NTNU – Trondheim
Norwegian University of
Science and Technology

Reliability Qualification of Safety Systems in the Offshore Petroleum Industry

Ole Jacob Seime

Subsea Technology	
Submission date:	June 2013
Supervisor:	Marvin Rausand, IPK
Co-supervisor:	Asbjørn Andersen, ExproSoft

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

NTNU – Trondheim
Norwegian University of
Science and Technology

Reliability Qualification of Safety Systems in the Offshore Petroleum Industry

Ole Jacob Seime

June 2013

MASTER THESIS

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Master Programme in Subsea Technology

Supervisor: Asbjørn Andersen

Responsible Supervisor: Marvin Rausand

NTNU

Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

Date	Our reference
2013.01.14	MR/KEDA

MASTER THESIS
2013
for
stud. techn. Ole Jacob Seime

RELIABILITY QUALIFICATION OF SUBSEA SAFETY SYSTEMS

(Pålitelighetskvalifisering av undervanns sikkerhetssystemer)

The offshore industry is pushing technology to become more cost-effective and safe. In many cases, the proven technology is no longer viable and new solutions need to be developed. One of these developments is related to replacing conventional annulus safety valves (ASVs) with fail-safe check valves in the wellhead on the annulus side.

At the same time requirements are changing. In recent years, the IEC 61508-requirements have been taken into the offshore industry requirements in Norway. This has resulted in the OLF 070 guideline. Appropriate evidence shall be available to document that the components and sub-systems are suitable for use in safety-instrumented systems. The level of detail of the evidence should be in accordance with the complexity of the considered component or sub-system and with the probability of failure claimed to achieve the required safety integrity level of the safety-instrumented function(s). The evidence of suitability will be different for *proven-in-use* components compared with components not proven in use.

The overall objective of this master thesis is to describe the steps components need to go through in order to be part of a safety function. The focus will be on the systems covered by the OLF 070 requirements, but other guidelines/standards may be used to demonstrate the "evidence of suitability".

The approach will be tested through a case study of a safety function used for protection against gas release from a gas lifted well. Two alternative configurations of the safety function for annulus gas protection shall be assessed:

- Safety function with hydraulic ASV
- Safety function with use of an M-SAS (surface annular safety) valve

Both these components are "proven in use" according to OLF/IEC. Therefore also an alternative with an electrical operated ASV (non proven) is included as part of the SAR (safety analysis report) task.

As part of this master thesis, the candidate shall:

1. Describe the gas lifted systems (both ASV and M-SAS configuration). Discuss pros and cons related to each solution.
2. Provide an overview of the requirements related to the annulus safety valve system. Describe the necessary documentation for both the solutions according to IEC/OLF (proven vs. not proven technology)
3. Describe the process of fulfilling the safety analysis report (SAR) for both non-proven and proven technology. Use a hydraulically operated ASV (proven) and an electrically operated ASV (non-proven) as cases and point out challenges/propose improvements.
4. Perform PFD calculation for:
    a. The safety function with ASV
    b. The safety function with M-SAS
    and discuss the results obtained.

5. Carry out an overall assessment of the two alternative safety function configurations (reliability, repair risk, etc.)

Following agreement with the supervisors, the various points may be given different weights.

Within three weeks after the date of the task handout, a pre-study report shall be prepared. The report shall cover the following:

- An analysis of the work task's content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.

The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

The report should be edited as a research report with a summary, table of contents, conclusion, list of reference, list of literature etc. The text should be clear and concise, and include the necessary references to figures, tables, and diagrams. It is also important that exact references are given to any external source used in the text.

Equipment and software developed during the project is a part of the fulfilment of the task. Unless outside parties have exclusive property rights or the equipment is physically non-moveable, it should be handed in along with the final report. Suitable documentation for the correct use of such material is also required as part of the final report.

The student must cover travel expenses, telecommunication, and copying unless otherwise agreed.

If the candidate encounters unforeseen difficulties in the work, and if these difficulties warrant a reformation of the task, these problems should immediately be addressed to the Department.

The assignment text shall be enclosed and be placed immediately after the title page.

Deadline: June 10th 2013.

Two bound copies of the final report and one electronic (pdf-format) version are required.

