic receiving input signals from several input elements. Courtesy of COPNO

Relevant hazards (demands) that shall cause the ESD logic to activate the final elements, are:

- Unignited hydrocarbon leak
- Ignited hydrocarbon leak
- Riser leak causing fire/explosion
- Extreme weather conditions
- Security breach upon a terrorist attack

SIF RELIABILITY BLOCK DIAGRAM

The reliability block diagram of the SIF can be seen below in *Figure 4.5.* As can be seen from the RBD, only one out of three valves need to be closed to shut in the well. The number of valves that are closed upon activation of the ESD logic depends on the cause of the demand.

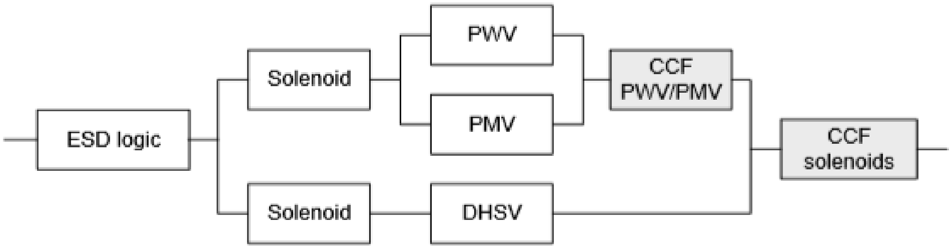


Figure 4.5: Reliability block diagram for the SIF "Isolation of one production bore "Isolation of production bore in one topside well" [5]

For example, if a demand is initiated due to gas detection (by an input gas detector not included in the case SIF), only the PMV and PWV is signalled to close, whereas upon a fire in the wellhead area the ESD logic will also signal the DHSV to close. However, the SIL requirement is given to the case SIF for the closure of all three valves (PMV, PWV and DHSV). Note that there is a potential for common cause failure between the PMV/PWV, and the solenoids for the PMV, PWV and DHSV, which is also taken into account in the RBD. [5]

ASSUMPTIONS

NOG 070, Appendix A.6 lists the following general assumptions for all isolation of topside well SIFs [5]:

- Response time is less than process safety time
- The state of the process will be defined by closure of the valves and isolation of well
- All closing valves are hydraulically fail-safe. Hence, the power sources will not be included in the quantification of this safety function
- The HPU pressure is monitored and loss of pressure and the HPU is therefore not included in the quantification
- ESD logic with redundant I/O and redundant CPU

4.2.2 Operating Environment

The Greater Ekofisk Area (GEA) is located in the southern North Sea, 300 km southwest of Stavanger. The sea depth in the area is 70 – 80 meters. There are several producing fields within the GEA *(Figure 4.6)*. Component operational data for the case SIF's final elements are collected from wells on installations producing from the Ekofisk (Mike, Zulu) and Eldfisk (Sierra) fields.

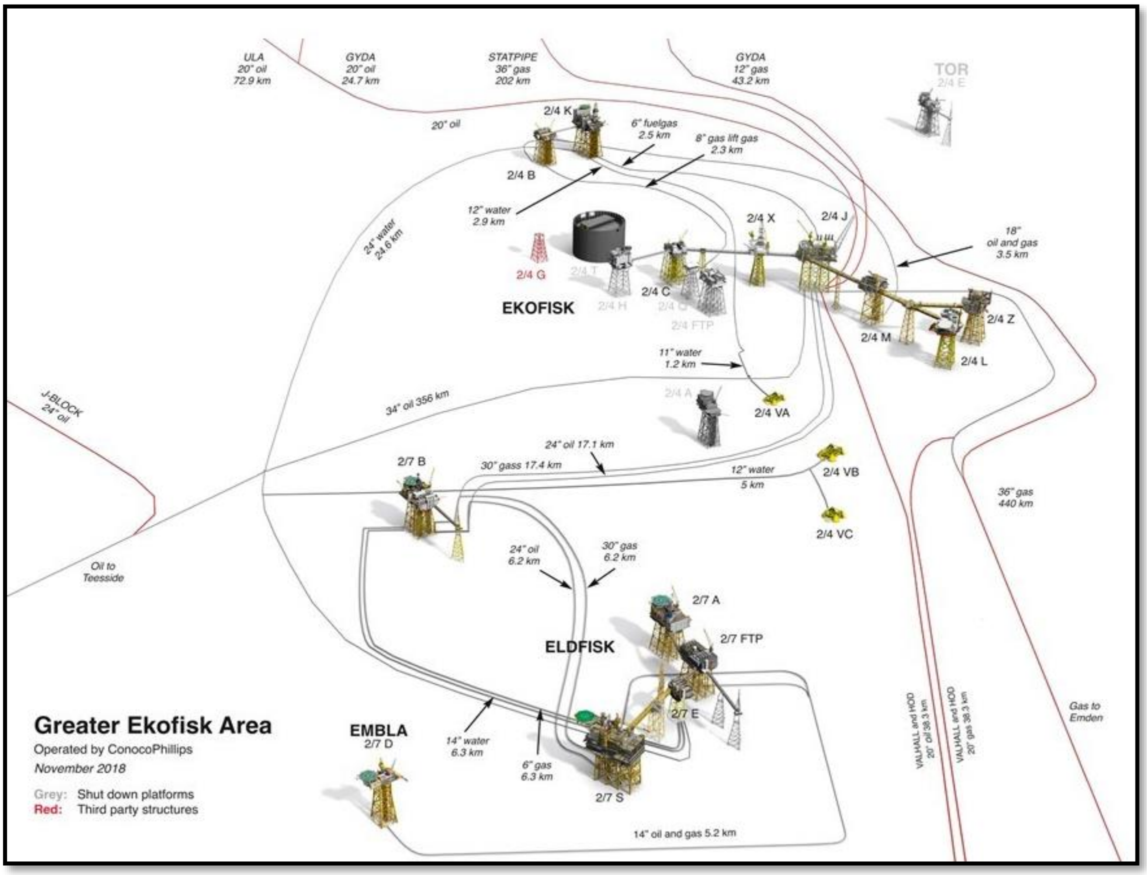


Figure 4.6: The Greater Ekofisk Area. [40]

The downhole pressure and temperature (P&T) and composition of produced fluids in the production wells will vary as a function of the reservoir fluids, and the depth and position of the production well. This gives rise to slight differences in operating environment for the components, such as one phase or two phase (oil and gas) flow, produced water, contents of sour (corrosive) substances and scale potential. These factors are dependent on the characteristics of the field the wells are producing from.

THE EKOFISK FIELD

The Ekofisk field was discovered in 1969 and started production in 1971, as the first field in Norwegian history. The reservoir is located at 3000m below sea level and produces both oil and gas. [41] The reservoir was initially produced with natural pressure depletion, but in 1987, pressure support by waterflooding was initiated to maintain high production rates. [42]

The Mike and Zulu installations included in this study are part of The Ekofisk Complex *(Figure 4.7)* on the central Ekofisk field [43]. Eko - Mike is a combined production and process installation and was installed in 2005. Eko - Zulu is a combined production and injection installation and was installed in 2013. Production wells on Mike produce mainly oil, whereas production wells on Zulu produce both oil and gas. [41]

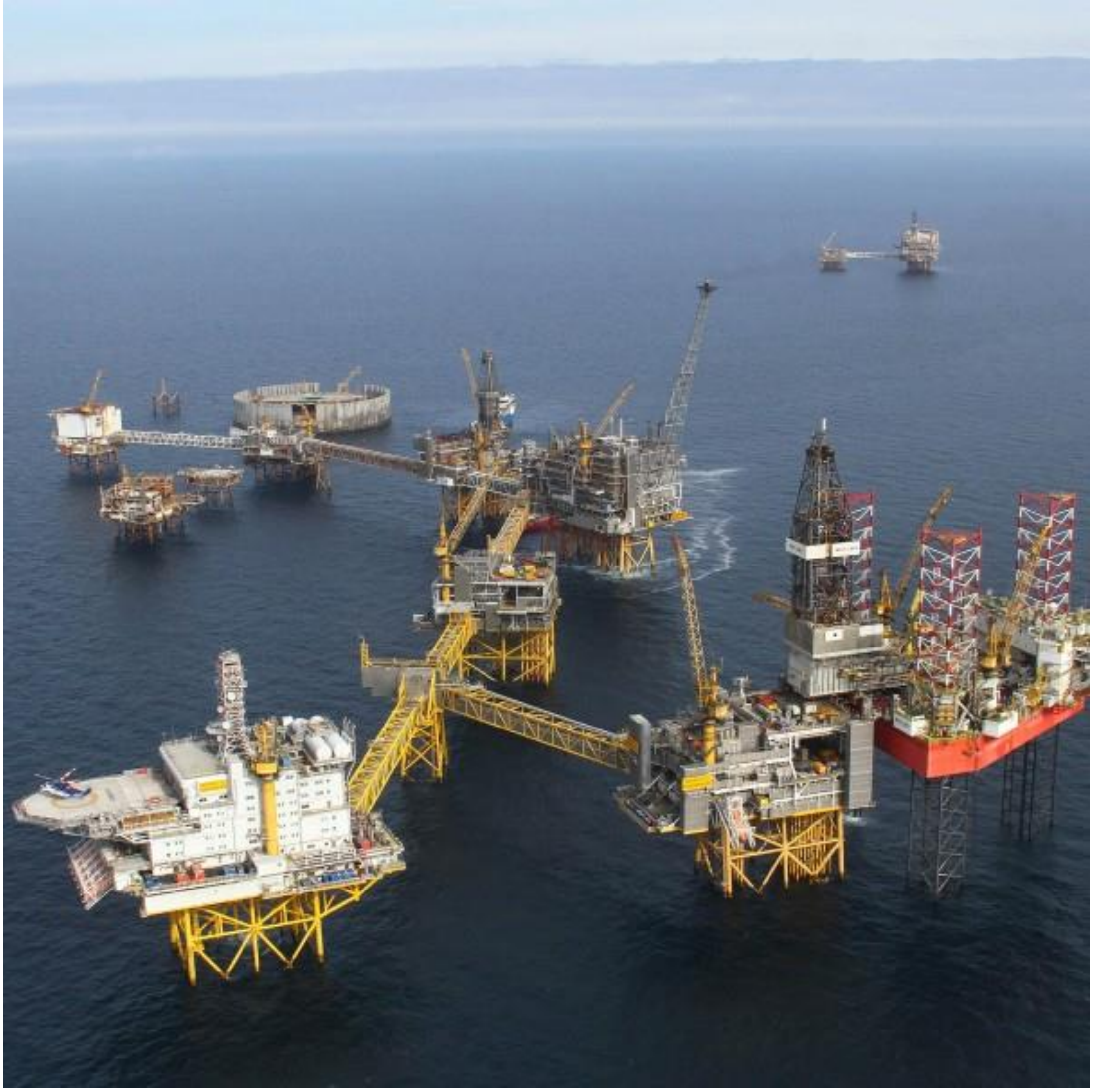


Figure 4.7: The Ekofisk Complex [40]

The downhole pressure and temperature in the Ekofisk field is within the approximate range 207 – 496 bar and 130ºC, which is considered normal P&T values.

THE ELDFISK FIELD

The Eldfisk field is located in the North Sea approximately 10km south of the Ekofisk field and entered into production in 1979. The reservoir is located at 2700 – 2900m below sea level and produces mainly oil. The reservoir was initially produced with natural pressure depletion before waterflooding was initiated in 1999. [44]

The Eld - Sierra installation included in this study is part of the Eldfisk Complex in the Eldfisk field *(Figure 4.8)*. The installation entered into production in 2015. [45] The wells on Sierra included in this study are oil production wells.

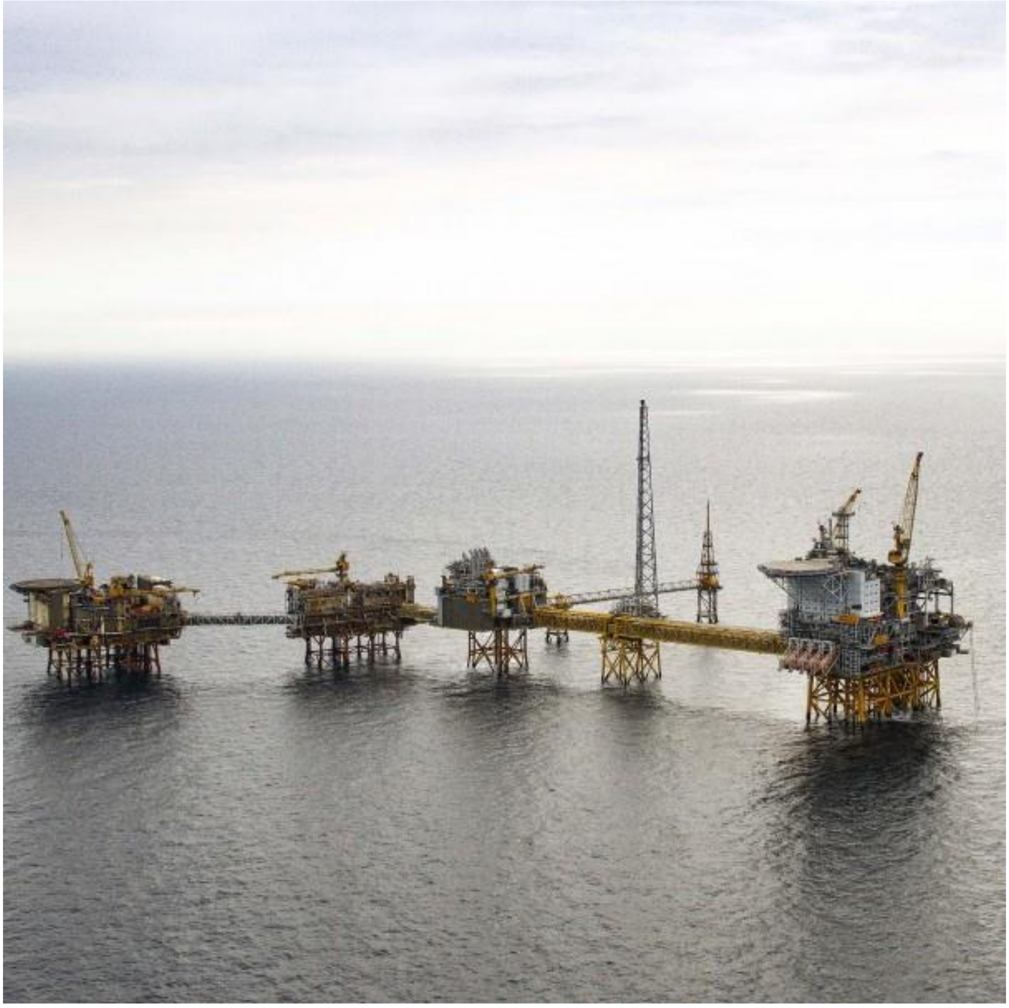


Figure 4.8: The Eldfisk Complex [40]

The downhole pressures at Eldfisk are slightly lower than in the Ekofisk field; approximately 172 – 462 bar, but the temperature is similar to the Ekofisk field.

Scale formation is a common problem in oil and gas production. As reservoir fluids move up the wellbore to the surface, pressure depletion and temperature changes in the well cause salts dissolved in the produced fluids, in particular water, to precipitate. This phenomenon is known as *scale*. As scale deposits on valves and other components in the well, it can affect their ability to function as intended, and high scale potential in wells is observed to shorten the lifetime of components. Issues with scale formation are observed in some wells on all three installations included in this study, but particularly on Eko - Mike due to early water break through from waterflooding.

Another factor that can affect the lifetime of components in wells, is the degree of souring in the produced fluids. Souring is related to the content of hydrogen sulphide and other acidic substances, and as these substances are corrosive, it can cause components in the well to degrade earlier in their lifetime. In recent years, increased souring has been observed in both the Ekofisk and Eldfisk fields. As these substances are water – soluble, the increase is related to the onset of water injection in these fields. The highest contents of hydrogen sulphide are registered in the wells where waterflooding is most mature. Although necessary actions are taken by COPNO to keep corrosion under control, this can be a performance influencing factor for components in the future.

Because water breakthrough also increases the likelihood of scale, it can be hypothesised that some wells are more prone to both scale and corrosive environments. For example, on Eko – Mike, where particular scale issues are reportedly experienced due to early water break through, the operating environment may also be particularly corrosive, which will cause components in these wells to be subject to an overall higher degree of wear and tear than in “good wells”, where these issues are not experienced.

5 CURRENT INTEGRITY REQUIREMENTS AND VERIFICATION OF WELL BARRIER (SIF) COMPONENTS

As was introduced in *Chapter 2.3.4*, there are three main performance requirements to well barriers: functionality, integrity and robustness. The focus of this thesis is limited to well barrier performance requirements and performance verification with respect to the integrity (reliability/availability) of well barriers. Based on the discussions in earlier sections of this thesis, it is noted that the case SIF and its final elements can be considered as well barrier elements.

In the context of well barrier integrity, there are two main sources referenced by PSAN: NORSOK D-010 [6] for well barrier elements, and IEC 61508/IEC61511/NOG 070 [3-5][10] for SISs. Although the PSAN specifically recommend the IEC61508/61511 standards and NOG 070 guideline to be used as a basis in the follow up of SIS on offshore installations *(Chapter 2.3.2/2.4.4/2.5)*, COPNO and other operators on the NCS follow the NORSOK D-010 standard for well integrity in the context of performance requirements and verification of SISs in wells.

This chapter will give an introduction to the current performance requirements and verification procedures for well barrier components (NORSOK D-010)/SIFs in wells (NOG 070) for the case SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)"

5.1 NORSOK D-010

The standard NORSOK D-010 Well integrity in drilling and well operations [6] defines requirements and guidelines to well integrity in drilling and well activities. According to NORSOK D-010 §8.7.1;

> *"all valves, available testable seals and lines which are part of the primary or secondary well barriers[11] shall have a maintenance program and be periodically tested to verify its function and integrity according to §15"*

[10] Through the remainder of this thesis, when referred to NORSOK D-010, the IEC standards and NOG 070, it is with reference to these sources.

[11] For elaborations on primary and secondary well barriers, reference is made to NORSOK D-010

5.1.1 Integrity Requirements

Requirements to the integrity of well barrier elements are provided in §8.7.1:

> *"If a safety critical valve type has a failure rate*[12] *on the installation which exceeds 2% within a 12-month period, measures shall be taken to improve the reliability of the valve type in general"*

5.1.2 Integrity Verification – Component Test Programmes

Verification and monitoring activities including minimum test frequencies are prescribed for the PMV, PWV and DHSV final elements in §15:

PMV/PWV[13]

- **Initial test and verification:** *The valves shall be tested with both low and high maximum differential pressure in the direction of flow. The low-pressure test shall be maximum 35 bar.*

- **Monitoring:**

  1) ***The automatic valves shall be tested at regular intervals as follows:***

- *Monthly, until three consecutive qualified tests have been performed; thereafter*
- *Every three months, until three consecutive tests have been performed; hereafter*
- *Every six months*

  2) ***The emergency shutdown function shall be tested yearly. It shall be verified acceptable shut down time and that the valve closes on signal.***

[12] In practice, the failure fraction (FF) is used: FF = number of failures/number of tests

[13] Reference is made to NORSOK D-010 §15, Table 33 – Surface tree

DHSV[14]

- **Initial test and verification:** *It shall be tested with both low and high differential pressure in the direction of flow. The low-pressure test shall be maximum 70bar*

- **Monitoring:**

1) ***The valve shall be leak tested at specified regular intervals as follows:***

- *Monthly, until three consecutive tests have been performed; thereafter*
- *Every three months, until three consecutive qualified tests have been performed; thereafter*
- *Every six months*

2) ***The emergency shutdown function shall be tested yearly. It shall be verified acceptable shut down time and that the valve closes on signal.***

It is noted that if a valve fails, the test procedure starts over again with one – month test intervals, extending to three and six months.

5.1.3 Updating Component Test Intervals

Considerations for updating the prescribed test intervals based on component reliabilities are provided in §8.7.1:

> *…The test frequency should be regulated based on:*
>
> *a) Experience data;*
>
> *b) Changes of the well flow composition increasing risk of deposits, scale, corrosion, erosion and high production and injection rates.*
>
> *The historic performance and reliability data used to justify a change in the test frequency shall be documented.*

[14] Reference is made to NORSOK D-010 §15, Table 8 – Downhole safety valve

5.2 NOG 070

The NOG 070 guideline [5] presents predefined performance requirements (minimum SIL requirements) to the integrity of specified global and local SIFs that are already required in standards adopted by the Norwegian Petroleum Sector. The minimum requirements have been set based on analysis of generic reliability data collected from the industry, e.g. provided in The PDS data handbook [33]. The calculated obtainable SIL for each SIF has been used as a basis for determining the minimum SIL requirement.

In the operational phase of an installation, it must be verified through maintenance and monitoring that the experienced SIL meets the required SIL for the SIF. According to the NOG 070 guideline, §10.5;

> *"The SIS shall be proof tested and maintained regularly during operation in order to ensure that the functional integrity is maintained... SIL classified safety functions and associated equipment shall be tested according to predefined proof test procedures scheduled in a PM programme as part of the maintenance system"*

5.2.1 SIL Requirements

Minimum SIL requirements to selected SIFs are presented in NOG 070 [5], §. 7.5. According to NOG 070, based on IEC 61508 and IEC 61511 [3, 4], there are three main requirement types that shall be fulfilled by a SIF implemented through SIS-technology in order to achieve a given SIL; a quantitative requirement to the SIFs reliability, and qualitative requirements to hardware fault tolerance and management of functional safety.

