University of
Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: **Offshore Technology / Risk management**	Spring semester, **2012** ~~Open~~ / **Restricted access**
Writer: **Md. Jahedul Islam**	(Writer's signature)

Faculty supervisor: **Prof. Eirik Bjorheim Abrahamsen (University of Stavanger)**

External supervisor(s):

Title of thesis: **Reliability of Subsea Equipment in order to Verify Safety Integrity Level (SIL) in Presence of Uncertainty**

Credits (ECTS): **30**

Key words: Oil and Gas; Reliability analysis; Safety Instrumented System; Safety Instrumented Functions; Safety Integrity level; SIL verification approaches; OREDA database; Subsea equipments; Failure rates; Uncertainty analysis; Uncertainty evaluation; MTO perspective; Decision making under uncertainty.	Pages: 41 + enclosure: 26 Stavanger, 14th June 2012

Abstract

The IEC standards 61508/61511 need to be defined and verified by the reliability targets or safety integrity targets for safety instrumented functions (SIF). The reliability targets or safety integrity targets are categorised as four safety integrity level (SIL). There are many design requirements for each SIL level, including requirements of the average probability of failure on demand (PFD_{avg}) (Abrahamsen and W. Roed, 2010). The main objective of this master thesis was to deal with reliability of several subsea equipments in order to verify SIL level by taking uncertainty into consideration. In line with main purpose of these thesis two different approaches of SIL verification of several subsea equipments was to demonstrate according to the IEC standards 61508. The verification of the SIL requirements for the PFD_{avg} is based on a quantitative analysis. The two approaches of SIL verification are known as the traditional approach and a new approach by Abrahamsen. The traditional approach is the approach where we can calculate PFD_{avg} directly and then compared with the criteria for different SIL level which is shown in figure 1. However, this approach cannot be considered as an adequately good basis for decision makers to verify SIL, only by focusing on the assigned probability of failure on demand. There is a need for immense requirements of SIL verification according to the assigned probability number that can be covered through a new approach proposed by Abrahamsen. The key aspect of new approach is related to the uncertainty. There will be more discussion related to those two approaches on the later part of my thesis.

The main difference between the two approaches can easily be referred as to which way we should proceed to get a more reliable operation. It is obvious that uncertainty of any particular equipment or system can give us the different SIL requirements as compared to the traditional way of finding SIL level. Then the decision may arise from that result as to take what further improvement measure for any system in SIS of reliability assessment. A literature study of uncertainty analysis was carried out in order to identify the main sources of uncertainty in reliability assessments for several subsea equipments and also to differentiate approaches for quantifying their effects. However, the broadly accepted standard for design and operation of SIS, IEC 61508, does not explicitly treat the subject of uncertainty. Therefore, my focus is to contemplate clear concepts on uncertainty factors before going to make decisions on SIL level verification. I have done several calculations of PFD_{avg} for various subsea equipments by considering different times of operation. I was highly fascinated to see the widely varying probability numbers from those calculations. And thus, I started to analyze why the failure rates are higher for some particular subsea equipments, which will be discussed in the later part of my thesis. Generally those failure rates comes from the uncertainties of those equipments which are causes of several factors such human involvement workplace, human error, hardware problem, software problem, lack of reliable data collection, poor management systems, typical work process between experienced and inexperienced personnel, inexperience personnel working on the new technologies etc. It was found that sensitivity analysis could also be an important measure to categorize uncertainties. There was important discussion about the human factors in process industries and several uncertainty evaluations according to the MTO (Human, Technology and Organization) perspectives.

Acknowledgement

This master thesis is carried out to analyze the reliability of several subsea equipments and to verify the safety integrity level by using two different approaches under the super vision of Professor Eirik Bjorheim Abrahamsen. During my work on the thesis I have received important and relevant information from several sources.

At first, I would like to thank professor, Eirik Bjorheim Abrahamsen, for introducing this subject and for helping me to get relevant information. I have received important support from him which has helped me to continue this thesis.

Furthermore, I would like to thank the professors from University of Stavanger, specially Ove Tobias Gudmestad, Terje Aven and Tore Markeset and my fellow classmates for giving me updates and news related to my thesis work. And I would also like to thank my family members for their everlasting support and encouragement for me to continue this thesis.

Terminology

IEC standards 61508- Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems

SIL – Safety Integrity Level

SIS – Safety Instrumented System

SIF – Safety Instrumented Functions

PFD – Probability of Failure on Demand

MTO – Human, Technology and Organization

OREDA – The Offshore Reliability Data

EPU – Electrical Power Unit

HPU – Hydraulic Power Unit

UPS – Uninterrupted Power Supply

MCS – Master Control Station

CIU – Chemical Injection Unit

SDM – Subsea Distribution Module

SCM – Subsea Control Module

SCV – Solenoid Control Valve

SSIV – Subsea Safety Isolation Valve

LHS – Latin Hypercube Sampling

LQM – Living Quarter Module

BBSM – Behavioural Based Safety Management

PTW – Permit to Work System

PLDC – Process Leak Detection and Control

ESD – Emergency Shutdown system

PSD – Process Shutdown

TSR – Temporary Safe Refuge

EPCI – Engineering, Procurement, Commissioning and Installation

Contents

List of Figures

List of Tables

1. Introduction

Functional safety occupies to identify specific requirements for safety process where hazardous failures lead to severe consequences (e.g. fatality) and then establishing highest tolerable incidence targets for each mode of failure. So any equipment whose failure contributes to a risk is termed as ‘’safety-related’’ (David and Kenneth, 2005).

Safety instrumented systems (SIS) consists of input elements, logic solvers and final elements in figure 1 which are engaged to manage and mitigate the risk to personnel, environment and assets in many industries and everyday life. The main purpose of SIS is to establish a safe state of equipment or the plant if a hazardous event happens (Abrahamsen and W. Roed, 2010). Each SIS has one or more Safety Instrumented Functions (SIF), where every SIF within an SIS has a Safety Integrity Level (SIL). The IEC standards 61508/61511 states four safety integrity levels (SIL 1 – SIL 4) which can be shown in table 1. The higher the safety integrity level, the more strict becomes the requirements. There are many design requirements for each SIL level, including requirements of the average probability of failure on demand (PFD_{avg}) (Abrahamsen and W. Roed, 2010)

Therefore, the SIS is crucial for controlling and mitigating risk, in many industries and everyday life. Because of the main principle of a SIS and its degree of independence of human actions, reliability is of high importance. Reliability assessments of SIS offers an important foundation for decision making and are performed as part of conformity studies in order to verify whether a SIS meets stated safety requirements or not. Unfortunately, there are several aspects in a reliability assessment that cause uncertainty associated with the results. Uncertainty in reliability assessments reduces the confidence in the results, increases the risk of making wrong decision and should therefore be communicated to the decision maker.

The main purpose of this master thesis is to deal with uncertainty in order to verify SIl level for several subsea equipments. Verification of safety integrity level can be established by two different ways according to this master thesis such as traditional approach and a new approach by Abrahamsen. The traditional approach is telling us the direct calculation of PFDavg and then compared with the criteria for the different SIL level. However, this approach cannot be adequately important basis for decision makers to verify SIL only by seeing beyond the assigned probability of failure on demand. There is a need for good design requirements of SIL verification according to the assigned probability number that can be covered in a new approach proposed by Abrahamsen. The key aspect of new approach is related to the uncertainty. The new approach is the way to tell more about how to treat uncertainties and argue that uncertainties should be taken into consideration more elaborately than we have seen in the traditional approach. In this approach we hereby acknowledge that the calculated probability should not be the only source for verifying the established quantitative SIL requirements. We are dealing uncertainties mainly by using reliable database such as OREDA, MTO perspectives and some experts’ knowledge. However, this master thesis is dealing with uncertainties by analyzing some factors of uncertainties in line with MTO perspectives and background information found in the OREDA database.

2. Reliability of Safety Instrumented Systems

Safety Instrumented Systems (SIS) provides a self-sufficient safety layer with the main objective to reduce the risk to personnel, environment and assets. There is a high importance of SIS where reliability and safety are to be considered as an important aspect and may be verified through conformity reports. This section represents important concepts and aspects related to SIS and its reliability.

2.1 General

A SIS is used to lessen risks associated with the operation of a specified hazardous system, by reducing the consequences. The specified hazardous system is term as equipment under control. The equipment under control is confined by safety instrumented functions (SIF) in a SIS or other appropriate safety measures that will control the hazard. The main features about SIS evaluated to other safety systems are capable to evaluate signals by the help of instrumentation. Figure 1 shows a simplified model of a SIS.

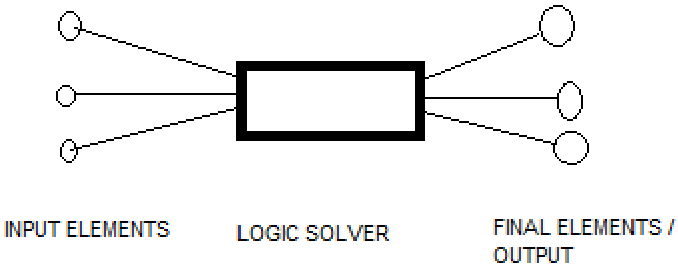


Figure 1 Simplified model of a safety instrumented system (SIS)

A SIS consists of three main elements; input elements for detection, logic solvers for evaluation and decisions and final elements for action if needed. Input elements may be gas or fire detectors, a logic solver may be a computer and the final element a safety valve.

The main reliability measure for a SIF is called Probability of Failure on Demand (PFD). This measure calculates the safety unavailability due to unsystematic hardware failures and denotes the probability that a SIF will fail to react sufficiently upon a demand, a so- called dangerous failure.

2.2 IEC 61508

IEC 61508 "Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems" is a mostly accepted standard for design and operation of SIS. In the standard, a SIS is referred to as an E/E/PE safety related system. It is applicable to all kinds of industries. The oil and gas industry often uses the standard IEC 61511 “Functional safety – Safety instrumented systems for the process industry” instead. IEC 61508 requires a quantitative and qualitative safety and reliability assessment in order to fulfil with the requirements given by the standard. There are two types of safety requirements (David and Kenneth, 2005);

- Functional safety requirements describes what the safety function shall perform
- Safety integrity requirements describes how well the safety function shall perform

2.2.1 Safety Integrity

The concept of safety integrity levels (SILs) is now widespread in the area of safety-critical systems and a number of standards support its use in the design and development of such systems. However, the outcomes of the SILs are not well understood. Whereas the concept is planned to assist the accomplishment and manifestation of safety, it is in many cases causing uncertainty and apprehension.

The highest tolerable failure rate for each hazard normally tends us to establish an integrity target for each part of equipment, depending upon its comparative input to the hazard. These integrity targets are known as ‘safety-integrity levels’ and are generally referred as four levels. A SIL is defined as “discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety related systems...”(IEC 61508, 1997).

SIL 4: the highest target and mostly difficult to achieve, requiring state of the art techniques (usually avoided)

SIL 3: less dangerous than SIL 4 but still requiring the use of sophisticated design techniques

SIL 2: requiring good design and operating practice to a level not unlike ISO 9000

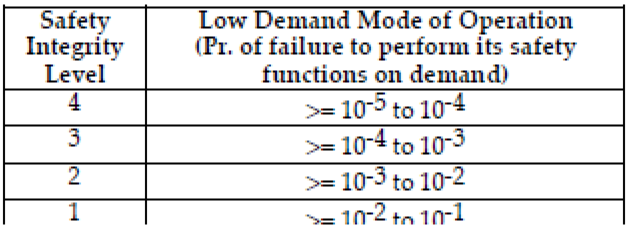
SIL 1: the minimum level but still implying good design practice

< SIL 1 or SIL 0: referred to (in IEC 61508) as ‘not-safety related’ in terms of conformity

(David and Kenneth, 2005)

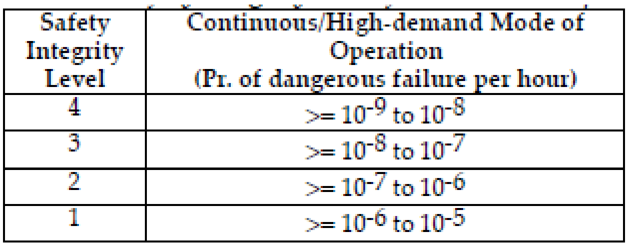
So it is defined as the “probability of a safety related system satisfactorily performing the required functions under all stated conditions within a stated period of time” (IEC 61508, 1997). Safety integrity can here thus be interpreted as reliability.

In order to document compliance with the standard, a reliability analysis of the SIS must document that the calculated PFD_{avg} satisfies the quantitative hardware requirement, as shown in Table 1 and 2.



Safety Integrity Level	Low Demand Mode of Operation (Pr. of failure to perform its safety functions on demand)
4	>= 10^{-5} to 10^{-4}
3	>= 10^{-4} to 10^{-3}
2	>= 10^{-3} to 10^{-2}
1	>= 10^{-2} to 10^{-1}

Table 1 Safety Integrity Levels on Low Demand mode of operation (IEC 61508, 1997)



Safety Integrity Level	Continuous/High-demand Mode of Operation (Pr. of dangerous failure per hour)
4	>= 10^{-9} to 10^{-8}
3	>= 10^{-8} to 10^{-7}
2	>= 10^{-7} to 10^{-6}
1	>= 10^{-6} to 10^{-5}

Table 2 Safety Integrity Levels on High Demand mode of operation (IEC 61508, 1997)

The IEC 61508 states two modes of the E/E/PE systems for employing the safety-related functions, i.e. the low demand mode of operation and the high demand mode of operation. A low demand mode of operation can be established when the frequency of demands for operation is no longer greater than one per year and on greater than twice the proof test frequency. A high demand mode of operation can be defined as the frequency of demand for operation one per year or greater than twice the proof test frequency (Tomasz et el., 2010). During the SIL verification process, the average probability of failure on demand (PFD_{avg}) is refer to the low demand mode of operation or the probability of dangerous failure per hour (PEH) is refer to the high demand mode of operation.

3. Different Approaches of SIL Verification

3.1 Traditional approach

The safety integrity levels for the different safety instrumented functions need to be verified according to the IEC standards 61508/61511. There are several ways to verify SIL but in this thesis we are highlighting traditional approach how to verify SIL according to the IEC 61508. This traditional approach for verification of the quantitative part (PFD) of the SIL level is generally done by a calculation of PFD and then by a comparison with SIL criterion established in IEC 61508.

The basis for this calculation of PFD is to check whether SIL is established for any particular equipment or not. If the probability of failure on demand is in that range we can decide how severe that particular equipment is. But we cannot make any decision only by checking SIL to calculate PFD because there must be lots of factors related to the equipment failure. We will also on the new approach of SIL verification in later part. This part we will focus only traditional way how to verify SIL.

The OREDA database was my most reliable data bank to calculate the average probability of failure on demand. I have done several calculations to determine SIL level by using failure rates from the OREDA database which can be shown both in traditional and new approaches of SIL verification sections. The main objective of the OREDA-2009 handbook is to present average failure rate estimates.

The concept of failure rate function comes from the preventive maintenance because all preventive maintenance management programs are time driven. Meaning that the maintenance tasks are based on elapsed time or hours of operation (Tore Markeset, 2011)

The failure rate function states how likely it is that an item that has continued to exist up to time, t, will tend to fail during next unit of time (OREDA, 2009). If any particular system or item is failing, this possibility will increase with the age t. For example, a person who has reached the age of 80 years will definitely have a higher probability of dying during the next year than a 20 years old person. Therefore, the failure rate function will be known as a function of the time – or, the age of that particular system or item. The mathematical expression for the failure rate function, z(t), is given below as (OREDA, 2009):

$$z(t) = \lim_{\Delta t \to 0} 1/\Delta t \, P(t < T \leq t + \Delta t \mid T > t)$$

Where, T is the time to failure, t means the item is still functioning at time t, Δt is the short time interval, $(t, t + \Delta t)$ means the item will fail in that interval.

The approximation of the above expression:

$$z(t). \Delta t = \Delta t \, P(t < T \leq t + \Delta t \mid T > t)$$

Therefore, the above expression determines that the probability of an item that has reached the age t will fail in the next interval (t, t + Δt).

The failure rate function has different shapes in the life of any technical item. The life of a technical item is divided into three main phases such as early failure phase, useful life phase and wear-out phase. Those phases and estimators of failure rate can be shown in the appendices (part 3).

The above mentioned failure rate is the starting point to analyze the traditional approach. In this part I am going to demonstrate how to calculate PFD_{avg} for several subsea equipments such as subsea manifold, subsea control systems, subsea control system-SSIV, subsea control system-Xmas tree, subsea flowlines and subsea pipelines.

3.1.1 Subsea manifold

Subsea manifold is the equipment for distributing oil and gas stream from the wells into the flowlines to be sent further the surface production facilities. Basically, subsea manifolds consist of steel pipes and valves designed for above purposes. It is one of the critical equipment because it regulates oil and gas flow to the topside. The figure below shows the block diagram of typical subsea manifold. The flowlines from the well is connected via manifold connector. Then the flow which is going to the main piping system of manifold is regulated by the branch valves. There is also one important features of subsea manifold which is the ability of facilitating of pigging operations. Pigging is the activities by launching specialized equipment for measuring important parameters in the piping systems and also for cleaning the internal pipe itself.

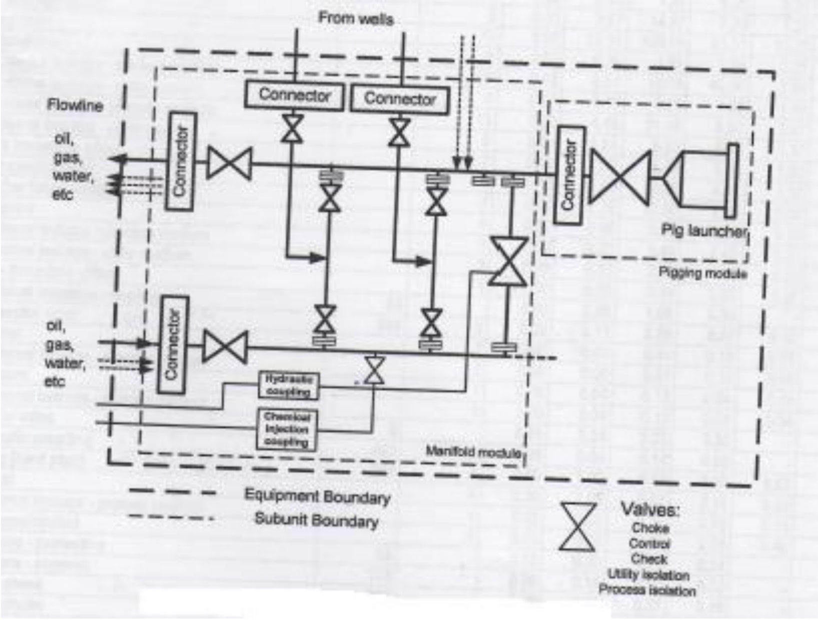


Figure 2 subsea manifolds, boundary definition (OREDA, 2009)

Reliability block diagram of manifold:

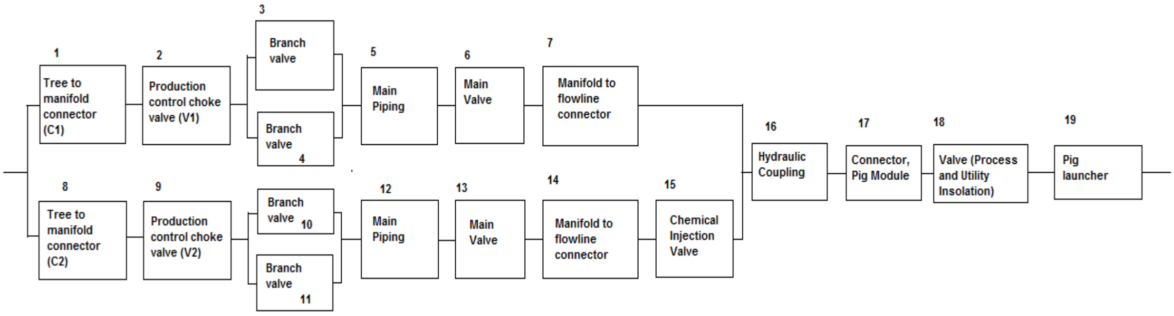


Figure 3 Reliability block diagram of manifold

From the reliability block diagram of manifold module consists of several elements such as:

C1, C2 is the tree to manifold connector,

V1, V2 is the production control check valve,

Brach valve, Main piping, Main valve, Manifold to flow-line connector, Chemical Injection valve and Hydraulic Coupling.

The pig module includes connector, valve both for process and utility isolation and pig launcher.

In this case we will find SIL level for this structure. By doing so, I used to follow OREDA database to calculate PFD average of each element. Here I use the mean failure rate per 10^6 hours from the OREDA database to calculate PFD average.

The actual PFD average formula for single event is as follows:

$$PDF_{avg} = 1 + \frac{1}{\lambda\tau}(e^{-\lambda\tau} - 1)$$

And the minimum cut sets of the above reliability block diagram are:

{1,8},{1,9},{1,10,11},{1,12},{1,13},{1,14},{1,15},

{2,8},{2,9},{2,10,11},{2,12},{2,13},{2,14},{2,15},

{3,4,8},{3,4,9},{3,4,10,11},{3,4,12},{3,4,13},{3,4,14},{3,4,15},

{5,8},{5,9},{5,10,11},{5,12},{5,13},{5,14},{5,15},

{6,8},{6,9},{6,10,11},{6,12},{6,13},{6,14},{6,15},

{7,8},{7,9},{7,10,11},{7,12},{7,13},{7,14},{7,15}, {16},{17},{18},{19}

The PFD average according to min cut sets:

$$PDF_{avg} = \sum_{j=1}^{k} \frac{1}{\left|K_j\right| + 1} \underset{i\varepsilon K_j}{\pi} \left(\lambda_i \tau\right)$$

$$\text{PFD}_{\text{avg}} = 0.0085366 = 8.5 \text{ x } 10^{-3} \text{ (SIL 2)}$$

The calculated PDF_{avg} is for 1 month of operation and it will also remain SIL 2 until 60 days of operation.

The PFD_{avg} until 180 days of operation is given below:

$$\text{PFD}_{\text{avg}} = 0.417157229 = 4.17 \text{ x } 10^{-1} \text{ (SIL 0)}$$

We can see clearly that the probability of failure on demand for subsea manifold increases when the operation time increase. It would be not safety related systems if we want to use after 60 days of operations. Therefore, there must be needed to focus after that time interval of operation by taking necessary maintenance and repair or checking of subsea manifold module.

3.1.2 Subsea Control systems

Subsea control system is the system used for controlling the operations of subsea related equipments as well as for gathering data collections and monitoring of important relevant parameters. The subsea control systems divided into two parts such as topside control system and subsea control system. The topside located systems such as Electrical Power Unit (EPU), Hydraulic Power Unit (HPU), and Master Control Station (MCS) and Chemical Injection Unit (CIU). The subsea control part covers Static Umbilical, Dynamic Umbilical, and Subsea Distribution Module (SDM), Subsea Control Module (s) (SCM), Sensors and Solenoid Control Valve.

Subsea control systems are the heart of subsea operations because it controls what the equipment in the seabed should do and communicate with them. Here electrical power unit is very sensitive because it provides the main power supply and it also covers the power backup system from UPS and battery unit. The means of subsea controlling is done by hydraulic fluid supplied from HPU in the topside meanwhile the control command is via electrical signal from MCS.