Supervisor at NTNU:	Marvin Rausand Phone: 73 59 25 42 E-mail: marvin.rausand@ntnu.no
Supervisor at ExproSoft:	Asbjørn Andersen E-mail: Asbjorn.Andersen@exprosoft.com

DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING

Per Schjølberg
Associate Professor/Head of Department

Marvin Rausand
Responsible Supervisor

Preface

This is a master thesis in the course TPK 4900 Production and Quality Engineering, Master Thesis. The thesis is a part of the Underwater Technology study program at the Norwegian University of Science and Technology (NTNU) and was carried out during the spring of 2013. The task was made by Asbjørn Andersen at ExproSoft AS who also provided most of the information needed to conduct this thesis. The topic was initially "Reliability Qualification of Subsea Safety Systems" but was later changed to become more suitable.

This thesis is written for readers with knowledge regarding annular reliability and safety in offshore gas lift applications. However, basic knowledge about these kinds of wells and equipment are provided and it is thus assumed that anyone with basic knowledge in reliability theory will understand this thesis.

Trondheim, 2013-06-10

Ole Jacob Seime

Ole Jacob Seime

Acknowledgements

This master thesis could not have been carried out without the help and support form ExproSoft AS. I would thus like to thank my supervisor Asbjørn Andersen at ExproSoft AS for great help and guidance during this master thesis. He provided me access to Exprobase and much of the information need to conduct this thesis. I will also like to thank Per Holand at ExproSoft AS for help and tips when performing fault tree analyses. Finally, I will like to thank Professor Marvin Rausand for help and guidance. He was the responsible supervisor during the thesis.

O.J.S.

Summary and Conclusions

This master thesis starts off by providing basic knowledge about relevant well type, well equipment, gas lift and well barriers. This is basic knowledge which is needed to understand the systems investigated throughout the rest of the thesis. Four annulus barrier configurations are found for gas lift systems. Their maintenance strategies are briefly described and general advantages and disadvantages are listed. Well barrier diagrams and well barrier schematics are also provided for each configuration.

The terms safety instrumented system and safety instrumented function are briefly explained. Governing regulations regarding barriers are provided both for Norway and for the United States of America. Requirements regarding safety instrumented system and annulus well barriers in Norway follow. These include requirements for documentation.

The safety analysis report (SAR) process is described both for non-proven and proven technology. This process and the included documentation vary for whether the components are certified as proven in use or prior use. The required documentation is also dependent on the system complexity. Relevant terms are discussed. Flowcharts for the various SAR processes are made for both non-proven and proven technology based on the OLF 070 guideline. Two case studies are used to describe the SAR process and to compare the process for non-proven versus proven technology. Some challenges when performing SAR are found and discussed. Potential improvements to the OLF 070 guideline and to IEC standards are also proposed.

Probability of unavailability (PFD) calculations are provided for each of the gas lift configuration options based on the well barrier schematics and the well barrier diagrams. The results are discussed and an overall assessment of these configurations is made. The result shows that three of the options can be recommended. The option with three barrier elements has slightly better reliability than the most used gas lift configuration which only includes two barriers. A system weakness is reviled and an improvement proposed. The suggested improvement proves increased system reliability which resulted in recommendation of all four configurations options. A specified configuration is recommended not to be used. However, the suggested improvement may not be used in practise due to blocking of monitoring. Another improvement is suggested and analysed, but showed minor changes.

Contents

Chapter 1

Introduction

This chapter presents the master thesis with its background, objectives, limitations, approach and structure of the report.

1.1 Background

The offshore industry is pushing technology to become more cost-effective and safe. In many cases, the proven technology is no longer viable and new solutions need to be developed. One of these developments is related to replacing conventional annulus safety valves (ASVs) with fail-safe check valves in the wellhead on the annulus side.

At the same time requirements are changing. In recent years, the IEC 61508- requirements have been taken into the offshore industry requirements in Norway. This has resulted in the OLF 070 guideline. Appropriate evidence shall be available to document that the components and sub-systems are suitable for use in safety-instrumented systems. The level of detail of the evidence should be in accordance with the complexity of the considered component or sub-system and with the probability of failure claimed to achieve the required safety integrity level of the safety-instrumented function(s). The evidence of suitability will be different for proven-in-use components compared with components not proven in use.

Problem Formulation

Annulus safety valves are risky, expensive and time-consuming to maintain. New technology has therefore been developed to reduce problems related to maintenance of these annulus barriers. IEC, OLF and other requirements must be followed in order to qualify the new technology as annulus barriers. The required qualification is dependent on whether the technology is proven suitable for its use or not. A structured way of performing these steps is of importance to the oil and gas industry and others.