The requirement types are presented below in *Table 5.1* [5]:

Table 5.1: SIF requirements to achieve a given SIL [5]

Requirement type	Description
Quantitative reliability requirement (SIL)	• On – demand SIF: Average probability of failure on demand (PFD_{avg}) • Continuous/high – demand SIF: Probability of dangerous failure per hour (PFH)
Qualitative requirement	• Compliance with HFT to SIS subsystems
Management of functional safety (avoidance and control of systematic faults)	• Avoidance and control of systematic faults *(see. Chapter 2.3.1)* demonstrated through *prior use* of components: - Unchanged specification - 10 systems in different applications - > 100 000 operating hours *(preferably ~ 3.0 E06)* - > 1 year of service history OR - Evidence of suitability *(reference is made to NOG 070 [5], p.42)* - *FMEA*

Quantitative SIL requirements are set to the SIF in terms of average probability of failure on demand (PFD_{avg}) for on – demand SIFs, and probability of dangerous failure per hour (PFH) for continuous/high – demand SIFs (*Table 5.2).*

Table 5.2: Quantitative SIL requirements, adapted from [5]

Safety Integrity Level	On – Demand Mode (PFD_{avg})	Risk Reduction Factor[15]	Continuous/ High – Demand Mode (PFH)
4	$\geq 10^{-5}$ to $< 10^{-4}$	100 000 to 10 000	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	10 000 to 1000	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10	$\geq 10^{-6}$ to $< 10^{-5}$

[15] For the on – demand mode: Risk reduction factor = 1/PFDavg [26]

The quantitative requirement applies to the entire function; including the sensor, logic solver and final element. For each SIL, there is an associated requirement to the SIFs HFT *(Table 5.3)*.

Table 5.3: Minimum HFT requirements per SIL for SIFs implemented through route 2_H (documented prior use) [5]

SIL	Minimum required HFT
1 (any mode)	0
2 (on demand mode)	0
2 (high demand/continuous mode)	1
3 (high demand/continuous mode)	1
4 (any moed)	2

The requirements shall be understood such that if the SIF meets the quantitative SIL requirement, the SIF is not verified SIL unless the qualitative requirements to HFT and management of functional safety are also fulfilled. [5]

In addition, IEC 61508/IEC61511/NOG 070 also make recommendations to [5]:

- **The quality of failure rate data:** If sufficient data is available, it is recommended to use historical field data as a basis for calculations of the quantitative requirement. To evaluate whether field data is qualified for use in calculations, NOG 070 presents considerations to the data collection approach, detailing level and failure registration.

- **Independence between safety systems:** Measures shall be implemented to avoid adverse effects between SIS and non-SIS systems and applications, and between SIS nodes.

- **Documentation from the design phase:** All requirements, assumptions and prerequisites from the design phase that may affect the operation and maintenance of SISs should be transferred in a consistent and complete manner to operation.

- **Focus on deviation from the list of assumptions underbuilding the SIL requirements set to typical SIFs in NOG 070:** Assumptions are listed to design, process conditions etc. these must be met by the operator for the minimum SIL requirements to be applicable to identified SIFs on the installation.

5.2.2 SIL Verification

To verify SIL requirements during operation, NOG 070 §F.1 recommends the establishment of a performance target (success) criteria on component level:

> *"The number of registered DU failures during operation will be the main integrity performance indicator during operation. The associated integrity target criteria can be calculated from the generic DU failure rate, since in design this parameter is used to show that the predicted PFD$_{avg}$ meets the required PFD$_{avg}$."*

By establishing:

λ_{DU}: *Assumed (generic) DU failure rate from design*

t_n: *Total aggregated time in operation for a population of n comparable components during the observation period t*

The expected number of DU failures on component level becomes:

$$E(X) = n \cdot t \cdot \lambda_{DU} = \ t_n \cdot \lambda_{DU} \quad \mathbf{(5.1)}$$

In operation, the experienced number of DU failures per component type shall be compared with the integrity target criteria, and the following considerations apply [5]:

- If the number of DU failures is *on target*, the situation is acceptable but the possibility of removing the failure cause should still be considered (ALARP principle)
- If the number of DU failures is *below the target criteria* the situation is acceptable (ALARP), but less frequent proof testing may in some cases be considered
- If the number of DU failures is *above the target criteria* a failure analysis shall be performed, and compensating measures should be considered including the need for more frequent proof testing.

5.2.3 Updating Component Test Intervals

If operational experience proves that SIF subsystem components are significantly more or less reliable than what was assumed in the design phase, NOG 070 recommends that it should be considered to update the test intervals. For a method and considerations to update component test intervals, NOG 070 refers to the SINTEF PDS report "Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase"[16] [8]. In short, the method presented in the PDS report is as follows:

1) Calculate updated failure rates for dangerous undetected failures ($\hat{\lambda}_{\mathrm{DU}}$) based on operational experience, or by combining operational experience with generic failure rate data

2) Establish a 90% confidence interval for $\hat{\lambda}_{\mathrm{DU}}$

3) Based on the 90% confidence interval, the following criteria is proposed for updating the test intervals by comparing with the originally assumed (generic) rate of dangerous undetected failures (λ_{DU}):

- ***If $\hat{\lambda}_{DU}$is less than half λ_{DU} <u>and</u> the entire estimated 90% confidence interval for $\hat{\lambda}_{DU}$ is below λ_{DU}, then the functional test interval can be considered doubled***

- ***If $\hat{\lambda}_{DU}$ is more than twice λ_{DU} <u>and</u> the entire estimated 90% confidence interval for $\hat{\lambda}_{DU}$ is above λ_{DU}, then the functional test interval must be halved***

In addition, it is noted that qualitative evaluations on factors such as the quality, confidence and relevance in collected data, quality of testing, number of operational hours, types of failures, benefits and practicalities of changing the test intervals, recommendations by vendors, and secondary effects (e.g. entering the wear – out phase) of changing the test intervals should be considered.

Note that the recommended use of 90% confidence intervals for the DU failure rates here is a way of expressing the uncertainty in the DU failure rate estimate. That is, if the confidence

[16] This report will hereby be referred to as "the PDS report"

interval is wide, the uncertainty in the estimate is large. Because the estimated DU failure rate can provide poor predictions, the implicated concern of the authors of the PDS report seems to be that the $\mathrm{PFD}_{\mathrm{avg}}$ will unintentionally exceed the minimum SIL requirement by extending the test interval. Therefore, it is not recommended to extend the test interval unless the *entire* 90% confidence interval is below the assumed DU failure rate from design.

Because operational conditions will to a large extent influence the performance of SIS components, it is recommended by NOG 070 §8.5.3 and the PDS report §6 that updated failure rates should be based primarily on operational experience. However, a challenge with this can be that there is limited operational data available, such that the statistical confidence in $\hat{\lambda}_{DU}$ becomes poor. Therefore, if insufficient operational data is available, updated failure rates should be calculated by combining operational data and manufacturer data, as seen in *Figure 5.1* below.

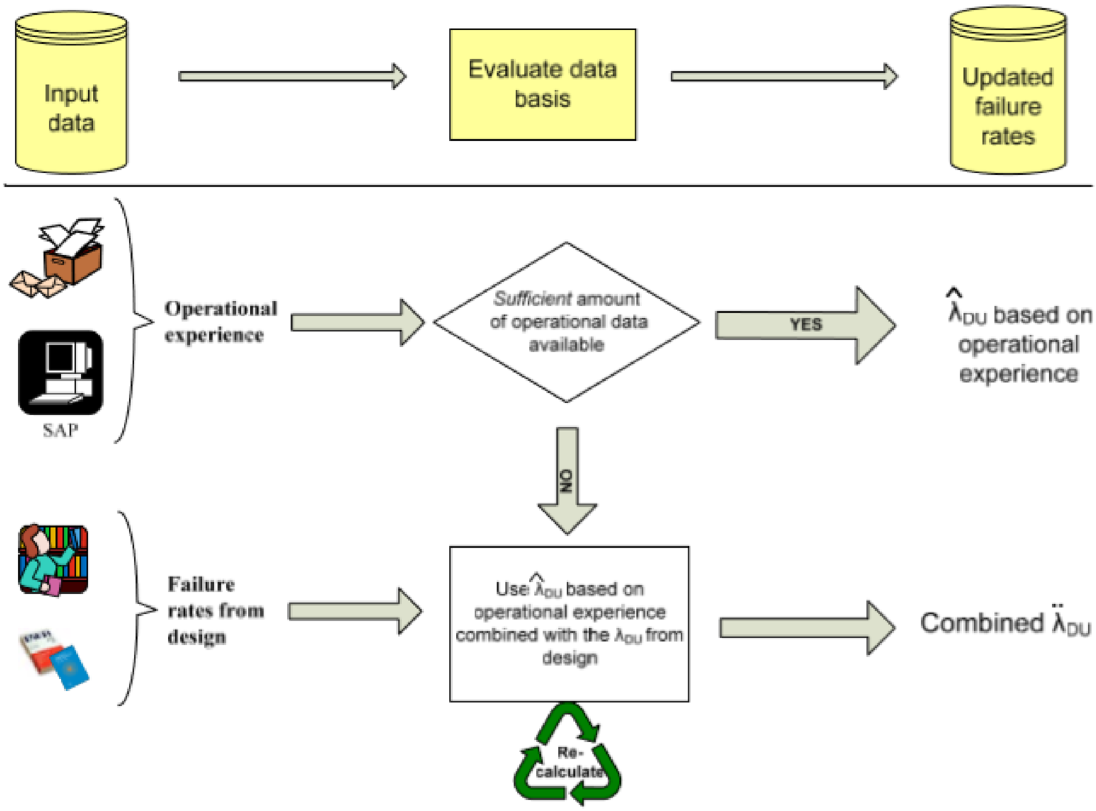
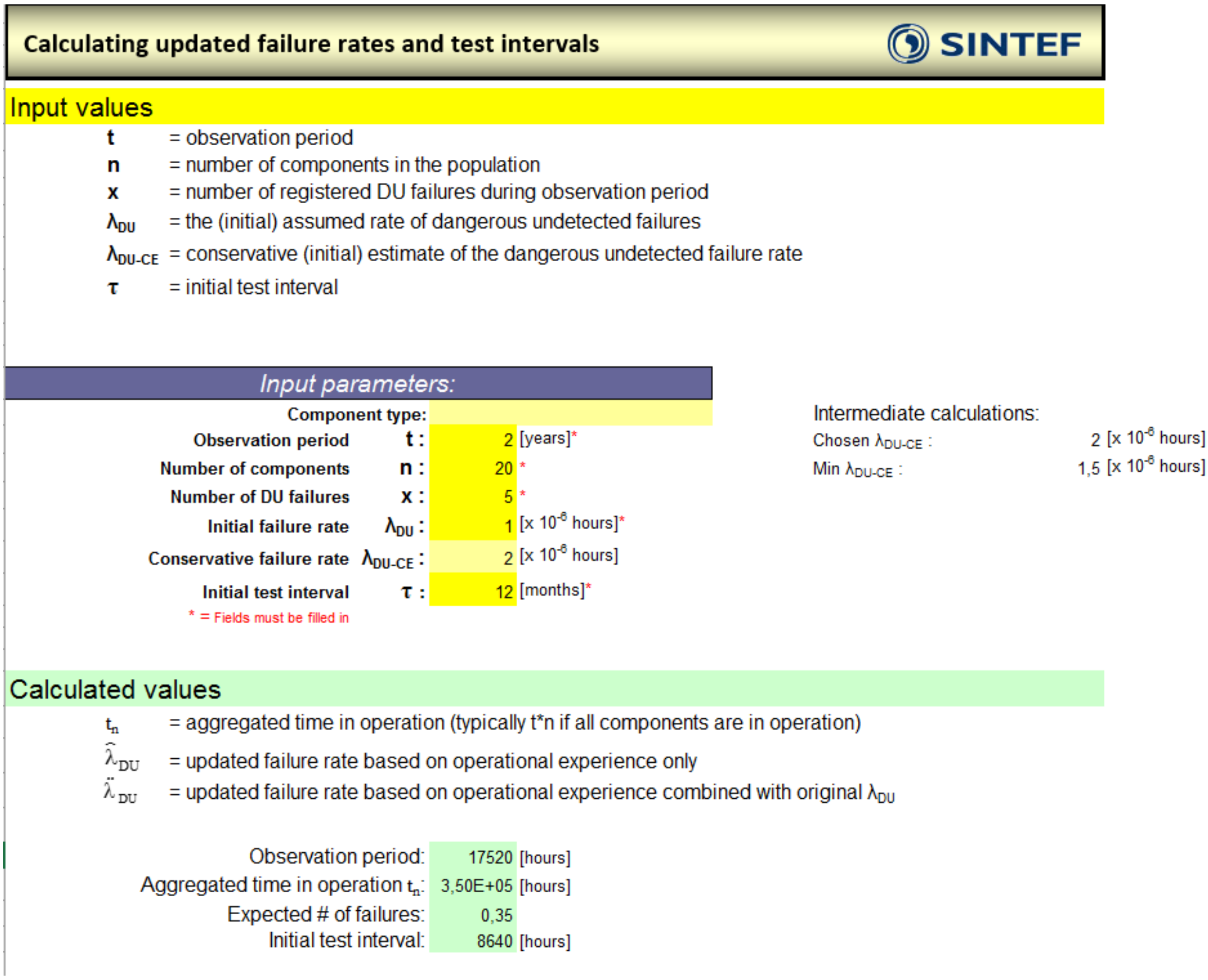

Input data
Evaluate data basis
Updated failure rates
Operational experience
SAP
Sufficient amount of operational data available
YES
$\hat{\lambda}_{DU}$ based on operational experience
NO
Failure rates from design
Use $\hat{\lambda}_{DU}$ based on operational experience combined with the λ_{DU} from design
Combined $\ddot{\lambda}_{DU}$
Re-calculate

Figure 5.1: Procedure for updating failure rates in the case of sufficient or insufficient operational data [8]

To simplify the suggested procedure for updating of component test intervals for end users, a MS-Excel spreadsheet model has been developed by SINTEF to accompany the PDS report.

The model *(Figure 5.2)* will evaluate whether sufficient operational data is available to calculate updated DU failure rates based solely on operational data, or if updated failure rates must be calculated by combining operational experience with λ_{DU} from design.

Based on input data, the model calculates updated DU failure rates using the appropriate method, and associated confidence intervals. Based on these values, the model concludes on whether the test interval should be doubled or halved.



Calculating updated failure rates and test intervals

Input values

t = observation period
n = number of components in the population
x = number of registered DU failures during observation period
λ_{DU} = the (initial) assumed rate of dangerous undetected failures
$\lambda_{DU\text{-}CE}$ = conservative (initial) estimate of the dangerous undetected failure rate
τ = initial test interval

Input parameters:

Component type:			
Observation period	**t :**	2	[years]*
Number of components	**n :**	20	*
Number of DU failures	**x :**	5	*
Initial failure rate	λ_{DU} **:**	1	[x 10^{-6} hours]*
Conservative failure rate	$\lambda_{DU\text{-}CE}$ **:**	2	[x 10^{-6} hours]
Initial test interval	**τ :**	12	[months]*

* = Fields must be filled in

Intermediate calculations:

Chosen $\lambda_{DU\text{-}CE}$:	2	[x 10^{-6} hours]
Min $\lambda_{DU\text{-}CE}$:	1,5	[x 10^{-6} hours]

Calculated values

t_n = aggregated time in operation (typically t*n if all components are in operation)
$\hat{\lambda}_{DU}$ = updated failure rate based on operational experience only
$\hat{\hat{\lambda}}_{DU}$ = updated failure rate based on operational experience combined with original λ_{DU}

Observation period:	17520	[hours]
Aggregated time in operation t_n:	3,50E+05	[hours]
Expected # of failures:	0,35	
Initial test interval:	8640	[hours]

Figure 5.2: MS – Excel spreadsheet model developed by SINTEF as an addition to the PDS report (screengrab)

5.3 Challenges and Discussion

The use of NORSOK D-010 is well established for operators on the NCS. However, the rationale underbuilding the frequency of the prescribed test intervals in NORSOK D-010 is questioned. One argument for the test frequency could be the lifetime characteristics of mechanical components. It is well known within the field of reliability that the lifetime characteristics of mechanical components such as valves tend to approximate a “bath tub curve”, with a high number of failures in the initial burn – in – phase, where weak components are weeded out *(“children’s diseases”)*. In such a case, it makes sense to test components frequently early in their operational life.

However, in practice, because components are tested at the manufacturer before they are distributed, and prior to start up at the installation, components with “children’s’ diseases” should have already been removed from the population of components that enters into operation, suggesting that the components put in operation have already entered their useful lifetime period where few failures are expected.

The latter argument is further reflected in the choice of availability model and assumed constant failure rate for calculation of the quantitative requirement in SIL verification according to the PDS method and NOG 070. There seems to be a theoretical mismatch on the assumed lifetime characteristics of well barrier components between NORSOK D-010 and NOG 070.

An assessed strength of the NOG 070 approach is that it sets requirements to the availability of the SIF at function level, rather than at component level. After all, for redundant SIFs, the main aspect of concern is not if *one component* is unavailable, but if the *function* is unavailable in a moment of demand. However, it is somewhat odd that although the SIL requirements are set at function level, the integrity performance indicators and integrity target criteria recommended to be monitored during operation is set at component level.

There has been some confusion within industry and academia as to the degree with which SIS components in wells should be understood and managed as a well barrier element, see for example [12]. The NOG 070 guideline was recently published in a revised edition, that clarifies the role of SIS, and safety instrumented functions realised by a SIS, as a (well) barrier element. This should also be apparent from the presented PSAN regulations and previous discussions in this thesis.

However, this confusion has raised the question of which standards and guidelines should be applied to SIS in wells, and how proof tests of SIS components in wells should be scheduled in the preventive maintenance programme. Hence, the recommended methods in the NOG 070 guideline has yet to be applied to the maintenance strategy for SIS in wells.

In addition, the recommended methods for SIL verification and updating of proof test intervals presented in NOG 070 and the associated PDS report has been criticised for not giving sufficient weight to the uncertainties of the analysis and its output results. Some contributions have been made within academia on how the methods for SIL verification and updating of proof test intervals according to NOG 070/the PDS report could be approved.

Abrahamsen and Røed [11] argues that the calculated PFD_{avg} should not be the only basis for verification of the quantitative SIL requirement, because the estimated PFD_{avg} is conditioned on assumptions and suppositions depending on the background knowledge. Seen as the background knowledge could be strong or weak, the uncertainties in the estimate can be large, but this is not reflected when the evaluation of SIL verification is restricted to probabilities. The authors therefore propose a semi – quantitative approach for SIL verification, where a qualitative assessment of uncertainties based on the SoK inspired by the work of Flage and Aven [35] is taken into consideration before a conclusion is made on the SIL. To evaluate the SoK, a workshop evaluation of performance influencing factors not predicted by the PFD_{avg} model is proposed prior to the decision of SIL verification, including human and operational aspects *(Figure 5.3):*

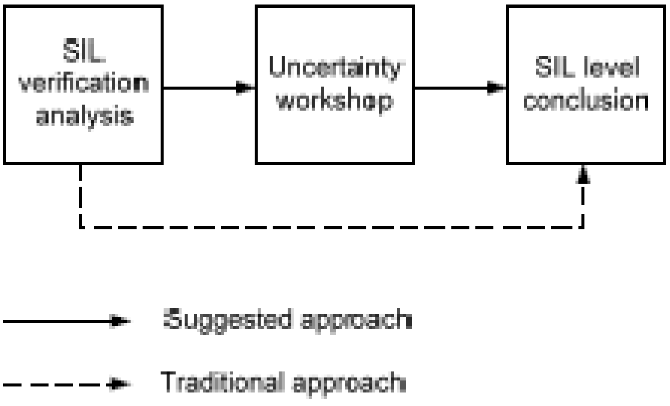


Figure 5.3: Suggested alternative approach to SIL verification by [11]

However, it is unclear how considerations of updating component test intervals should be performed by the operator based on this method; especially if it is decided to conclude on an alternative SIL than the calculated quantitative SIL based on operational data.

Sultana, S. [10] Uses a Monte Carlo simulation for uncertainty propagation in SIL verification based on the PDS method, and a semi – quantitative method where qualitative performance – influencing factors are identified and their impact on SIL uncertainty is quantified. This will provide a better overview to the decision maker of the uncertainties in the analysis and the implications for the results, and additional risk reducing measures can be applied if necessary. However, such approaches will likely be too resource demanding compared to the added value to be adopted by operators in practice.

Gelyani et.al. [12] Discuss whether the decision criteria for halving/doubling of test intervals for SIS proposed in the PDS report/NOG 070 is appropriate for well barriers. Firstly, this illustrates the confusion that has been present as to whether SIFs in wells should be considered a well barrier, and depending on that, whether they should be followed up according to NORSOK D-010 or NOG 070.

Second, the authors point to some issues in the method proposed by the PDS report/NOG 070. This includes that by using the failure rates as decision criteria, a danger is that attention is drawn away from the implications a change in the test interval will produce in the PFD_{avg}. Particularly, further analysis of data should be performed to evaluate whether some components are in “the grey zone”, close to the decision criteria. In addition, the method is not believed to include a proper handling of the assumptions made during the analysis, which is particularly critical to the decision of extending the test intervals. Uncertainties can be hidden in the assumptions. Following the same basic ideas as the PDS report, a slightly modified decision criteria is proposed for the doubling of test intervals based on the updated DU failure rate.

6 SUGGESTED APPROACH FOR OPTIMISATION OF TEST INTERVALS FOR WELL BARRIER (SIF) COMPONENTS

6.1 Motivation for the Suggested Approach

Prior to the commencement of this study, preliminary reliability analyses of well barrier components in production wells performed as part of the well barrier monitoring programme at COPNO has indicated high component reliabilities for the PMV, PWV and DHSV final elements of the SIF "“Isolation of production bore in one topside well from the production manifold/flowline (ESD)". This is in accordance with the general impression of professionals at COPNO in terms of high reliability of components that are part of the SISs in wells.

Survivability plots provided from the well integrity department at COPNO of the PMV, PWV and DHSV based on data collected from production wells on the Mike, Zulu and Sierra installations can be seen below in *Figure 6.1* and *Figure 6.2*. Note that in the plots, each DU failure has two datapoints to improve the graphics of the curve.