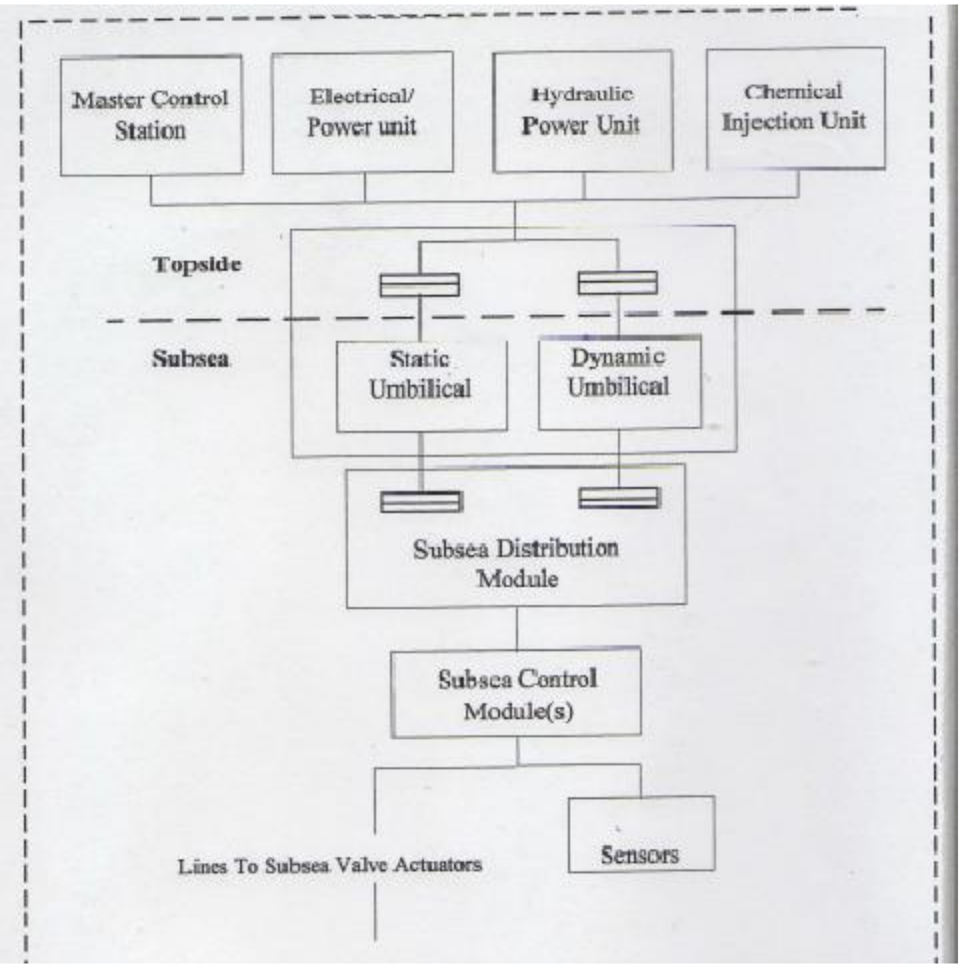


Figure 4 Subsea control systems, boundary definition (OREDA, 2009)

Reliability block diagram of subsea control systems:

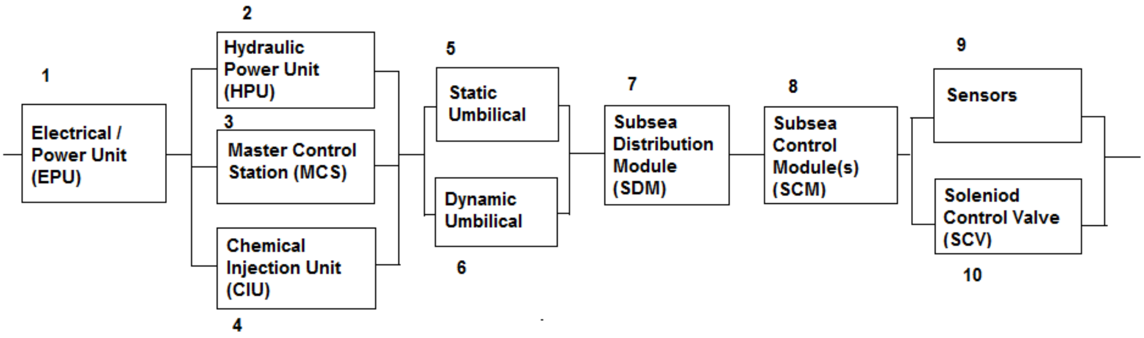


Figure 5 Reliability block diagram of subsea control systems

In this case we will find SIL level for this structure. By doing so, I used to follow OREDA database to calculate PFD average of each element. In this case I use the mean failure rate per 10^6 hours from the OREDA database to calculate PFD average.

The actual PFD average formula for single event is as follows:

$$PDF_{avg} = 1 + \frac{1}{\lambda\tau}(e^{-\lambda\tau} - 1)$$

And the minimum cut set of this reliability block diagram:

{1},{2,3,4},{5,6},{7},{8},{9,10}

The PFD average according to min cut set:

$$PDF_{avg} = \sum_{j=1}^{k} \frac{1}{\left|K_j\right| + 1} \pi_{i \varepsilon K_j} \left(\lambda_i \tau\right)$$

$$PFD_{avg} = 0.017422075 = 1.74 \text{ x } 10^{-2} \text{ (SIL 1)}$$

The calculated PDF_{avg} is for 1 month of operation and it will also remain SIL 1 until 180 days of operation. So the PFD_{avg} until 180 days of operation is given below:

$$PFD_{avg} = 0.1052 = 1.05 \text{ x } 10^{-1} \text{ (SIL 1)}$$

From the above two calculations of PFD_{avg} , we can define which of the probability of failure on demand for subsea control systems is appropriate for SIL requirements. Both calculations show that we can use that subsea control systems until 180 days of operation without any maintenance. However, it does not appropriate decision for the decision maker whether we should proceed or take into consider some other steps to get appropriate idea for SIL verification. We will discuss this one in uncertainty part also to see the variation of SIL level.

3.1.3 Subsea Control systems – SSIV

The SSIV (Subsea Safety Isolation Valve) is the safety critical equipment to isolate the pipelines in case of emergency condition. Subsea control systems contain the algorithm of how the SSIV should response in this condition. And it also provides hydraulic fluids to operate the valve.

By using same reliability block diagram of subsea control systems we can calculate PDF_{avg} for SSIV control systems.

$PFD_{avg} = 0.0056709432 = 5.67$ x 10^{-3} (SIL 2) for 1 month of operation

PFD_{avg} = 0.034658501 = 3.47 x 10^{-2} (SIL 1) for 6 months of operation

We can see that the probability of failure on demand for SSIV control systems increases when the operation time increase.

3.1.4 Subsea Control systems – Xmas tree

Subsea control systems for the Xmas tree involves the control of valves installed on the trees and it also involves monitoring of flow related parameters in the trees through the sensors installed. The means of controls is provided by SCM installed in each and every Xmas tree which provide the electrical and hydraulic power needed.

The Xmas tree is the first and main connection to the well. If something happens in the wells which need immediate actions, the valve arrangement in the tree is the one that provides the means of isolation and protection.

By using the following reliability block diagram of subsea control systems for Xmas tree we can calculate PDF_{avg} for Xmas tree control systems.

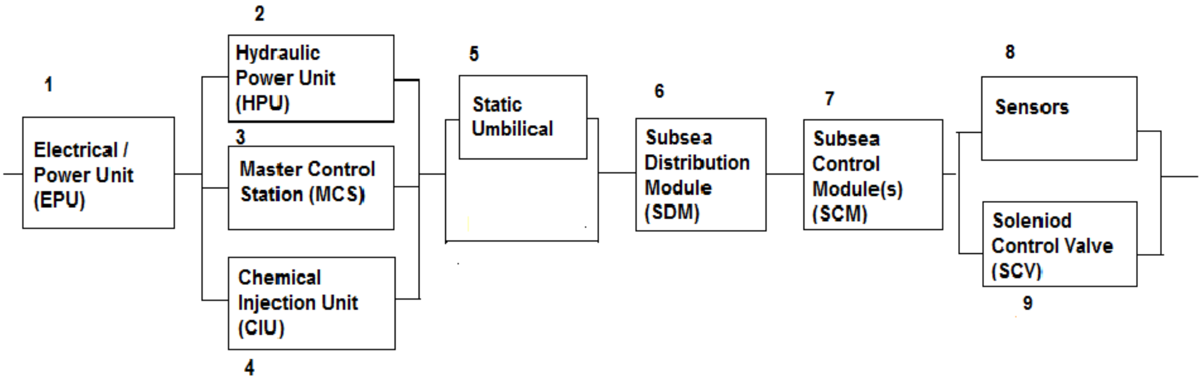


Figure 6 Reliability block diagram of subsea control systems

PFD_{avg} = 0.02375278 = 2.38 x 10^{-2} (SIL 1) for 1 month of operation

PFD_{avg} = 0.165500087 = 1.66 x 10^{-1} (SIL 1 but close SIL 0) for 6 months of operation

Therefore, in that part also shows the variation of probability failure on demand for different time of operations. We will look through above criteria in uncertainty part in order to tell what is the safety integrity requirements should communicate well establish in safety related system.

3.1.5 Subsea Flowlines

Subsea flowlines is the line that connects and transfers fluids (oil, gas, water or chemical) from one subsea unit to another subsea unit.

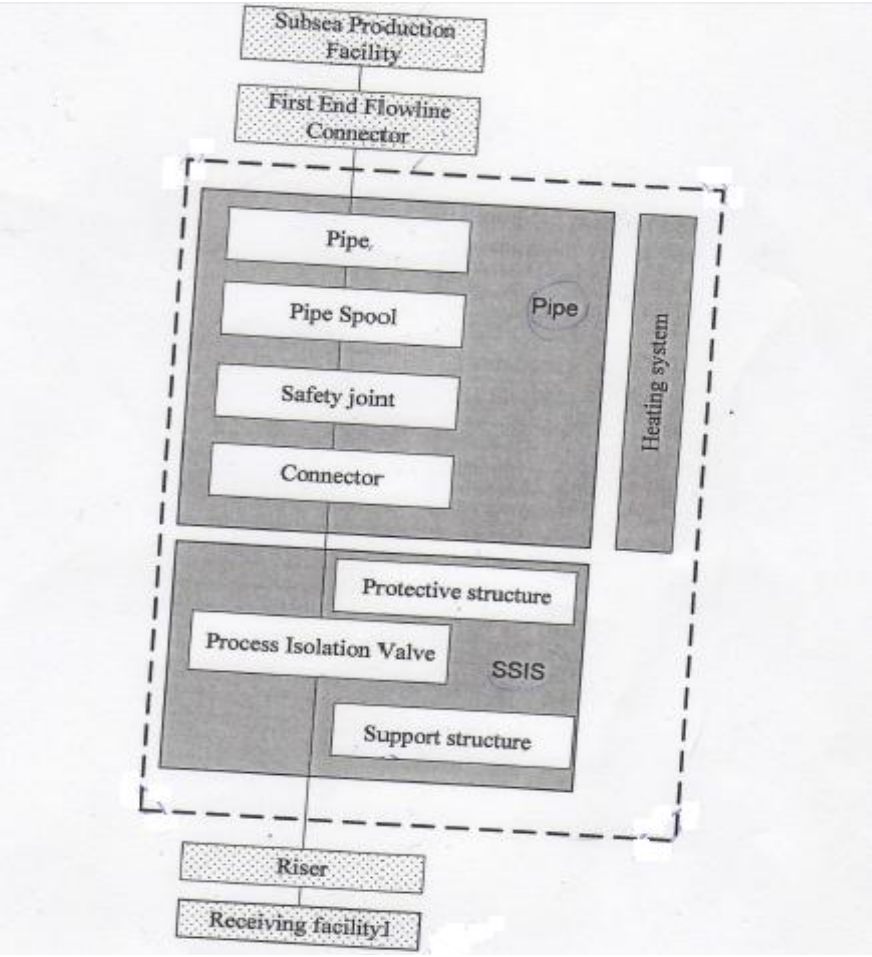


Figure 7 Subsea flowlines, boundary definition (OREDA, 2009)

Reliability block diagram of subsea flowlines:

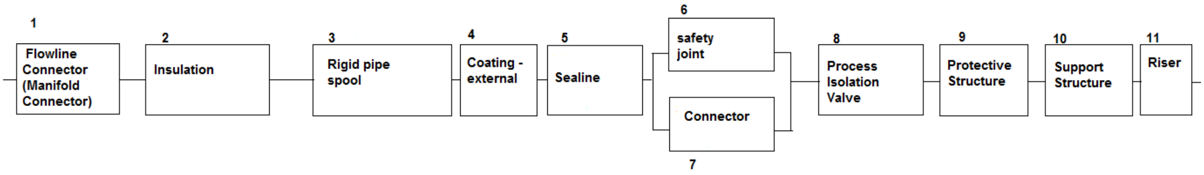


Figure 8 Reliability block diagram of subsea control systems

The subsea flowlines mainly consists of two parts such as pipe and subsea isolation system. The flowline – pipe includes external coating, connector, flexible and rigid pipe spool, insulation, safety joint, sealine. The subsea isolation system covers process isolation valve, protective and support structure.

In this case we will find SIL level for this structure. By doing so, I used to follow OREDA database to calculate PFD average of each element. In this case I use the mean failure rate per 10^6 hours from the OREDA database to calculate PFD average.

The actual PFD average formula for single event is as follows:

$$PDF_{avg} = 1 + \frac{1}{\lambda\tau}(e^{-\lambda\tau} - 1)$$

And the minimum cut set of this reliability block diagram:

{1},{2},{3},{4},{5},{6,7},{8},{9},{10},{11}

The PFD average according to min cut set:

$$PDF_{avg} = \sum_{j=1}^{k} \frac{1}{\left|K_j\right| + 1} \underset{i \varepsilon K_j}{\pi} \left(\lambda_i \tau\right)$$

$$PFD_{avg} = 0.0377324 = 3.77\text{x } 10^{-2} \text{ (SIL 1)}$$

The calculated PDF_{avg} is for 1 month of operation and it will also remain SIL 1until 90 days of operation.

The PDF_{avg} is for 6 months of operation will no longer be determined SIL requirements because of high failure rate comes from the long time operation.

So the PDF_{avg} is 0.226 for 6 months of operation (SIL 0)

3.1.6 Subsea Pipelines

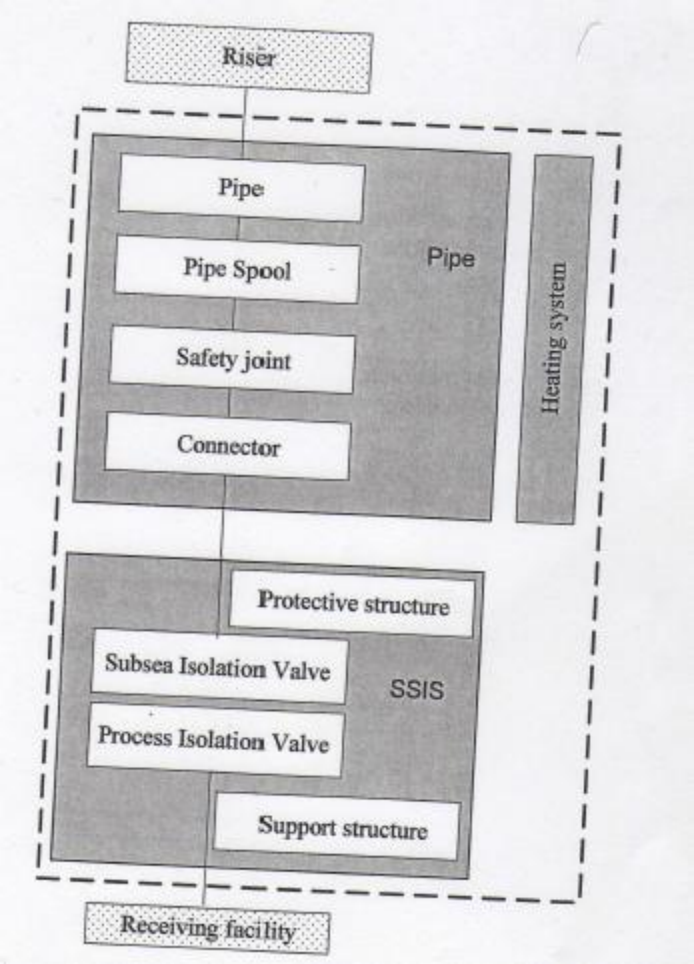


Figure 9 Subsea pipelines, boundary definition (OREDA 2009)

Reliability block diagram of subsea pipelines:

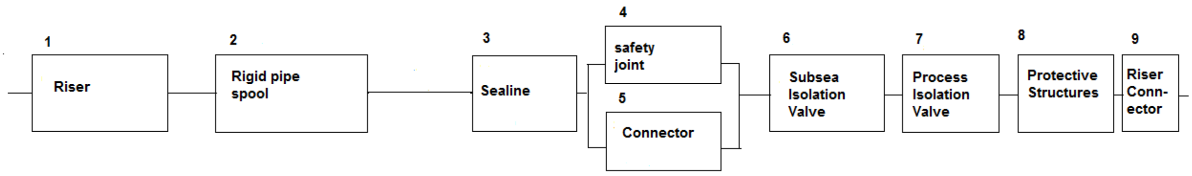


Figure 10 Reliability block diagram of subsea pipeline

The subsea pipelines mainly consist of two parts such as pipe and subsea isolation system. The pipe includes connector, rigid pipe spool, safety joint, sealine. The subsea isolation system covers subsea isolation valve, process isolation valve, protective and support structure.

In this case we will find SIL level for this structure. By doing so, I used to follow OREDA database to calculate PFD average of each element. In this case I use the mean failure rate per 10^6 hours from the OREDA database to calculate PFD average.

The actual PFD average formula for single event is as follows:

$$PDF_{avg} = 1 + \frac{1}{\lambda\tau}(e^{-\lambda\tau} - 1)$$

And the minimum cut set of this reliability block diagram:

{1},{2},{3},{4,5},{6},{7},{8},{9}

The PFD average according to min cut set:

$$PDF_{avg} = \sum_{j=1}^{k} \frac{1}{|K_j| + 1} \underset{i \in K_j}{\pi} \left(\lambda_i \tau\right)$$

$$PFD_{avg} = 0.\ 015695206366 = 1.57 \times 10^{-3} \text{ (SIL 1)}$$

The calculated PDF_{avg} is for 1 month of operation and it will also remain SIL 2 until 60 days of operation.

The PDF_{avg} is for 6 months of operation will be also determined SIL 1 requirements but the probability of failure is tend to be higher than the above calculation for 1 month of operation. So the PDF_{avg} is 0.0942914 for 6 months of operation (SIL 1)

After doing the direct calculation of the average probability failure on demand for above all subsea equipments, we cannot tell whether that mean failure rate can give us appropriate idea of verifying SIL level. Therefore, the traditional approach cannot be well accepted approach to verify SIL requirements.

3.2 A New Approach by Eirik Bjorheim Abrahamsen

The safety integrity verification for safety related systems are an important step in safety life cycle and PFD_{avg} which must be calculated to verify the safety integrity level (SIL). Since IEC 61508 does not show detailed explanations of the definitions and PFD_{avg} calculations, it is quite difficult for reliability engineers to apply the use of standards as guidance. Moreover, the traditional approach does not give us any clue how to treat uncertainty to verify SIL. Hence, Abrahamsen proposed a new approach on how to take uncertainty into consideration when we are verifying SIL. In this master thesis we are considering uncertainty more extensively than seen in the traditional approach.

The assigned probability for failure on demand is conditioned on a number of assumptions and suppositions which can be useful information for decision makers, but it is still necessary to consider uncertainty. The traditional approach only calculates the probability on failure demand, P (failure on demand) but if we consider uncertainty factors related to the particular equipment, to tell the reliability of that equipment we need to rely on experts’ judgement or accessors' degree of belief of that failure probability. That experts' judgement may be our background knowledge. In this case the mathematical expression can be expressed as P (failure on demand |K) where K is the background knowledge. The background knowledge includes historical system performance data, system performance characteristics and experts' degree of belief. This master thesis also covers background information to collect reliable data to calculate PFD according to OREDA database.

This new approach totally based on uncertainty workshop meaning that how we are dealing with uncertainty in real life situation. The assigned probability for the safety system is not an ideal tool to express uncertainty because calculated probabilities are conditioned on specific background information and knowledge (K). Therefore, there are more possibilities to produce poor predictions of the SIL requirements. By doing so, we are investing what are the factors or aspects of uncertainty that should be taken into consideration when a conclusion is made on the SIL level.

At present the oil and gas industry does not consider any non-technical aspects of uncertainties in the PFD calculation methods. The Abrahamsen states that there is a close relation between the PFD calculation results and the SIL level conclusion. Hence we argue that uncertainties should be taken into consideration before making a final decision on the SIL level. For example, this could be established qualitatively in a workshop to the quantitative SIL verification analysis. Afterwards, we can make a decision to see the calculated new PFD prior to the SIL level conclusion. This approach is presented in figure 11 below refereeing both the traditional approach and the new approach suggested by Abrahamsen. We will give more examples of how information about uncertainties could be taken into consideration in the uncertainty evaluation part.

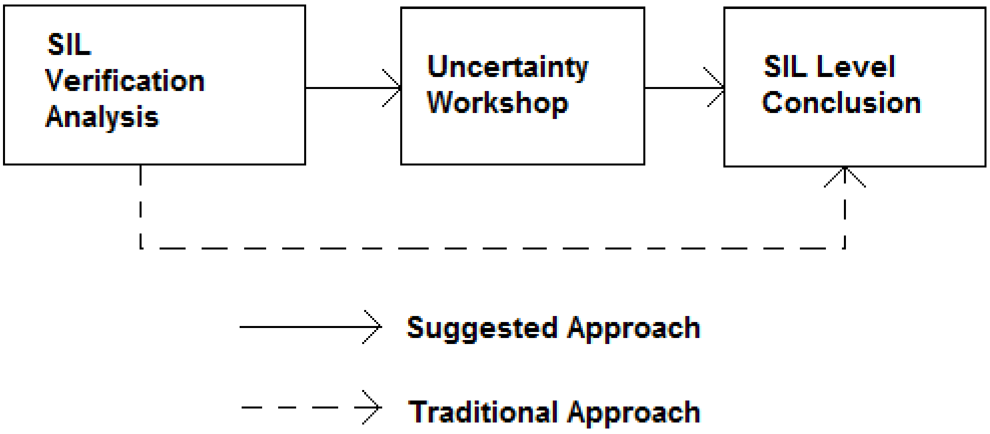


Figure 11 Main principles of the suggested approach. (Abrahamsen, 2010)

To make a better decision we hereby classified uncertainties into three categories: High, medium and low. The categorisation process found in both (Abrahamsen, 2010) and (Flag and Aven, 2009):

High uncertainty:

One or more of the following conditions are met:

- The assumptions made in calculations of P are seen as strong impacts on SIL verification
- Data are not available, or are unreliable
- There is a lack of agreement among experts
- Less experience personnel handling new technologies

Low uncertainty:

All of the following conditions are met:

- The assumptions made in calculations of P are seen as very reasonable
- Much reliable data are available
- There is a broad agreement among experts

Medium uncertainty:

All of the following conditions are met:

- The conditions between those characterising high and low uncertainty
- Environmental data collection during harsh situation

Therefore, it is important to note that the degree of uncertainty must be seen through the effect of the probabilities changes which are assigned to the system for the calculation. For example, high uncertainty comes from the higher failure rates (λ) meaning that higher effect on the assigned probability number will refer us that the uncertainty parameter is high. The failure rates are the potential indicators to determine our uncertainty categorization. But it does not mean that higher failure rates lead to the higher uncertainty because of the other non-technical failure mechanism. There are a lot of factors related to the failure of any particular systems i.e. human error, hardware problem, software problem, poor management systems and typical work process between experienced and inexperienced personnel etc.