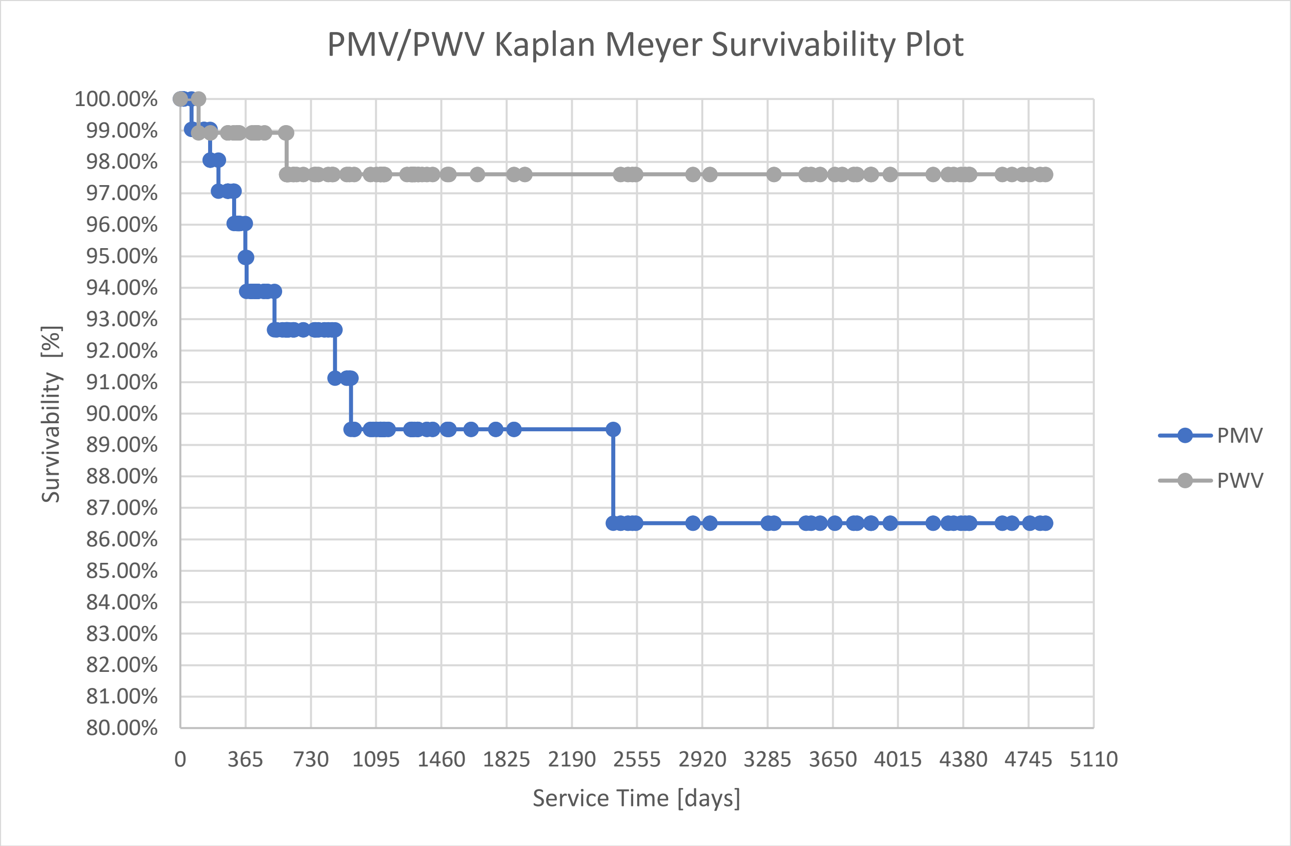


Figure 6.1 Kaplan Meyer Survivability plot of the PMV and PWV final elements of the SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)". Courtesy of COPNO

As can be seen from the survival plot in *Figure 6.1* above, the reliability of the PMV does not fall below 98% until after 214 days, whereas the PWV does not fall below 98% until after 589 days. Earlier and more frequent failures are experienced for the DHSVs, as seen in the survival plot below in *Figure 6.2*, but even for the DHSV, the reliability after six months is still at 80%. Note particularly the difference in the survival curves for the DHSV when scale wells are included and excluded from the input data.

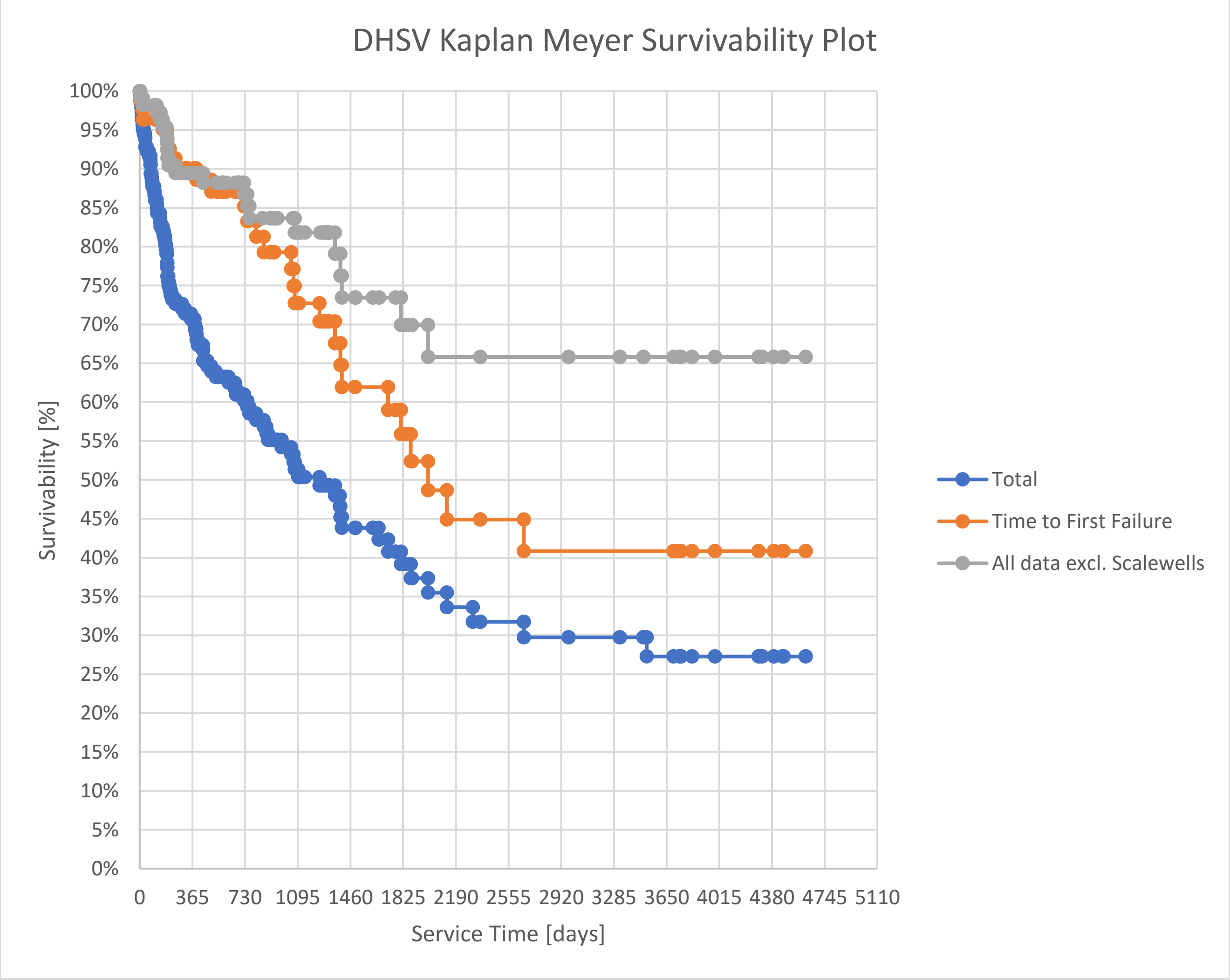


Figure 6.2: Kaplan Meyer survivability plot of the DHSV final element in the SIF "Isolation of production bore in one topside well from the production/manifold flowline (ESD)". Courtesy of COPNO

Therefore, the rationale for testing these components with 1 – month test intervals, extending to three and six months, is questioned based on demonstrated component reliabilities in operation. In addition, proof tests are highly time and resource demanding. It is therefore in the interest of COPNO to investigate whether it is feasible to extend the scheduled proof test intervals in the maintenance programme of well barrier components, including the PMV, PWV and DHSV.

From *Chapter 5.1*, it is clear that NORSOK D-010 opens up for extending component test intervals based on experience data, if it can be *justified* based on documented historical component performance and reliability data.

The question then becomes; what exactly *justifies* a change?

NORSOK D-010 does not provide any guidance on this matter. However, according to PSAN regulations, it is clear that follow – up of SIS and its components in wells should not be based on NORSOK D-010 as it is today, it should be based on the recommendations in IEC61508/61511/NOG 070. Hence, an obvious solution to this problem is to turn to the recommendations for determining proof test intervals based on demonstrated safety integrity performance presented in NOG 070 and the associated PDS report.

However, extending the proof test intervals is a major decision that should not be made without due consideration, and the methods for SIL verification and subsequent considerations for updating of proof test intervals recommended in NOG 070 has been criticised for not giving sufficient weight to uncertainties.

Some suggested modifications to the recommended methods in NOG 070 and the associated procedure for updating test intervals according to the PDS report were discussed in the previous section. Through discussions with professionals at COPNO, some additional remarks and rooms for improvement have been identified in this work:

- ***The PFD$_{avg}$ should be used as performance target indicator in SIL Verification:***
  The registered number of DU failures and failure rates at component level can be mathematically expressed as a function of the PFD$_{\text{avg}}$. Thus, they are equivalent to the PFD$_{\text{avg}}$ as performance target indicators for SIL verification and updating of component test intervals. However, it is a concern that by focusing on these indicators, attention is drawn away from the trend in the PFD$_{\text{avg}}$ for the SIF at function level. Hence, the analyst/decision maker might not notice that although the performance indicators are below the target criteria, the PFD$_{\text{avg}}$ of the SIF is moving dangerously close to the upper SIL limit.

It is therefore proposed that the PFD_{avg} for the SIF at function level should be used as performance target indicator relative to the SIFs minimum SIL requirement (performance target criteria).

- ***SIL Verification and updating of test intervals should be an integrated process:***
  NOG 070 presents SIL verification and updating of component test intervals as two related, but separated tasks. If the experienced SIL is above target, it can be *considered* to update the test intervals. Contributions are made within academia on how to better represent and assess the uncertainties in either a) SIL verification or b) updating test intervals. Yet, a key uncertainty of concern is the implications extending the proof test interval will have on the SIL at function level, and whether components close to the performance target criteria will exceed the criteria. This becomes less apparent when the two tasks are performed in separate processes.

  It is therefore proposed that quantitative SIL verification and considerations of updating component proof test intervals should be performed dynamically in the same process, based on the mathematical relation between the PFD_{avg} performance target indicator at function level and the length of the proof test interval (τ) of the final elements.

- ***Impractical considerations of halving and doubling test intervals:***
  The matter of interest is not whether the test intervals should be halved or could be doubled, but rather how long can the proof test interval be while still keeping the SIF within its SIL requirement with a sufficient degree of certainty.

  It is therefore proposed that the SIFs SIL should be assessed at different test interval lengths (τ) by assessing the SIFs PFD_{avg} as a function of τ.

- ***Care should be shown using strict decision criteria:***
  In practice, the persons to evaluate whether a SIF is verified SIL and whether or not the test interval for the SIFs subsystem components can be extended are likely not risk and reliability professionals, but well integrity engineers. If strict decision criteria are used, the calculations for SIL verification and updating of test intervals will likely be performed in a pre-developed MS - Excel spreadsheet model, such as the spreadsheet provided by SINTEF, yielding answers such as “SIF Within SIL? “Yes”;”No””, “The

test interval can be doubled" and so on. There is a hazard that such models will be used mechanistically, without further evaluations for example on whether the performance indicator is below the target with small or large margins.

It is therefore proposed that the remaining SIL margin for the PFD$_{avg}$ performance target indicator at function level to exceed the SIL performance target criteria should be made apparent to the analyst and decision maker.

- ***A qualitative assessment of uncertainties in the reliability/availability analysis should be provided along with the estimated PFD$_{avg}$ to the decision maker:***
  In the analysis and calculation process of estimating the PFD$_{avg}$ at different test interval lengths, there are several factors contributing to uncertainties in the data, parameter, model and completeness of the analysis. These are not believed to be properly expressed by the PFD$_{avg}$ and confidence intervals for DU failure rates, as recommended by NOG 070/the PDS report. Uncertainties can be hidden in the probabilistic estimates, as the strength of knowledge underbuilding the analysis can be strong or weak.

  It is therefore proposed that a qualitative assessment of uncertainties in the analysis based on the strength of the background knowledge should be performed and presented qualitatively alongside the PFD$_{avg}$ and remaining SIL margin, so that both can be evaluated before a decision is made on optimum test intervals. This means that the decision is based the semi – quantitative assessment of uncertainties (PFD$_{avg}$, SoK) in the estimated SIL at different test interval lengths

6.2 Suggested Approach for Determining Optimum Test Intervals

Based on the identified challenges and proposed measures for improvement in SIL verification and updating of component proof test intervals presented above, an integrated and dynamic approach to SIL verification and optimisation of proof test intervals, with added weight to uncertainties, is hereby suggested.

The suggested procedure has been developed based on the requirements, methods and recommendations in NOG 070 [5] and the PDS report [8] as a starting point, but modified according to the identified measures of improvement.

The suggested approach is comprised of the following parts:

- ***Part 1 - SIL Verification:***
  In the first step of the analysis, it should be verified using the PFD_{avg} as performance target indicator whether the SIF meets the predefined SIL requirement (indicator target criteria) based on operational data. It must be checked whether there is sufficient operational data available, and that the qualitative and quantitative requirements for SIL verification in NOG 070 are met.

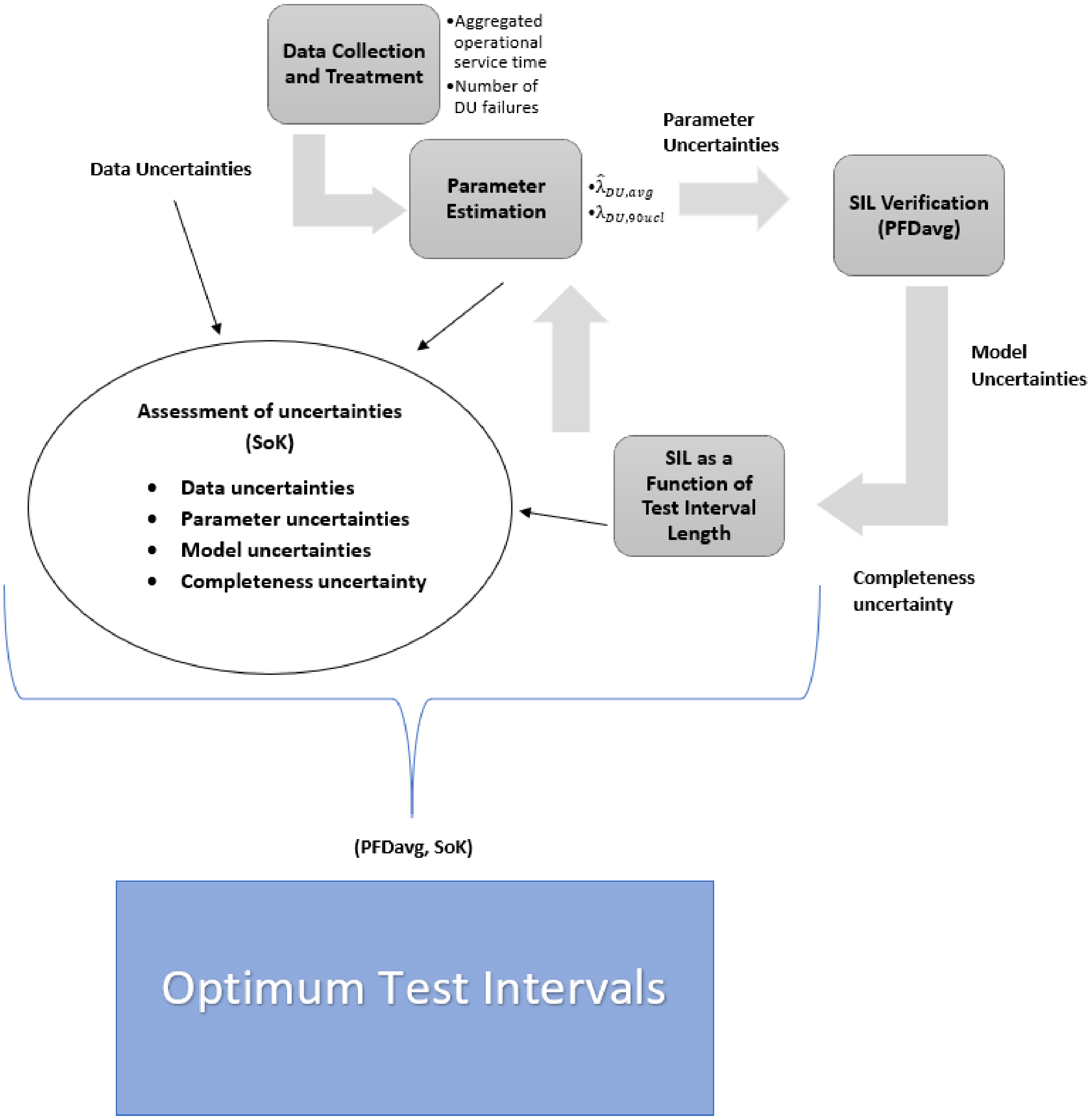
- ***Part 2 – SIL as a Function of Test Interval Length:***
  Having verified whether the SIF meets the SIL requirement in operation or not, the effect on the SIL (PFD_{avg}) at function level by changing the input value for the test interval length (τ) with different values in the calculation model can be analysed and provided for comparison to the decision maker in the context of updating test intervals for SIF subsystem components.

- ***Part 3 - Assessment of Uncertainties:***
  The strength of the background knowledge supporting the different stages of the reliability analysis (PFD_{avg} calculation) and its results should be qualitatively evaluated, as this reflects the uncertainty in the estimated PFD_{avg}. To support this part of the procedure, a checklist has been developed to evaluate the strength of knowledge (uncertainty) in the data, parameters, model and completeness of the analysis. The results should be presented alongside the calculated PFD_{avg} and remaining SIL margin to provide broad decision support.

- ***Part 4 – Optimisation of Test Intervals:***
  A framework has been developed to guide the decision maker in identifying optimum test intervals in light of uncertainty, taking both the SIL (PFD_{avg}) as a function of test interval length and the SoK supporting the analysis result (PFD_{avg}) into account. This means a semi – quantitative assessment of uncertainties in the SIFs calculated SIL as a function of test interval length in the form (PFD_{avg}, SoK).

7 CASE ANALYSIS AND RESULTS

In this chapter, the suggested approach for integrated SIL verification optimisation of test intervals for well barrier (SIF) components will be applied to the case SIF *"Isolation of production bore in one topside well from the production manifold/flowline (ESD)"*. The analysis and analysis results using the suggested approach will be presented and discussed. A simplified flowchart of the procedure is presented below in *Figure 7.1*.



Data Collection and Treatment
•Aggregated operational service time
•Number of DU failures
Data Uncertainties
Parameter Estimation
•$\hat{\lambda}_{DU,avg}$
•$\lambda_{DU,90ucl}$
Parameter Uncertainties
SIL Verification (PFDavg)
Model Uncertainties
Assessment of uncertainties (SoK)
• Data uncertainties
• Parameter uncertainties
• Model uncertainties
• Completeness uncertainty
SIL as a Function of Test Interval Length
Completeness uncertainty
(PFDavg, SoK)
Optimum Test Intervals

Figure 7.1: Suggested approach for optimisation of test intervals for SIS subsystem components in wells, inspired by NOG 070.

7.1 Hypotheses

The main hypotheses underbuilding the current work are:

- Based on high component reliabilities, the proof test intervals for SIS components in wells can be extended beyond the initial 1- month test intervals in NORSOK D-010 while still maintaining the SIF within its required SIL (acceptable levels of risk)
- SIL verification and determination of optimum test intervals performed in an integrated process using the PFD_{avg} as integrity performance indicator is a more practical approach to monitor that an extension of proof test intervals does not cause the SIF to exceed the minimum SIL requirement
- There are sources of uncertainty in the reliability/availability analysis of SIL (PFD_{avg}) that are not properly reflected by todays approach (NOG 070/The PDS report) prior to updating test intervals for SIS components in wells.

7.2 Part 1: SIL Verification

For all wells included in the analysis, the case SIF has been certified ***SIL 3*** from the design and engineering phase by COPNO. The minimum SIL requirements, guidelines and recommendations in NOG 070 are therefore confirmed applicable to the case SIF. In the first part of the procedure, it must be verified from operational data that the case SIF in operation meets the minimum SIL requirements laid down in design. Therefore, this part of the analysis begins with the process of data collection and treatment *(Chapter 7.2.1)* and parameter estimation *(Chapter 7.2.2),* before an evaluation is made on whether the SIF meets the qualitative SIL requirements *(Chapter 7.2.3).* Thereafter, the obtained SIL is calculated from operational data for the case SIF to verify the quantitative SIL requirement *(Chapter 7.2.4).*

7.2.1 Data Collection and Treatment

A MS-Excel workbook containing lifetime and test data of the PMV, PWV and DHSV components[17] was provided from the Well Integrity department at COPNO. The data was collected from SAP for the PMV and PWV from a total of 89 wells and DHSV from a total of 91 wells from three installations of different age located in the Greater Ekofisk Area.

[17] The PMV, PWV and DHSV of the case SIF will hereby be referred to as the "components"

For each field, platform and wellbore the workbook included columns on:

- Component types (PMV, PWV, DHSV)
- Vendor
- Date drilled
- Component installation day[18]
- Component failure date/service time end[19]
- Last good test date[20]
- Component service time [days]
- Registered failure
- Failure Cause
- Failure repair/removal
- Scale related? Yes/no

The dataset was cleaned and prepared for analysis by professionals in the Well Integrity department at COPNO before it was provided to the analyst (author) of the current work. The data was further controlled by the author to make sure dates, failure reporting and calculated service times were correct. Some errors were detected, and the workbook was updated and further cleaned by Well Integrity before it was controlled again by the analyst prior to further analysis of the data.

NOG 070 §8.5.3 provides recommendations for data collection and detailing level of the collected data. Based on the collection approach and detailing level in the provided workbook and following quality treatment by Well Integrity and the analyst, these are assessed to be complied with in the current analysis.