However, if the degree of uncertainty seems to be higher but the assigned probability number is relatively insensitive to changes in the certain quantities, then the uncertainty classified could be medium or low. For example, if the probability number is same within the SIL range, then we classify uncertainty according to the calculated higher to lower probability in that level. In that case the calculated PFD_{avg} for subsea flowlines is in the SIL 1 for both traditional approach and new approach, but calculated probability of failure is higher in the new approach. This means that we have to take some steps i.e. risk reducing measures, to establish better SIL level. However, the uncertainty is not high for the subsea flowlines.

3.2.1 SIL requirement for the subsea manifold by using this new approach

We can recall the reliability block diagram of subsea manifold in figure 3. Here we are considering the upper value of failure rate per 10^6 hours of operation. The uncertainty lies here to estimate failure rate by using confidence interval. I am following the 90% confidence interval of failure rate (OREDA, 2009). So the uncertainty of the estimate failure rate may be presented as a 90% confidence interval.

$$\mathrm{P}\ (\lambda_L \ \leq \ \lambda \ \lambda_{\backslash u}) = 90\%$$

In general the upper value of failure rate is not practicable. It is very risky when we obtain the higher failure rate. The equipment will no longer be reliable if we get such kind of failure rate during operation.

By considering the upper limit of failure rate, we calculated the PFD average for the subsea manifold for 1 month of operation is approximately 0.029749218 or 2.97 x 10^{-2}. It can establish SIL 1. Therefore, this value indicates us to consider the safety integrity level 1 for subsea manifold. The PFD average for 6 month of operation is approximately 4.17 x 10^{-1}. It can go to the SIL 0 which is no longer being acceptable to do the operation in that case.

Therefore, here one thing comes in my mind why the probability of failure on demand is very higher if we go for operation up to certain time period. And continuously failure probability is higher during next unit time because of the abrupt comes from that particular equipment. There are a lot of factors related to that high failure which can be discussed in the uncertainty evaluation and uncertainty categorization part later on, but human factors is one of the most critical factors in the uncertainty studies. Because of the high failure rate for the subsea manifold we can expect operation until 30 days by using of it. Hence, it will no longer be accepted by reliability researchers or experts' working on it because that equipment cannot satisfy the SIL level if we want to use after 30 days of operations.

3.2.2 SIL requirement for the subsea control systems by using this new approach

Now we are going to do the same process for the subsea control systems as we did in subsea manifold. According to the figure 5 we can calculate the probability of failure on demand for subsea control systems.

By considering the upper limit of failure rate, the calculated PFD average for the subsea control systems which is approximately 0.073403423 or 7.34 x 10^{-2}. It can establish SIL 1. Therefore, this value refers us to consider the safety integrity level 1 for subsea control systems during 1 month of operation. But the probability of failure on demand goes higher as we consider more than 1 moth of operation. For example, the subsea control systems will longer be able to reliable at the time 180 days where we calculated $\mathrm{PFD}_{\mathrm{avg}}$ is 0.449199 or 4.4 x 10^{-1} (SIL 0).

In that case, we can recommend using subsea control systems until 30 days of operations because it would be difficult to establish stated safety requirements for SIL level afterwards. The calculated probability failure on demand for 6 months of operations tends us to see how severe that subsea control systems and it goes to go the SIL 0 or even higher probability of failure. The causes of failures for subsea control systems can be seen in the uncertainty evaluation and uncertainty categorization part later on.

3.2.3 SIL requirement for the subsea control systems - SSIV by using this new approach

Here we will calculate probability of failure on demand for the subsea control systems - SSIV. We can refer the reliability block diagram of subsea control systems in figure 5

By using the upper limit of failure rate, we calculated the PFD average for the subsea control systems - SSIV for 1 month of operation is approximately 2.04×10^{-2}. It can establish SIL 1. The PFD average for 6 month of operation is approximately 1.27×10^{-1}. It can go to the SIL 1. Therefore, those two different values indicate us to consider the safety integrity level 1 until 180 days of operation for subsea control systems - SSIV. The uncertainty is not very higher up to that particular time of operations.

3.2.4 SIL requirement for the subsea control systems – Xmas tree by using this new approach:

We are going to same process as we did earlier part for the subsea control systems – Xmas tree. By using the reliability block diagram of subsea control systems – Xmas from figure 6 we can calculate the probability of failure on demand.

The PFD average for the subsea control systems – Xmas tree for 1 month of operation is 4.47×10^{-2}. It can establish SIL 1. Therefore, this value tells us to consider the safety integrity level 1 for subsea control systems – Xmas. The PFD average for 6 month of operation is about 4.50×10^{-1}. It can go to the SIL 0 which is no longer being acceptable to do the operation in that case.

The subsea control systems for Xmas tree again critical to do operation after 1 month, however, it can establish SIL level 1 up to 60 days of operations. Therefore, this system will no longer be reliable system if we want to use until 180 days of operations because of the high integrity of that equipment during longer period of time.

3.2.5 SIL requirement for the subsea flowlines by using this new approach

Now we are going to do the process for the subsea flowlines as we did in above part. We can recall the reliability block diagram of subsea flowlines in figure 8

By considering the upper limit of failure rate, we calculated the PFD average for the subsea flowlines for 1 month of operation is approximately $1.45 \mathrm{x} 10^{-1}$. It can establish SIL 1. Therefore, this value indicates us to consider the safety integrity level 1 for subsea flowlines. The PFD average for 6 month of operation is approximately $8.\ 71 \mathrm{x} 10^{-1}$. It can go to the SIL 0 which is no longer being acceptable to do the operation in that case.

3.2.6 SIL requirement for the subsea pipelines by using this new approach

Now we are going to do the process for the subsea pipelines as we did in earlier sections. We can recall the reliability block diagram of subsea pipelines in figure 10.

By considering the upper limit of failure rate, we calculated the PFD average for the subsea pipelines for 1 month of operation is approximately 4.72 x 10^{-2}. It can establish SIL 1. Therefore, this value indicates us to consider the safety integrity level 1 for subsea pipelines. The PFD average for 6 month of operation is approximately 2.85 x 10^{-1}. It can go to the SIL 0 which is no longer being acceptable to do the operation in that case.

By doing so, my thesis concept of uncertainty can become immense interest. I started to analyse what are the factors related to those failure of subsea equipment and how to treat uncertainties. It is very obvious that human error is a major concern when we treat uncertainty. Human may make mistakes and that can go to serious damage of any system.

My thesis work mainly deals with MTO perspective and it is my uncertainty workshop to analyse further improvement of SIL requirements.

4. Uncertainty Analyses

Uncertainty is the major consideration of this thesis in order to verify safety integrity level or SIL. Here I will discuss total thorough details of uncertainty factors related to the different phenomenon. The traditional method shows the SIL, only by the direct calculation of PFD average without uncertainty taken into consideration. My aim is to give appropriate ideas of uncertainty factors in this part. I will focus mainly on MTO perspective to threat uncertainty. At the same time I will give some theoretical background of uncertainty. Therefore, my background knowledge to threat uncertainty is the MTO perspective, OREDA database and some experts' judgment.

Uncertainty is defined as the term "not certainly ascertainable or predetermined" (Webster 1989). Uncertainty in reliability assessments thus shrinks our confidence in the results. It is very important to consider that the decision makers are aware of how the uncertainties are involved in the assessment process.

Risk is something related to unpredictable and negative aspects of any future events A and their consequences C. It is well said that we cannot predict perfectly if these events will happen or not, and if these events occur, what the outcomes or consequences will be. Meaning that there is uncertainty U related to the both A and C. Therefore, the likelihood of those events and the consequences certainly comes from the calculated probabilities P, based on the experts' judgment or background knowledge (K).

Uncertainty refers to something of unknown events and its consequences of any future activities which means that today we actually do not know what is going on in any particular events and what is the probability number of that event.

Hence, we can refer risk is equal to the uncertainty about the consequences of an event seen in relation to the severity of the consequences, where severity is the way to represent the consequences. So the uncertainties are mainly due to the consequences of any particular event.

We are often confused to define risk and uncertainty. It is said that a low degree of uncertainty does not mean a low risk, or a high degree of uncertainty does not mean a high risk. Actually it depends on the assign probability distributions in this case. But in real case we cannot replace uncertainty U with the probability P. Because probability is only a tool to express uncertainty with respect to the event A and the consequence C. However, we cannot even agree with that tool because uncertainty is always hiding in the background knowledge (K). For example in the offshore oil and gas platform topside's equipment such as Electrical Power Unit (EPU), the failure of electrical power unit (EPU) may arise from the critical failure mood of open circuit test or the failure from the transmission line of power supply unit. But in real case it might not be the reason, it may come from the degraded failure mood of insufficient power supply or short circuit test.

Therefore, risk is described by (A, C, C*, U, P, K), where A equals the initiating events, C equals the consequences of the activity, C* is a prediction of C, U is the uncertainty about what value C will take, and P is the probability of specific events and outcomes, given the background knowledge K.

4.1 Uncertainty is a major factor to determine SIL requirements

Uncertainty is a vital part of my thesis to determine SIL requirements. As we have discussed the relation between risk and uncertainty, here we will see how uncertainty affects our real life phenomenon. Our target was to calculate PDF average to determine SIL requirement which is termed as a traditional way of representing SIL. But in that method we cannot say about the reliability of any equipment or system. The IEC 61508 also states the SIL requirement for both low and high demand mood of operation. The traditional way is also a correct method to check whether the equipment meets the SIL requirement or not. Nowadays, most of the oil and gas companies also follow those methods.

However, this thesis work is dealing with uncertainties to give clear idea of reliable operation up to certain periods of time. As we know all the subsea equipments must have certain life time of performance. So we cannot expect more reliable operation if we use those equipments for a long time. Because those equipments must be checked, controlled, maintained and repaired. According to the OREDA database, it shows the failure rate of such equipment is taking per 10^6 hours of operation. I have done a lot of calculations by using OREDA database. I have made several assumptions to check whether those equipments are meeting the SIL requirements or not. It is noted that risk analyses are always based on number of such assumptions.

By doing so, we can analyze various types of systems to give clear idea of risk score of the uncertainties (U). We are giving concept of uncertainty in relation to the MTO perspectives and some other uncertainty factors. If the assessments of uncertainties are shown high, then the factors are also of high risk.

Evaluation of uncertainty is also an important measure to be taken that is shown in the later parts.

4.2 Types of Uncertainty

Reliability analysis expresses the uncertainty about the failure behaviour of a system. Uncertainty can be measured and described by its mathematical language, probability. Generally uncertainty or lack of knowledge can be quantified with the expert’s degree of doubt about a parameter. In this case true values are unknown and can be only estimated.

There are two types of uncertainty: (Spouge 1999)

- Aleatory or Random uncertainty due to natural randomness that can be estimated by the repeated measurements.
- Epistemic uncertainty due to lack of knowledge that can include uncertainties in modeling, data availability and collection.

Reliability analysis deals with many processes and systems which consist of aleatory uncertainties. It is for example impossible to predict exactly on which demand a Safety Instrumented System (SIS) will fail to respond. This is due to variability in the system that cannot be eliminated because of inherent randomness which causes events with stochastic properties. This is why also aleatory uncertainty often is referred to as "stochastic uncertainty" (Mosleh, et al. 1995). The epistemic uncertainty is the only reducible uncertainty, it is crucial to address the uncertainties correctly in order to achieve reduction if possible.

At present time, with available technology and resources, it is practicable impossible to achieve complete knowledge about every system or process within reasonable time. The only advantage must be to separate those uncertainties that can be reduced from those that are less prone to reduction in nearest future (Kiureghian and Ditlevsen 2009).

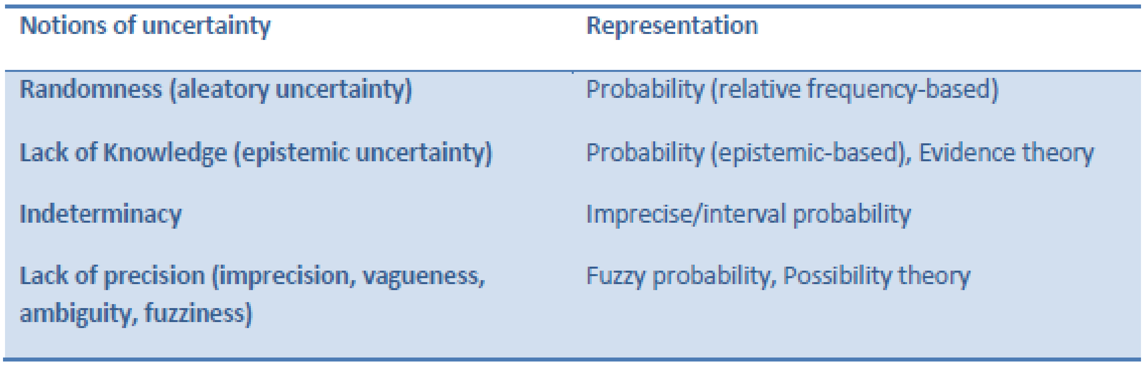
4.3 Interpretations of uncertainty

Uncertainty can be defined as "lack of knowledge about the performance of a system" (Aven 2003). Reliability assessments communicate the uncertainty about future events, often in terms of probabilities. Application of probability is a confession of our lack of knowledge, because it states the uncertainty related to the unknown events. This is also why probability has a wide area of utilization; it realizes quantification of uncertainty by using mathematical expressions. The mathematical theories behind probability are widely accepted, but how we interpret it, is not. This is an important issue when it comes to reliability analysis as a decision support; how we understand the results may be different, depending on our point of view.

We can interpret uncertainty in two ways:

I. Realist interpretation: This is according to the realist interpretation which sees probability as a measure of a property, just like any other physical property (Watson 1993).This one is in conflict with knowledge beyond what is considerably needed. It can be divided as classical, relative frequency and a priori theories.

II. Subjective interpretation: The subjective interpretation of probability defines probability as a degree of belief, which means that the same event can have different probability. The subjective probability represent is purely epistemic due to its nature of only being knowledge-based. The use of subjective probability is lacking the objectivity that is required in scientific problem solving or analyses of severe problems like reliability analysis. But subjective probability can often be used in combination with other applications when there is lack of quality data. Bayesian update with expert judgment is an example of that.



Notions of uncertainty	Representation
Randomness (aleatory uncertainty)	Probability (relative frequency-based)
Lack of Knowledge (epistemic uncertainty)	Probability (epistemic-based), Evidence theory
Indeterminacy	Imprecise/interval probability
Lack of precision (imprecision, vagueness, ambiguity, fuzziness)	Fuzzy probability, Possibility theory

Table 3 Concepts of uncertainty and related representations (Flage, Aven and Zio, 2009)

4.4 Different approaches of uncertainty assessments

Risk and reliability assessments occupy uncertainties due to the nature of the assessment methods. Uncertainty assessment is an important medium when decision makers making decisions under uncertainty. There is an important relation between the reliability assessment and the uncertainty assessment. But the main difference between a reliability assessment and an uncertainty assessment is that reliability assessments define the aleatory uncertainty about the future failure attitude of a system, while uncertainty assessments say more about epistemic uncertainty about the information (model output) which the reliability assessment provide. There are three main methods used for quantifying the effect uncertainty assessments:

I. **Sensitivity analysis**
II. **Importance measures**
III. **Uncertainty propagation**

4.4.1 Sensitivity analysis

Sensitivity can be defined as the how the variation in the model output to change in the input. An input may be a model element like a numerical parameter value for a component or a model assumption. Simulation models are needed to carry out sensitivity studies. We can utilize them as a tool to understand complex phenomena and to support decisions (Owen et al., 2011). The knowledge base is characterized by a large degree of uncertainty: imperfect understanding, subjective values and etc. In reservoir modelling, for example, the high degree of uncertainty relates to geophysical parameters, temperature and pressure. Drawing the figure is the easiest way to present the simplified concept of sensitivity studies:

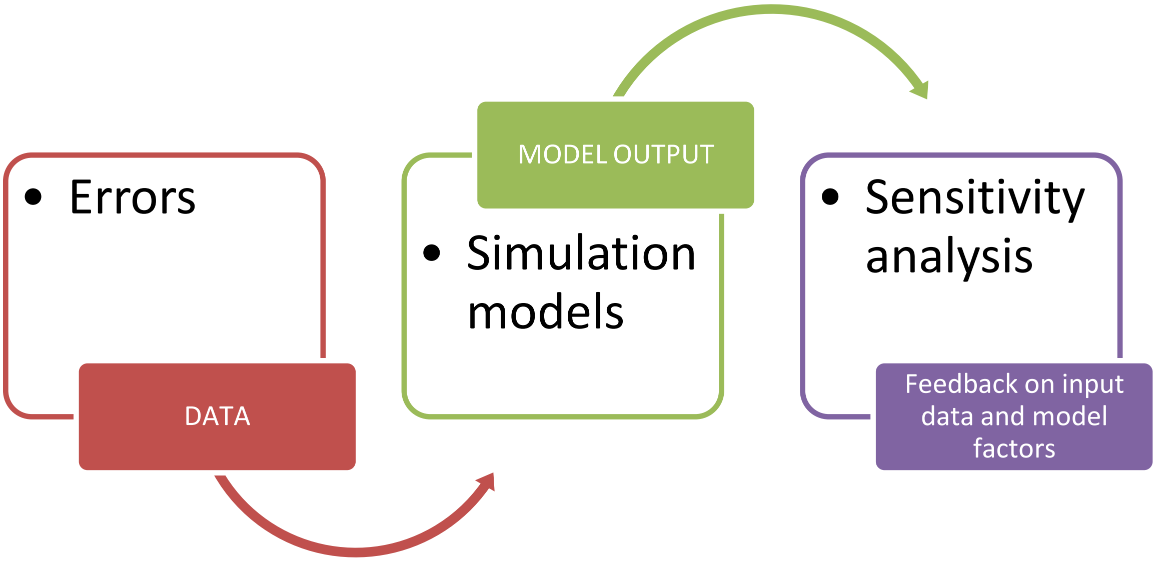


Figure 12 Simplified diagram for the sensitivity analysis (Owen et al., 2011)

The diagram demonstrates that errors in the data go further to simulation models. By adding resolution levels, model structures and parameters we get a result from the simulation model to be used in the sensitivity analysis. With the help of it the feedback on input data and model factors goes back to the beginning of the sequence and the process starts again.

However, the simplified diagram of sensitivity analysis is not actual model for my master thesis because I have not done any further computer simulation. But I have covered basic concept of sensitivity analysis by doing several iterations of probability of failure on demand. I have analyzed different PFD_{avg} values and its effect on the SIL verification.

Sensitivity analysis study's how the uncertainty in the model output can be related to different uncertainties in the model input. That will identify inputs that are relevant for prediction and find the way to mitigate the uncertainty in order to increase the reliability of predictions (Frantzich, 1998). The result of sensitivity analysis will be robust only if the amount of alternative assumptions is wide enough and interval of inferences is narrow enough.

Sensitivity analyses can therefore be considered as useful methods to identify what are the sources of uncertainty where we can study those parameters in reliability analysis. Afterwards, sensitivity analyses can also be used as a quality assurance tool for the better application in reliability studies. Therefore, model uncertainty does not exist in case of sensitivity studies and hence avoidance of model uncertainty comes from that concept.

4.4.2 Importance measures

A sensitivity studies provides the relevant background knowledge about how the output parameter changes by considering different input values. It is always good approach to have appropriate measures after considering sensitivity analysis. The different reliability structures can bring the different results or even the same component in that reliability structures may have different importance measures. For example, the series structure must have to achieve higher reliability than the parallel structures. It is necessary to consider the component importance in both aspects of model input and model structures. It is therefore important to rank components with respect to quantitative sensitivity assessment which is called important measures. There are several ways to rank the relative values of the components with regard to improvement potential and contribution to unavailability. After the ranking of those components we can refer for further analysis to mitigate risk or to control the failure of such systems. There may be several methods to the risk analysis in that case and at the same time we can also analyse risk based decision making. Therefore, Importance measures can be a key element of sensitivity analyses.

4.4.3 Uncertainty propagation

When the sensitivity analysis and important measures gives direct impact on the changing input values to the output values, uncertainty propagation will be importantly considerable because of how uncertainty related to the input values changes onto the output values (deRocquigny, Devictor and Tarantola 2008). The uncertainty is generally following the probabilistic approach.

The probabilistic framework for uncertainty propagation follows a two step process (NASA 2002);

I. First, assign a probability of failure on demand (PFD_{avg}) to each of the random (uncertain) input parameters. The PFD_{avg} reflects the state of knowledge and represents the epistemic uncertainty related to the parameter. The PFD_{avg} can be selected from different distributions, depending on what properties that is best suited for the component or system they represent. In reliability analysis, the lognormal or gamma distribution is usually used as PFD_{avg} for data uncertainty. In my thesis, I used the PFD average formula for single components by using minimum cut sets methods.

II. Then, generating a PFD_{avg} for the output function by combining the input PFD_{avg}

In this method we can refer the combined PFD_{avg} to reflect the uncertainty associated with reqired reliability target of SIL. Figure 13 shows the relation between the uncertain parameters, λ, the uncertain events like the unavailability of components, x, and the reliability of the system as a function of x, $R = h\ (x1, x2\ ...)$. In this process, there are three methods are used to propagate uncertainty; simulation, moment propagation and discrete probability distribution (NASA 2002). This tool is quite useful in simulation techniques due to the integrated software solutions.

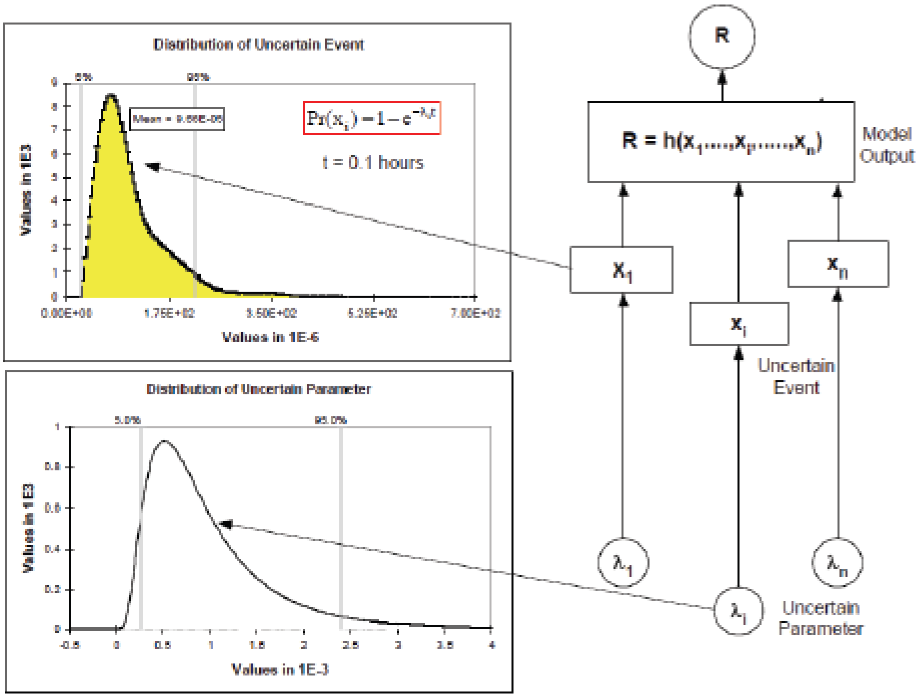


Figure 13 Uncertainty propagation (NASA 2002)

There are two common sampling techniques in software tools at present time using widely which is the Monte Carlo or Latin Hypercube sampling (LHS).