[18] Marks the start of component operational lifetime

[19] Marks the end of the component operational lifetime (DU failure)

[20] Marks the end of the component operational lifetime (censored data point)

OBSERVATION PERIOD

The wells included in the analysis were drilled between the period of 2004 – 2018. Components were installed and put in operation between 2005 – 2018. Test data is recorded from 2005 until 31.12.2018. The observation period is approximately 13.5 years.

CENSORING

Data is collected from wells on three installations of different age. During the observation period, new wells have been drilled and components have been installed in new wells. In addition, some components have been replaced by new components within the observation period. It is thus not the case that all components in the analysis were installed and put in operation at the same time (t=0) and have been observed for 13.5 years; components are installed and replaced at different points in time. At the end of the observation period, the last measurement point is the last good test date (censored datapoint). Hence, the data set is multiple censored.

The time spread of the first component installation dates in wells can be seen below in *Figure 7.2* and *Figure 7.3*

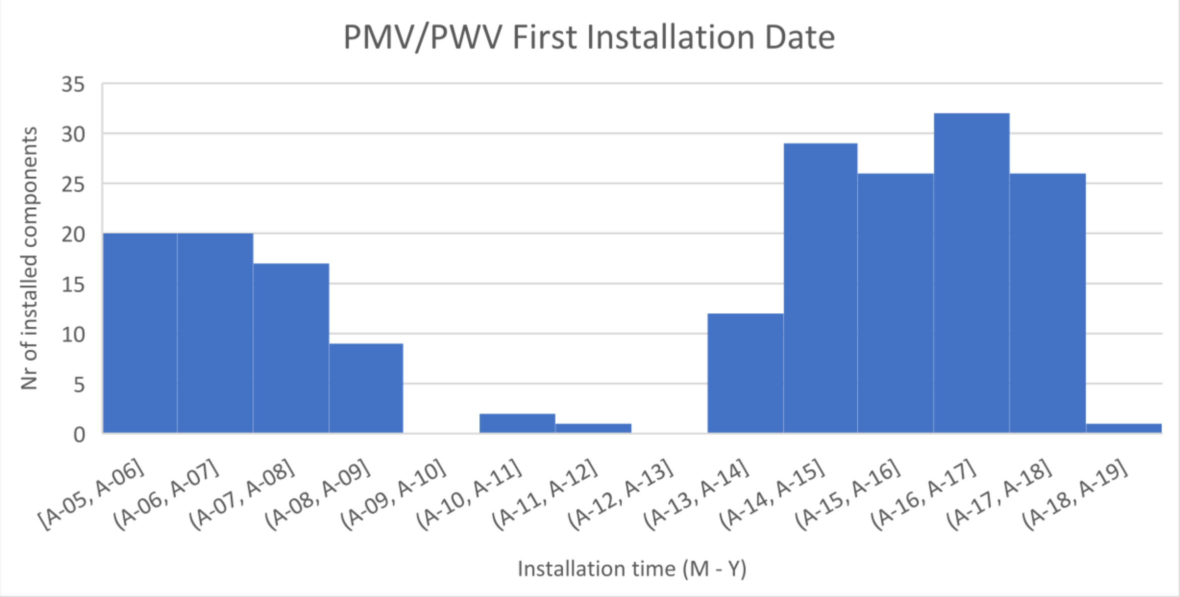


Figure 7.2: PMV and PWV installation dates

It is tempting to relate the shape of the spread in installation dates to approximate a reliability bathtub curve and suspect that the installation pattern is reflective of component failure patterns (because of replacement). However, few failures are experienced for the components during the observation period; most components have not failed since they were first installed and put in operation. The histograms show the installation of the first component in a well (e.g., the first DHSV installed in a newly drilled well), not replaced components. The pattern therefore rather reflects the point in time the wells were drilled and X-mas trees/components were installed in wells.

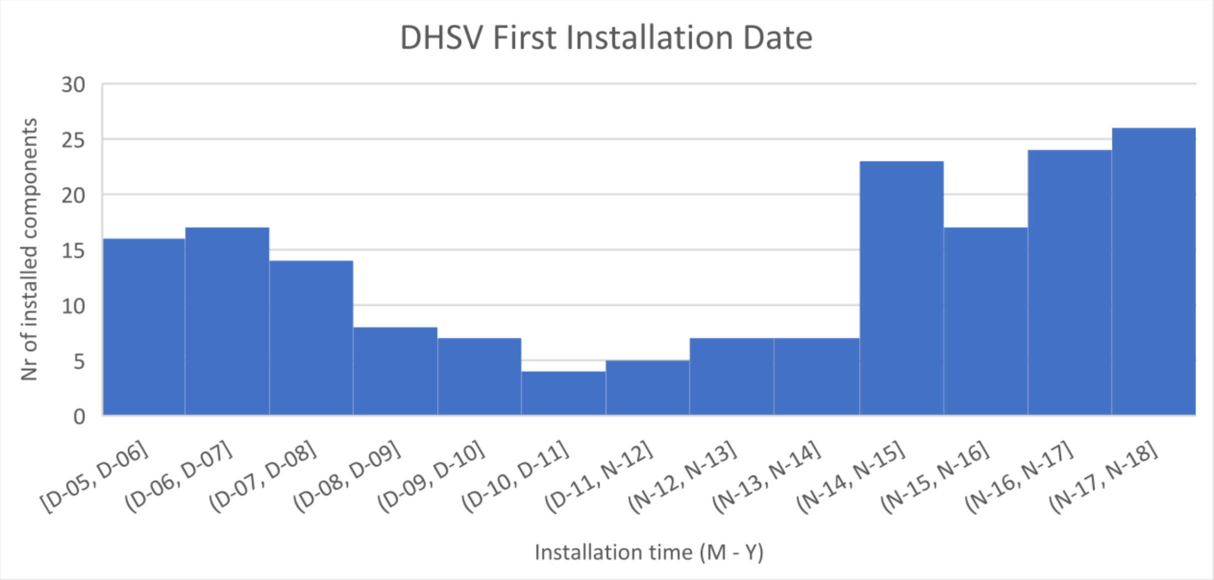


Figure 7.3: DHSV installation dates (first installation, no replacements)

The important point is that a bulk of the components in the data set were installed a long time ago, whereas another bulk are of newer date. This means that not just are a bulk of the components older, but the wells are too. Hence, some of the components in the dataset are old components in old wells, and some are newer components in newer wells.

In general, there is likely a slightly different operating environment between older and newer wells due to factors such as pressure depletion and water break-through, leading to a more corrosive environment and potential for scale issues.

OPERATIONAL SERVICE TIME

From *Chapter 5.2.2*, it is recalled that:

$$t_n: total\ aggregated\ time\ in\ operation\ for\ a\ population\ of\ n\ comparable\ components\ during\ the\ observation\ period\ t$$

The total aggregated time in operation for the PMV, PWV and DHSV is found for the populations of comparable components by summing the registered component service time per component across all wells in a MS-Excel pivot table. The obtained total aggregated operational service time per component type can be seen below in *Table 7.1*.

Table 7.1: Aggregated operational service time per component type

	Aggregated operational service time (t_n) [days]	**Aggregated operational service time (t_n) [hrs]**
PMV	170 106	4 082 544
PWV	170 501	4 092 024
DHSV	165 439	3 970 536

NUMBER OF DU FAILURES

During the total observation period, the following number of DU component failures are registered:

- **PMV:** 9
- **PWV:** 2
- **DHSV:** 88

The registered number of DU failures for the DHSV compared to the PMV and PWV is striking. However, it is generally expected to be more operational problems and failures for the DHSV than valves further up the well, because DHSVs are subject to much harsher environments, with high pressures and temperatures, and abrupt pressure/temperature drops. These factors also increase the likelihood of well problems such as scale formation, which is generally a bigger problem for components further down the well than components higher up.

7.2.2 Parameter Estimation

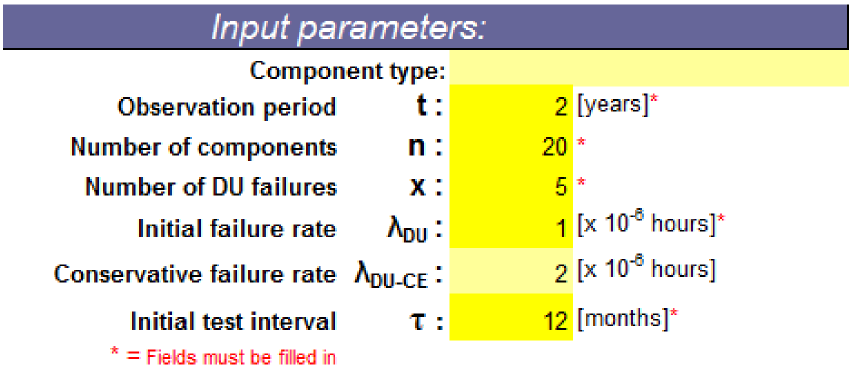
The calculation model for availability (PFD_{avg}) of on – demand SIFs was presented in *Chapter 2.6.4*. From the model, there are two input parameters that must be known:

- The updated rate of DU failures ($\hat{\lambda}_{DU}$)
- The length of proof test intervals (τ)

Of which the updated DU failure rate parameter must be estimated from operational data. As was discussed in *Chapter 5.2.3*, the estimation of the updated failure rate $\hat{\lambda}_{DU}$ should preferably be based solely on operational data, if sufficient amounts of operational data are available that the confidence in the updated failure rate estimate equals the confidence in the original failure rate estimate from design. This has been found to be appropriate when the aggregated operational service time of the component multiplied with the number of failures exceeds $3{,}0 \cdot 10^6$ hours. [8] Hence, in the case of only one observed failure, $3{,}0 \cdot 10^6$ hours of operational service time is required, and less if more failures are observed. Otherwise, an updated failure rate must be calculated by combining operational and manufacturer data.

UPDATING FAILURE RATES USING PRE-DEVELOPED EXCEL CALCULATION FILE (SINTEF)

To make this evaluation, the MS-Excel model for updating of failure rates and doubling/halving of test intervals prepared by SINTEF, as briefly discussed in *Chapter 5.2.3*, could have been used, with the added value of also automatically calculating updated failure rates, associated confidence intervals and making recommendations on whether the test interval can be doubled. However, an immediate challenge was discovered with this approach because the required input parameters *(Figure 7.4)* did not combine with the collected operational data in practice.



Input parameters:

Component type:			
Observation period	t :	2	[years]*
Number of components	n :	20	*
Number of DU failures	x :	5	*
Initial failure rate	λ_{DU} :	1	[x 10^{-6} hours]*
Conservative failure rate	$\lambda_{DU\text{-}CE}$:	2	[x 10^{-6} hours]
Initial test interval	τ :	12	[months]*

* = Fields must be filled in

Figure 7.4: Required input parameters to SINTEF calculation model for updated failure rates and test intervals (screengrab)

Here, the required input parameters are the observation period *(t)*, the number of components in the population of comparable units *(n)*, the number of observed DU failures *(x)* and the initial failure rate assumed from design (λ_{DU}). The amount of operational experience is then calculated by *Eq. 7.1* [8]:

$$Operational\ experience = \quad t \cdot n \cdot x \quad (\mathbf{7.1})$$

Further, if it is concluded that sufficient operational experience is achieved, the updated failure rate based solely on operational experience is calculated by *Eq. 7.2* [8]:

$$\hat{\lambda}_{DU,SINTEF} = \frac{x}{t \cdot n} \quad (\mathbf{7.2})$$

Hence, it is assumed that all *n* components are put in operation simultaneously at *t*=0, and observed during the time period *t*. Because the collected data is multiple censored, with components put in operation and withdrawn from operation at different times throughout the time period, these formulas cannot be used. Therefore, it is concluded that this predeveloped calculation file is not necessarily as easily adopted by end users (operators) in practice as intended.

PREFERRED METHOD FOR CALCULATION OF UPDATED FAILURE RATES

Because of this, the preferred method for updating failure rates in this analysis was to use the general formula for calculation of DU failure rates in the case of sufficient operational experience according to the PDS report [8] *(Eq. 7.3)*:

$$\hat{\lambda}_{DU} = \frac{Number\ of\ DU\ failures}{t_n} \quad (\mathbf{7.3})$$

This is appropriate in the current case analysis, as in reference to *Chapter 7.2.1*, the number of DU failures and aggregated operational service time per component (t_n) yields well above 3,0 $\cdot 10^6$ hours of operational experience for the PMV, PWV and DHSV. Had it not been the case, operational data must have been combined with the a priori DU failure rate, e.g. based on generic or manufacturer data. Reference is made to the PDS report.

Based on *Eq. 7.3* and the registered number of DU failures and data presented in *Table 7.1* in *Chapter 7.2.1*, the DU failure rate estimate ($\hat{\lambda}_{DU}$) was calculated for the PMV, PWV and DHSV, see *Table 7.2*. According to NOG 070, p. 46; IEC 61511 states that data uncertainties shall be assessed and contributed for in the calculation of failure rate estimates. To obtain a conservative point estimate, IEC 61511 recommends using an upper bound 70% confidence interval for the failure rate. However, NOG 070 argues that provided all relevant failure modes and failure causes that can occur during operation has been included in the underlying field experience data, it is sufficient to apply average figures to the analysis. However, a confidence interval (70% or 90%) should be provided to reflect the uncertainties in the point estimate and the amount of operating experience underlying this estimate. [5]

Consequently, in line with the PDS report, a 90% confidence interval for the rate of DU failures ($\hat{\lambda}_{DU}$) was calculated according to Rausand and Høyland [28]:

$$\left(\frac{1}{2t_n} z_{0.95,2x}, \frac{1}{2t_n} z_{0.05,2(x-1)}\right) \quad \mathbf{(7.4)}$$

Where $Z_{0.95,\,v}$ and $Z_{0.05,\,v}$ denotes the upper 95% and 5% percentiles for the χ^2 distribution with v degrees of freedom, respectively. [8] The average rate of DU failures ($\hat{\lambda}_{DU,avg}$) per component, and the lower and upper 90% confidence interval point estimates of component DU failure rates ($\hat{\lambda}_{\mathrm{DU,L90}}$, $\hat{\lambda}_{\mathrm{DU,U90}}$), hereby referred to as the L90/U90 DU failure rates, are summarized in *Table 7.2* below.

Table 7.2: Average DU failure rates, lower and upper 90% confidence interval point estimates

Component	**Lower 90% confidence estimate [hrs^{-1}] ($\hat{\lambda}_{DU,L90}$)**	**Average estimate [hrs^{-1}] ($\hat{\lambda}_{DU,avg}$)**	**Upper 90% confidence estimate [hrs^{-1}] ($\hat{\lambda}_{DU,U90}$)**
PWV	8.68E-08	4.89E-07	1.55E-06
PMV	1.15E-06	2.20E-06	3.85E-06
DHSV	1.84E-05	2.22E-05	2.62E-05

A graph illustrating the scale and width of the 90% confidence intervals of $\hat{\lambda}_{\mathrm{DU}}$ per component was created and can be seen below in *Figure 7.5*. As expected, given the registered number of

DU failures as presented in *Chapter 7.2.1*, the failure rate of the DHSV is the highest, followed by the PMV and PWV. The higher number of failures (data points) also results in a narrower confidence interval, which means that the uncertainty in the estimate is lower. The DU failure rate estimate of the PWV, where only two failures were observed, is however less certain, and surprises are more likely to occur relative to the average estimate $\hat{\lambda}_{\text{DU,avg}}$.

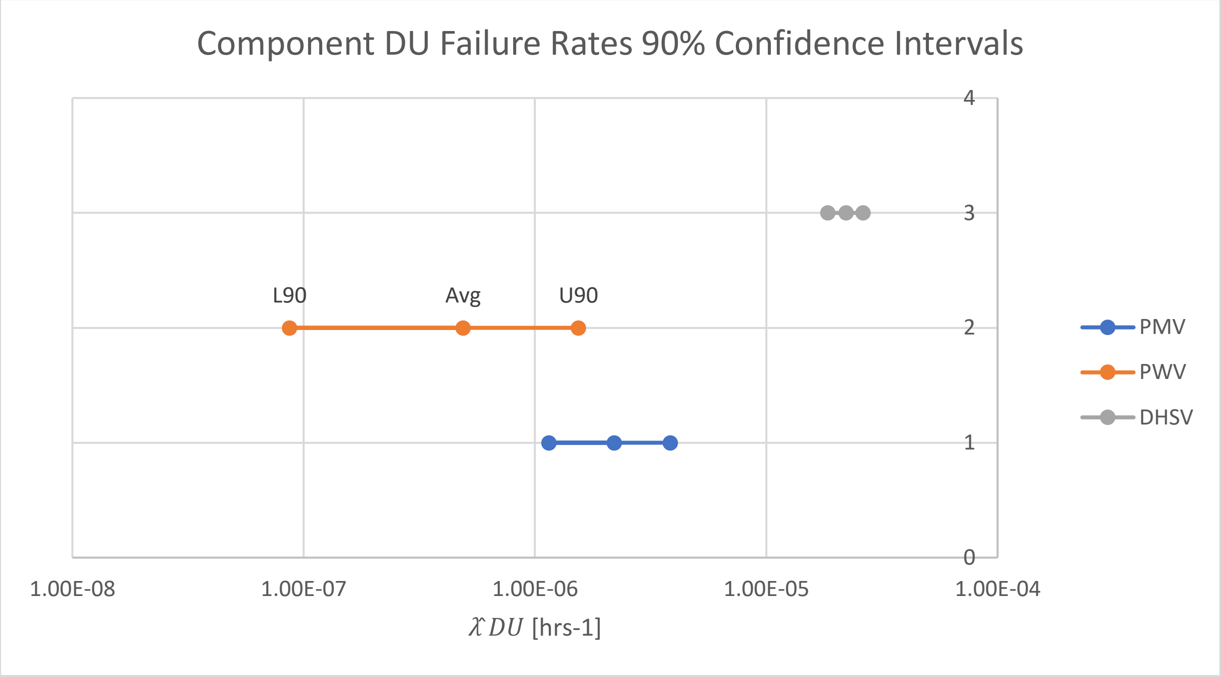


Figure 7.5: The width of the 90% confidence intervals for the PMV, PWV and DHSV DU failure rate estimates. The point estimates corresponding to the lower 90%, average and upper 90% point estimates is illustrated for the PWV.

This is generally a challenge when analysing highly reliable components; the occurrence of few failures (lack of data) makes it more difficult to produce parameter estimates with high statistical confidence. However, considering the large amount of operational service time for the components in this case, the confidence in the estimates is regarded as reasonable. It is noted that the PWV, which has the least registered number of DU failures (2), also has the most hours of operational service time (4 092 024 hrs); thus, the number of DU failures multiplied with the aggregated operational service time exceeds $8{,}0\cdot10^{6}$, which is well above the recommended minimum of $3{,}0 \cdot 10^{6}$ hrs of operational experience. An important conclusion from the observed failure rate confidence intervals, is that the reliability of the PMV and PWV is significantly better than the DHSV.

7.2.3 Verification of Qualitative SIL Requirements

The case SIF cannot be verified SIL 3 unless it can demonstrate compliance to both the qualitative and quantitative SIL requirements. A table summarizing the quantitative and qualitative requirements was presented in *Chapter 5.2.1*. Based on the collected data and previous discussions in the analysis, it can now be evaluated whether the SIF meets the qualitative requirements (*Table 7.3)*.

Table 7.3: Assessment of compliance with qualitative SIL requirements

Requirement type	Description	Comments	Compliance?
Quantitative reliability requirement (SIL)	• On – demand SIF: Average probability of failure on demand (PFDavg) • Continuous/high – demand SIF: Probability of dangerous failure per hour (PFH)	-	-
Qualitative requirement	• Compliance with HFT to SIS subsystems	All SIFs specified in NOG 070 fulfil HFT requirements to the given SIL[21]. Hence, if the design of the case SIF is in accordance with the specification in NOG 070, this requirement is fulfilled.	**Yes**
Management of functional safety (avoidance and control of systematic faults)	• Avoidance and control of systematic faults *(see. Chapter 2.3.1)* demonstrated through *prior use* of components: - Unchanged specification - 10 systems in different applications - > 100 000 operating hours *(preferably ~ 3.0 E06)* - > 1 year of service history OR - Evidence of suitability *(reference is made to NOG 070 [5], p.42)* - *FMEA*	For the PMV, PWV, DHSV, the specification is unchanged. Data is collected from 89 (PMV/PWV) and 91 (DHSV) systems (wells). $>3.0\cdot10^6$ operating hours per component type and 13.5 years of service history available. Hence, Management of functional safety (avoidance and control of systematic failures) is demonstrated through *prior use*.	**Yes**

As can be seen from *Table 7.3,* it is concluded that the case SIF meets the qualitative SIL requirements.

[21] For HFT requirements to different SILs, reference is made to NOROG 0-70, p. 41, route 2H, Table 8.4

7.2.4 Verification of Quantitative SIL Requirement

The SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)" operates in on – demand mode. To be verified SIL 3, this implies that the SIF must have a PFD_{avg} within the range (10^{-4}, 10^{-3}). Compliance with this requirement is to be evaluated in this part of the analysis based on collected operational data for the case SIF.

LIST OF ASSUMPTIONS

Based on the presented theory, case and previous discussions in this thesis, the following list of assumptions can be summarized for the calculation of average unavailability in a situation of demand (PFD_{avg}) for the case SIF:

- Data collection takes place during the useful lifetime of components
- Data is collected from a population of comparable components in comparable environments
- Component lifetimes are exponentially distributed with constant DU failure rate $\hat{\lambda}_{\mathrm{DU,avg}}$
- Test intervals are of length τ
- Unavailability due to planned downtime is neglected
- All recommendations to the quality of failure rate data, considerations of comparisons between sensors and human machine interfaces, independence between safety systems, documentation from the design phase and focus on deviation from the list of assumptions underbuilding the SIL requirements set in NOG 070 as presented in *Chapter 5.2.1* are complied with
- The state of the system can only be known by performing a proof test
- After a test (repair), the system is assumed as good as new
- Only one valve must close to isolate the wellbore
- All DU failures are detected during proof tests
- Loop monitoring is assumed
- Simultaneous proof testing
- Response time is less than safety time
- The safe state is defined by closure of the valves and isolation of the well
- All valves are hydraulically fail-safe

CALCULATION APPROACH

The PFD_{avg} is calculated based on the theory and equations presented in *Chapter 2.6*, the RBD for the SIF *(Figure 7.6)* and the example calculation for the SIF and data dossier presented in NOG 070, Appendix A.6.2 and A.2.2, respectively.