4.4.3.1 Monte Carlo sampling

Monte Carlo sampling is random methods for sampling tools where this method generates random failure times for each component's failure distribution.

A problem with Monte Carlo sampling is that the samples are more likely to be shown from areas of the distribution where the probability of occurrence is higher. The extreme values are then likely to not be represented sufficiently in samples. In order to solve this problem, a high number of repetitions are needed and this may be quite extensive and time consuming. This issue is problematic for reliability models that employ skewed probability distributions like the lognormal or gamma distribution, where the right tail may be long (Morgan and Henrion 1990).

4.4.3.2 Latin Hypercube sampling (LHS)

Latin Hypercube sampling (LHS) was developed in order to solve the problem with sampling of extreme values which Monte Carlo sampling introduced. In order to ensure that the whole spectre from a distribution is represented in a sample, LHS use a stratified, also known as sampling method. The cumulative distribution function for an input parameter is divided into n intervals, where n is the number of simulations to be run. In contrast to Monte Carlo sampling, LHS samples a random value from the input PFD from within each interval, without replacement. The generation of a random variable within an interval is found in the same way as for Monte Carlo sampling. It is the layered sampling, where one interval is selected only once, that is the main difference. In this way, the coverage of the distribution domain is uniform and more representative and hence a smaller number of samples are needed.

4.5 Failure rates as an uncertainty

The failure rate is an important aspect to be considered in uncertainty analysis. I have done several calculations by using failure rates to calculate PFD average for several subsea equipments. For different failure rates we have decided to consider different SIL level. It is important measures to be considered as a measure of uncertainty because of the different probability number in various cases. Then decision makers can make good decisions to see different SIL level for those subsea equipments.

4.6 Sensitivity vs. Uncertainty

It is common to mix the expressions “uncertainty” and “sensitivity”. Generally speaking, uncertainty and sensitivity analyses investigate the robustness of a study including mathematical modelling. But it should be noticed that a sensitivity analysis is not the same as uncertainty analysis, also called uncertainty propagation. This is because the sensitivity analysis does not express the uncertainty related to the uncertain inputs, only the effect of changes of them. The analyst may, however, based on the sensitivity study understand which model input or assumptions that may be crucial for level of uncertainty in the assessment, based on their importance. Hence, a sensitivity study is well suited as a basis for an uncertainty analysis.

While sensitivity analysis identifies what source of uncertainty weights more on the study's conclusions, an uncertainty analysis is the only technique that actually describes the level of uncertainty related to the conclusions.

4.7 Decision making under uncertainty

Decision making is an important aspect to be considered in uncertainty analysis. The following discussion of decision making analysis might be good measures to analyse further decision to make appropriate decision to verify SIL level.

The risk management and decision making under uncertainty can be divided into four tasks: (Aven 2003)

I. Identification and generation of options
II. Assessment of these options
III. A complete evaluation and judgement of options
IV. Decision: selection of options

A complete model for decision making under uncertainty is presented in Figure 14

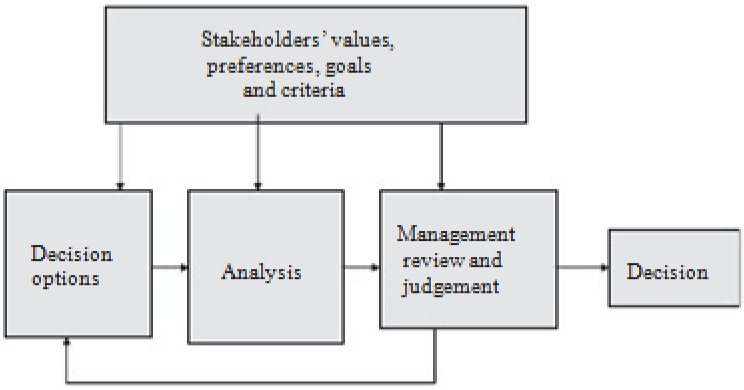


Figure 14 A model for decision making under uncertainty (Aven 2003)

The decision support created by the analyses must be checked by the decision maker prior to making decision. However, most of the experts and managers accept a perspective for decision making under uncertainty that is mostly risk -based rather than risk- informed. Their aim is to enhance the analysis (Scientific) part and reduce the management (non-scientific) part.

The uncertainties associated with the results should be reported to the decision maker such that he or she is aware of the risks related to the decision. A framework for integrating uncertainty into the basis for decision making is presented in Figure 15.

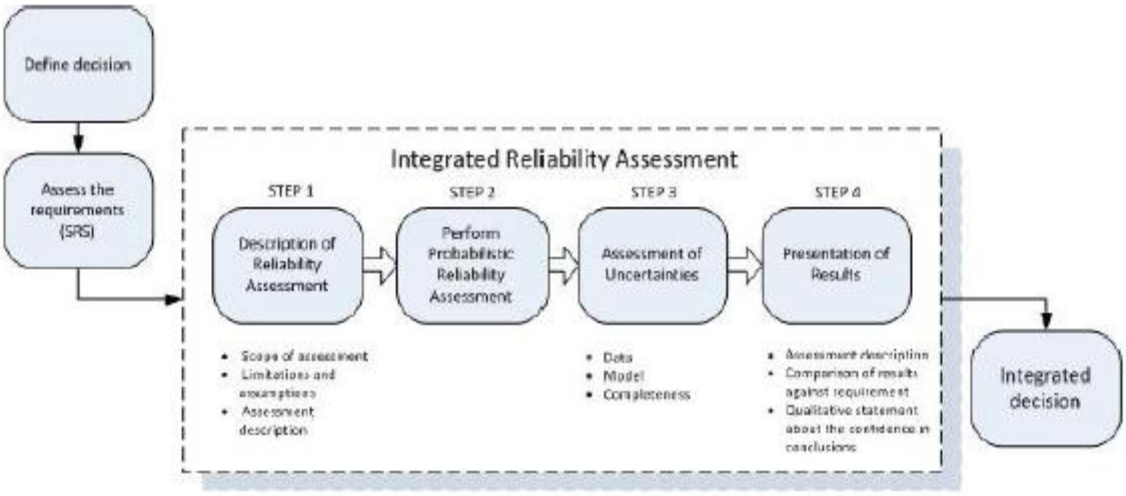


Figure 15 Integrated decision making for hardware safety integrity

4.8 Human involvement in operating production facilities and its characteristics

Human can become asset as well as liability in operating complex production facilities. Every business activity including production facility involves human as its driver. Human are there to make the production facility runs according to the needs from which it is built. Therefore, human have important role in operating production facility. Human can become asset which means that human directly or indirectly generate income for the company they work for in operating facility. Human manage, monitor, control and optimize almost each and every activity or part in the production facility in order to make sure the production facility runs 24 hours a day and 7 days a week without downtime. It shall have positive outcome to a company so human are asset a company has. Besides having been seen as asset, human are also considered as liability for a company. Human make mistakes and human have limits physiologically, psychologically as well as emotionally. In addition to that, operating complex production facility is not a simple task and it often pushes human to their limit. It makes them vulnerable to do slips or mistakes which may cause loss to a company. That’s why human are also seen as liability possible to cause negative outcome to a company.

Human characteristics approach to illustrate human as asset and as liability at the same time:

- Physiological

  Human relies on five senses to orient themselves with their surroundings. Human sense (to some extent) can be more reliable compare to technological equipment seen from cost-effective analysis. In offshore living quarters module (LQM), there are many manual break glass to activate alarm system. The manual break glass is the safety supplemental equipment to all active smoke detectors located in ceiling (to detect burning furniture) and above ceiling (to detect burning cable). These active detectors fail simultaneously and will be hidden undetected until next inspection routine. If something happen to the cable inside ceiling which might firstly cause smoke, it will remain undetected by technology, but human have senses to smell or see the smoke. He can use the break glass and control system will do further set up logic to suppress the problem. In this way, human are asset in operating complex facility. Human senses gradually decrease along with physical fatigue. Working for many hours in front of big monitors in control room causes sight sense decreases leading to a possibility in wrong parameter reading and wrong action taking. It may cause negative outcome to the facility and therefore human is also a liability.

- Psychological

  Human have thinking and emotions. Quick thinking in taking critical decision is one of the most favorable soft competencies to a company operating complex facility. This is related to cognitive perspective in human information processing. In offshore platform control room, many operation parameters are being monitored and controlled. All this information can be very complex especially mature platform where equipments have degraded, huge amount of data have been stored, software calculation and equipments response time have decreased. In this case, role of experience operators who know the facility very well becomes critical. Human act as compensator to those problems. Their quick thinking and problem solving ability make it possible to avoid negative outcomes. In the other hand, human working in hazardous and complex facility without anything goes wrong will gradually forget safety precaution. They may take shortcut such as suppress safety precaution. For example: Deepwater Horizon personnel live with a lot of false alarms. This condition forced them to suppress the alarm which made them vulnerable to intercept the real problem quick enough.

- Sociological

  Human have a wide opportunity to develop interpersonal relationship. This interpersonal skill can be helpful to increase safety and positive work manner. For example: there is a program called behavioral based safety management (BBSM) applied by Shell in offshore production activity. The program is intended to remove unsafe acts in their offshore day to day activities. Each personnel is trained to observe other personnel working behavior and talks to whom they consider are doing unsafe act and provides safe solutions. This program provides wide opportunity to develop interpersonal relationship among personnel working in the same platform so that possibility of negative outcome can be suppressed further down. But in real implementation, this program is not 100% reliable. For example: very experience personnel such as ship captain or drilling superintendent sometimes are very difficult to give advice to especially by young and new personnel in their facility. This is the drawback whose solution needs to be found by management level.

- Behavioral

  Human have a diverse views toward working behavior. This makes human as both asset and liability in operating production facility. Young and new engineers have tendency to accept many tasks and tries to show exceptional work. They often try to work harder and reach target earlier than schedule. This is of course favorable to company. While senior engineers with all of their experiences are no longer hard workers but they work efficiently and give advices to young engineers. This is also favorable to a company. The difference in working behavior places human as asset in operating production facility as they give potential benefit to the company. On the other hand, the working behavior showed by young engineers exposed them to making mistakes. Taking too many tasks in the same time makes split their concentration. Lack of concentration in doing work may cause wrong judgment which is possible to lead to errors. Here is the liability part of human in operating complex production facility as seen from behavioral characteristics.

4.9 Evaluation of uncertainty

After doing all the analysis for uncertainty analysis, it is important to consider evaluation of uncertainty. However, there are lots of uncertainty factors to be unknown due to the proper way to handing uncertainty in oil and gas sectors. I started to think why the failure rates are very high. For example, if we can remember the Piper Alpha accident or BP’s Gulf of Mexico accident, how severe it was? Those accidents were extremely sad news for oil and gas industries as well as the great impact on the environment. In my thesis I presented the barrier failures of Piper Alpha accidents only because to start what are the uncertainty factors involved in any particular accidents or dangers failure of any systems. It was easier in this thesis to analyze uncertainty factors for the several subsea equipments. Table 4 and 5 shows the uncertainty evaluation according to the MTO perspectives for the Piper Alpha accidents and the subsea control systems, respectively.

Barriers	Human		Technology		Organization		Work process	
	Evaluation	*Applicability*	*Evaluation*	*Applicability*	*Evaluation*	*Applicability*	*Evaluation*	*Applicability*
1.Permit to work system (PTW)	-Lack of formal trained contractor's staff. -Didn't pay attention how to make safe system of work.	-Need better trained personnel	Absence of a guideline for locking off isolation valves	-Provide secure techniques to lock isolation valves. -To computerize the PTW system	-Operator did not monitor the standardization of PTW system and they did not follow the act abide by Performing Authority. -Authority was unable to support a good communication system.	-Check regularly validation of PTW. -Authority must provide a better communication system to make sure that planned critical tasks from all affected staff.	-Lack of criticality of maintenance. -Lack of operators safety philosophy and methods of doing work.	-Provide detailed communication during crew change. -Monitoring regularly the PTW task. -Special emphasis on SMS.
2.Process Leak Detection and control (PLDC)	-Lack of communication -Between maintenance crew and control room operators or poorly engineered system	Provide experienced, trained operating crew	-Lack of new technology to construct, operate and maintain such system	-New technologies can cope with complex design and close coupling to control process leak	-Management did not realize in crisis management. -And proper detection system.	-Management must invest in better training , better incentives to qualified operators, human-system interfacing devices	-Lack of effective early warning system. - Lack of physical detection system, emergency shutdown system and fire suppression system.	-Improved PLDC can reduce the fire and explosion (See table in appendices)
3.Fire and gas detection and emergency shutdown systems	-The crew did not follow the guidelines for the process of how to set off ESD valve.	-The crew must follow the list of valve operation	-Signals from gas detection system had led to automatic ESD -the ESD of gas pipeline was separated from platform ESD -Some of ESD was not closed fully	- Gas ,smoke and fire detection must set off ESD -Use of IR(infra-red) fire detector much more reliable rather than UV (ultra-violet) devices	-The safety and compliance management did not put emphasis on Fire Fighting Equipment regulations -Didn't follow the procedures for flow control	-Company must take control of the design, operation and maintenance of process plant	-They could not detect the signals from gas pipelines -Improper arrangement of ESD	-Need high quality information of gas detection -Proper activation of ESD valves in case of safety case

Table 4 Evaluation of MTO perspective on the Piper Alpha barriers failure (cont. next page)

Barriers	Human		Technology		Organization		Work process	
	Evaluation	*Applicability*	*Evaluation*	*Applicability*	*Evaluation*	*Applicability*	*Evaluation*	*Applicability*
4.Control of fire and explosion **-Blowdown of ESD** **-Explosion mitigating by venting** **-Active and passive fire protection** **-Water suppression system** **-Fire pump system**	-Crew had low level of understanding of test procedure of process shutdown(PSD) and emergency shutdown. -From the 'reference area' concept the fire fighting team did not follow guidelines for water deluge system.	-The crew must understand the criticality of equipment and its PSD and ESD system. -Personnel should follow safety assessment of fire and explosion protection system	-Ventilation and ballast wall system was not good enough to mitigate explosion - Lack of hydrocarbon fire test	-Sufficient Ventilation is needed to remove flammable gases. -Provide electrical installation (Equipment) to reduce ignition.	-The authority did not monitor regular update from the operation and safety representative	-The authority must put strict rules and regulations for safety systems of different fire and explosion hazards	-the Water deluge system including fire pump system was not able to survive severe accident conditions -the operators was unable to conduct a fire risk analysis because they were waiting for legislation from regulatory body	-the location and resistance of fire and ballast walls must be determined by safety assessment -the function, capacity, availability, and protection of Water deluge system should follow safety assessment
5.Failure to prevent fatalities **-Temporary safe refuge** **-Protection of accommodation** **-Evacuation, Escape and Rescue**	-The crew specially OIM did not give order for evacuation during emergency situation	-crew must have safety training. -the OIM specialist should maintain the follow up procedure during Evacuation, escape.	- The alarm system did not work properly -Most technical error occurred after the initial explosion	- Should use the better device to keep the system work so that crew will be aware of the even in emergency conditions.	-The authority did not follow up the routine maintenance work and regular emergency exercises	-Regulatory body should check the evidence and regulatory requirements for safe and complete evacuation, escape and rescue	-The safety team had a problem to give order during emergency situation at PA so that most of the worker did not get any information what to do in short time.	-TSR should the centre of safety case. -Goal-setting regulations in offshore industry must be followed in case of emergency situation to set up flexible working hours.

Equipment	Humans		Technology		Organization		Work process	
	Evaluation	*Applicability*	*Evaluation*	*Applicability*	*Evaluation*	*Applicability*	*Evaluation*	*Applicability*
1.Electrical Power Unit (EPU)	-Lack of formal trained staff. -Less attention how to make safe system of work.	-Need better trained personnel	-electrical failure due to erratic output. -Sticking of power coupler due to the common cause and fail to lock. -Less knowledge of new equipment	-Provide secure technology. -Limited experience with the subsea electrical system.	-Head of power of branch should monitor the standardization of power supply unit. -Lack of good communication system.	-Check regularly validation of EPU. -Authority must provide a better communication system to make sure that planned critical tasks from all affected staff.	-Blockage of power and electrical failure of power supply unit due to transmission failure. -Lack of operators safety philosophy and methods of doing work.	-Provide detailed communication during crew change. -Monitoring regularly the general electrical task.
2. Hydraulic Power Unit (HPU)	-Lack of understanding of signal. -Control failure.	Provide experienced, trained operator	-Some unknown material failure. -Lack of new technology to construct, operate and maintain such system.	-New technologies can cope with complex design can give information of the faulty signal	-Management does not have more control to collaborate with operator working here.	-Management must invest in better training, better incentives to provide better technical equipment.	-Lack of effective early warning system. -Human-system interfacing devices are needed.	-Need to establish alarm system to avoid unwanted fault of signals.
3.Master Control Station (MCS)	-The control or signal failure due to less experience operator	-The crew must follow the proper guidelines of control systems of MCS.	-Some times fail to function on demand. -Failure due to the spurious operation.	- Need fully function technology . - Need fully integrated solutions.	-The management should arrange meeting to know regular updates of signal and its control.	-Company must take control of the design, operation and maintenance of such system	-Some times fail to detect the signal from the EPU. -Improper arrangement of control system.	-Need high quality information of equipment solution
4. Chemical Injection Unit (CIU)	-Leakage of chemical injection coupling so it is coming from utility of external leakage. -human error is accounted as medium risk of fluid lost.	-The crew must understand the external leakage of chemical coupler	-Lack of good design of process area	-Sufficient utility medium should establish. -Need good design of chemical coupler.	-The authority does not monitor regular update from the operation	-The authority must put strict rules and regulations for safety systems of different chemical injection systems	-The problem with new subcontractors.	-The location must be guided by the experience subcontractors.
5. Static and Dynamic Umbilical	-The control failures involve the personnel working on the umbilical termination unit.	-Crew must have known better understanding of control failures.	- The dynamic umbilical failure are mostly severe than the static umbilical failure	- Should use the better device to control the seal, tension and motion of equipment.	-The authority does not follow up regular maintenance programs.	-regulatory body should make a regular inspection in ordewr to reduce control failures of umbilicals	-The topside and subsea umbilical termination must have Proper knowledge of work process	-Should follow some procedures for control faiulures of umbilical unit

Table 5 Uncertainty evaluation of subsea control system

4.9.1 Uncertainty Categorization for different subsea equipments

The uncertainty evaluation of several subsea equipments was the good approximation to come up with an ideal solution how to treat uncertainties. By considering MTO perspective we can say that failure arise in generally human involvement work places, some technical aspects like new technologies, hardware and software problem etc., some operational aspects like joining new subcontractor from different continent or less experience subcontractors etc. The above mentioned factors can be carried out main consideration on the MTO perspectives because of the higher uncertainty. However, there some other factors also related to medium and low category of uncertainty such as crew training on human involvement work place, environmental location such as operation carried out in harsh environment situation, some procedures and standards for documentation and maintenance task as operational aspects. The following table 6 shows the uncertainty categorizations for the subsea manifold, subsea control systems, subsea control systems – SSIV, subsea control systems – Xmas tree, subsea flowlines and subsea pipelines.

No	**Subsea Equipments**	**Uncertainty categorization**		
		High	Medium	Low
1	**Manifold**	Leakage and material failure of process isolation valve, Deformation of main or branch valve	Blockage of main or branch valve, Corrosion in main piping, Sticking and corrosion of process isolation valve	Leakage and material failure of manifold connector, Blockage of main piping and process isolation valve, Wear and breakage of process isolation valve

2	**Subsea control systems**	Control failure of subsea electronic module and subsea umbilical termination unit; Isolation fault of power coupler; Leakage of solenoid control valve.	Leakage of chemical injection coupling and subsea umbilical termination unit; Faulty signal of combined pressure and temperature sensors, subsea electronic module, subsea umbilical termination unit; Blockage of pressure sensor and solenoid control valve; Electrical and software failure of subsea umbilical termination unit; Burst of hydraulic/chemical jumper.	Breakage, deformation, isolation fault, fatigue, material failure, mechanical failure, out of adjustment, no power and sticking of subsea umbilical termination unit; Leakage of topside umbilical termination unit, subsea electronic module, hydraulic coupling, hydraulic/chemical jumper, hydraulic line and subsea accumulator; Blockage of flow sensor, hydraulic coupling, hydraulic/chemical jumper, hydraulic line, power coupler and other components; No signal from combined pressure and temperature sensor, pressure sensor, subsea electronic module.
3	**Subsea control systems – SSIV**	Blockage of hydraulic/chemical line failure; Control failure of hydraulic power unit; Some unknown failure from dynamic umbilical unit.	Failure from the subsea and topside umbilical termination unit, power line of dynamic umbilical, combined pressure and temperature, hydraulic coupling and power supply unit.	Hydraulic line failure in static umbilical unit; failure of power jumper in subsea distribution unit; failure from the solenoid control valve and subsea electronic module in subsea control module; failure of pressure and temperature sensor

4	**Subsea control systems – Xmas tree**	Control/signal failure of master control station and HPU; External and internal leakage, spurious operation and abnormal instrument reading of HPU.	Transmission failure and insufficient power from EPU; Abnormal instrument reading, low performance, short circuit, stuck and vibration from the HPU; Erratic output, insulation failure and spurious operation from the MCS; Subsea control module (SCM) fail to function on demand; Control/signal failure from sensors.	Sensors fail to function on demand; Failure from the flow/pressure/temperature/valve position sensor; Failure of hydraulic line, power line, armour, subsea and topside umbilical termination unit in static umbilical; Failure from the subsea accumulator, filter, hydraulic coupling, power supply unit, power coupler, solenoid control valve and subsea electronic module in subsea control module (SCM); Failure from the subsea accumulator, chemical injection coupling, hydraulic coupling, hydraulic jumper, power coupler and power jumper in subsea distribution module (SDM).
5	**Subsea flowlines**	Failure of protective structure in subsea isolation system; Insulation failure of pipe; Trawl board impact due to structural deficiency in sealine.	Leakage of flexible pipe spool and pipe connector; Failure of safety joint in pipe; Control failure of process isolation valve.	Blockage and material failure of sealine; Failure of external coating in pipe; Support structure in subsea isolation system.
6	**Subsea pipelines**	Process isolation valve fail to close on demand and fail to open/unlock.	Mechanical failure of subsea isolation valve due to delayed operation/control failure/external leakage in subsea isolation system;	Blockage and control failure of process isolation valve; Corrosion, leakage, material and instrument failure of subsea process isolation valve; Failure from the sealine and rigid pipe spool.

Table 6 Uncertainty categorization for several subsea equipments

5. Summary of SIL level calculation for two different approaches

The following table 7 shows the summary of the PFD_{avg} calculations and the SIL level for each subsea equipments by using two different approaches. From the above all calculation we can see how SIL level varies from the traditional approach to the new approach. For some subsea equipments even were not meet the SIL requirements. For example, SIL level for subsea manifold go down very quickly in the new approach of SIL verification.