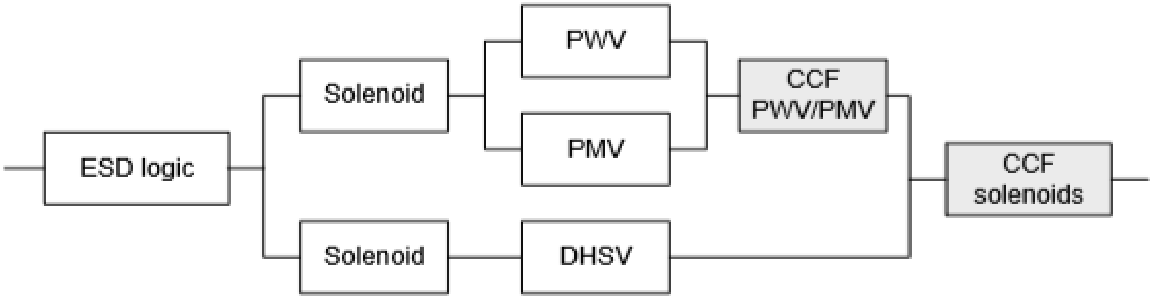


Figure 7.6: Reliability block diagram of the SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)"[5]

The data dossier in NOG 070 presents generic reliability data based on and documented by the PDS method [8] and OREDA [46] handbooks. The data is based on operational experience through a combination of sources such as RNNP and operational reviews, and thus reflects average component field performance. For the PFD_{avg} calculations in the current analysis, reliability data presented in the data dossier is used for the ESD logic and solenoids, and collected operational data is used for the valves. The relevant data for SIF subsystem components found from the data dossier and collected operational data is presented below in *Table 7.4*.

Table 7.4: Subsystem component data according to data dossier in NOG 070 [5], App. A Table A.2.3. Note that the DU failure rate for the PMV/PWV and DHSV is based on collected operational data ($\hat{\lambda}_{DU,avg}$). β - and correction factors are provided in NOG 070 App. A.6.2.

Component	**Proof test interval τ [hrs]**	**DU Failure rate [hrs^{-1}]**
Control Logic Units – Programmable safety system		
ESD Analogue input	8760	1.60 E-07
ESD Logic – CPU	8760	4.80 E-07
ESD Digital Output	8760	1.60 E-07
Total ESD Logic		8.00 E-07
Final elements		
PMV/PWV Solenoid	8760	6.00 E-07
DHSV Solenoid	8760	6.00 E-07
PMV/PWV	4380[22]	1.04 E-06[23]
DHSV	4380	2.22 E-05
	β – factor	
Valves/solenoids	10%	
ESD logic	5%	
Correction factor		
4/3		

The length of proof test intervals for the ESD logic and solenoids according to the data dossier are verified by COPNO. The proof test interval for the PMV/PWV is changed relative to the data dossier for the PMV/PWV to make the calculations realistic, see[23]. Note that this is the longest test interval the valves will have in their operational life; in reality, the interval can be as short as one month, see *Chapter 5.1.2.* Note also that the failure rates for the valves used in the current analysis are the updated *average* DU failure rates ($\hat{\lambda}_{DU,avg}$) for the components as presented in *Chapter 7.2.2*, in accordance with the recommendations in NOG 070.

In the example PFD$_{avg}$ calculation for the case SIF in NOG 070, Appendix A.6.2, the same generic failure rate is used for the PMV and PWV. This is presumably because the valves are of the same type. However, because they are situated in different locations in the well and therefore might have slightly different operating conditions, as well as the observed difference in number of DU failures between the two, the geometric mean of their respective estimated average DU failure rates is suggested to be used instead in the current analysis.

The logic solver has redundant I/O and CPU and is thus voted 1oo2. As can be seen from the RBD, the PMV and PWV are redundant and voted 1oo2. The DHSV and solenoids are voted

[22] In NOROG 0-70, Appendix A Table A.2.3, τ for the PMV/PWV is set to 8760 hours, which is not regarded as realistic here because the longest proof test interval per time based on NORSOK D-10 is 4380 hours.

[23] Geometric mean of $\hat{\lambda}_{DU,avg}$ for the PMV (2.20E-06 hrs^{-1}) and PWV (4.89E-07 hrs^{-1})

1oo1. There is a possibility for CCFs for the redundant ESD logic, PMV and PWV, and for the solenoids. The failure contribution from CCFs for the logic and valves are included in the equation for PFD_{avg} for these components in accordance with equation *2.26 (Chapter 2.6.4)*, whereas CCFs between solenoids are included as an own block in the RBD.

Based on the above data dossier, RBD and mentioned considerations, the PFD_{avg} calculation for the case SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)" was performed in MS – Excel *(See Appendix A.1)*. The calculation table and results can be seen below in *Table 7.5.* Note that an additional column (Remaining SIL 3 margin) is added to the PFD_{avg} calculation to indicate the percentage of the SIL 3 interval that remains before the PFD_{avg} for the SIF will exceed the upper SIL 3 limit (10^{-3}).

Table 7.5: Calculation for Quantitative SIL Verification (PFD_{avg}). DU failure rates marked in red are estimated from operational data.

Isolation of production bore in one topside well from the production manifold/flowline (ESD) - PFD_{avg} Calculation						
	DU Failure Rate	**Test Interval (τ) [hrs]**	**Voting**	**PFD_{avg} per Component**	**PFD_{avg}**	
					CCF	**Indep.**
ESD Logic	8.00E-07	8760	1oo2	1.92E-04	-	1.92E-04
PMV/PWV Solenoid	6.00E-07	8760	1oo1	2.63E-03	-	3.50E-04
PMV/PWV	1.04E-06	4380	1oo2	2.27E-03	2.27E-04	
Total Upper branch (indep.)				4.90E-03	2.27E-04	
DHSV Solenoid	6.00E-07	8760	1oo1	2.63E-03	-	
DHSV	2.22E-05	4380	1oo1	4.85E-02	-	
Total Lower branch (indep.)				5.12E-02	-	
CCF Solenoids	6.00E-07	8760			2.63E-04	
Total for Function					8.04E-04	
Remaining SIL 3 Margin						20%

As can be seen from *Table 7.5* above, the PFD$_{avg}$ for the SIF (Total for Function) is calculated to 8.04E-04. Hence, using updated average failure rates, the case SIF complies with the quantitative SIL requirement with a 20% margin and is by that verified SIL 3 based on collected operational data *(Table 7.6).*

Table 7.6: SIL Verification of the SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)"

Requirement type	Description	Comments	Compliance?
Quantitative reliability requirement (SIL)	• On – demand SIF: Average probability of failure on demand (PFD$_{avg}$) • Continuous/high – demand SIF: Probability of dangerous failure per hour (PFH)	SIL (PFD$_{avg}$) is calculated to be 6.93E-04 from operational data, which is within SIL 3.	**Yes**
Qualitative requirement	• Compliance with HFT to SIS subsystems	All SIFs specified in NOG 070 fulfil HFT requirements to the given SIL. Hence, if the design of the case SIF is in accordance with the specification in NOG 070, this requirement is fulfilled.	**Yes**
Management of functional safety (avoidance and control of systematic faults)	• Avoidance and control of systematic faults *(see. Chapter 2.3.1)* demonstrated through *prior use* of components: - Unchanged specification - 10 systems in different applications - > 100 000 operating hours *(preferably ~ 3.0 E06)* - > 1 year of service history OR - Evidence of suitability *(reference is made to NOG 070 [5], p.42)* - *FMEA*	For the PMV, PWV, DHSV, the specification is unchanged. Data is collected from 89 (PMV/PWV) and 91 (DHSV) systems (wells). >$3.0 \cdot 10^6$ operating hours per component type and 13.5 years of service history available. Hence, Management of functional safety (avoidance and control of systematic failures) is demonstrated through *prior use*.	**Yes**

7.3 Part 2: SIL as a Function of Test Interval Length

With the case SIF being verified SIL 3 with an additional 20% margin, it is interesting to evaluate whether the current test intervals for the PMV, PWV and DHSV can be extended from the prescribed requirements in NORSOK D-010 *(Chapter 5.1.2)*. On the contrary, had it *not* been verified SIL 3, the question of interest would be what length need the proof test interval be reduced to in order to maintain the PFD_{avg} below the upper SIL 3 limit between proof test intervals. *(Figure 7.7)*

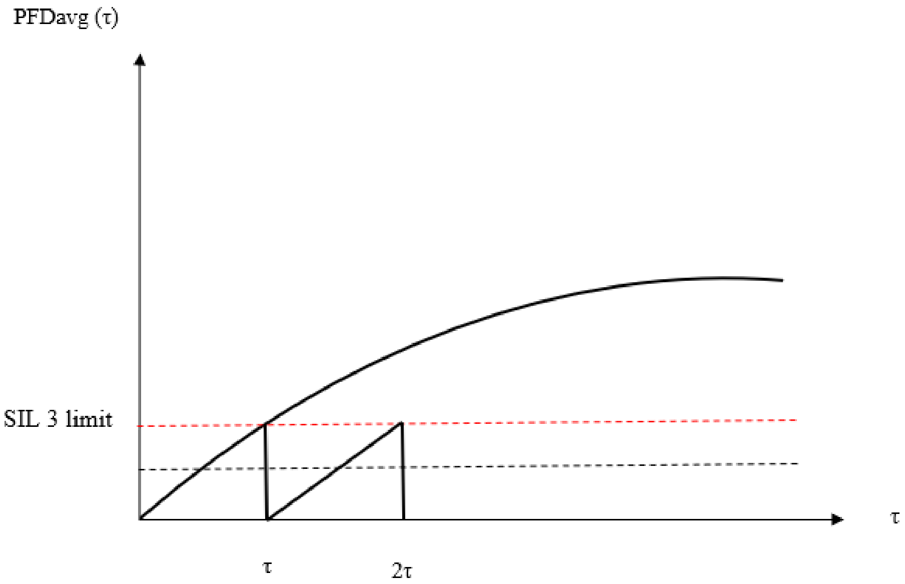


Figure 7.7: Test interval length (τ) vs PFD_{avg} (τ)

This can be analysed by changing the input value for the test interval (τ) for the PMV/PWV and DHSV in the calculation table for quantitative SIL verification *(Table 7.5)* used in the previous section. Consequently, in this part of the analysis, the PFD_{avg} for the case SIF will be recalculated according to *Table 7.5* using different input values for the length of the test interval (τ) for the PMV/PWV and DHSV.

It is agreed with the authors of the PDS report [8] that there should be a high degree of confidence in the estimates used as a basis to update component test intervals. Inspired by the use of 90% confidence intervals of the DU failure rate as part of the decision criteria for updating test intervals in the PDS report, the suggested procedure in this approach is to perform PFD_{avg} calculations at different test interval lengths using both the estimated average DU failure rates

($\hat{\lambda}_{DU,avg}$) and U90 DU failure rates ($\hat{\lambda}_{DU,U90}$) as presented in *Chapter 7.2.2* for the PMV/PWV and DHSV. There are three main arguments to this approach:

- Using the U90 DU failure rate gives a conservative PFD$_{avg}$ with added weight to uncertainties in the failure rate estimate and PFD$_{avg}$ output results (e.g. assuming "worst case").

- It provides a source of comparison between the calculated PFD$_{avg}$ and compliance to the SIL requirement when using average and U90 DU failure rates. This clarifies the effect of the estimated failure rate on the calculated PFD$_{avg}$/SIL to the analyst and decision maker.

- Based on system knowledge, confidence in the estimates, risk appetite etc., the decision maker can choose whether to base the decision of updating proof test intervals on "worst case estimates" of the PFD$_{avg}$ using U90 DU failure rates, which will result in shorter recommended test intervals based on the calculated PFD$_{avg}$, or the less conservative PFD$_{avg}$ estimate based on average DU failure rates.

Hence, PFD$_{avg}$ (Total for Function) and remaining SIL 3 margin was calculated for the case SIF according to *Table 7.5*, by changing the input values for τ and the DU failure rate for the PMV/PWV and DHSV according to *Table 7.7*.

Table 7.7: Summary of input failure rates to the calculation of PFD$_{avg}$ as a function of test interval length

Component	$\hat{\lambda}_{DU,avg}$	**Geom. Mean ($\hat{\lambda}_{DU,avg}$)**	$\hat{\lambda}_{DU,U90}$	**Geom.mean ($\hat{\lambda}_{DU,U90}$)**
PMV	2.20E-06	1.04E-06	3.85E-06	2.43E-06
PWV	4.89E-07		1.55E-06	
DHSV	2.22E-05	-	2.62E-05	-

A summary of the results for different test interval lengths and DU failure rates are presented below in *Table 7.8*. Note that for the PMV/PWV, the geometric mean of the two component DU failure rates as presented in *Table 7.7* are used, in accordance with the discussion and calculation method for SIL verification in *Chapter 7.2.4*.

Table 7.8: PFD$_{avg}$ as a function of test interval length using $\hat{\lambda}_{DU,avg}$ and $\hat{\lambda}_{DU,U90}$

Component	Test Interval (τ) [hrs] (months)	DU Failure Rate	PFD$_{avg}$ (Total for Function)	Remaining SIL 3 Margin
PMV/PWV	730 (1)	$\hat{\lambda}_{DU,avg}$	4.98E-04	50%
DHSV	730 (1)	$\hat{\lambda}_{DU,avg}$		
PMV/PWV	730 (1)	$\hat{\lambda}_{DU,U90}$	5.13E-04	49%
DHSV	730 (1)	$\hat{\lambda}_{DU,U90}$		
PMV/PWV	2190 (3)	$\hat{\lambda}_{DU,avg}$	5.93E-04	41%
DHSV	2190 (3)	$\hat{\lambda}_{DU,avg}$		
PMV/PWV	2190 (3)	$\hat{\lambda}_{DU,U90}$	6.86E-04	31%
DHSV	2190 (3)	$\hat{\lambda}_{DU,U90}$		
PMV/PWV	4380 (6)	$\hat{\lambda}_{DU,avg}$	8.04E-04	20%
DHSV	4380 (6)	$\hat{\lambda}_{DU,avg}$		
PMV/PWV	4380 (6)	$\hat{\lambda}_{DU,U90}$	1.13E-03	-13%
DHSV	4380 (6)	$\hat{\lambda}_{DU,U90}$		
PMV/PWV	8760 (12)	$\hat{\lambda}_{DU,avg}$	1.47E-03	-47%
DHSV	8760 (12)	$\hat{\lambda}_{DU,avg}$		
PMV/PWV	8760 (12)	$\hat{\lambda}_{DU,avg}$	9.75E-04	3%
DHSV	4380 (6)	$\hat{\lambda}_{DU,avg}$		
PMV/PWV	8760 (12)	$\hat{\lambda}_{DU,U90}$	1.60E-03	-60%
DHSV	4380 (6)	$\hat{\lambda}_{DU,U90}$		
PMV/PWV	4380 (6)	$\hat{\lambda}_{DU,avg}$	6.38E-04	36%
DHSV	2190 (3)	$\hat{\lambda}_{DU,avg}$		
PMV/PWV	4380 (6)	$\hat{\lambda}_{DU,U90}$	8.09E-04	19%
DHSV	2190 (3)	$\hat{\lambda}_{DU,U90}$		

The development in PFD_{avg} for the case SIF as a function of test interval length is illustrated graphically below in *Figure 7.8*.

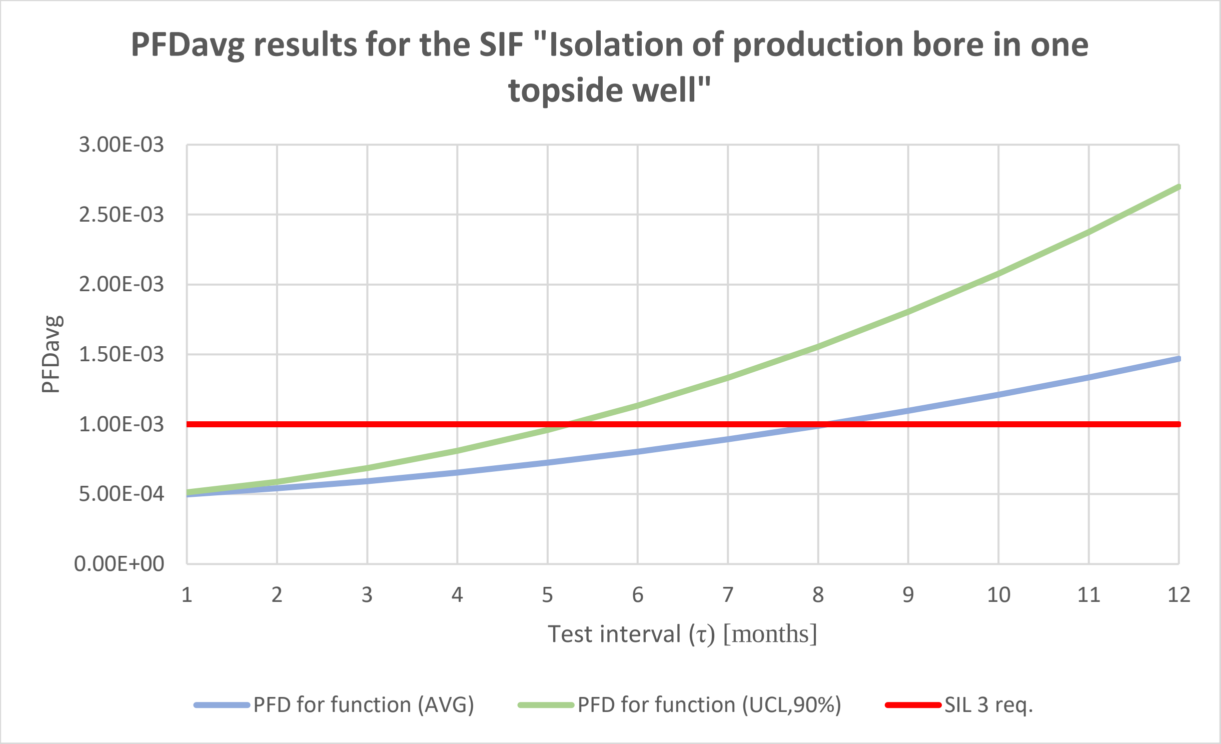


Figure 7.8: PFD_{avg} as a function of test interval calculated from average (AVG) and upper 90% confidence interval (UCL,90%) DU failure rate

As can be seen from *Table 7.8* and *Figure 7.8*, using the U90 DU failure rate, the PFD_{avg} (Total for Function) will exceed the SIL 3 requirement when the test interval for the PMV/PWV and DHSV is extended beyond three months (at approximately five months). However, using the average DU failure rate, the PFD_{avg} won't exceed the SIL 3 requirement until the test interval for the PMV/PWV and DHSV is extended beyond six months (at approximately eight months).

Knowing that the DU failure rates are significantly higher for the DHSV than for the PMV/PWV, combinations with shorter test intervals for the DHSV than the PMV/PWV is also analysed in *Table 7.8*. The PFD_{avg} for the case SIF is within the SIL 3 requirement using both the average and U90 DU failure rate when the test interval is set to six months for the PMV/PWV and three months for the DHSV.

It should be noted that if the component test interval is set to one month or three months for both the PMV/PWV and DHSV, the remaining SIL 3 margin even if using U90 DU failure rates is as much as 49% and 31%, respectively.

An interesting case is the difference in remaining SIL 3 margin between the calculated PFD_{avg} for the SIF using average versus U90 DU failure rates. For one – and three-month test intervals, there is only a 10% difference in the remaining SIL 3 margin between the two. However, when the test interval is extended beyond three months, there is a significant difference. In particular, for the combination of 12-month test interval for the PMV/PWV and 6 month test interval for the DHSV, the PFD_{avg} has a 3% remaining SIL 3 margin using the average DU failure rate, whereas using the U90 DU failure rate, the remaining SIL 3 margin is at astonishing -60%.

It is noteworthy that based on these differences; if SIL verification, as was performed in *Chapter 7.2.4,* was performed using U90 DU failure rates instead of average, the case SIF would not have been verified SIL 3 based on the assumed current test intervals in the data dossier.

It is clear that for a decision context of extending the test interval to or beyond six months, where the decision was based solely on the quantitative PFD_{avg} estimate without taking further assessments of uncertainty or other considerations into account, the decision would be greatly dependent on whether average or U90 confidence estimates were used in the calculation.

Hence, if a decision was to be made for the case SIF based on its PFD_{avg} with input DU failure rate $\hat{\lambda}_{\mathrm{DU,U90}}$, the maximum component test intervals to not exceed the quantitative SIL 3 requirement is the combination of six months for the PMV/PWV and three months for the DHSV. However, if the decision was to be made based on the PFD_{avg} with input DU failure rate $\hat{\lambda}_{\mathrm{DU,avg}}$, component test intervals could be extended to the combination of 12 months for the PMV/PWV and six months for the DHSV.

7.4 Part 3: Assessment of Uncertainties

In the current work, it is proposed that the PFD_{avg} of SIFs is used as performance indicator for evaluation of SIL verification and updating of component test intervals. It is acknowledged that the choice of calculation model and all input parameters are based on the currently available background knowledge of the analyst; including recommendations from regulations, standards and guidelines, system knowledge, historical operational data, assumptions and presuppositions. The knowledge can be strong or weak, and uncertainties can be hidden in the PFD_{avg} estimates.

In Parts 1 and 2 of the analysis, confidence intervals are used as a tool to quantitatively express the uncertainty in the estimates of DU failure rates and resulting PFD_{avg} for the case SIF. However, based on the discussions in *Chapter 3.1.6* and *5.3*, it is the opinion of the author (analyst) of the current work that a purely quantitative (probabilistic) assessment of uncertainties has its limitations in properly capturing and communicating the uncertainties of the analysis. It is agreed with the views of Rausand [26];

> *"The person most capable of making judgements about the uncertainty is the analyst, and she should communicate to the decision maker her "degree of belief" about the uncertainty together with the results from the reliability analysis of the SIF. Her "degree of belief" must be communicated qualitatively and supplemented by some quantitative arguments"*

Therefore, an additional qualitative assessment of uncertainties in the analysis and output results of the quantitative SIL (PFD_{avg}) for the SIF is proposed based on an evaluation of the strength of background knowledge (SoK) supporting the analysis. The approach is inspired by the ideas of Flage and Aven [35], discussed in *Chapter 5*.3. To guide the assessment, a checklist has been developed to evaluate the SoK in the different stages of the PFD_{avg} calculation based on the identified classes of uncertainty in reliability analyses in *Chapter 3*. The checklist is partly inspired by earlier work on qualitative uncertainty assessments in SIL verification by Abrahamsen and Røed [11].