Subsea equipment / SIL level	Average probability of failure demand for a different proof-test interval			
	Traditional Approach		New Approach	
	1 month interval (per 10^6 hours of operation)	6 months interval (per 10^6 hours of operation)	1 month interval (per 10^6 hours of operation)	6 months interval (per 10^6 hours of operation)
Manifold	8.54 x 10^{-3}	2.38 x 10^{-1}	2.97 x 10^{-2}	4.17 x 10^{-1}
SIL level for manifold	SIL 2	SIL 0	SIL 1	SIL 0
Subsea control systems	1.74 x 10^{-2}	1.05 x 10^{-1}	7.34 x 10^{-2}	4.49 x 10^{-1}
SIL level for Subsea control systems	SIL 1	SIL 1	SIL 1	SIL 0
Subsea control system : SSIV	5.67 x 10^{-3}	3.47 x 10^{-2}	2.04 x 10^{-2}	1.27 x 10^{-1}
SIL level for subsea control system : SSIV	SIL 2	SIL 1	SIL 1	SIL 1
Subsea control system : Xmas tree	2.38 x 10^{-2}	1.66 x 10^{-1}	4.47 x 10^{-2}	4.50 x 10^{-1}
SIL level for subsea control system : Xmas tree	SIL 1	SIL 1 (but very close to SIL 0)	SIL 1	SIL 0

Subsea flowlines	3.77x 10^{-2}	2.26x 10^{-1}	1.45 x 10^{-1}	8.71 x 10^{-1}
SIL level for subsea flowlines	SIL 1	SIL 1	SIL 1	SIL 0
Subsea Pipelines	1.57 x 10^{-2}	9.43 x 10^{-2}	4.72 x 10^{-2}	2.85 x 10^{-1}
SIL level for subsea pipelines	SIL 1	SIL 1	SIL 1	SIL 0

Table 7 The PFDavg calculations and SIL levels for two different approaches

6. Conclusion

The main purpose of this thesis was to study the reliability of several subsea equipments in order to verify safety integrity level in presence of uncertainty. The appropriate reliability targets for safety instrumented functions were carried out in case of SIL verification process. This thesis presents two approaches for SIL verification in order to achieve the reliability of several subsea equipments.

The two approaches for SIL verification, the traditional approach and a new approach by Abrahamsen, was the introductory focal point of this thesis where the concern was that whether a SIS meets the required SIL or not. The traditional approach for SIL verification is generally based on the average probability of failure on demand only because it does not provide valuable information to decision makers in order to achieve reliability of SIS. In line to establish the appropriate verification approach for SIL, in this thesis we argue that to cover uncertainty assessment qualitatively in a workshop is more convenient. Therefore, E.B. Abrahamsen introduced a new approach for SIL verification.

This thesis was mainly dealing on how to verify the appropriate reliability targets for safety instrumented functions by using the new approach. This approach acknowledges that the calculated average probability of failure on demand for a safety function cannot be adequately verified only by seeing bond assigned probability number. There was a need to consider the important aspects of uncertainty before a conclusion is made on SIL level in that approach.

Several subsea equipments were taken into account to illustrate both approaches. For both approaches, the OREDA database was a reliable data while calculating PFD_{avg}. Several calculations have been done in that case in order to decide an appropriate SIL level which might be useful for decision makers. But in most of cases for the few subsea equipments presented in this thesis, the result could not meet the desired SIL level due to the higher failure rate that arises from those equipments, meaning that those equipments were no longer acceptable to continue the operation. In this case additional risk reducing measures should be implemented prior to the operation. We have observed that there was higher probability of failure in that new approach. It is therefore a very important aspect to consider the uncertainty factors due to those higher probabilities of failure that arose in our calculations.

The result from uncertainty analysis should be seen considerably while identifying the possible uncertainty factors due to failure of such subsea equipments. Those uncertainty factors can be seen thoroughly in the evaluation of uncertainty. This thesis also covered the uncertainty evaluations according to MTO perspectives. It was clear that human error, technical aspects, operational aspects and work process are the main contributors of any particular failure. But this thesis also discussed some other possible factors of uncertainty. The decision makers should always consider the uncertainty evaluation in order to reach an appropriate decision. It is therefore easier to categorize uncertainty by using uncertainty evaluation.

Therefore, this is an important discussion that is to be considered in the new approach of SIL verification in reliability studies. The decision makers can easily come up with an ideal solution if there is a possibility to reduce the uncertainty factors. Hereby I can conclude that this new approach would be an appropriate analysis for SIL verification which considers the important aspects of uncertainty factors.

7. Recommendation

The objectives of this master thesis are to verify safety integrity level for several subsea oil and gas equipments, to propose two different approaches of SIL verification, to use reliable database such as OREDA database, to propose uncertainty evaluation according to MTO perspectives, to propose the reduction of uncertainty factors how to be considered and to present appropriate SIL verification approach for decision makers.

According to the experience from the Norwegian Offshore Industries for SIL analyses, there is still some uncertainty in relating to how the IEC standards 61508 and 61511 should be implemented. There has been lots of discussion going on about how to determine and verify appropriate SIL level. However, there is still need for an appropriate approach to verify SIL level.

The new approach proposed by Abrahamsen will be a good indicator of future development in oil and gas industries. It was my immense interest to analyze his approach to this master thesis. Most of the oil and gas industries do not consider the uncertainty analyses when decision comes to the verification of SIL level because this is still under-developed for the reliability engineers. In line with this new approach I started to analyze how to treat uncertainty especially in case of SIL verification. My objective was to investigate what are those uncertainty factors that are to be considered in the failure of those subsea equipments.

For the development of future studies we might need appropriate uncertainty model to treat uncertainty up to a certain limit for SIL verification in reliability analysis. It is worth to mention that we cannot say zero risk or no uncertainty at all can be found in the oil and gas operation. There is always risk involved but we can mitigate those risks up to a certain extent. In case of equipment failure there might be need of a broad implementation of risk reducing measures if the uncertainty factors can be detected properly. Then those subsea equipments will be performing reliably so that SIL verification of new approach will be a promising approach for the development of oil and gas industry.

The increasing use of EPCI (Engineering, Procurement, Commissioning and Installation) contracts for all service companies in oil and gas industry must need to follow the appropriate approach for SIL verification. Especially some service companies, mainly subsea equipments supplier, are one of the major players when it comes to supporting the national oil and gas operators. Those equipments are required to be verified and defined in order to establish reliability targets for safety instrumented functions according to the IEC standards 61508 and 61511. Therefore, the new approach for SIL verification will be a proper guideline for those service companies in line with IEC standards 61508 and 61511.

8. References

Aven, Terje. Foundations of Risk Analysis - A Knowledge and Decision-oriented Perspective. Chichester: Wiley, 2003.

Aven, T. (2009) A new scientific framework for quantitative risk assessments. International Journal of Business Continuity and Risk Management, 1, 67–77.

David J Smith and Kenneth G Simpson Functional Safety : A Straightforward guide to applying IEC 61508 and related standards, 2nd edition, 2005 deRocquigny, Etienne, Nicolas Devictor, and Stefano Tarantola. Uncertainty in Industrial Practice: A Guide to Quantitative Uncertainty Management. Chichester: Wiley, 2008.

Drouin, M., G. Parry, J. Lehner, G. Martinez- Guridi, and J., Wheeler, T. LaChance. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. Office of Nuclear Regulatory Research, Office of Nuclear Reactor Regulation, 2009.

Flage, R., Aven T. Expressing and communicating uncertainty in relation to quantitative risk analysis, 2009. Risk and Reliability – Theory and Application 2(13): 9-18.

Flage, R., T. Aven, and E. Zio. “Alternative representations of uncertainty in system reliability and risk analysis Review and discussion.” Safety, Reliability and Risk Analysis: Theory, Methods and Applications, 2009.

E.B. Abrahamsen, Willy Roed. A new approach for verification of Safety Integrity Levels, 2010

Frantzich, H., 1998. Uncertainty and risk analysis in fire safety engineering. Business. Available at: http://swepub.kb.se/bib/swepub:oai:lup.lub.lu.se:18715?tab2=abs&language=en [Accessed November 11, 2011].

GE oil and gas: Subsea manifolds and connection systems, complete technologies and services for long-term reliability and safety, 2011

http://www.ge-energy.com/content/multimedia/_files/downloads/GE_DP_MC_FINAL.pdf

IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Standard, Geneva: International Electrtechnical Commision, 1997.

IEC 61508-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. Standard, Geneva: International Electrtechnical Commision, 1997

John Girling, Orbis Energy Limited. Orlando Field Development Environmental Statement, MPX North Sea Ltd, December 2011.

http://www.mpx-limited.com/admin/pages/upload/General/MPX-Orlando-Field-Development-Environmental-Statement-Rev-A01.pdf

Kiureghian, Armen Der, and Ove Ditlevsen. “Aleatory or epistemic? Does it matter?” Structural Safety, 2009: 105- 112.

Kristin subsea, NTNU,
http://www.ipt.ntnu.no/~jsg/undervisning/prosessering/gjester/Kristin140205SubseaGrytdal.pdf

Moore, W. & Bea, R., 1993. Human And Organizational Error In Operations Of Marine Systems: Occidental Piper Alpha And High-Pressure Gas Systems On Offshore Platforms. In Offshore Technology Conference. Available at: http://www.onepetro.org/mslib/servlet/onepetropreview?id=OTC-7121-MS&soc=OTC [Accessed October 11, 2011].

Morgan, M. G, and M. Henrion. Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge: Cambridge Press, 1990.

Mosleh, Ali, Nathan Siu, Carol Smidts, and Christiana Lui. Model Uncertainty: Its Characterization and Quantification. Maryland: Center for Reliability Engineering, University of Maryland, 1995.

NASA. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. Guideline, Washington: NASA Office of Safetyand Mission Assurance, 2002.

OREDA database. The Offshore Reliability Data (OREDA) project, volume 2 – Subsea Equipment, 2009.

Owen, K., Stevenson, M. a & Sanson, R.L., 2011. A sensitivity analysis of the New Zealand standard model of foot and mouth disease. Revue scientifique et technique (International Office of Epizootics), 30(2), pp.513-26. Available at: **http://www.ncbi.nlm.nih.gov/pubmed/22023865**.

Parry, Gareth W. “The characterization of uncertainty in Probabilistic Risk Assessments of complex systems.” Reliability Engineering and System Safety, 1996: 119- 126.

Rausand, Marvin, and Arnljot Høyland. System Reliability Theory: Models, Statistical Methods and Applications. New Jersey: Wiley, 2004.

Spouge, J., 1999. A Guide To Quantitative Risk Assessment for Offshore Installations Principal Author. Offshore (Conroe, TX).

Tomasz Barnert, Kazimierz T. Kosmowski, Marcin Sliwinski. The operation Modes of E/E/PE Sysytem and their Influence on Determining and Verifying the Safety Integrity Level, ISSN 1895-8281, Journal of KONBiN 1 (13) 2010.

Tore Markeset, Professor at the University of Stavanger. Condition Monitoring and Management lecture note slide about preventive maintenance, 2011.

Watson, Stephen R. “The meaning of probability in probabilistic safety analysis.” Reliability Engineering and System Safety, 1993: 261269.

Webster. Webster's Encyclopedic Unabridged Dictionary of the English Language. New York: Random House, 1989.

9. Appendices

I. A simple reliability block diagram method for SIL verification according to IEC 61508

I.I Reliability block diagram

The safety integrity verification for safety related systems to be a important step in safety life cycle and PFD_{avg} must be calculated to verify the safety integrity level (SIL). Since IEC 61508 does not show detailed explanations of the definitions and PFD_{avg} calculations, it is quite difficult for reliability engineers to apply the use of standards as guidance. Here we are investing different architectures of reliability block diagram.

Reliability block diagram (RBD) is a graphical analysis technique, which expresses the system bas connections of a number of components in accordance with their logical relation of reliability.

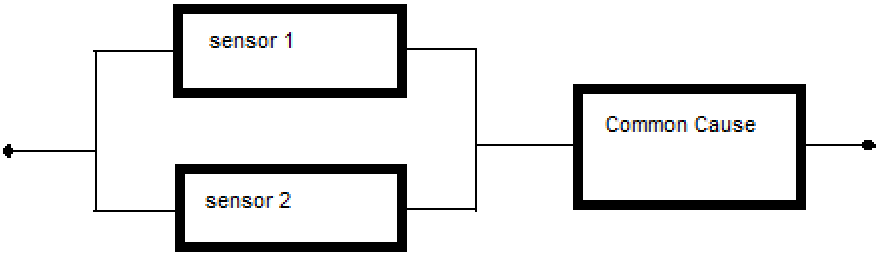


Figure 16 A RBD example

I.II Different reliability architectures for calculating PFD_{avg} in both low and high demand mode of operation

For low demand mode of operation:

Average probability of failure on demand of a safety function for the E/E/PE safety-related system is determined by calculating the average prob. Of failure on demand for all the subsystems which together include the safety function. This can be expressed by the following:

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

Where

PFD_{SYS} is the average prob. of failure on demand of a safety function for the E/E/PE safety-related system;

PFD_S is the average prob. of failure on demand for the sensor subsystem;

PFD_L is the average prob. of failure on demand for the logic subsystem; and

PFD_{FE} is the average prob. of failure on demand for the final element subsystem.

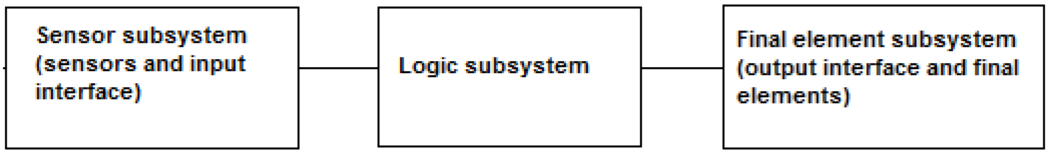


Figure 17 Subsystem structure

High demand mode of operation:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE}$$

Where

PFH_{SYS} is the average prob. of failure per hour of a safety function for the E/E/PE safety-related system;

PFH_S is the average prob. of failure per hour for the sensor subsystem;

PFH_L is the average prob. of failure per hour for the logic subsystem; and

PFH_{FE} is the average prob. of failure per hour for the final element subsystem.

(IEC 61508-6)

I.II.I 1oo1 architecture

This architecture consists of a single channel, where any potential failure leads to a failure of the safety function when a demand establishes.

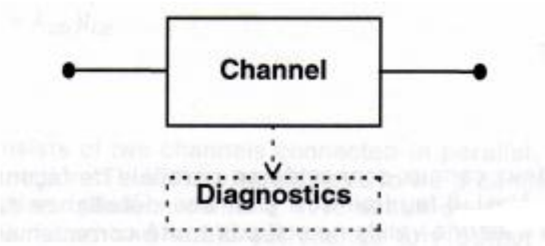


Figure 18 Physical block diagram of 1oo1 architecture (IEC 61508-6)

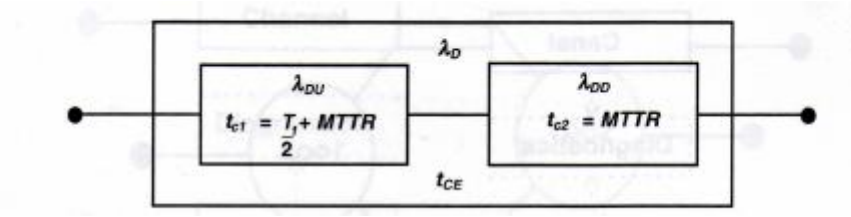


Figure 19 Reliability block diagram of 1oo1 architecture (IEC 61508-6)

Low:

The dangerous failure for the channel is given by:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

Where, λ_{DU} is the undetected failures, λ_{DD} is the detected failures and λ is the constant failure rate.

The channel equivalent mean down time t_{CE} , adding individual down times for both components, t_{c1} and t_{c2}, in direct proportion to each components probability of failure on demand.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC) \; ; \; \lambda_{DD} = \frac{\lambda}{2} DC$$

For a channel with down time t_{CE} resulting from dangerous failures

$$\begin{aligned} PFD &= 1 - e^{-\lambda_D t_{CE}} \\ &\approx \lambda_D t_{CE} \qquad \text{since } \lambda_D t_{CE} << 1 \end{aligned}$$

Therefore, the average probability failure on demand for 1oo1 architecture is

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Here are the all terms that we are using for the different reliability architectures:

Abbreviation	Term (units)
T_1	Proof test interval (h). For example, 1month (720 h), 6 months (4320 h)
MTTR	Mean time to restoration (h). For example, 8h
DC	Diagnostic coverage. For example, 0%, 90%
β	The fraction of undetected failures that have a common cause
B_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause
λ	Failure rate (per hour) of a channel in a subsystem
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0.5λ
λ_{DD}	Undetected dangerous failure rate (per hour) of a channel in a subsystem
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem
λ_{SD}	Detected safe failure rate (per hour) of a channel in a subsystem

t_{CE}	Channel equivalent mean down time (h) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures
t_{GE}	Voted group equivalent mean down time (h) for 1oo2D architecture
t_{CE}'	Channel equivalent mean down time (h) for 1oo2 and 2oo3 architectures
t_{GE}'	Voted group equivalent mean down time (h) for 1oo2D architecture
T_2	Interval between demands (h)

Figure 20 Various terms for different reliability architectures

High:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\lambda_{DU} = \frac{\lambda}{2}(1 - DC);\ \lambda_{DD} = \frac{\lambda}{2} DC$$

The average probability failure on demand for 1oo1 architecture is

$$PFH_G = \lambda_{DU}$$

I.II.II 1oo2 architecture

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Therefore, the there might have to be a dangerous failure in both channels before a safety function failed on demand. The figure xx shows the 1oo2 architecture.

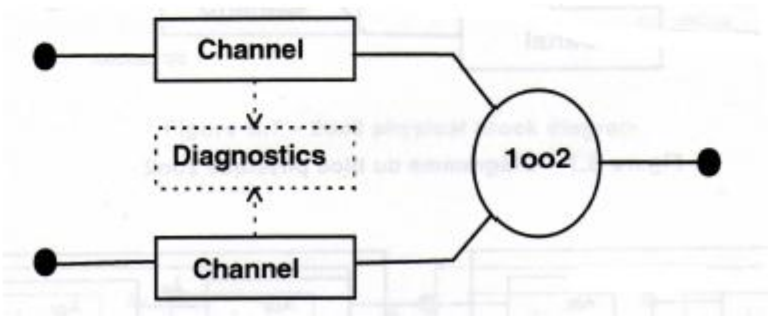


Figure 21 Physical block diagram of 1oo2 architecture (IEC 61508-6)

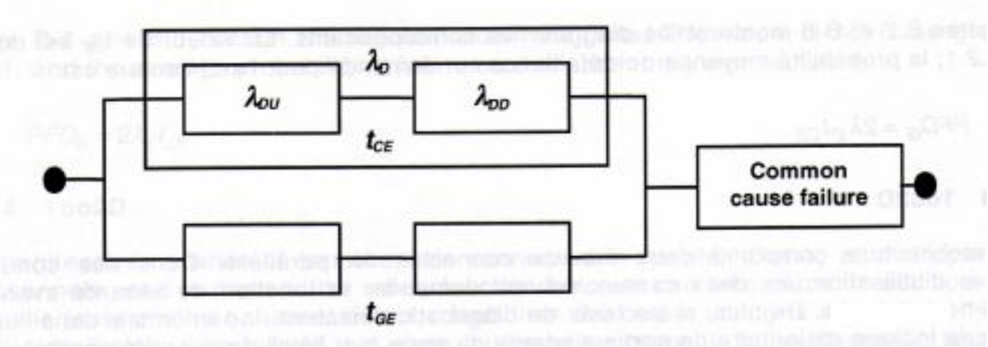


Figure 22 Reliability block diagram of 1oo2 architecture (IEC 61508-6)

Low:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

The average probability failure on demand for 1oo2 architecture is

$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

High:

The average probability failure on demand for 1oo2 architecture is

$$PFH_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DU}$$

I.II.III 2oo2 architecture

This architecture consists of two channels connected in parallel, so that both channels need to demand the safety function before it can start to act. The figure xx shows the architecture of 2oo2 system.

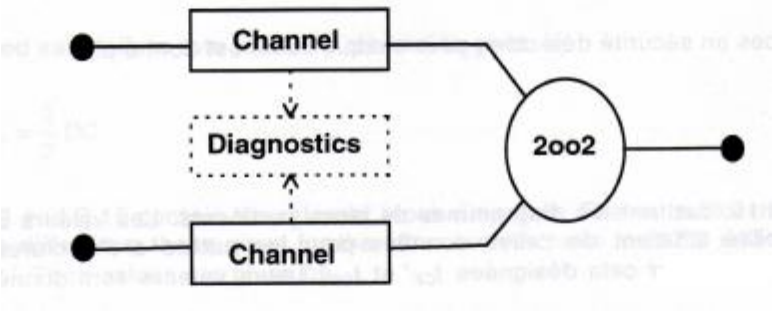


Figure 23 Physical block diagram of 2oo2 architecture (IEC 61508-6)

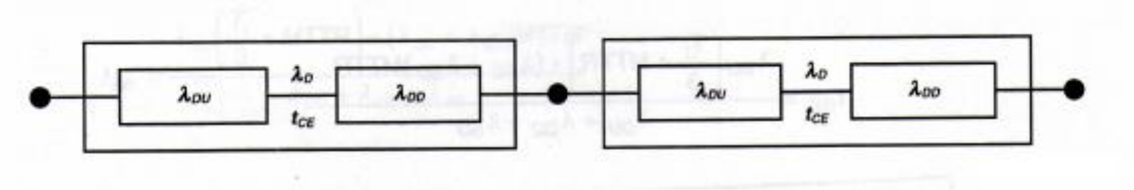


Figure 24 Reliability block diagram of 2oo2 architecture (IEC 61508-6)

Low:

The average probability failure on demand for 2oo2 architecture is

$$PFD_G = 2\lambda_D t_{CE}$$

High:

The average probability failure on demand for 2oo2 architecture is

$$PFH_G = 2\lambda_{DU}$$

I.II.IV 1oo2D architecture

This architecture consists of two channels connected in parallel. During normal operation, both channels need to demand the safety function before it can start to act.

If the diagnostic tests in either channel fail then output are tend to adapt so that overall output state then follows by the other channel. If the diagnostic tests find failure from the both channels then output goes to the safe state (IEC 61508 - 6). The architecture of 1oo2D can be shown in the below in figure xx.

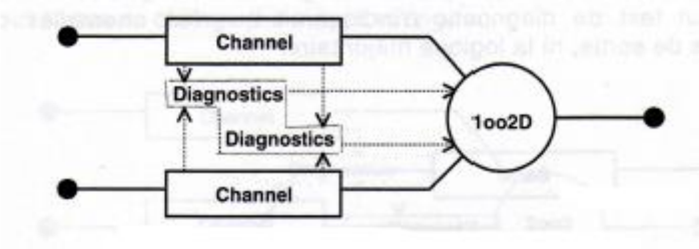


Figure 25 Physical block diagram of 1oo2D architecture (IEC 61508-6)

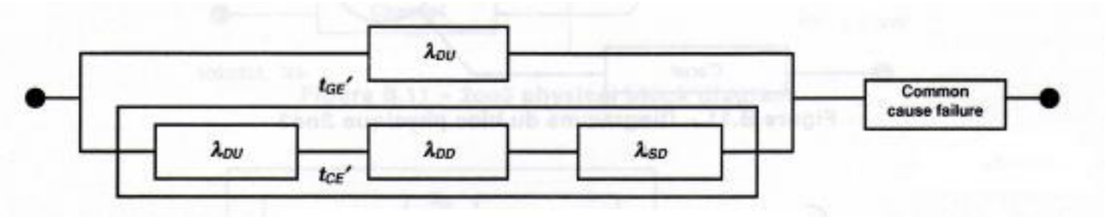


Figure 26 Reliability block diagram of 1oo2D architecture (IEC 61508-6)

Low:

$$\lambda_{SD} = \frac{\lambda}{2} DC$$

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$t_{GE}' = \frac{\lambda_{DU}\left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

Therefore, the average probability failure on demand for 1oo2D architecture is

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}'t_{GE}' + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

High:

The average probability failure on demand for 1oo2D architecture is

$$\lambda_{SD} = \frac{\lambda}{2}DC$$

$$t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}' + \beta_D\lambda_{DD} + \beta\lambda_{DU}$$

I.II.V 2oo3 architecture

This architecture consists of three channels connected in parallel with a majority selection of arrangement for the output signals. In that architecture, the output state is not changed if only one channel shows a different result which cannot be identical with other two channels. The following figure xx shows that kind of architecture.

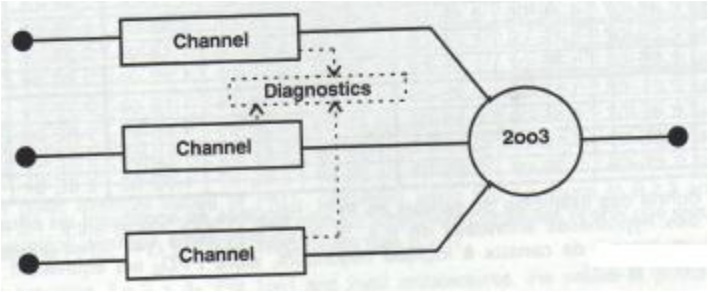


Figure 27 Physical block diagram of 2oo3 architecture (IEC 61508-6)

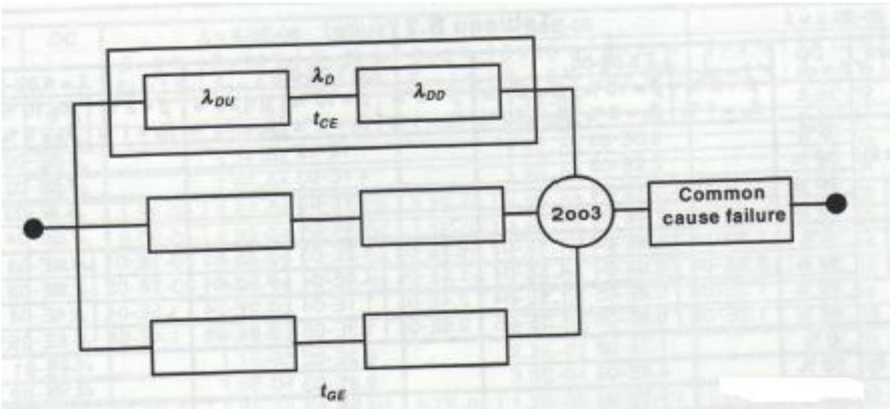


Figure 28 Reliability block diagram of 2oo3 architecture (IEC 61508-6)

Low:

The average probability failure on demand for 2oo3 architecture is

$$PFD_G = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

High:

The average probability failure on demand for 2oo3 architecture is

$$PFH_G = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} + \beta_D \lambda_{DD} + \beta \lambda_{DU}$$

III. Failure rate

The life of any item or machine-train can be split into three phases: the early failure (burn-in) phase, the useful life phase and the wear-out phase. The following figure xx shows the statistical life time of a technical item. The mean-time-to-failure (MTTF) or bathtub curve shows that new equipment or a new machine has a higher probability of failure due to installation problems, at the beginning of operation. The failure rate function at the beginning of operation or in the burn-in phase is quite high, close to constant in useful life phase. And then probability of failure increases sharply with elapsed time. If we assume that the failure rate function is constant during useful life phase, this means that the item is not failing during this phase. But the failure of that item will start if the item will enters the ear-our phase. Therefore, the item should be maintained or replaced before they enter the wear-our phase where the wear-out tends to give us very high failure rate.

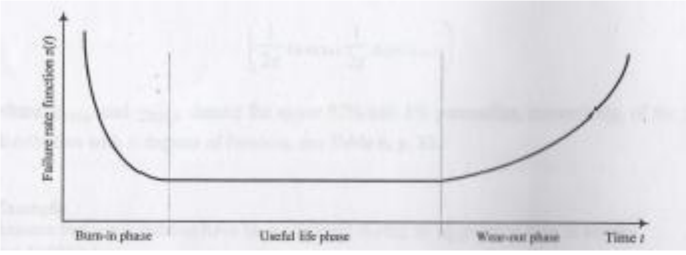


Figure 29 Bathtub shape of the failure rate (OREDA, 2009)

The failure rates are assumed to be exponentially distributed with parameter λ. The failure rate function is constant and independent of time, in which case $z(t) = \lambda$.

Based on the assumption of an estimated constant failure rate, the mean time to failure, MTTF, may be shown as:

$$\text{MTTF} = 1/\lambda$$

The estimate of failure rate λ, is defined as the ratio between the observed number of failures, n, and the aggregated time in service, τ.

The maximum likelihood estimator of λ is given by:

$$\hat{\lambda} = \text{Number of failures / Aggregated time in service} = n / \tau$$

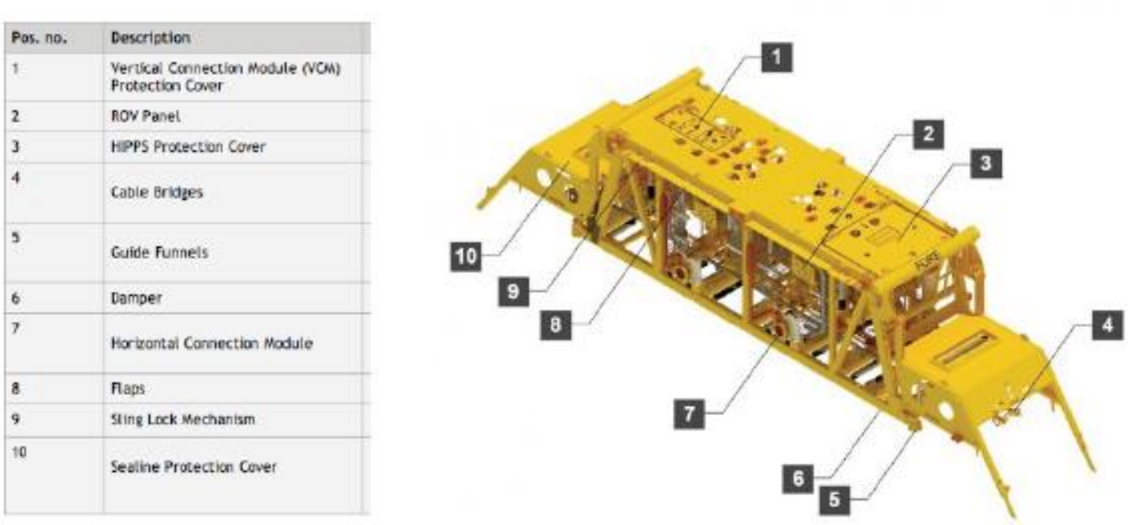
Confidence interval for the failure rate:

The uncertainty of the estimate failure rate $\hat{\lambda}$ may be presented as a 90% confidence interval.

$$P\ (\lambda_L \leq \lambda < \lambda_U) = 90\%$$

IV. Important features and diagrams of several subsea equipments

IV.I Subsea manifold



Pos. no.	Description
1	Vertical Connection Module (VCM) Protection Cover
2	ROV Panel
3	HIPPS Protection Cover
4	Cable Bridges
5	Guide Funnels
6	Damper
7	Horizontal Connection Module
8	Flaps
9	Sling Lock Mechanism
10	Sealine Protection Cover

Figure 30 Typical subsea manifold (Eilib, lecture slide from subsea technology course, UIS, 2011)

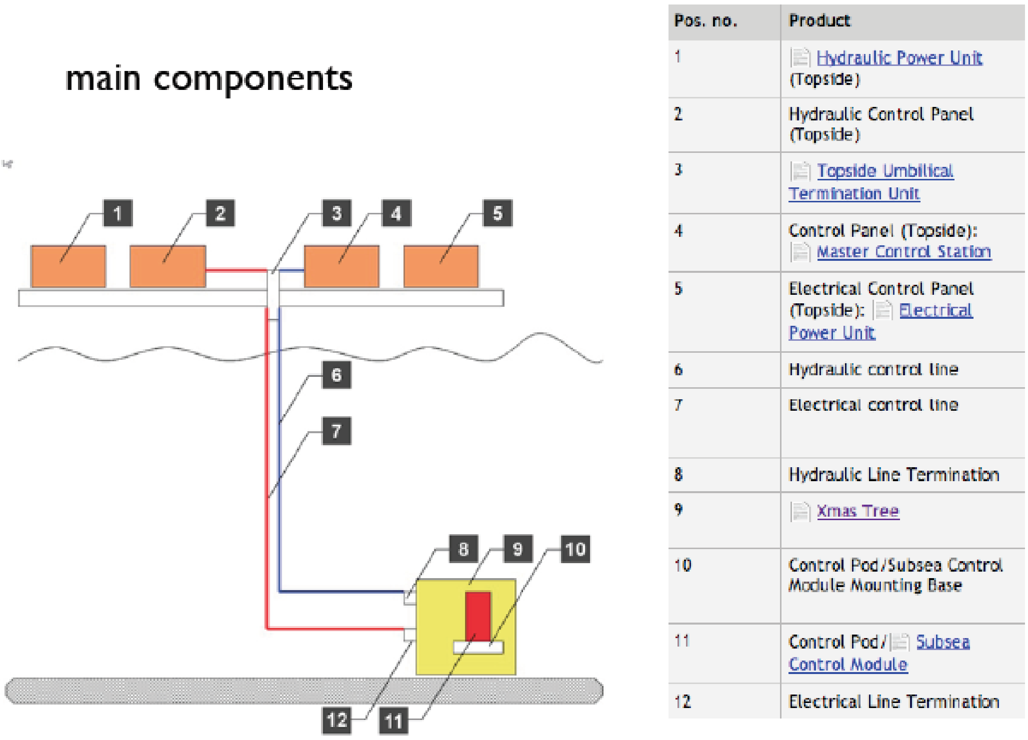
Pos. no.	Interface description
1	Lifting point
2	ROV Interface
7	Guide Posts
-	Template

Figure 31 Typical subsea manifold interfaces (Eilib, lecture slide from subsea technology course, UIS, 2011)

Figure 32 Subsea manifold and connection systems (GE oil and gas, 2011)

Figure 33 Typical subsea manifolds set up for installation in offshore (GE oil and gas, 2011)

IV.II Subsea control systems



Pos. no.	Product
1	Hydraulic Power Unit (Topside)
2	Hydraulic Control Panel (Topside)
3	Topside Umbilical Termination Unit
4	Control Panel (Topside): Master Control Station
5	Electrical Control Panel (Topside): Electrical Power Unit
6	Hydraulic control line
7	Electrical control line
8	Hydraulic Line Termination
9	Xmas Tree
10	Control Pod/Subsea Control Module Mounting Base
11	Control Pod/ Subsea Control Module
12	Electrical Line Termination

Figure 34 Main components of subsea control systems (Eiliv, lecture slide from subsea technology course, UIS, 2011)

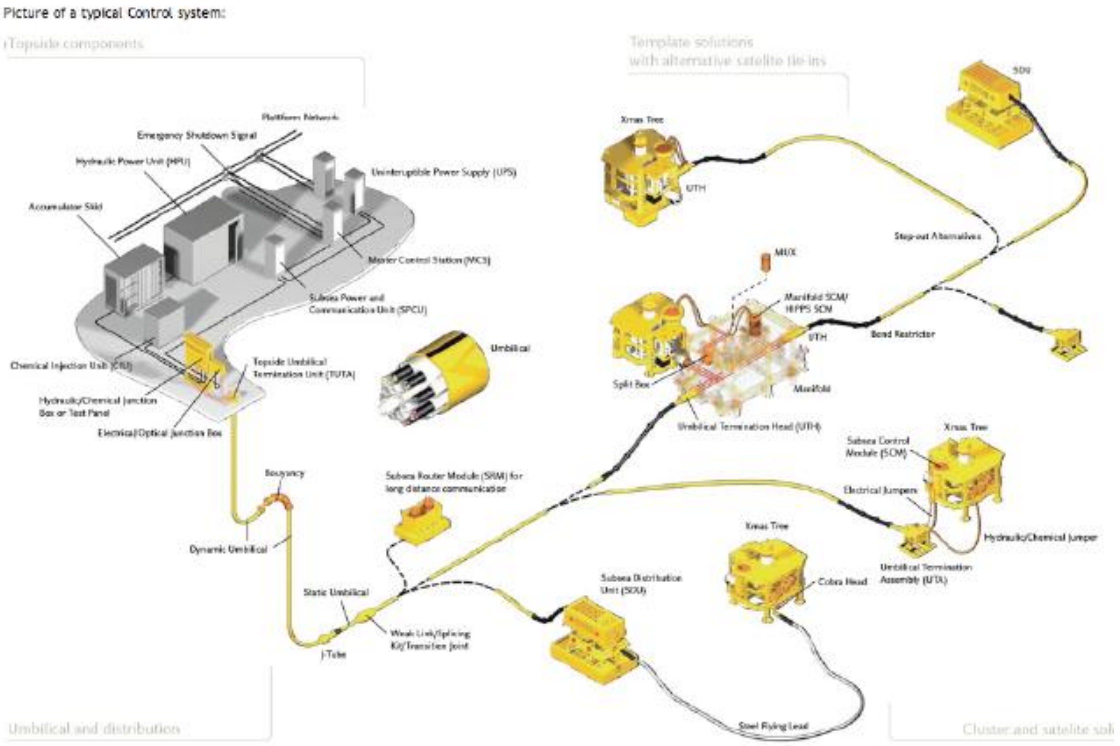

Picture of a typical Control system:

Figure 35 Picture of typical subsea control systems (Eilib, lecture slide from subsea technology course, UIS, 2011)

IV.III Subsea control system – SSIV

Subsea safety isolation valve is generally placed as close as possible to the platform to minimise the riser inventory and meet the platform safety requirements whilst avoiding potential interactions with existing infrastructure.

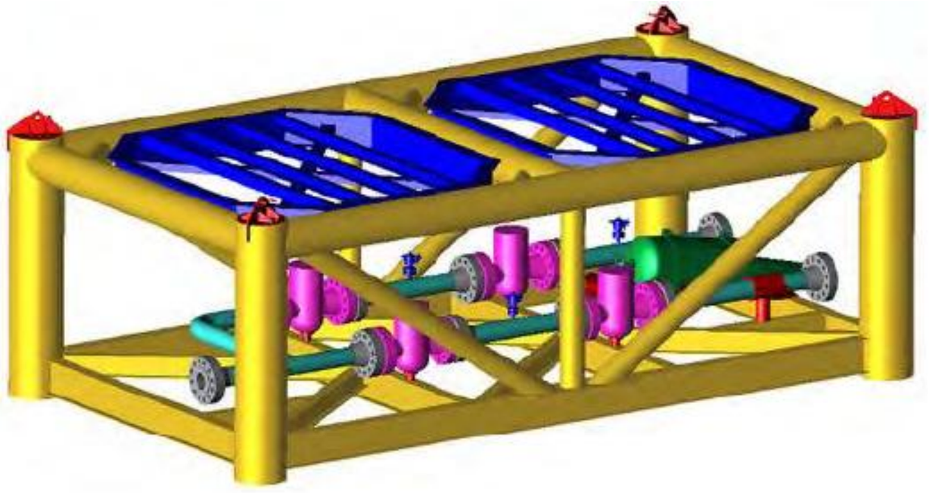


Figure 36 A diagram of SSIV for Orlando field (John Girling, 2011)

IV.IV Subsea control system – Xmas tree

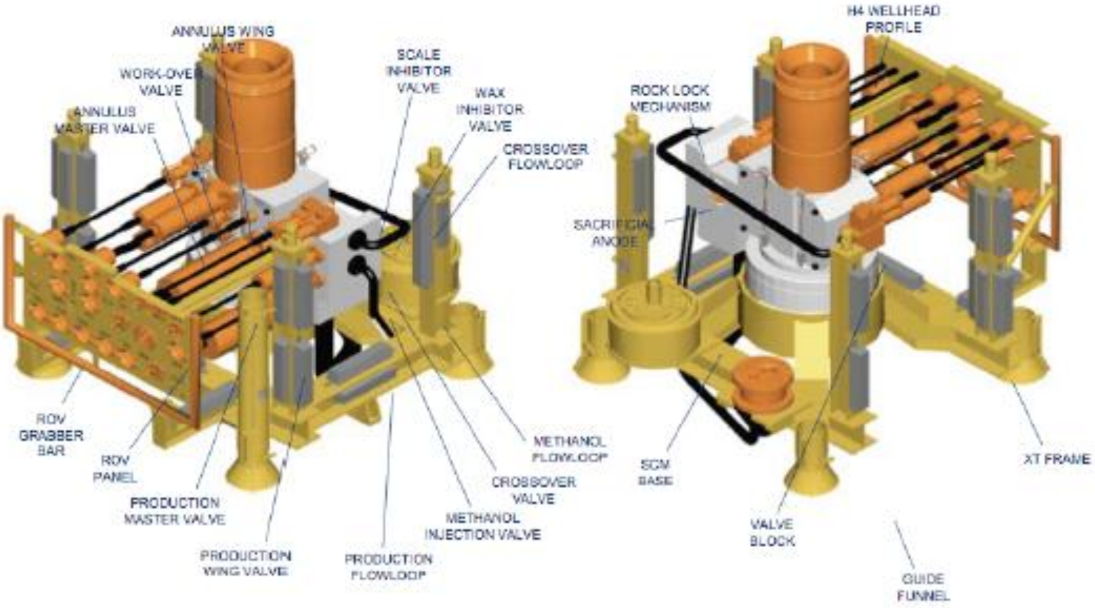
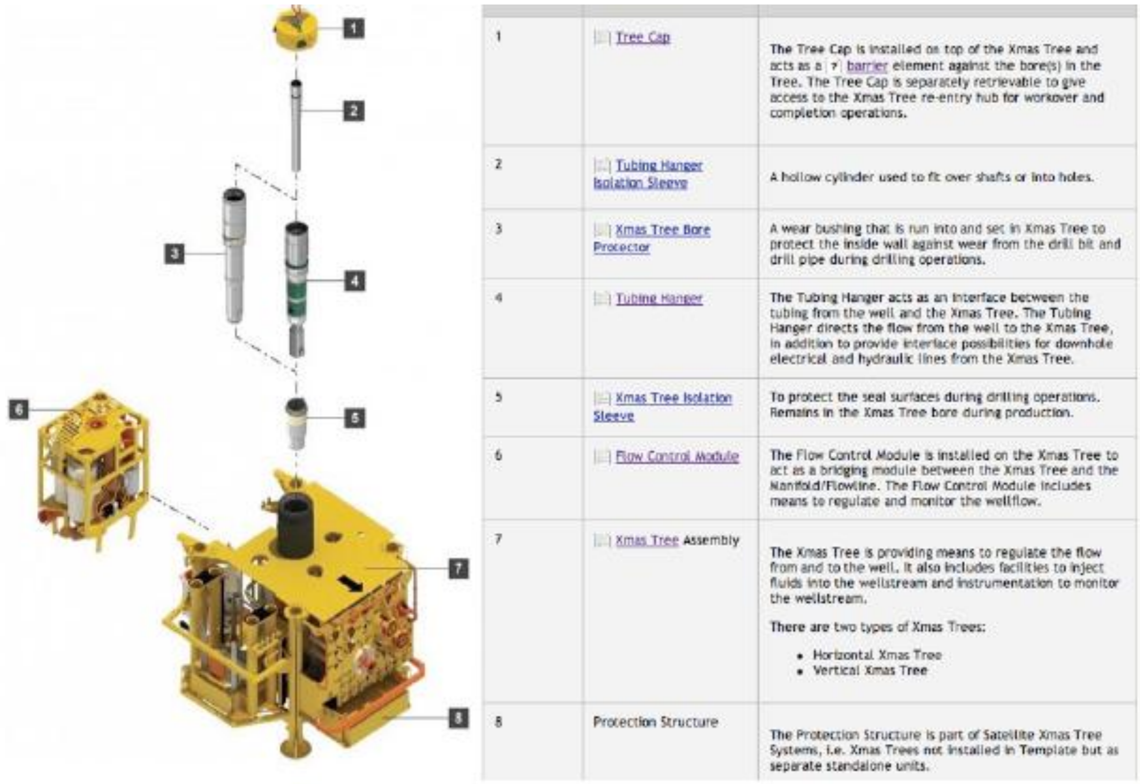


Figure 37 Typical subsea Xmas tree (Eilib, lecture slide from subsea technology course, UIS, 2011) xx:



1	Tree Cap	The Tree Cap is installed on top of the Xmas Tree and acts as a barrier element against the bore(s) in the Tree. The Tree Cap is separately retrievable to give access to the Xmas Tree re-entry hub for workover and completion operations.
2	Tubing Hanger Isolation Sleeve	A hollow cylinder used to fit over shafts or into holes.
3	Xmas Tree Bore Protector	A wear bushing that is run into and set in Xmas Tree to protect the inside wall against wear from the drill bit and drill pipe during drilling operations.
4	Tubing Hanger	The Tubing Hanger acts as an interface between the tubing from the well and the Xmas Tree. The Tubing Hanger directs the flow from the well to the Xmas Tree, in addition to provide interface possibilities for downhole electrical and hydraulic lines from the Xmas Tree.
5	Xmas Tree Isolation Sleeve	To protect the seal surfaces during drilling operations. Remains in the Xmas Tree bore during production.
6	Flow Control Module	The Flow Control Module is installed on the Xmas Tree to act as a bridging module between the Xmas Tree and the Manifold/Flowline. The Flow Control Module includes means to regulate and monitor the wellflow.
7	Xmas Tree Assembly	The Xmas Tree is providing means to regulate the flow from and to the well. It also includes facilities to inject fluids into the wellstream and instrumentation to monitor the wellstream. There are two types of Xmas Trees: • Horizontal Xmas Tree • Vertical Xmas Tree
8	Protection Structure	The Protection Structure is part of Satellite Xmas Tree Systems, i.e. Xmas Trees not installed in Template but as separate standalone units.