The suggested checklist for assessment of the SoK (uncertainty) in quantitative SIL verification (PFD_{avg} calculation) is presented below in *Table 7.9.* A short explanation of the checklist will be provided before it is applied to the current analysis of the case SIF.

Table 7.9: Suggested checklist for evaluating the SoK (uncertainty) in quantitative SIL verification

Class of Uncertainty	Checklist	Evaluation	SoK	Criticality	SoK increasing measures
Data	Applicability of historical data				
	Data completeness				
	Quality of reporting				
	Data interpretation and treatment				
Parameter	Sufficient operational experience				
	Few registered failures				
	Similar operational environments				
	Effect of CCFs & component dependencies properly included				
	Conservativeness of estimate				
Model	Model applicability				
	Competence of analyst				
	Conservativeness of result				
Completeness	Known				
	Unknown				
PFD_{avg}	**Evaluation**	**SoK**			

For each class of uncertainty; data uncertainty, parameter uncertainty, model uncertainty and completeness uncertainty, some common factors that contribute to increasing the uncertainty was identified in *Chapter 3*. An evaluation of these factors in the analysis should be made and summarized in the evaluation column. It can be understood such that:

- If most factors can be considered to be good/true, the SoK in the data/parameter/model is strong and the uncertainty in the data/parameter/model is low
- If most factors can be considered to be poor/false, the SoK in the data/parameter/model is weak and the uncertainty in the data/parameter/model is large
- If somewhere in between, the SoK in the data/parameter/model is medium and the uncertainty in the data/parameter/model is medium

A case specific evaluation should be made on known/unknown factors contributing to completeness uncertainty, as these factors can differ greatly. The assessed criticality of each class of uncertainty can differ between analyses. An evaluation should be made on whether the criticality of data, parameter, model or completeness uncertainty is regarded as low, moderate or high for the specific analysis case.

Based on the assessed SoK underbuilding the data collection and treatment, parameter estimation, model and completeness of the analysis, and the respective criticality, an assessment can be made on the overall SoK underbuilding the estimated PFD_{avg} for the SIF. To increase the SoK underbuilding the analysis in the future SIL verification and updating of component test intervals, a column is added on SoK increasing measures.

The SoK assessment shall supplement the results of Part 1 and Part 2 of the analysis to be provided for the decision maker in the context of identifying optimum component test intervals. The decision maker can then make a better-informed decision based on the semi – quantitative assessment of uncertainty (PFD_{avg}, SoK), as will be presented in Part 4.

In the following, the suggested use of the checklist is applied to the analysis of quantitative SIL verification for the case SIF. The evaluations are based on discussions with well integrity and reliability experts at COPNO.

DATA UNCERTAINTIES (SOK IN THE DATA)

Historical data is collected by COPNO from a large population of comparable components in wells with comparable pressure and temperature environments. The follow-up of test procedures offshore is unknown to the analyst. However, COPNO has a high focus on critical failure reporting and has received very positive feedbacks on their quality of reporting compared to operators in general. The detailing level in the data set provided to the analyst was very good and in accordance with the recommendations in NOG 070. The data set was quality controlled a total of four times by the analyst and a well integrity expert. The data completeness, quality of reporting and data interpretation and treatment is therefore assessed to be good in the current analysis.

However, as was identified in Part 1 of the analysis, some of the components are significantly older, and located in older wells. Although the wells on both Eko – Mike and Eld – Sierra are oil production wells, wells on Eko – Zulu produces both oil and gas, which will cause different flow patterns and potential for slugging within these wells. In addition, some of the wells included in the analysis have problems with scale formation, which is a significant performance influencing factor, and some have increasing corrosive environments. It is likely that wells that are subject to scale formation also have more corrosive environments, as these phenomena are both enhanced by the presence of water due to mature waterflooding and water break through.

Therefore, the applicability of collected historical data as a whole might not be as good to represent future performance for these wells, which contributes to uncertainty in the applicability of historical data. However, although there was not sufficient time and resources to filter on well age and scale potential in the current analysis, this could easily have been done, which would significantly reduce this source of uncertainty.

Overall, because the knowledge about potential issues in applicability of historical data is strong and this source of uncertainty is easily reducible, it is concluded that the SoK in the data is strong, and the data uncertainty is low. The criticality of data uncertainty is considered to be high. Filtering the data set on well age and scale potential will increase the SoK and reduce the uncertainty in the data. It should also be considered to include information on water breakthrough in the dataset.

PARAMETER UNCERTAINTIES (SOK IN THE PARAMETER ESTIMATION)

For the PMV and PWV components, few DU failures are experienced during the observation period. This is good in the way that it indicates high component reliabilities. However, it increases the uncertainty in the estimated DU failure rates. This was reflected by the width of the 90% confidence intervals for the DU failure rates of these components. However, the aggregated operational service time per component in the current analysis is well above the minimum recommendation according to NOG 070. In particular, most operational service time is available for the component with the fewest failures (PWV). Hence, sufficient operational experience is available to calculate updated DU failure rates solely on operational data. Uncertainty arising due to insufficient operational experience and few registered failures is therefore assessed to be low, and the knowledge underbuilding the DU failure rates are considered to be strong.

However, data uncertainties related to the applicability of historical data due to differing operational environments propagates to the estimated DU failure rates. It is believed that if scale wells were excluded from the analysis, the DU failure rates would be much lower. Hence, the DU failure rates may be too conservative for the general population of components. For the same reason, the estimated DU failure rates may be too optimistic for components in wells with significant scale potential.

In the PFD_{avg} calculation, the DU failure rate contribution from CCFs is based on the modified β-factor model according to the PDS method. The β-factor included in the calculation was provided in NOG 070, as was the correction factor for component dependencies. Although the values of these factors are based on expert opinions, the applicability and SoK underbuilding these recommendations are unknown (uncertain) to the analyst.

It is concluded that the SoK in the DU failure rate parameter is medium and the parameter uncertainty is medium. The criticality is assessed as medium/high. Adding conservativeness in the estimate by using the U90 DU failure rate point estimate will increase the SoK and reduce the uncertainty in the parameter.

MODEL UNCERTAINTY (SOK IN THE MODEL)

The PFD_{avg} model used to calculate the SIFs (un)availability in the suggested approach for SIL verification and updating of test intervals is based on the recommendations in NOG 070 (The PDS method), which is developed by experts in reliability and SIS and widely deployed within the oil and gas industry. It is therefore generally assessed that its applicability to model unavailability of SIFs is based on strong knowledge.

However, the suitability of the model to SIFs in *wells* has been questioned at COPNO. Because of knowledge of the mechanical components (valves) and the harsh environments in wells, it is speculated that the components will be affected by wear and tear and enter the wear – out phase after some time in operation. Thus, assuming components to be in the useful lifetime with constant failure rate throughout their operational life might not be appropriate. It is therefore questioned whether the average unavailability of the PMV, PWV and DHSV, as well as other valves in the well not included in the current analysis, are better modelled by the Weibull distribution.

Therefore, an additional coarse analysis of component lifetime distributions was carried out in this part of the analysis. A challenge with performing lifetime distribution analysis on the valves was the high component reliabilities and few registered failures during the 13.5-year observation period. Therefore, two different methods were applied to analyse component lifetime distributions based on the available volume of registered DU failures.

DHSV

For the DHSV, there was enough registered DU failures (88) to run a meaningful goodness of fit – test. This was performed using the "Distribution Fitting" tool in the MS - Excel add-in Palisade @risk software, provided by the University of Stavanger. Given a range of input data from a large population, the distribution fitting tool fits selected lifetime distributions to the data. For each of the specified distributions, the tool estimates the parameters that most closely fit the input data using maximum likelihood estimation[24]. The resulting lifetime distributions are then ranked according to goodness – of – fit tests.

A drawback of this tool is that it can't be differentiated between censored and complete input data. Hence, the assumption was made here that the collected data of DHSV lifetimes is complete and comprised of the 88 registered lifetimes (service time to DU failure) for the DHSV; that is, censored lifetimes were excluded. It is assessed that this will not significantly affect the shape of the resulting pdf of component lifetimes, but only skew it towards higher probabilities of component failure within each time interval. Therefore, it is assumed that the ranked goodness-of-fit of the exponential and Weibull distributions is still representative to assess the lifetime distribution that best models DHSV lifetimes.

The procedure used for the distribution fitting analysis in @risk is as follows:

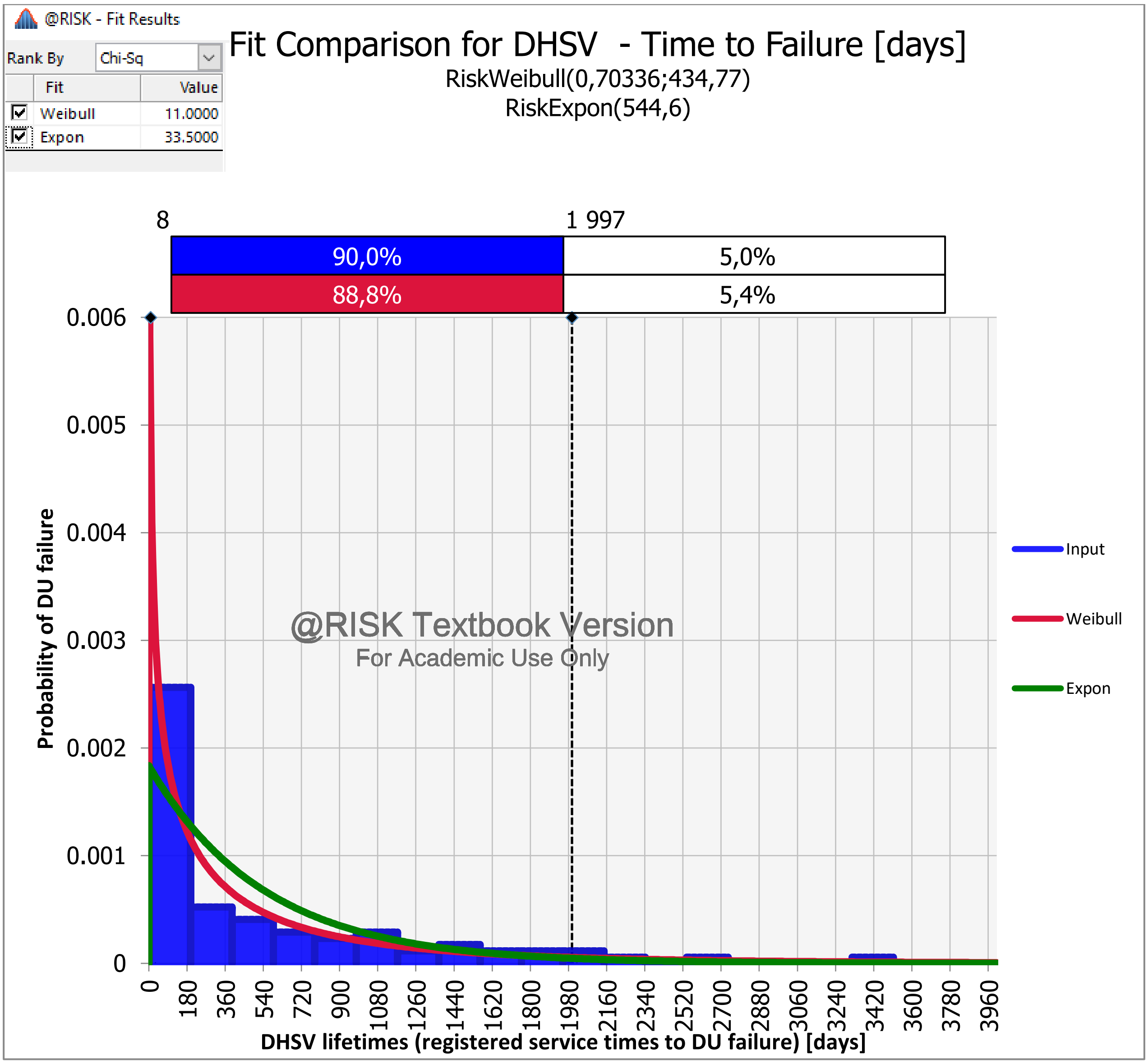
1) A range of input sample data (here: the 88 registered times to failure for the DHSV) is selected and marked as continuous sample data.

2) The distributions to be fit to the data must be selected. For the context of the current analysis, the exponential and Weibull distributions are selected, with a fixed lower limit of 0 and unsure upper limit.

[24] For elaborations on MLE estimation, the reader is referred to basic statistical textbooks such as [47]

3) Weibull and exponential distributions are automatically fit to the data. The χ^2 goodness-of-fit – test was chosen to rank the best fitting distribution based on the discussions in *Chapter 2.6.3*.

The results of the exponential/Weibull goodness of fit – test for the DHSV can be seen from the graph in *Figure 7.9* below.



@RISK - Fit Results

Rank By: Chi-Sq

	Fit	Value
☑	Weibull	11.0000
☑	Expon	33.5000

Figure 7.9: Goodness of fit – comparison between the exponential and Weibull lifetime distributions for the registered lifetimes of the DHSV (Assuming complete data).

As can be seen from *Figure 7.9*, the Weibull distribution is ranked as the best fit based on the χ^2 goodness of fit – test. Some interesting observations can also be identified from the graph.

Firstly, it is noted that the shape parameter α of the Weibull distribution (0.70336) is less than one, which means that the failure rate function is decreasing. Albeit the estimated parameters are uncertain due to the assumption of complete data, it can thus actually be more realistic to assume components to be in their early useful lifetime than at the end of their useful lifetime; entering the wear-out phase, as was suspected initially.

Second, it is observed that the exponential distribution will underestimate the probability of failure during the first six months of operation, whereas it will overestimate the probability of failure beyond six months of operation. Also, it can be seen that the exponential distribution will give more conservative predictions than the Weibull distribution after approximately four months of operation.

From the above, it can be concluded that although the Weibull distribution is a better fit to the data, it is not inappropriate to assume the DHSVs, when considering the population as a whole, to be within the (early) useful lifetime during the observation period, and hence the exponential distribution is not inappropriate to use as a simplified model. However, it should be noted that the exponential distribution can tend to underestimate the probability of failure the first months of operation and overestimate the probability of failure in the following years.

PMV/PWV

For the PWV, there are only two registered DU failures, and hence no meaningful statistical analysis could be performed to evaluate its lifetime distribution with the time and resources at hand. However, based on the knowledge that the PMV and PWV is of the same valve type, it is assumed that the PMV and PWV will likely follow the same lifetime distribution, and it will be sufficient to perform an analysis on the PMV.

Because there were only 11 registered failures for the PMV, it was assessed that a goodness- of – fit analysis based on the assumption of complete data as was done for the DHSV would be inappropriate in this case. Instead, a hazard plot was created of the registered DU failures of the PMV to analyse if component lifetimes are likely exponentially or Weibull distributed. The hazard plot can be seen below in *Figure 7.10.*

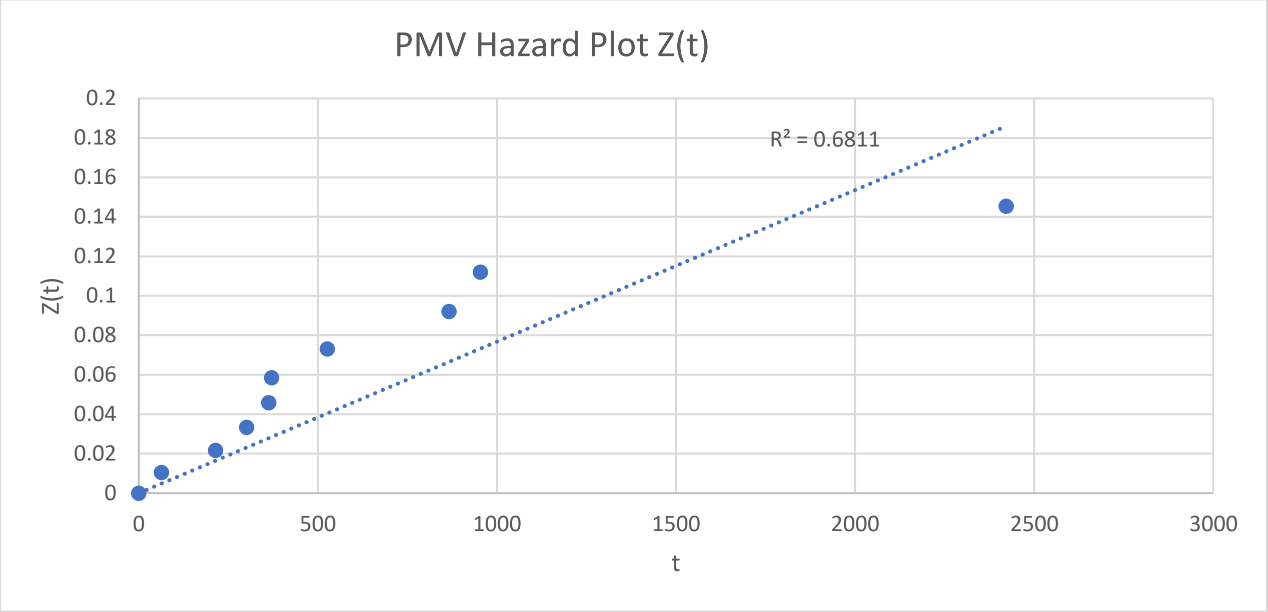


Figure 7.10. PMV hazard plot

The hazard plot does not seem to fall on a linear line through origin. To analyse whether the component lifetimes are better modelled by the Weibull distribution, a logarithmic hazard plot was created *(Figure 7.11)*. As can be seen from the R^2 values of the regression lines in *Figure 7.10* and *Figure 7.11*, the datapoints in the logarithmic hazard plot to a greater extent fall on a straight line.

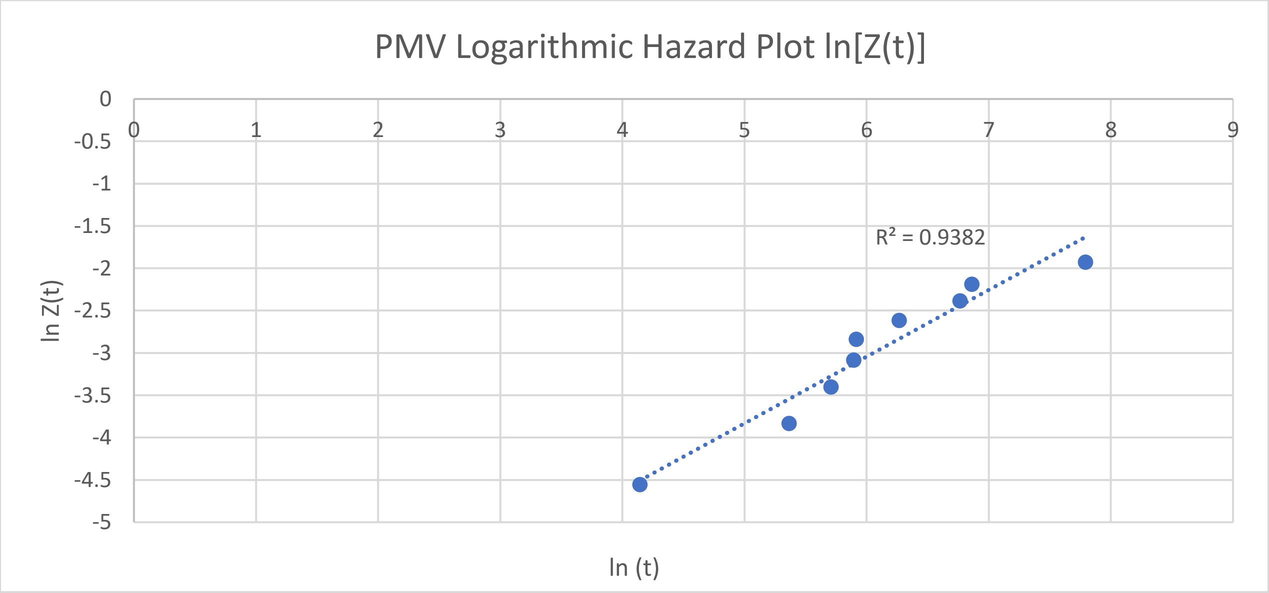


Figure 7.11: PMV logarithmic hazard plot

Therefore, it can be concluded that the lifetimes of the PMV and PWV are also Weibull distributed.

Overall, it is assessed that the unavailability of the PMV, PWV and DHSV are more appropriately modelled by the Weibull distribution. However, a challenge with this approach is that the α and β parameters need to be identified from analyses of failure data. Due to the few registered failures, the estimated parameters will be uncertain, and a thorough analysis will be resource demanding. In addition, it is assessed that although the Weibull distribution better models the component lifetimes than the exponential distribution, the exponential distribution is not inappropriate and will likely add conservativeness in the calculated PFD_{avg} after approximately six months of operation.

The modelling and analysis of lifetime distributions was performed by a graduate analyst (the author). However, the analyst was supported by experts at COPNO, and the analysis methods and results were followed up regularly.

It is concluded that the SoK in the model is medium, and the model uncertainty is medium. The criticality is assessed to be medium. Future research on using the Weibull distribution to model the lifetimes for SIS components in wells will increase the SoK and reduce the uncertainty in the model.

COMPLETENESS UNCERTAINTY (SOK IN THE ANALYSIS COMPLETENESS)

Of known factors contributing to completeness uncertainty, it is acknowledged that assumptions and simplifications were made in the analysis due to time, resource and competence constraints.

For example, it was assumed full proof test coverage, and although it was a high awareness about the effects of scale on component failure rates and resulting PFD_{avg}, the data set was not filtered on scale wells to be subject to a separate analysis due to time constraints. In addition, it was discovered that the Weibull distribution better models the component lifetimes. However, the knowledge about said effects are considered to be good and the use of the exponential distribution is not considered inappropriate. All methods used in the analysis are seen as reasonable.