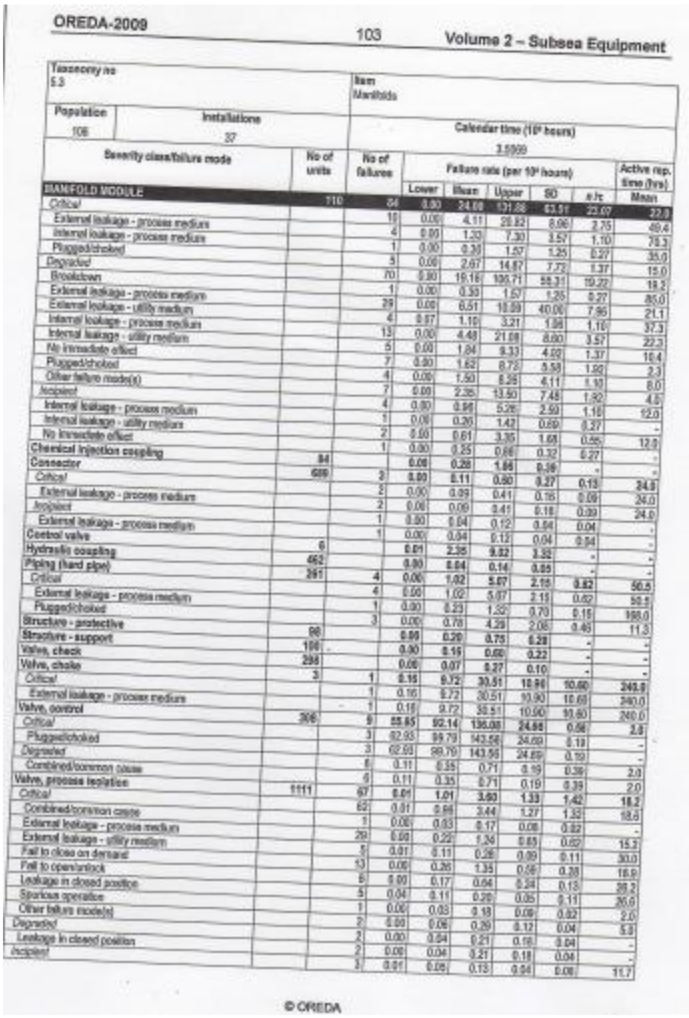
Figure 38 Main components of Xmas tree (Eilib, lecture slide from subsea technology course, UIS, 2011)

IV.VI Subsea pipelines

Figure 39 Subsea pipeline installation from offshore platform (Kristin subsea, NTNU)

V. Data collected from OREDA database

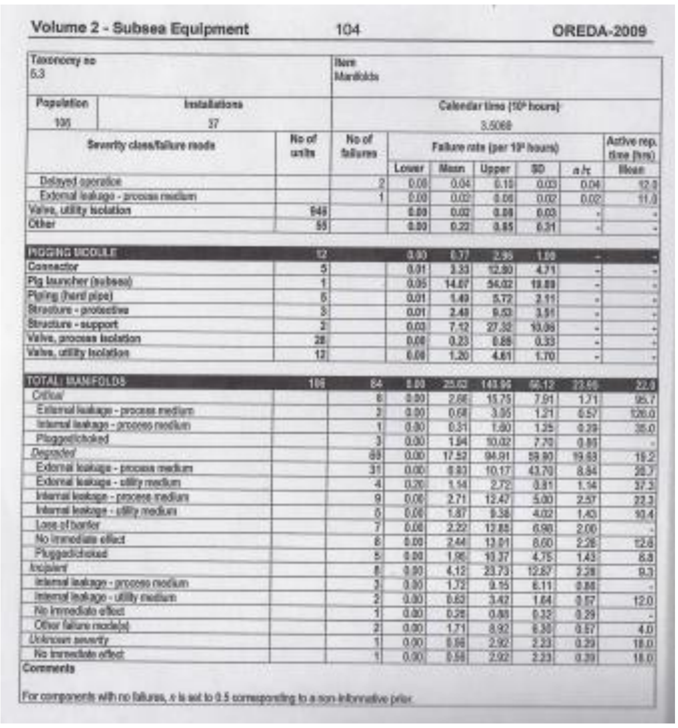
V.I Useful data for subsea manifold



OREDA-2009 103 Volume 2 – Subsea Equipment

Taxonomy no 5.3		Item Manifolds						
Population 106	Installations 37	Calendar time (10^6 hours) 3.5999						
Severity class/failure mode	No of units	No of failures	Failure rate (per 10^6 hours)					Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ	Mean
MANIFOLD MODULE	110	84	0.00	24.08	131.88	63.51	23.07	22.0
Critical		10	0.00	4.11	20.82	8.96	2.75	49.4
External leakage - process medium		4	0.00	1.32	7.30	3.57	1.10	79.3
Internal leakage - process medium		1	0.00	0.30	1.57	1.25	0.27	35.0
Plugged/choked		5	0.00	2.67	14.87	7.72	1.37	15.0
Degraded		70	0.90	19.16	106.71	58.31	19.22	18.2
Breakdown		1	0.00	0.30	1.57	1.25	0.27	85.0
External leakage - process medium		29	0.00	6.51	18.89	40.00	7.96	21.1
External leakage - utility medium		4	0.87	1.10	3.21	1.98	1.10	37.3
Internal leakage - process medium		13	0.00	4.48	21.08	8.80	3.57	22.3
Internal leakage - utility medium		5	0.00	1.84	9.33	4.02	1.37	10.4
No immediate effect		7	0.00	1.62	8.72	5.58	1.92	2.3
Plugged/choked		4	0.00	1.50	8.26	4.11	1.10	8.0
Other failure mode(s)		7	0.00	2.36	13.50	7.48	1.92	4.5
Incipient		4	0.00	0.96	5.26	2.59	1.10	12.0
Internal leakage - process medium		1	0.00	0.26	1.42	0.69	0.27	-
Internal leakage - utility medium		2	0.00	0.61	3.35	1.68	0.55	12.0
No immediate effect		1	0.00	0.25	0.86	0.32	0.27	-
Chemical injection coupling	84		0.08	0.28	1.86	0.38	-	-
Connector	689	3	0.00	0.11	0.60	0.27	0.13	24.0
Critical		2	0.00	0.09	0.41	0.16	0.09	24.0
External leakage - process medium		2	0.00	0.09	0.41	0.16	0.09	24.0
Incipient		1	0.00	0.04	0.12	0.04	0.04	-
External leakage - process medium		1	0.00	0.04	0.12	0.04	0.04	-
Control valve	6		0.01	2.35	9.82	3.32	-	-
Hydraulic coupling	462		0.00	0.04	0.14	0.05	-	-
Piping (hard pipe)	291	4	0.00	1.02	5.07	2.15	0.82	50.5
Critical		4	0.00	1.02	5.07	2.15	0.82	50.5
External leakage - process medium		1	0.00	0.23	1.32	0.70	0.15	168.0
Plugged/choked		3	0.00	0.78	4.29	2.06	0.46	11.3
Structure - protective	98		0.00	0.20	0.75	0.28	-	-
Structure - support	106		0.00	0.15	0.60	0.22	-	-
Valve, check	298		0.00	0.07	0.27	0.10	-	-
Valve, choke	3	1	0.15	9.72	30.51	10.96	10.60	240.0
Critical		1	0.16	9.72	30.51	10.90	10.60	240.0
External leakage - process medium		1	0.16	9.72	30.51	10.90	10.60	240.0
Valve, control	306	9	55.85	92.14	136.08	24.98	0.58	2.8
Critical		3	62.93	99.79	143.58	24.69	0.19	-
Plugged/choked		3	62.93	99.79	143.56	24.69	0.19	-
Degraded		6	0.11	0.35	0.71	0.19	0.39	2.0
Combined/common cause		6	0.11	0.35	0.71	0.19	0.39	2.0
Valve, process isolation	1111	67	0.01	1.01	3.60	1.33	1.42	18.2
Critical		62	0.01	0.96	3.44	1.27	1.32	18.6
Combined/common cause		1	0.00	0.03	0.17	0.06	0.02	-
External leakage - process medium		29	0.00	0.22	1.24	0.65	0.62	15.2
External leakage - utility medium		5	0.01	0.11	0.28	0.09	0.11	30.0
Fail to close on demand		13	0.06	0.26	1.35	0.56	0.28	16.9
Fail to open/unlock		6	0.00	0.17	0.64	0.24	0.13	28.2
Leakage in closed position		5	0.04	0.11	0.20	0.05	0.11	26.6
Spurious operation		1	0.00	0.03	0.18	0.08	0.02	2.0
Other failure mode(s)		2	0.00	0.06	0.29	0.12	0.04	5.3
Degraded		2	0.00	0.04	0.21	0.16	0.04	-
Leakage in closed position		2	0.00	0.04	0.21	0.18	0.04	-
Incipient		3	0.01	0.08	0.13	0.04	0.08	11.7

© OREDA

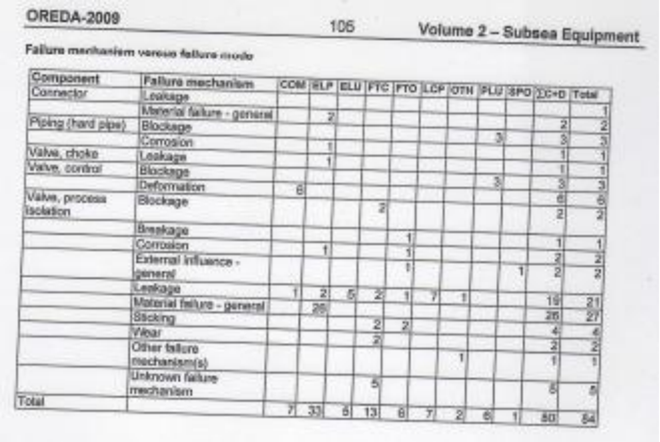


Volume 2 - Subsea Equipment 104 OREDA-2009

Taxonomy no 6.3			Item Manifolds						
Population 106	Installations 37		Calendar time (10^6 hours) 3.5068						
Severity class/failure mode	No of units	No of failures	Failure rate (per 10^6 hours)						Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ		Mean
Delayed operation		2	0.00	0.04	0.10	0.03	0.04		12.0
External leakage - process medium		1	0.00	0.02	0.06	0.02	0.02		11.0
Valve, utility isolation	946		0.00	0.02	0.08	0.03	-		-
Other	55		0.00	0.22	0.85	0.31	-		-
PIGGING MODULE	12		0.00	0.77	2.96	1.00	-		-
Connector	5		0.01	3.33	12.80	4.71	-		-
Pig launcher (subsea)	1		0.05	14.07	54.02	19.89	-		-
Piping (hard pipe)	6		0.01	1.49	5.72	2.11	-		-
Structure - protective	3		0.01	2.48	9.53	3.51	-		-
Structure - support	2		0.03	7.12	27.32	10.06	-		-
Valve, process isolation	28		0.00	0.23	0.88	0.33	-		-
Valve, utility isolation	12		0.00	1.20	4.61	1.70	-		-
TOTAL: MANIFOLDS	106	84	0.00	25.02	143.96	56.12	23.95		22.0
Critical		6	0.00	2.66	15.75	7.91	1.71		95.7
External leakage - process medium		2	0.00	0.68	3.05	1.21	0.57		126.0
Internal leakage - process medium		1	0.00	0.31	1.60	1.25	0.29		35.0
Plugged/choked		3	0.00	1.64	10.02	7.70	0.86		-
Degraded		69	0.00	17.52	94.91	59.90	19.68		19.2
External leakage - process medium		31	0.00	8.83	10.17	43.70	8.84		20.7
External leakage - utility medium		4	0.20	1.14	2.72	0.81	1.14		37.3
Internal leakage - process medium		9	0.06	2.71	12.47	5.00	2.57		22.3
Internal leakage - utility medium		5	0.06	1.87	9.38	4.02	1.43		10.4
Loss of barrier		7	0.06	2.22	12.85	6.90	2.00		-
No immediate effect		8	0.00	2.44	13.01	8.60	2.28		12.6
Plugged/choked		5	0.00	1.96	10.37	4.75	1.43		6.8
Incipient		8	0.00	4.12	23.73	12.67	2.28		9.3
Internal leakage - process medium		3	0.00	1.72	9.15	6.11	0.86		-
Internal leakage - utility medium		2	0.00	0.63	3.42	1.64	0.57		12.0
No immediate effect		1	0.00	0.28	0.88	0.32	0.29		-
Other failure mode(s)		2	0.00	1.71	8.92	6.30	0.57		4.0
Unknown severity		1	0.00	0.56	2.92	2.23	0.29		18.0
No immediate effect		1	0.00	0.56	2.92	2.23	0.29		18.0

Comments

For components with no failures, n is set to 0.5 corresponding to a non-informative prior.

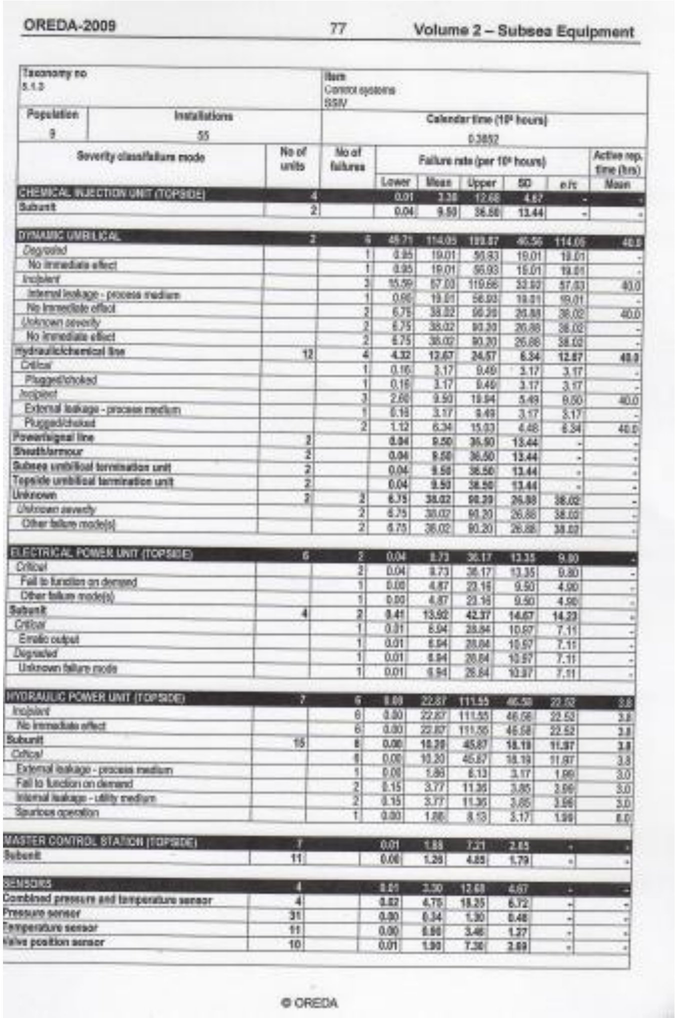


OREDA-2009 106 Volume 2 – Subsea Equipment

Failure mechanism versus failure mode

Component	Failure mechanism	COM	ELP	ELU	FTC	FTO	LCP	OTN	PLU	SPO	ΣC+D	Total
Connector	Leakage											1
	Material failure - general		2								2	2
Piping (hard pipe)	Blockage								3		3	3
	Corrosion		1								1	1
Valve, choke	Leakage		1								1	1
Valve, control	Blockage								3		3	3
	Deformation	6									6	6
Valve, process isolation	Blockage				2						2	2
	Breakage					1					1	1
	Corrosion		1			1					2	2
	External influence - general					1				1	2	2
	Leakage	1	2	5	2	1	7	1			19	21
	Material failure - general		26								26	27
	Sticking				2	2					4	4
	Wear				2						2	2
	Other failure mechanism(s)							1			1	1
	Unknown failure mechanism				5						5	5
Total		7	33	5	13	6	7	2	6	1	80	84

V.II Useful data for subsea control system - SSIV



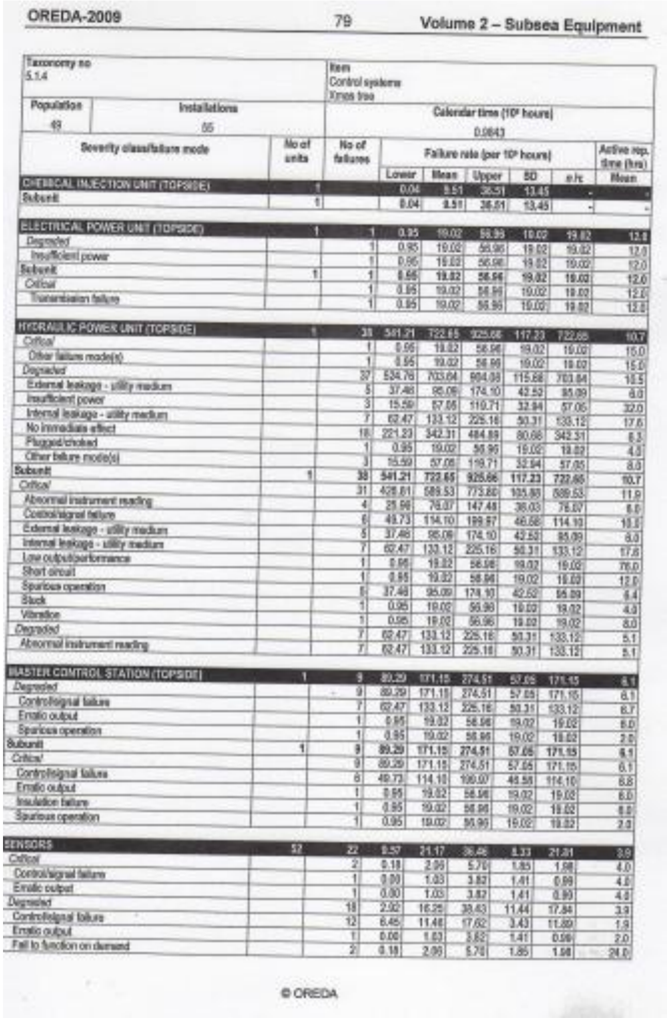
OREDA-2009 77 Volume 2 – Subsea Equipment

Taxonomy no 5.1.2			Item Control systems SSIV						
Population 9	Installations 55		Calendar time (10^6 hours) 0.3852						

Severity class/failure mode	No of units	No of failures	Failure rate (per 10^6 hours)					Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ	Mean
CHEMICAL INJECTION UNIT (TOPSIDE)	4		0.01	3.30	12.68	4.67	-	-
Subunit	2		0.04	9.50	36.50	13.44	-	-
DYNAMIC UMBILICAL	2	6	45.71	114.05	199.87	46.56	114.05	40.0
Degraded		1	0.95	19.01	56.93	19.01	19.01	-
No immediate effect		1	0.95	19.01	56.93	19.01	19.01	-
Incipient		3	15.59	57.03	119.66	32.93	57.03	40.0
Internal leakage - process medium		1	0.98	19.01	56.93	19.01	19.01	-
No immediate effect		2	6.75	38.02	90.20	26.88	38.02	40.0
Unknown severity		2	6.75	38.02	90.20	26.88	38.02	-
No immediate effect		2	6.75	38.02	90.20	26.88	38.02	-
Hydraulic/chemical line	12	4	4.32	12.67	24.57	6.34	12.67	40.0
Critical		1	0.16	3.17	9.49	3.17	3.17	-
Plugged/choked		1	0.16	3.17	9.49	3.17	3.17	-
Incipient		3	2.60	9.50	19.94	5.49	9.50	40.0
External leakage - process medium		1	0.16	3.17	9.49	3.17	3.17	-
Plugged/choked		2	1.12	6.34	15.03	4.48	6.34	40.0
Power/signal line	2		0.04	9.50	36.50	13.44	-	-
Sheath/armour	2		0.04	9.50	36.50	13.44	-	-
Subsea umbilical termination unit	2		0.04	9.50	36.50	13.44	-	-
Topside umbilical termination unit	2		0.04	9.50	36.50	13.44	-	-
Unknown	2	2	6.75	38.02	90.20	26.88	38.02	-
Unknown severity		2	6.75	38.02	90.20	26.88	38.02	-
Other failure mode(s)		2	6.75	38.02	90.20	26.88	38.02	-
ELECTRICAL POWER UNIT (TOPSIDE)	6	2	0.04	8.73	36.17	13.35	9.80	-
Critical		2	0.04	8.73	36.17	13.35	9.80	-
Fail to function on demand		1	0.00	4.87	23.16	9.50	4.90	-
Other failure mode(s)		1	0.00	4.87	23.16	9.50	4.90	-
Subunit	4	2	0.41	13.92	42.37	14.67	14.23	-
Critical		1	0.01	6.94	28.84	10.97	7.11	-
Erratic output		1	0.01	6.94	28.84	10.97	7.11	-
Degraded		1	0.01	6.94	28.84	10.97	7.11	-
Unknown failure mode		1	0.01	6.94	28.84	10.97	7.11	-
HYDRAULIC POWER UNIT (TOPSIDE)	7	6	0.00	22.87	111.55	46.58	22.52	3.8
Incipient		6	0.00	22.87	111.55	46.58	22.52	3.8
No immediate effect		6	0.00	22.87	111.55	46.58	22.52	3.8
Subunit	15	8	0.00	10.20	45.87	18.19	11.97	3.8
Critical		8	0.00	10.20	45.87	18.19	11.97	3.8
External leakage - process medium		1	0.00	1.88	8.13	3.17	1.99	3.0
Fail to function on demand		2	0.15	3.77	11.36	3.85	3.98	3.0
Internal leakage - utility medium		2	0.15	3.77	11.36	3.85	3.98	3.0
Spurious operation		1	0.00	1.88	8.13	3.17	1.99	6.0
MASTER CONTROL STATION (TOPSIDE)	7		0.01	1.88	7.21	2.85	-	-
Subunit	11		0.00	1.28	4.85	1.79	-	-
SENSORS	4		0.01	3.30	12.68	4.67	-	-
Combined pressure and temperature sensor	4		0.02	4.76	18.25	6.72	-	-
Pressure sensor	31		0.00	0.34	1.30	0.48	-	-
Temperature sensor	11		0.00	0.90	3.46	1.27	-	-
Valve position sensor	10		0.01	1.90	7.30	2.69	-	-

© OREDA

V.III Useful data for subsea control system – Xmas tree

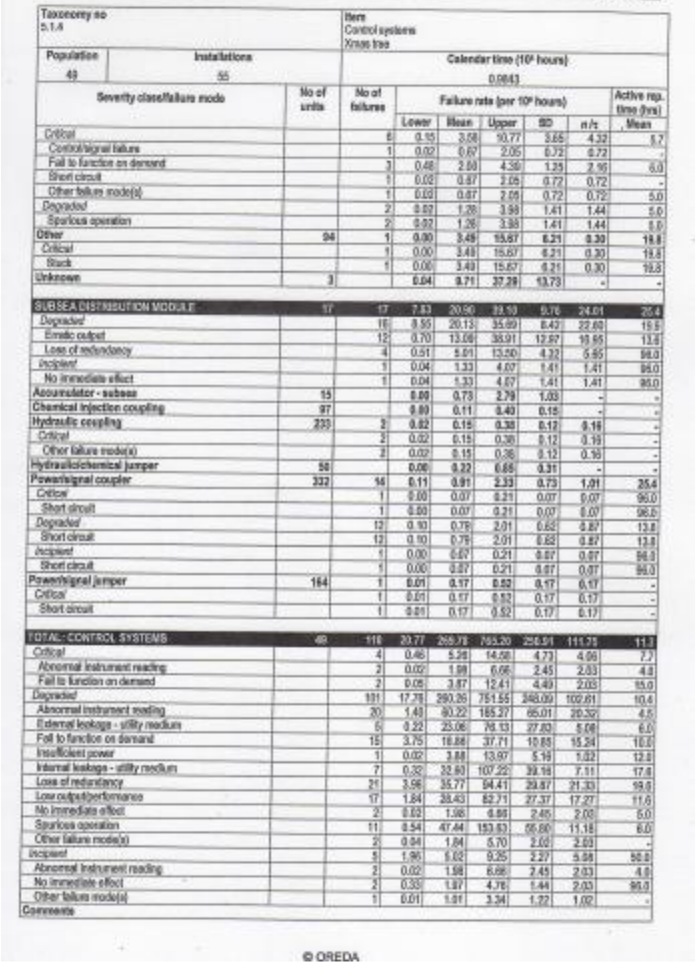


OREDA-2009 79 Volume 2 – Subsea Equipment

Taxonomy no 5.1.4	Item Control systems Xmas tree
Population 49 / Installations 65	Calendar time (10⁶ hours) 0.0843

Severity class/failure mode	No of units	No of failures	Failure rate (per 10⁶ hours)					Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ	Mean
CHEMICAL INJECTION UNIT (TOPSIDE)	1		0.04	9.51	36.51	13.45	-	-
Subunit	1		0.04	9.51	36.51	13.45	-	-
ELECTRICAL POWER UNIT (TOPSIDE)	1	1	0.95	19.02	56.96	19.02	19.02	12.0
Degraded		1	0.95	19.02	56.96	19.02	19.02	12.0
Insufficient power		1	0.95	19.02	56.96	19.02	19.02	12.0
Subunit	1	1	0.95	19.02	56.96	19.02	19.02	12.0
Critical		1	0.95	19.02	56.96	19.02	19.02	12.0
Transmission failure		1	0.95	19.02	56.96	19.02	19.02	12.0
HYDRAULIC POWER UNIT (TOPSIDE)	1	38	541.21	722.65	925.66	117.23	722.65	10.7
Critical		1	0.95	19.02	56.96	19.02	19.02	15.0
Other failure mode(s)		1	0.95	19.02	56.96	19.02	19.02	15.0
Degraded		37	534.76	703.64	904.08	115.68	703.64	10.5
External leakage - utility medium		5	37.48	95.09	174.10	42.52	95.09	8.0
Insufficient power		3	15.59	57.05	119.71	32.94	57.05	32.0
Internal leakage - utility medium		7	62.47	133.12	225.16	50.31	133.12	17.6
No immediate effect		18	221.23	342.31	484.89	80.66	342.31	6.3
Plugged/choked		1	0.95	19.02	56.96	19.02	19.02	4.0
Other failure mode(s)		3	15.59	57.05	119.71	32.94	57.05	8.0
Subunit	1	38	541.21	722.65	925.66	117.23	722.65	10.7
Critical		31	428.61	589.53	773.80	105.88	589.53	11.9
Abnormal instrument reading		4	25.96	76.07	147.48	38.03	76.07	8.0
Control/signal failure		6	49.73	114.10	199.97	46.58	114.10	10.8
External leakage - utility medium		5	37.48	95.09	174.10	42.52	95.09	8.0
Internal leakage - utility medium		7	62.47	133.12	225.16	50.31	133.12	17.6
Low output/performance		1	0.95	19.02	56.96	19.02	19.02	76.0
Short circuit		1	0.95	19.02	56.96	19.02	19.02	12.0
Spurious operation		5	37.48	95.09	174.10	42.52	95.09	6.4
Stuck		1	0.95	19.02	56.96	19.02	19.02	4.0
Vibration		1	0.95	19.02	56.96	19.02	19.02	8.0
Degraded		7	62.47	133.12	225.16	50.31	133.12	5.1
Abnormal instrument reading		7	62.47	133.12	225.16	50.31	133.12	5.1
MASTER CONTROL STATION (TOPSIDE)	1	9	89.29	171.15	274.51	57.05	171.15	6.1
Degraded		9	89.29	171.15	274.51	57.05	171.15	6.1
Control/signal failure		7	62.47	133.12	225.16	50.31	133.12	6.7
Erratic output		1	0.95	19.02	56.96	19.02	19.02	6.0
Spurious operation		1	0.95	19.02	56.96	19.02	19.02	2.0
Subunit	1	9	89.29	171.15	274.51	57.05	171.15	6.1
Critical		9	89.29	171.15	274.51	57.05	171.15	6.1
Control/signal failure		6	49.73	114.10	199.07	46.58	114.10	6.8
Erratic output		1	0.95	19.02	56.96	19.02	19.02	6.0
Insulation failure		1	0.95	19.02	56.96	19.02	19.02	8.0
Spurious operation		1	0.95	19.02	56.96	19.02	19.02	2.0
SENSORS	52	22	9.57	21.17	38.46	8.33	21.81	3.9
Critical		2	0.18	2.06	5.70	1.85	1.98	4.0
Control/signal failure		1	0.00	1.03	3.82	1.41	0.99	4.0
Erratic output		1	0.00	1.03	3.82	1.41	0.99	4.0
Degraded		18	2.92	16.25	38.43	11.44	17.84	3.9
Control/signal failure		12	6.45	11.46	17.62	3.43	11.89	1.9
Erratic output		1	0.00	1.03	3.82	1.41	0.99	2.0
Fail to function on demand		2	0.18	2.06	5.70	1.85	1.98	24.0

© OREDA



OREDA-2009 81 Volume 2 – Subsea Equipment

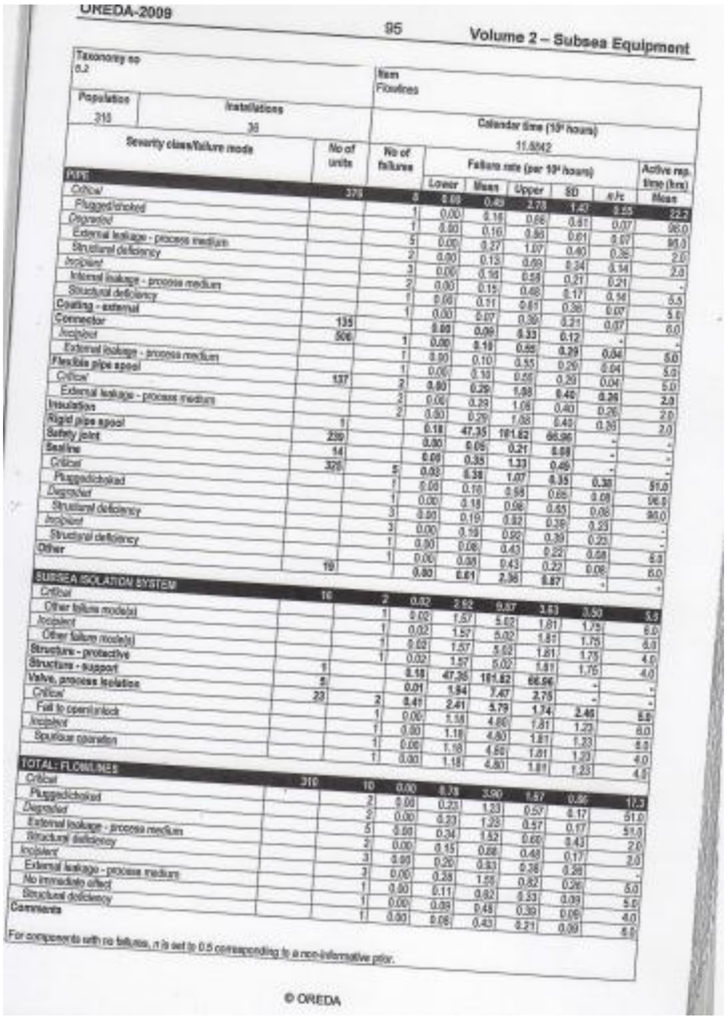
Taxonomy no 5.1.4		Item Control systems Xmas tree
Population 49	Installations 55	Calendar time (10^6 hours) 0.9843

Severity class/failure mode	No of units	No of failures	Failure rate (per 10^6 hours)					Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ	Mean
Critical		6	0.15	3.08	10.77	3.65	4.32	5.7
Control/signal failure		1	0.02	0.67	2.05	0.72	0.72	-
Fail to function on demand		3	0.48	2.88	4.38	1.25	2.16	6.0
Short circuit		1	0.02	0.67	2.05	0.72	0.72	-
Other failure mode(s)		1	0.02	0.67	2.05	0.72	0.72	5.0
Degraded		2	0.07	1.28	3.98	1.41	1.44	5.0
Spurious operation		2	0.07	1.28	3.98	1.41	1.44	5.0
Other	94	1	0.00	3.49	15.87	6.21	0.30	19.8
Critical		1	0.00	3.49	15.87	6.21	0.30	19.8
Stuck		1	0.00	3.49	15.87	6.21	0.30	19.8
Unknown	3		0.04	8.71	37.28	13.73	-	-
SUBSEA DISTRIBUTION MODULE	17	17	7.83	20.90	39.10	9.76	24.01	25.4
Degraded		16	8.55	20.13	35.89	8.42	22.60	19.5
Erratic output		12	0.70	13.08	38.91	12.97	16.95	13.6
Loss of redundancy		4	0.51	5.01	13.50	4.32	5.65	98.0
Incipient		1	0.04	1.33	4.07	1.41	1.41	96.0
No immediate effect		1	0.04	1.33	4.07	1.41	1.41	96.0
Accumulator - subsea	15		0.00	0.73	2.79	1.03	-	-
Chemical injection coupling	97		0.00	0.11	0.40	0.15	-	-
Hydraulic coupling	233	2	0.02	0.15	0.38	0.12	0.16	-
Critical		2	0.02	0.15	0.38	0.12	0.16	-
Other failure mode(s)		2	0.02	0.15	0.38	0.12	0.16	-
Hydraulic/chemical jumper	50		0.00	0.22	0.85	0.31	-	-
Power/signal coupler	332	14	0.11	0.91	2.33	0.73	1.01	25.4
Critical		1	0.00	0.07	0.21	0.07	0.07	96.0
Short circuit		1	0.00	0.07	0.21	0.07	0.07	96.0
Degraded		12	0.10	0.79	2.01	0.62	0.87	13.8
Short circuit		12	0.10	0.79	2.01	0.62	0.87	13.8
Incipient		1	0.00	0.07	0.21	0.07	0.07	96.0
Short circuit		1	0.00	0.07	0.21	0.07	0.07	96.0
Power/signal jumper	164	1	0.01	0.17	0.52	0.17	0.17	-
Critical		1	0.01	0.17	0.52	0.17	0.17	-
Short circuit		1	0.01	0.17	0.52	0.17	0.17	-
TOTAL: CONTROL SYSTEMS	49	116	20.77	265.78	765.20	250.91	111.75	11.3
Critical		4	0.46	5.28	14.58	4.73	4.06	7.7
Abnormal instrument reading		2	0.02	1.98	6.66	2.45	2.03	4.8
Fail to function on demand		2	0.08	3.87	12.41	4.49	2.03	15.0
Degraded		101	17.78	280.26	751.55	248.09	102.61	10.4
Abnormal instrument reading		20	1.40	60.22	185.27	65.01	20.32	4.5
External leakage - utility medium		6	0.22	25.06	78.13	27.83	5.08	6.0
Fail to function on demand		15	3.75	18.88	37.71	10.85	15.24	10.0
Insufficient power		1	0.02	3.88	13.97	5.16	1.02	12.0
Internal leakage - utility medium		7	0.32	32.80	107.22	39.16	7.11	17.6
Loss of redundancy		21	3.96	35.77	94.41	29.87	21.33	19.8
Low output/performance		17	1.84	28.43	82.71	27.37	17.27	11.6
No immediate effect		2	0.02	1.98	6.66	2.45	2.03	5.0
Spurious operation		11	0.54	47.44	153.63	55.80	11.18	6.0
Other failure mode(s)		2	0.04	1.84	5.70	2.02	2.03	-
Incipient		5	1.96	5.02	9.25	2.27	5.08	50.0
Abnormal instrument reading		2	0.02	1.98	6.66	2.45	2.03	4.0
No immediate effect		2	0.33	1.87	4.76	1.44	2.03	96.0
Other failure mode(s)		1	0.01	1.01	3.34	1.22	1.02	-

Comments

© OREDA

V.IV Useful data for subsea manifold



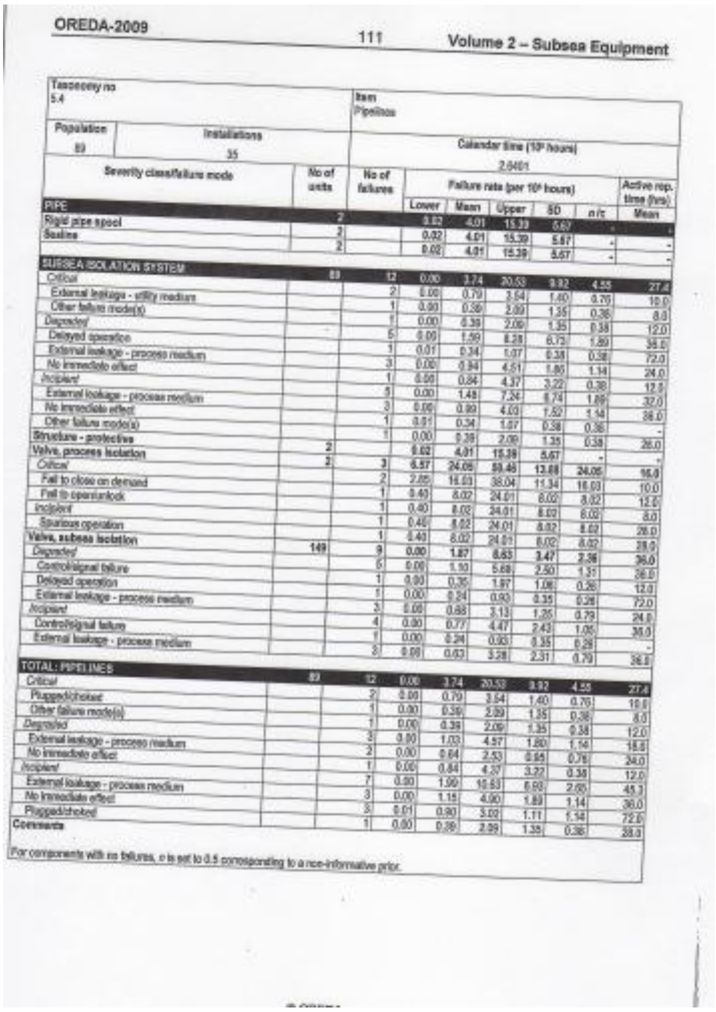
OREDA-2009 95 Volume 2 – Subsea Equipment

Taxonomy no 6.2			Item Flowlines					
Population 310	Installations 36		Calendar time (10^6 hours) 11.5842					
Severity class/failure mode	No of units	No of failures	Failure rate (per 10^6 hours)					Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ	Mean
PIPE	378	8	0.08	0.49	2.78	1.47	0.55	22.2
Critical		1	0.00	0.16	0.86	0.61	0.07	96.0
Plugged/choked		1	0.00	0.16	0.86	0.61	0.07	96.0
Degraded		5	0.00	0.27	1.07	0.40	0.36	2.0
External leakage - process medium		2	0.00	0.13	0.69	0.34	0.14	2.0
Structural deficiency		3	0.00	0.16	0.58	0.21	0.21	-
Incipient		2	0.00	0.15	0.48	0.17	0.14	5.5
Internal leakage - process medium		1	0.00	0.11	0.61	0.36	0.07	5.0
Structural deficiency		1	0.00	0.07	0.39	0.21	0.07	6.0
Coating - external	135		0.00	0.09	0.33	0.12	-	-
Connector	506	1	0.00	0.10	0.55	0.29	0.04	5.0
Incipient		1	0.00	0.10	0.55	0.29	0.04	5.0
External leakage - process medium		1	0.00	0.10	0.55	0.29	0.04	5.0
Flexible pipe spool	137	2	0.00	0.29	1.08	0.40	0.26	2.0
Critical		2	0.00	0.29	1.08	0.40	0.26	2.0
External leakage - process medium		2	0.00	0.29	1.08	0.40	0.26	2.0
Insulation	1		0.18	47.35	181.82	66.96	-	-
Rigid pipe spool	239		0.00	0.05	0.21	0.08	-	-
Safety joint	14		0.00	0.35	1.33	0.49	-	-
Sealine	326	5	0.03	0.38	1.07	0.35	0.30	51.0
Critical		1	0.00	0.18	0.98	0.65	0.08	96.0
Plugged/choked		1	0.00	0.18	0.98	0.65	0.08	96.0
Degraded		3	0.00	0.19	0.92	0.39	0.23	-
Structural deficiency		3	0.00	0.19	0.92	0.39	0.23	-
Incipient		1	0.00	0.08	0.43	0.22	0.08	6.0
Structural deficiency		1	0.00	0.08	0.43	0.22	0.08	6.0
Other	19		0.00	0.61	2.36	0.87	-	-
SUBSEA ISOLATION SYSTEM	16	2	0.02	2.62	9.87	3.63	3.50	5.0
Critical		1	0.02	1.57	5.02	1.81	1.75	6.0
Other failure mode(s)		1	0.02	1.57	5.02	1.81	1.75	6.0
Incipient		1	0.02	1.57	5.02	1.81	1.75	4.0
Other failure mode(s)		1	0.02	1.57	5.02	1.81	1.75	4.0
Structure - protective	1		0.18	47.36	181.82	66.96	-	-
Structure - support	5		0.01	1.94	7.47	2.75	-	-
Valve, process isolation	23	2	0.41	2.41	5.79	1.74	2.46	5.0
Critical		1	0.00	1.18	4.80	1.81	1.23	6.0
Fail to open/unlock		1	0.00	1.18	4.80	1.81	1.23	6.0
Incipient		1	0.00	1.18	4.80	1.81	1.23	4.0
Spurious operation		1	0.00	1.18	4.80	1.81	1.23	4.0
TOTAL: FLOWLINES	310	10	0.00	0.79	3.90	1.57	0.86	17.3
Critical		2	0.00	0.23	1.23	0.57	0.17	51.0
Plugged/choked		2	0.00	0.23	1.23	0.57	0.17	51.0
Degraded		5	0.00	0.34	1.52	0.60	0.43	2.0
External leakage - process medium		2	0.00	0.15	0.88	0.48	0.17	2.0
Structural deficiency		3	0.00	0.20	0.93	0.36	0.28	-
Incipient		3	0.00	0.28	1.55	0.82	0.26	5.0
External leakage - process medium		1	0.00	0.11	0.62	0.33	0.09	5.0
No immediate effect		1	0.00	0.09	0.48	0.30	0.06	4.0
Structural deficiency		1	0.00	0.06	0.43	0.21	0.09	5.0
Comments								

For components with no failures, n is set to 0.5 corresponding to a non-informative prior.

© OREDA

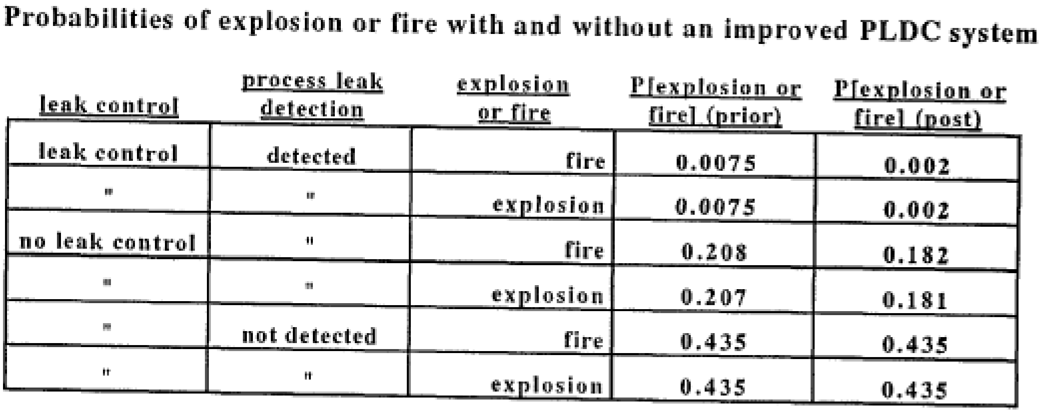
V.V Useful data for subsea manifold



OREDA-2009 111 Volume 2 – Subsea Equipment

Taxonomy no 5.4			Item Pipelines					
Population 89	Installations 35		Calendar time (10^6 hours) 2.0401					
Severity class/failure mode	No of units	No of failures	Failure rate (per 10^6 hours)					Active rep. time (hrs)
			Lower	Mean	Upper	SD	n/τ	Mean
PIPE								
Rigid pipe spool	2		0.02	4.01	15.39	5.67	-	-
Sealine	2		0.02	4.01	15.39	5.67	-	-
	2		0.02	4.01	15.39	5.67	-	-
SUBSEA ISOLATION SYSTEM	89	12	0.00	3.74	20.53	9.82	4.55	27.4
Critical		2	0.00	0.79	3.54	1.40	0.70	10.0
External leakage - utility medium		1	0.00	0.39	2.09	1.35	0.38	8.0
Other failure mode(s)		1	0.00	0.39	2.09	1.35	0.38	12.0
Degraded		5	0.00	1.59	8.28	6.73	1.89	36.0
Delayed operation		1	0.01	0.34	1.07	0.38	0.38	72.0
External leakage - process medium		3	0.00	0.94	4.51	1.86	1.14	24.0
No immediate effect		1	0.00	0.84	4.37	3.22	0.38	12.0
Incipient		5	0.00	1.48	7.24	8.74	1.89	32.0
External leakage - process medium		3	0.00	0.89	4.03	1.52	1.14	36.0
No immediate effect		1	0.01	0.34	1.07	0.38	0.38	-
Other failure mode(s)		1	0.00	0.39	2.09	1.35	0.38	28.0
Structure - protective	2		0.02	4.01	15.39	5.67	-	-
Valve, process isolation	2	3	6.57	24.05	59.46	13.68	24.05	16.0
Critical		2	2.85	16.03	38.04	11.34	16.03	10.0
Fail to close on demand		1	0.40	8.02	24.01	8.02	8.02	12.0
Fail to open/unlock		1	0.40	8.02	24.01	8.02	8.02	8.0
Incipient		1	0.40	8.02	24.01	8.02	8.02	28.0
Spurious operation		1	0.40	8.02	24.01	8.02	8.02	28.0
Valve, subsea isolation	149	9	0.00	1.87	8.63	3.47	2.36	36.0
Degraded		6	0.00	1.10	5.68	2.50	1.31	36.0
Control/signal failure		1	0.00	0.35	1.97	1.08	0.26	12.0
Delayed operation		1	0.00	0.24	0.93	0.35	0.26	72.0
External leakage - process medium		3	0.00	0.68	3.13	1.25	0.79	24.0
Incipient		4	0.00	0.77	4.47	2.43	1.05	36.0
Control/signal failure		1	0.00	0.24	0.93	0.35	0.26	-
External leakage - process medium		3	0.00	0.63	3.28	2.31	0.79	36.0
TOTAL: PIPELINES	89	12	0.00	3.74	20.53	9.82	4.55	27.4
Critical		2	0.00	0.79	3.54	1.40	0.70	10.0
Plugged/choked		1	0.00	0.39	2.09	1.35	0.38	8.0
Other failure mode(s)		1	0.00	0.39	2.09	1.35	0.38	12.0
Degraded		3	0.00	1.03	4.57	1.80	1.14	18.0
External leakage - process medium		2	0.00	0.64	2.53	0.85	0.76	24.0
No immediate effect		1	0.00	0.84	4.37	3.22	0.38	12.0
Incipient		7	0.00	1.99	10.63	6.90	2.65	45.3
External leakage - process medium		3	0.00	1.15	4.90	1.89	1.14	36.0
No immediate effect		3	0.01	0.90	3.00	1.11	1.14	72.0
Plugged/choked		1	0.00	0.39	2.09	1.35	0.38	28.0
Comments								

For components with no failures, α is set to 0.5 corresponding to a non-informative prior.



Probabilities of explosion or fire with and without an improved PLDC system

leak control	process leak detection	explosion or fire	P[explosion or fire] (prior)	P[explosion or fire] (post)
leak control	detected	fire	0.0075	0.002
"	"	explosion	0.0075	0.002
no leak control	"	fire	0.208	0.182
"	"	explosion	0.207	0.181
"	not detected	fire	0.435	0.435
"	"	explosion	0.435	0.435

Table 8 Probability of explosion or fire with and without an improved PLDC system (W. Moore & R. Bea 1993)