By nature, it is difficult to evaluate factors contributing to *unknown* uncertainty. However, COPNO has more than 50 years of experience as an operator on the NCS, and the finale element valves of the case SIF are well known. It is assessed as unlikely that a completely new phenomena significantly affecting the operating environment in wells and component reliabilities will occur at this time.

It is concluded that the SoK in the completeness of the analysis is strong, and the completeness uncertainty is low. The criticality is assessed to be medium.

The evaluations of SoK (uncertainty), criticality and SoK increasing measures are summarised in the developed checklist below in *Table 7.10*. Based on the assessments of SoK (uncertainty) in the data, parameter, model and completeness of the analysis, it was concluded that the SoK underbuilding the calculated PFD_{avg} for the SIF is medium. If U90 DU failure rates are used in the calculation, the SoK will be medium – strong.

Table 7.10: SoK Evaluation for the case analysis of PFD_{avg} for the SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)"

	Checklist	**Evaluation**	**SoK**	**Criticality**	**SoK increasing measures**
Data	Applicability of historical data Data completeness Quality of Reporting Data interpretation and treatment	• Differing well/component age and scale potential/corrosion in wells reduces the applicability of historical data to estimate future performance of components in all wells • Good quality and understanding of collected data. • Test procedure uncertain, quality of reporting generally good • High focus on critical failure reporting	🟩	High	Filter dataset on well age and scale potential Update dataset with information on water breakthrough
Parameter	Sufficient operational experience Few registered failures Similar operational environments Effect of CCFs & component dependencies properly included Conservativeness of estimate	• There is sufficient operational experience despite few registered DU failures • Differing operational environments in the collected data affects the estimated DU failure rates • Effect of CCFs and component dependencies uncertain, but estimated based on expert opinions from joint industry study • U90 DU failure rate adds conservativeness in the parameter	🟨	Medium/high	Estimate DU failure rates for scale vs non scale wells Use U90 DU failure rate point estimate
Model	Model applicability Competence of analyst Conservativeness of result	• Applicability of model is considered sufficient given that it is based on conservative estimates • Graduate analyst supported by experienced multidisciplinary team of subject matter experts • The conservativeness of the model output increases with time	🟨	Medium	Future research on applicability of exponential/Weibull distributions for SIFs in wells Future research on Weibull distribution to model SIF unavailability
Completeness	Known Unknown	• Assumed full proof test coverage • Environmental factors (scale) • With 50 years of experience on the NCS, unknown factors are considered to have a limited effect at his time	🟩	Medium	
PFD_{avg}	**Evaluation**	**SoK**			
		🟨			The SoK will be medium – strong if U90 DU failure rates are used

7.5 Part 4: Optimisation of Test Intervals

Part 4 of the case analysis aims to answer the motivational question of how long the SIFs' component test intervals can be, while still keeping the SIF within its SIL requirement with a *sufficient degree of certainty*. Answering such questions in a decision context is often referred to as decision making under uncertainty. [12] This inspired the development of a decision framework to guide the decision maker in identifying optimum component test intervals based on a semi – quantitative assessment of uncertainty in the SIFs calculated SIL as a function of test interval length in the form (PFD_{avg}, SoK). In this part of the analysis, the framework will be applied to identify optimum test intervals for the case SIF.

For this case analysis, it is concluded that the maximum component test intervals for the PMV/PWV and DHSV to keep the PFD_{avg} of the SIF "Isolation of production bore in one topside well (ESD)" below the upper SIL 3 requirement is 12 and 6 months based on $\hat{\lambda}_{DU,avg}$, and 3 and 6 months based on $\hat{\lambda}_{DU,U90}$. These combinations of test interval lengths represent the decision alternatives for updated component test intervals for the case SIF.

The calculated PFD_{avg} and remaining SIL 3 margin for the SIF, and the SoK underbuilding the identified PFD_{avg} for these decision alternatives are summarized below in *Table 7.11*.

Table 7.11: Summary of SIL as a function of test interval length, remaining SIL 3 margin and SoK for test interval decision alternatives

Component	**Test Interval (τ) [hrs^{-1}] (months)**	**DU Failure Rate**	**PFD_{avg} (Total for Function)**	**Remaining SIL 3 Margin**	**SoK in PFD_{avg}**
PMV/PWV	8760 (12)	$\hat{\lambda}_{DU,avg}$	9.75E-04	3%	Medium - strong
DHSV	4380 (6)	$\hat{\lambda}_{DU,avg}$			
PMV/PWV	730 (6)	$\hat{\lambda}_{DU,U90}$	8.09E-04	19%	Medium
DHSV	730 (3)	$\hat{\lambda}_{DU,U90}$			

The developed framework to guide the decision maker in identifying optimum component test intervals based on the combination (PFD_{avg}, SoK) is presented below in *Table 7.12*. The framework is inspired by a similar framework for the semi-quantitative assessment of uncertainties (P, SoK) presented by Aven [17].

Table 7.12: Semi – quantitative framework for identification of optimum test intervals for well barrier (SIF) components based on (PFD_{avg}, SoK). Green = small uncertainties, orange = medium uncertainties, red = large uncertainties.

Probability based justification (PFD_{avg})	Large margin above min SIL	🟧	🟩 $\hat{\lambda}_{DU,U90}$	🟩
	Small margin above min SIL	🟥	🟧 $\hat{\lambda}_{DU,avg}$	🟩
	On target	🟥	🟥	🟧
		Weak	Medium	Strong
	SoK			

By combining the probability-based justification (PFD_{avg}) and the SoK supporting the estimated PFD_{avg} for each decision alternative, which was identified by the SoK checklist in the previous chapter, the uncertainty in the decision alternative based on the combination (PFD_{avg}, SoK) is simply identified and communicated by colour code. Here, green signals small uncertainties, orange signals medium uncertainties, and red signals large uncertainties in the estimated SIL as a function of test interval length.

This work only seeks to provide decision support, and hence no suggestions for acceptance criteria in terms of where in the framework one ends up will be given, as that is up to the decision maker. However, it can be advised that a conservative and risk averse approach will be to only extend the test interval if the uncertainty based on the (PFD_{avg}, SoK) uncertainty assessment is within the low (green) region.

For the case SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)" the identified uncertainty in the two decision alternatives based on the semi – quantitative assessment (PFD_{avg}, SoK) is indicated in *Table 7.12.* From the framework, it was decided that optimum test intervals for the SIF final elements (well barrier components) are 6 months for the PMV/PWV and 3 months for the DHSV.

8 DISCUSSION

8.1 On the Practical Implementation of the Suggested Approach

The suggested approach presented in this thesis for integrated SIL verification and optimisation of test intervals for well barrier (SIF) components was developed during the pursuit of identifying optimum test intervals for the SIF "Isolation of production bore in one topside well from the production manifold/flowline (ESD)" based on a reliability/availability analysis of operational data provided by ConocoPhillips Norway.

Initially, the scope was to base the analysis on the theory, methods and recommendations for SIL verification and updating of component test intervals presented in the NOG 070 guideline [5] and the associated PDS report [8]. Additional recommendations from academia on how uncertainties in SIL verification and updating of test intervals according to these methods was identified and considered to be used. However, transferring theory into practice can sometimes be a challenge, and as is reflected in *Chapters 5 – 7* of this thesis, some challenges were identified with applying the available methods and procedures to operational data. Thus, the approach for an integrated and dynamic process of SIL verification and optimisation of component test intervals with added weight to uncertainties suggested in this work was developed on a supply and demand basis as a practical solution to these challenges.

From the experience gained from performing the case analysis using the suggested approach, it is believed that it offers a more practical method for SIL verification and identification of optimum test intervals for operators and other end users of NOG 070. In particular, it is believed to offer practical support when faced with challenges such as large amounts of (censored) operational data, and for identifying and communicating sources of uncertainty when the analyst (decision maker) is not necessarily a risk and reliability professional. Through the developed checklist for sources of uncertainties (SoK) in the different steps of the reliability analysis of SIFs and framework for identification of optimum test intervals in light of uncertainties by the semi quantitative assessment framework (PFD_{avg}, SoK), the results and uncertainties of the analysis are communicated in comprehensive manner to the decision maker that allows for different decision strategies to be adopted.

8.2 On the Appropriateness of the Suggested Approach in Decision Making Under Uncertainty

Each SIL corresponds to an expected level of risk reduction. In a decision context of how frequently well barrier (SIF) components should be tested, the decision maker must balance the costs of performing tests at a given frequency with the obtained SIL at the given test frequency; that is, the cost of testing versus the achieved risk reduction at different test intervals. The obtained SIL is estimated through calculations of the PFD_{avg}, and the "true" PFD_{avg} of the SIF between tests is uncertain. Hence, this is decision making under uncertainty.

The common framework to use for decision making under uncertainty, is the use of cost – benefit analyses[25]. Following such a framework, monetary values are assigned to the burdens (testing) and benefits (achieved risk reduction) of the different decision alternatives, and the attractiveness of each alternative is determined from the net present value of balancing the expected costs and benefits of the alternative; E[NPV] = E[Benefits] – E[Costs]. [49] The most attractive decision alternative is the one where the E[NPV] is maximized.

In the current context, the expected benefit from the achieved level of risk reduction based on the calculated PFD_{avg} can be thought of as E [Benefits $\vert PFD_{avg}$]. To calculate the E [Benefits $\vert PFD_{avg}$], the reduced likelihood of loss of assets, human lives, reputation etc., must be transferred to monetary value. For an example of how this can be done in a similar context, see [49]. A common method to include (quantify) uncertainties in the PFD_{avg} based on this way of thinking, would be for example to increase the rate of return as a means to outweigh the possibilities for unfavourable outcomes. [49].

Such an approach could be considered an "extreme economic strategy" for decision making, whereas in an "extreme safety strategy", the focus is solely on risk reduction (achieving safety) and no consideration is given to the costs and benefits of the different decision alternatives. One could arguably say that the NOG 070 approach to SIL verification and updating of component test intervals is more in line with the "extreme economic strategy", as decisions are based on expected values such as PFD_{avg}, expected DU failures and failure rates, whereas following the NORSOK D-010 approach to schedule proof tests in the PM programme is an "extreme safety strategy", as test intervals are then scheduled without consideration to the costs versus benefits

[25] For an explanation on cost – benefit, cost effectiveness and multi attribute analyses, the reader is referred to [48]

of testing at the given frequency, and the main focus is to maintain well integrity – whatever the cost.

Accepted principles for good decision-making state that the decision-making process should be *transparent* and *consistent;* meaning that how the decision was reached and its implications should be apparent, and that similar approaches should be adopted in similar circumstances to meet similar ends. It has been shown that the decision-making process in a safety context will neither be transparent nor consistent if one is not to some extent willing to transfer all the attributes (costs of testing, achieved risk reduction) to comparable units. [48]

In this regard, the methods presented in NOG 070/the PDS report for SIL verification and updating component test intervals are more in line with accepted principles for good decision making. However, it is important to be aware that all statistical expected values are conditioned on the background knowledge. The calculated PFD_{avg} for the SIF is based on all available background knowledge of the analyst and can be written as [$PFD_{avg} \mid K$]. Because the background knowledge can differ between analysts, the calculated expected PFD_{avg} can differ greatly. [11] Hence, the estimated E [Benefits $\mid PFD_{avg}$] can be misleading. There are uncertainties.

Based on such considerations, Abrahamsen and Røed [11] proposed a modified method for SIL verification, where the final decision on SIL is based on a qualitative uncertainty workshop, as presented in *Chapter 5.3*. However, this is to make an initially transparent and consistent method for SIL verification and, in particular, identification of optimum component test intervals, cloudy and inconsistent.

In this thesis, it is acknowledged that uncertainties are hidden in the background knowledge that the calculated PFD_{avg} is conditioned on. To aid the decision maker in identifying optimum test intervals for well barrier (SIF) components, a framework was developed to semi – quantitatively assess the uncertainty in the calculated SIL as a function of test interval length by the pair (PFD_{avg}, SoK).

It is believed that the suggested approach for integrated SIL verification and optimisation of test intervals presented in this thesis provides more appropriate decision support for decision making under uncertainty in a safety context. The combination (PFD_{avg}, SoK) provided to the decision maker allows for cost benefit analyses to be performed based on the calculated PFD_{avg}, for a transparent and consistent decision-making process. However, being informed of the uncertainties in the estimated PFD_{avg}, added weight can be given to safety, and the final decision will ultimately depend on the risk appetite of the decision maker.

8.3 On the Justification of Regulating Well Barrier (SIF) Component Test Intervals Compared to NORSOK D-010 Requirements

According to NORSOK D-010, the test interval of well barrier components should be regulated based on experience data, and the historical performance and reliability data used to justify a change in test frequency shall be documented. In earlier sections of this thesis, the question was raised; what exactly justifies a change?

It is believed that the results of the case analysis in this thesis provides the documentation that the initial test frequency of newly installed components can justifiably be extended beyond the 1 – month test frequency for the PMV, PWV and DHSV components based on historical reliability performance data. This is due to the observation that the SIL of the case SIF is almost at SIL 4 when the test frequency is set to one month, with a remaining SIL 3 margin of as much as 49% *even if* the conservative U90 DU failure rate is used in the PFD_{avg} calculation.

Taking both the demonstrated integrity performance of the valves and assessment of uncertainty in the analysis into account, it was identified that the optimal test intervals for the PMV/PWV and DHSV to be scheduled in the PM programme is 6 months for the PMV/PWV, and 3 months for the DHSV. This observation has two important implications compared to the prescribed test frequency in NORSOK D-010 for these valves:

1) The initial one – month test frequency for valves that are recently put in operation is unreasonable based on historical reliability performance data
2) The extension to a six – month test frequency for both the PMV/PWV and DHSV cannot be justified based on historical reliability performance data

Hence, the current test intervals for the PMV, PWV and DHSV as prescribed in NORSOK D-010 are identified to be inappropriate in both ends based on the demonstrated reliability performance in operation for these valves.

One could of course argue that because the current method for optimisation of test intervals looks at the population of well barrier (SIF) components as a whole, whereas NORSOK D—010 makes recommendations on a well – by – well level, the prescribed test intervals in NORSOK D-010 are still appropriate because they relate to the performance per well. And, as previously discussed, the future performance of components can differ between wells due to differences in age and operating environment, which was identified as a source of uncertainty in the case analysis.

However, the observation is interesting, and optimum test intervals for wells when age and operating environment is taken into account should also be analysed using the suggested approach to make better predictions on a well – by – well level. For example, it is the belief of the analyst (author) that components in scale wells might appropriately be tested at 6 – and 3-month intervals, whereas the intervals can likely be further extended for non – scale wells.

In addition, it must be verified that the identified optimum test intervals for the PMV, PWV and DHSV are also applicable to the other final elements of the ESD SIS in wells (e.g. other valves not included in the current analysis). However, as other valves in the well are of the same type, and the DHSV is facing the roughest environments and most failures are expected for this valve, one could hypothesise that similar results for optimum test intervals will be true for other valves that are part of the SISs in wells too.

8.4 On the Incentives of Operators for Extending Well Barrier (SIF) Component Test Intervals

It is a fair assumption that different incentives can lead operators to want to invest less in safety measures such as proof testing than what is optimal from a societal point of view. It has been common to assume the effects of proof testing as purely positive in terms of increased component reliability. Because an accidental event in offshore petroleum activities will cause negative externalities[26] towards society, it can be shown based on expected utility theory[27] that society likely wants to invest more in safety measures than what is optimal for operators in their optimisation problem. [50] Societal interests are safeguarded by PSAN regulations and standards such as NORSOK D-010. Hence, one could argue that a high test frequency, where

[26] Economically significant effect due to activities of a party that does not influence said party's' production, but influences other parties' decisions [50]

[27] For elaborations on expected utility theory, the reader is referred to [50]

test intervals are shorter than what is deemed optimal by the operator, might still be appropriate in a safety perspective.

However, if one does *not* disregard the potential for negative side effects of testing, such as the introduction of systematic failures to SIS components or test induced leaks and accidents, the utility of test activities changes also from a societal point of view. The same frequency of proof tests is then likely also too strict from a societal point of view. [50]

In a study by Vinnem and Røed [51], the circumstances of hydrocarbon leaks on the NCS was analysed. The study included all reported hydrocarbon leaks above 0.1kg/s from process inventories on offshore installations on the NCS between 2008 – 2014. The analysis showed that roughly 60% of leaks occurred during manual intervention on normally pressurized systems – of which the dominating activity carried out when leaks occurred, were preventive maintenance tasks (~ 30%), including test activities.

Clearly, the assumption that the effect of carrying out proof tests is purely positive in terms of added component reliabilities and reduced accident risk, is misleading. As commented by Vinnem and Røed [51];

> *"It should be noted that preventive maintenance is carried out as a risk reducing measure; so this is a measure that is intended to reduce risk, when multiple times, it has in fact introduced risk"*

8.5 On the Alignment with Keeping the Risk of the Activities ALARP

The responsible party of petroleum activities on the NCS shall choose the solutions that will offer the best results in reducing the risk, unless the costs are significantly disproportionate to the achieved risk reduction. [15] This is frequently referred to as “The ALARP Principle”, stating that risk should be kept As Low As Reasonably Practicable. [52]

In the context of updating component test intervals for SISs in wells, it is relevant to make some evaluations on how the change in test intervals, and the methods and procedures used to derive at said test interval, aligns with the ALARP principle.

As a thought experiment, consider the number of tests to be performed on the SIF “Isolation of production bore in one topside well from the production manifold/flowline (ESD)” in a well with newly installed PMV/PWV and DHSV during the first year.

If test intervals are scheduled for the components in the PM programme according to NORSOK D-010, this means a total of 6 proof tests (every 1 -,1 -,1 -,3 -,3 -,3 - months) to be performed. According to the results for SIL as a function of test interval length presented in *Chapter 7.2*, this will keep the SIF within SIL 3 with a 49% and 31% SIL 3 margin for the one - and three – month test intervals, respectively.

If test intervals are scheduled for the components in the PM programme based on the results of performing an analysis of optimum test intervals for the components according to the suggested approach in this study, this implies a total of 4 tests during the first year (every 3 -, 3 (6) -, 3 -, 3 (6) - months) months, as the PMV/PWV and DHSV can be tested in the same process when the three month test interval for the DHSV and 6 month test interval for the PMV/PWV overlap. This will, according to the results in *Chapter 7.2*, maintain the SIF within SIL 3 with a 19% SIL 3 margin.

Hence, the necessary level of risk reduction set to the SIF (SIL 3) is reached in both test programmes, although the risk is further reduced if tests are scheduled according to NORSOK D-010. However, is this necessary when the SIF will already achieve the required risk reduction if tests are run at 3 – and 6 – month intervals? It could be argued that the cost of running two additional tests is in gross disproportion to the achieved risk reduction, since the desired level of risk reduction is already achieved.

In addition, other risks arise – the risk of a test induced accident or hydrocarbon leak, or the introduction of a latent systematic failure due to human errors in performing the test. Taking this into consideration, it can be argued that one should test as seldom as possible while still keeping the SIF within its SIL requirement with sufficient certainty in order to keep the risk of the activities ALARP.

On the other hand, as already discussed, when the components enter into 6 – months test frequency according to NORSOK D-010, SIL 3 is not achieved, and additional risk reducing measures need to be implemented in order to achieve the necessary level of risk reduction, the costs of which might also be significant.

It is therefore the opinion of the author of the current work that maintaining well barrier (SIF) integrity such that risk is kept as low as reasonably practicable is best achieved by optimising component test intervals based on the demonstrated reliability performance of components in operation. It is the hope of the author that the suggested approach presented in this thesis can aid operators in performing such analyses in the future.

9 CONCLUSION

In this thesis, a reliability/availability case analysis of the safety instrumented function “Isolation of production bore in one topside well from the production manifold/flowline (ESD)” in offshore production wells was performed to identify optimum test intervals for the PWV, PMV and DHSV well barrier components based on demonstrated reliability in operation. Historical data of the components collected from production wells in the Greater Ekofisk Area was provided by ConocoPhillips Norway.

The starting point of the analysis was the methods and recommendations for SIL verification and considerations for updating component test intervals in NOG 070/The PDS report. Academic contributions on assessment of uncertainties in SIL verification and updating of component test intervals was evaluated for practical implementation. However, some challenges were identified in applying these methods to operational data of well barrier components. Consequently, a new approach for an integrated and dynamic process of SIL verification and optimisation of component test intervals with added weight to uncertainties was suggested in this work as a practical solution to these challenges for operators and other end users. A checklist and decision framework to identify and communicate the uncertainties of the reliability/availability analysis was developed to provide broad decision support.

The key findings from performing the case analysis using the suggested approach are:

- There was sufficient operational data available to calculate updated DU failure rates based solely on operational experience. The 90% confidence intervals of DU failure rates showed that the reliability of the PWV and PMV is significantly higher than the DHSV.
- Water breakthrough due to mature waterflooding is observed in some of the wells included in the analysis. This increases the likelihood of both scale formation and corrosive environments in these wells, which are component performance influencing factors. This is believed to affect component lifetimes, and hence DU failure rates and optimum test intervals between wells.
- From the case analysis, it was identified that optimum component test intervals are 6 months for the PMV/PWV and 3 months for the DHSV with a 19% remaining SIL 3 margin for the safety instrumented function “Isolation of production bore in one topside

well from the production manifold/flowline (ESD)". The test interval can likely be further extended if it is separated between scale and non-scale wells.

- It was identified that the Weibull distribution is a better fit than the exponential distribution recommended in NOG 070 to model component lifetimes. However, it was identified that the components are likely within their useful lifetime and the exponential distribution will yield conservative estimates after about six months into operation. The recommended reliability model in NOG 070 is therefore not concluded to be inappropriate to model the lifetimes of well barrier components.
- Uncertainty arises in the data collection and treatment, parameter estimation, model and completeness of reliability analyses of safety instrumented functions in wells. In the case analysis, the key source of uncertainty was identified to be differing operational environments between components in wells e.g. due to scale potential and corrosive environments. This source originates in the data but will increase the uncertainty in the DU failure rates and ability of model output results to predict future component performance.
- Based on the documented historical reliability performance data in this thesis, it can be justified to extend component test intervals beyond the 1 – and 3 – month requirements in NORSOK D - 010. It is believed that the test intervals can be further extended for good wells if it is filtered on scale and/or water breakthrough in the reliability analysis. However, 6-month test intervals for both the PMV/PWV and DHSV as prescribed in NORSOK D-010 cannot currently be recommended based on demonstrated component reliabilities as the function will then exceed the quantitative SIL 3 requirement.
- The current test intervals for the PMV, PWV and DHSV as prescribed in NORSOK D-010 are identified to be inappropriate in both ends based on the demonstrated reliability performance. It is therefore the recommendation of the author of this thesis that changing to a performance – based strategy for scheduling proof test intervals is more appropriate in the task of maintaining well barrier integrity such that the risk of the activities is kept as low as reasonably practicable (ALARP).

10 RECOMMENDATIONS FOR FUTURE RESEARCH

During the case analysis in this thesis, some factors were identified that increases the uncertainty in the reliability/availability analysis of safety instrumented functions and components in wells. These should be subject to further research to improve the analysis methods for a reliability performance and cost optimal identification of component test intervals.

- ***Environmental effects on component reliability/availability:*** According to production specialists COPNO, both scale and the presence of corrosive substances in some wells are enhanced due to early water breakthrough/mature waterflooding. It is therefore recommended that information of water break through should be added to the dataset provided the analyst. In the reliability/availability analysis, it should be separated between wells subject to mature waterflooding/water breakthrough and/or scale potential, and "normal" wells. Updated DU failure rates should be calculated, and optimum component test intervals identified for these different classes of wells.

- ***Develop Weibull Distribution Models for the Availability of Safety Instrumented Functions:*** It was identified that both the PMV, PWV and DHSV is better modelled by the Weibull than the exponential distribution. Methods to apply the Weibull distribution to model the availability of safety instrumented functions should be developed, in particular focusing on the challenges with adequate methods for estimating shape and scale parameters in the presence of few registered DU failures (the no data – problem).

- ***The costs and benefits of reliability – optimized component test intervals:*** An economic analysis should be performed in order to assess if the optimum test intervals based on demonstrated reliability performance of the components, is also optimal from an economic perspective. In particular, the cost of having separate test intervals for the PMV/PWV and DHSV should be evaluated.

REFERENCES

1. Petroleum Safety Authority Norway (PSAN), *The management regulations §5 Barriers* 2016: ptil.no.
2. Petroleum Safety Authority Norway (PSAN), *Principles for barrier management in the petroleum industry BARRIER MEMORANDUM 2017*. 2017: ptil.no.
3. IEC (International Electrotechnical Commission), *IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems* 2010, IEC: Geneva.
4. IEC (International Electrotechnical Commission), *IEC 61511: Functional Safety - Safety Instrumented Systems for the Process Industry*. 2004, IEC: Geneva.
5. Norwegian Oil and Gas Association, *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)*. 2001, revised 2018.
6. Standards Norway (NORSOK), *D-010 Well integrity in drilling and well operations*. 2013.
7. Turander, E. *Risk-based approach to valve testing in wells could save US$10m annually per asset* 2015; Available from: https://www.dnvgl.com/news/risk-based-approach-to-valve-testing-in-wells-could-save-us-10m-annually-per-asset-28232.
8. Hauge, S. and Lundteigen, M.A., *Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase*. 2008, SINTEF Technology and Society Safety and Reliability: Trondheim, Norway.
9. Lundteigen, M.A., *Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation*, in *Department of Production Quality Engineering*. 2009, Norwegian University of Science and Technology Norway.
10. Sultana, S., *A new approach of uncertainty treatment in the verification of safety integrity level of safety instrumented system*. 2015, University of Stavanger, Norway.
11. Abrahamsen, E.B. and Røed, W., *A New approach for verification of safety integrity levels.* Reliability: Theory & Applications, 2011. **6**(1 (20)).
12. Gelyani, A.M., Selvik, J.T., and Abrahamsen, E.B., *Decision criteria for updating test intervals for well barriers.* Journal of Risk Research, 2016. **19**(3): p. 305-315.
13. Petroleum Safety Authority Norway (PSAN), *The framework regulations §24 Use of recognised standards* 2018: ptil.no.
14. Committee on Foundations of Risk Analysis, *Society for Risk Analysis Glossary*. 2015, Society for Risk Analysis: sra.org.
15. Petroleum Safety Authority Norway (PSAN), *The framework regulations §11 Risk reduction principles*, in *11*, PSAN, Editor. 2018: ptil.no.
16. Aven, T., *Risk Analysis*. 2015: John Wiley & Sons.
17. Aven, T., *Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management*. 2014: Routledge.
18. Aven, T., *Pålitelighets-og risikoanalyse*. 1998: Universitetsforlaget.
19. Petroleum Safety Authority Norway (PSAN), *The management regulations §4 Risk reduction*. 2016: ptil.no.
20. Standards Norway (NORSOK), *Z-013 Risk and emergency preparedness assessment* 2010.
21. Petroleum Safety Authority Norway (PSAN), *The facilities regulations §48 Well barriers* 2016: ptil.no.
22. Petroleum Safety Authority Norway (PSAN), *The facilities regulations §8 Safety functions* 2016: ptil.no.
23. Petroleum Safety Authority Norway (PSAN), *The activities regulations §47 Maintenance programme*. 2018: ptil.no.
24. Petroleum Safety Authority Norway (PSAN), *The activities regulations §45 Maintenance*. 2018: ptil.no.
25. Hauge, S. and Øien, K., *Guidance for barrier management in the petroleum industry*. 2016, SINTEF: Trondheim.

26. Rausand, M., *Reliability of safety-critical systems: theory and applications*. 2014: John Wiley & Sons.
27. Moss, T.R., *The reliability data handbook*. 2005: Wiley-Blackwell.
28. Rausand, M. and Høyland, A., *System reliability theory: models, statistical methods, and applications*. Vol. 396. 2004: John Wiley & Sons.
29. Arild, Ø. *Lecture: The average probability of failure on demand (PFDavg/MFDT)*. in *Pålitelighetsanalyse (RIS510)*. 2018. University of Stavanger.
30. ReliaSoft Corporation, *Life Data Analysis Reference*. 2015: Tucson, Arizona USA.
31. Palisade Corporation, *User's guide @RISK Risk Analysis and Simulation Add-In for Microsoft Excel*. 2016.
32. Arild, Ø. *Lecture: Analysis of reliability data*. in *Pålitelighetsanalyse (RIS510)*. 2018. University of Stavanger.
33. Hauge, S., et al., *Reliability Prediction Method for Safety Instrumented Systems*. 13 ed. PDS Method Handbook 2013: SINTEF Technology and Society.
34. Rao, K.D., et al., *Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies.* 2007. **92**(7): p. 947-956.
35. Flage, R. and Aven, T., *Expressing and communicating uncertainty in relation to quantitative risk analysis.* Reliability: Theory & Applications, 2009. **4**(2-1 (13)).
36. Durga Rao, K., et al., *Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies.* Reliability Engineering & System Safety, 2007. **92**(7): p. 947-956.
37. O'Hagan, A. and Oakley, J.E., *Probability is perfect, but we can't elicit it perfectly.* Reliability Engineering & System Safety, 2004. **85**(1): p. 239-248.
38. Corneliussen, K., *Well Safety Risk Control in the Operational Phase of Offshore Wells* in *Department of Production and Quality Engineering*. 2006, The Norwegian University of Science and Technology: Trondheim.
39. Norwegian Oil and Gas Association, NTNU, and UiS, *An Introduction to Well Integrity*. 2012: norskoljeoggass.no.
40. ConocoPhillips Company. *Press Photos*. 2019; Available from: http://www.conocophillips.no/newsroom/press-photos/ Accessed: 08.06.2019.
41. Norwegian Petroleum Directorate (NPD). *Faktasider - Felt I Produksjon - Ekofisk*. 2019; Available from: https://npdfactpages.npd.no/factpages/Default.aspx?culture=no Accessed: 08.06.2019.
42. Fostenes, C., *A systematic approach to optimize and improve the Well Integrity Risk Ranking System in ConocoPhillips Norway, COPNO*, in *Department of Petroleum Technology*. 2011, University of Stavanger: Stavanger.
43. ConocoPhillips Company. *Ekofisk*. 2019; Available from: http://www.conocophillips.no/our-norway-operations/greater-ekofisk-area/ekofisk/ Accessed: 08.06.2019.
44. Norwegian Petroleum Directorate (NPD), *Faktasider - Felt i Produksjon - Eldfisk.* 2019.
45. ConocoPhillips Company. *Eldfisk*. 2019; Available from: http://www.conocophillips.no/our-norway-operations/greater-ekofisk-area/eldfisk/ Accessed: 08.06.2019.
46. SINTEF and OREDA, *OREDA: Offshore reliability data handbook*. 4 ed. 2002, Trondheim: OREDA Participants Distributed by: Det norske veritas.
47. Walpole, R.E., Myers, R.H., and Myers, S.L., *Probability & statistics for engineers and scientists* 9ed. 2014, Harlow: Pearson Education.
48. Abrahamsen, E., Asche, F., and Aven, T., *To what extent should all the attributes be transformed to one comparable unit when evaluating safety measures.* The Business Review, 2011. **19**(1): p. 70-76.
49. Abrahamsen, E.B., et al., *Safety management and the use of expected values.* Risk, Decision and Policy, 2004. **9**(4): p. 347-357.
50. Gelyani, A.M., et al., *Some considerations on how often safety critical valves should be tested.* International Journal of Business Continuity Risk Management, 2015. **6**(1): p. 59-67.

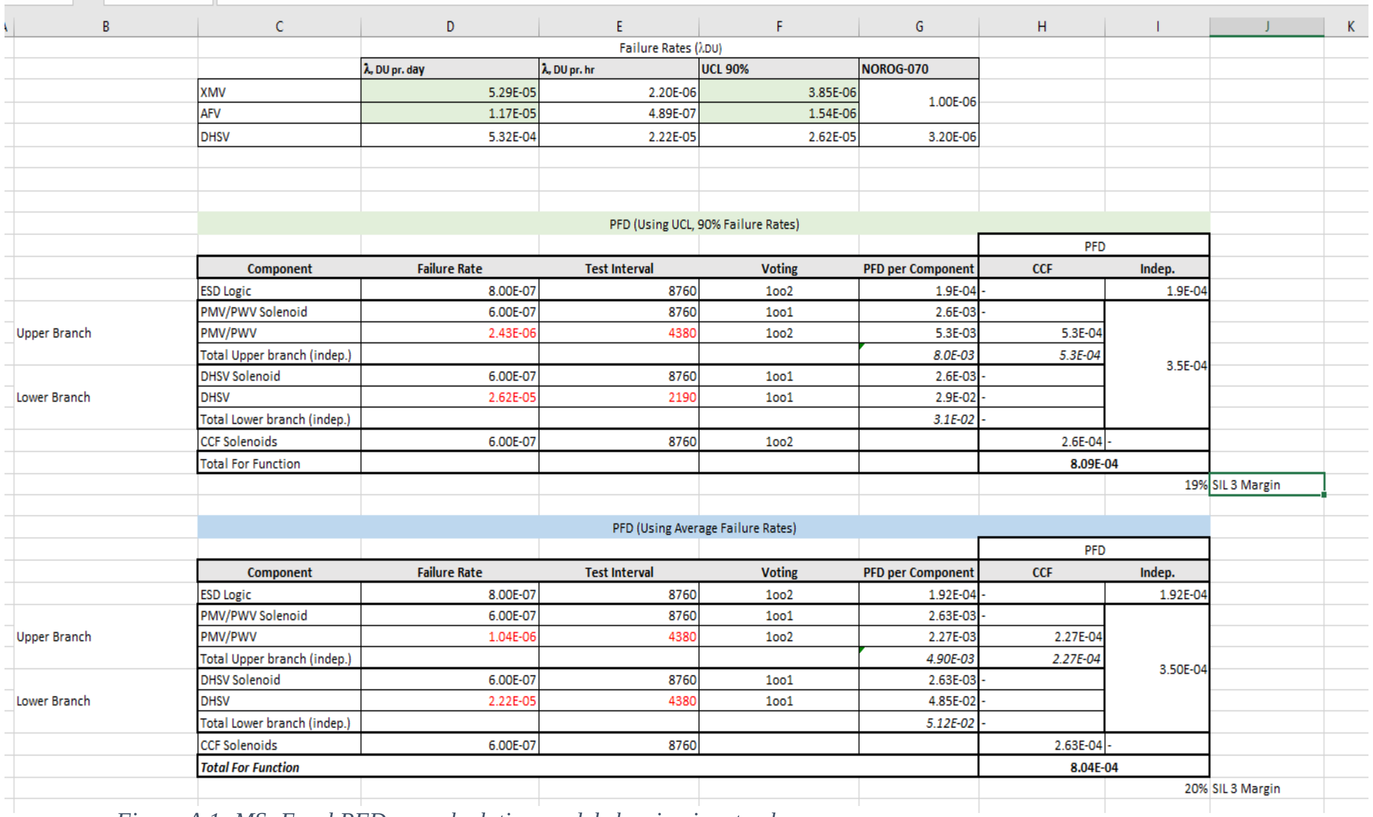
51. Vinnem, J.E. and Røed, W., *Root causes of hydrocarbon leaks on offshore petroleum installations.* Journal of Loss Prevention in the Process Industries 2015. **36**: p. 54-62.

52. Aven, T. and Abrahamsen, E., *On the use of cost-benefit analysis in ALARP processes.* International Journal of Performability Engineering, 2007. **3**(3): p. 345.

APPENDIX

A.1 MS-Excel Calculation Model for PFDavg

The MS-Excel calculation model used to derive the PGDavg for the case SIF using average and U90 DU failure rates can be seen with input values without calculation formulas *Figure A.1* below, and with calculation formulas *Figure A.2* below.



Failure Rates (λDU)

	λ, DU pr. day	λ, DU pr. hr	UCL 90%	NOROG-070
XMV	5.29E-05	2.20E-06	3.85E-06	1.00E-06
AFV	1.17E-05	4.89E-07	1.54E-06	
DHSV	5.32E-04	2.22E-05	2.62E-05	3.20E-06

PFD (Using UCL, 90% Failure Rates)

						PFD	
	Component	Failure Rate	Test Interval	Voting	PFD per Component	CCF	Indep.
	ESD Logic	8.00E-07	8760	1oo2	1.9E-04	-	1.9E-04
	PMV/PWV Solenoid	6.00E-07	8760	1oo1	2.6E-03	-	3.5E-04
Upper Branch	PMV/PWV	2.43E-06	4380	1oo2	5.3E-03	5.3E-04	
	Total Upper branch (indep.)				*8.0E-03*	*5.3E-04*	
	DHSV Solenoid	6.00E-07	8760	1oo1	2.6E-03	-	
Lower Branch	DHSV	2.62E-05	2190	1oo1	2.9E-02	-	
	Total Lower branch (indep.)				*3.1E-02*	-	
	CCF Solenoids	6.00E-07	8760	1oo2		2.6E-04	-
	Total For Function					**8.09E-04**	

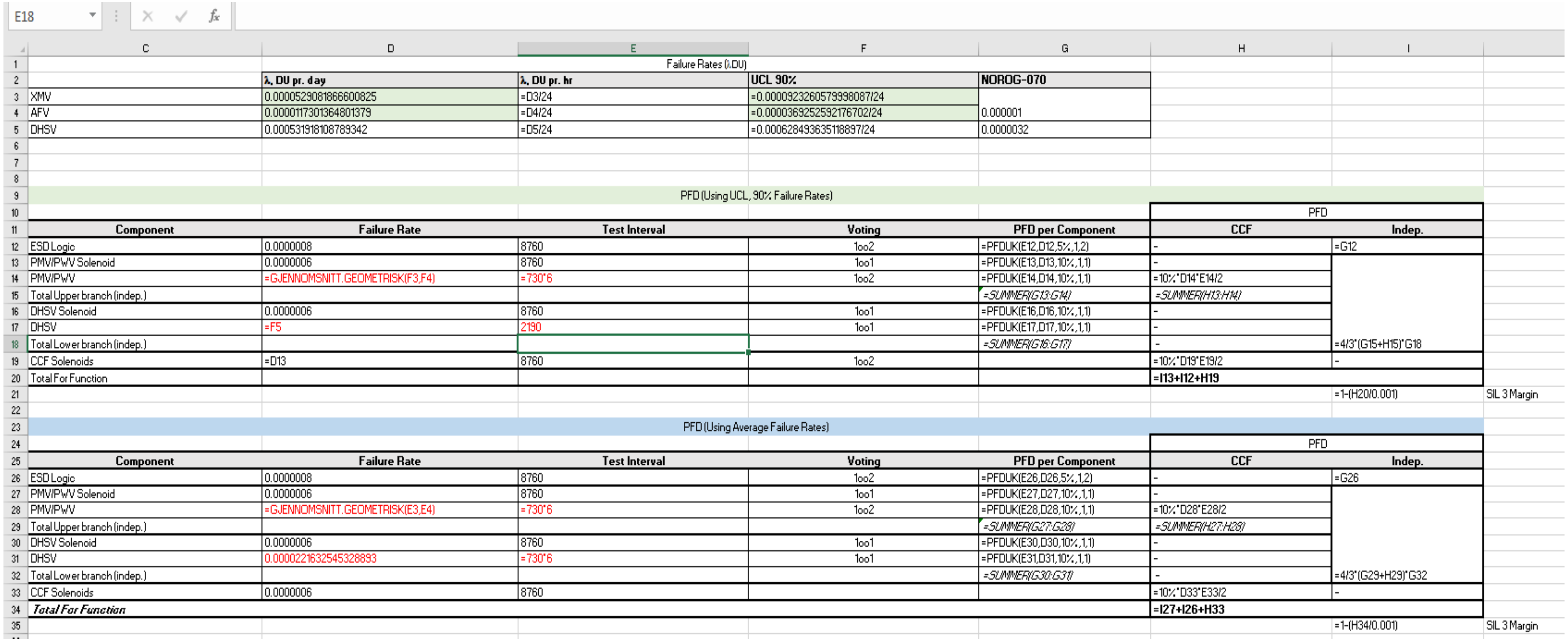
19% SIL 3 Margin

PFD (Using Average Failure Rates)

						PFD	
	Component	Failure Rate	Test Interval	Voting	PFD per Component	CCF	Indep.
	ESD Logic	8.00E-07	8760	1oo2	1.92E-04	-	1.92E-04
	PMV/PWV Solenoid	6.00E-07	8760	1oo1	2.63E-03	-	3.50E-04
Upper Branch	PMV/PWV	1.04E-06	4380	1oo2	2.27E-03	2.27E-04	
	Total Upper branch (indep.)				*4.90E-03*	*2.27E-04*	
	DHSV Solenoid	6.00E-07	8760	1oo1	2.63E-03	-	
Lower Branch	DHSV	2.22E-05	4380	1oo1	4.85E-02	-	
	Total Lower branch (indep.)				*5.12E-02*	-	
	CCF Solenoids	6.00E-07	8760			2.63E-04	-
	Total For Function					**8.04E-04**	

20% SIL 3 Margin

Figure A.1: MS- Excel PFDavg calculation model showing input values



E18 fx

	C	D	E	F	G	H	I	
1		Failure Rates (λDU)						
2		**λ, DU pr. day**	**λ, DU pr. hr**	**UCL 90%**	**NOROG-070**			
3	XMV	0.0000529081866600825	=D3/24	=0.0000923260579998087/24				
4	AFV	0.0000117301364801379	=D4/24	=0.0000369252592176702/24	0.000001			
5	DHSV	0.000531918108789342	=D5/24	=0.000628493635118897/24	0.0000032			
6								
7								
8								
9	PFD (Using UCL, 90% Failure Rates)							
10						PFD		
11	**Component**	**Failure Rate**	**Test Interval**	**Voting**	**PFD per Component**	**CCF**	**Indep.**	
12	ESD Logic	0.0000008	8760	1oo2	=PFDUK(E12,D12,5%,1,2)	-	=G12	
13	PMV/PWV Solenoid	0.0000006	8760	1oo1	=PFDUK(E13,D13,10%,1,1)	-		
14	PMV/PWV	=GJENNOMSNITT.GEOMETRISK(F3,F4)	=730*6	1oo2	=PFDUK(E14,D14,10%,1,1)	=10%*D14*E14/2		
15	Total Upper branch (indep.)				*=SUMMER(G13:G14)*	*=SUMMER(H13:H14)*		
16	DHSV Solenoid	0.0000006	8760	1oo1	=PFDUK(E16,D16,10%,1,1)	-		
17	DHSV	=F5	2190	1oo1	=PFDUK(E17,D17,10%,1,1)	-		
18	Total Lower branch (indep.)				*=SUMMER(G16:G17)*	-	=4/3*(G15+H15)*G18	
19	CCF Solenoids	=D13	8760	1oo2		=10%*D19*E19/2	-	
20	Total For Function					**=I13+I12+H19**		
21							=1-(H20/0.001)	SIL 3 Margin
22								
23	PFD (Using Average Failure Rates)							
24						PFD		
25	**Component**	**Failure Rate**	**Test Interval**	**Voting**	**PFD per Component**	**CCF**	**Indep.**	
26	ESD Logic	0.0000008	8760	1oo2	=PFDUK(E26,D26,5%,1,2)	-	=G26	
27	PMV/PWV Solenoid	0.0000006	8760	1oo1	=PFDUK(E27,D27,10%,1,1)	-		
28	PMV/PWV	=GJENNOMSNITT.GEOMETRISK(E3,E4)	=730*6	1oo2	=PFDUK(E28,D28,10%,1,1)	=10%*D28*E28/2		
29	Total Upper branch (indep.)				*=SUMMER(G27:G28)*	*=SUMMER(H27:H28)*		
30	DHSV Solenoid	0.0000006	8760	1oo1	=PFDUK(E30,D30,10%,1,1)	-		
31	DHSV	0.000022163254532889З	=730*6	1oo1	=PFDUK(E31,D31,10%,1,1)	-		
32	Total Lower branch (indep.)				*=SUMMER(G30:G31)*	-	=4/3*(G29+H29)*G32	
33	CCF Solenoids	0.0000006	8760			=10%*D33*E33/2	-	
34	***Total For Function***					**=I27+I26+H33**		
35							=1-(H34/0.001)	SIL 3 Margin

Figure A.2: MS- Excel PFDavg calculation model showing calculation formulas