Literature Survey

This thesis is based on books, web pages, articles and theses. The second chapter utilizes information found in http://www.ExproBase.com/ (ExproSoft (2013)) and standards such as NORSOK and OLF 070 when presenting basic information about the relevant type of well, well equipment, gas lift and barriers.

Chapter three presents the different annulus barrier configurations which are based on information found in http://www.ExproBase.com/ and technical reports provided by ExproSoft AS.

Chapter four presents terms in reliability theory which is found in Rausand and Høyland (2004) and is of importance in chapter five, six and seven.

Chapter five presents requirements regarding annulus safety. Governing regulations in the United States of America are published at http://www.ecfr.gov/ while governing regulations in Norway are published at http://www.ptil.no. Specific requirements regarding annulus barriers are fund in NORSOK standards (see NORSOK (2012), NORSOK (2004) and NORSOK (2002)) and in the OLF 070 guideline (see OLF (2004)). IEC 61508 and IEC 61511 have also been used in this chapter.

Chapter six describes the safety analysis report (SAR) process for both non-proven and proven technology based on OLF 070 and technical reports (see ConocoPhillips (2013b) and ConocoPhillips (2013a)) provided by ExproSoft AS.

Chapter seven utilizes theory found in Rausand and Høyland (2004) and technical reports provided by ExproSoft AS to perform probability of failure on demand (PFD) calculations. Offshore reliability data (OREDA), WellMaster, PTS and OLF 070 has been used as sources to reliability data in this chapter.

Remaining Work

The PFD calculation (objective 4) needs more work. This is mainly because the result was unexpected and the suggested improvements did not solve the problem. It is suggested to obtain newer reliability data from different databases and to construct new fault trees to enhance the result.

The task can also be extended to include blowout from reservoir. More components must then be included and the analysis will be more extensive. This is a large objective which can be included in another master thesis.

More work can be done to improve the system.

There is also remaining work regarding challenges and potential improvements to the IEC standards and the OLF guideline. Only a few challenges related to OLF 070 and the safety analysis report (SAR) process were pointed out due to limited time and lack of experience. More challenges can effectively be obtained if one or several more experienced person(s) are available.

There is also remaining work regarding follow-up of the proposed improvements. E.g. alternative methods of obtaining reliability data for new technology should be investigated further.

It is also suggested to investigate the likelihood of having a mandatory retrieval of the ASV if it is stuck in closed position. If this happens often, the M-SAS configurations may not be recommended.

1.2 Objectives

The overall objective of this master thesis is to describe the steps components need to go through in order to be a part of a safety function. The focus will be on the systems covered by the OLF 070 requirements, but other guidelines/standards may be used to demonstrate the "evidence of suitability". The approach will be tested through a case study of a safety function used for protection against gas release from a gas lifted well. Two alternative configurations of the safety function for annulus gas protection shall be assessed:

- (Safety function with hydraulic ASV)
- (Safety function with use of an M-SAS (surface annular safety) valve)

Both these components are “proven in use” according to OLF or IEC. Therefore also an alternative with an electrically operated ASV (non proven) is included as part of the SAR (safety analysis report) task. To meet the overall objective the following objectives are treated:

1. Describe the gas lifted systems (both ASV and M-SAS configuration). Discuss pros and cons related to each solution.

2. Provide an overview of the requirements related to the annulus safety valve system. Describe the necessary documentation for both the solutions according to IEC or OLF (proven vs. not proven technology)

3. Describe the process of fulfilling the safety analysis report (SAR) for both non-proven and proven technology. Use a hydraulically operated ASV (proven) and an electrically operated ASV (non-proven) as cases and point out challenges/propose improvements.

4. Perform PFD calculation for:

    - The safety function with ASV
    - The safety function with M-SAS

    and discuss the results obtained.

5. Carry out an overall assessment of the two alternative safety function configurations (reliability, repair risk, etc.)

1.3 Limitations

This task is limited to offshore topside oil production wells that use gas lift through A-annulus. This is because M-SAS valves are only relevant in these applications. The focus regarding leakage will be limited to lift gas release from annulus reservoir (A-annulus). Blowout from the reservoir through A-annulus is not taken into account. Neither is blowout through the completion string.

The focus regarding requirements will be limited to Norway. However, governing regulations regarding barriers will be provided both for the United States of America and for Norway.

Note that the reliability data used in this thesis are selected using specific filters for specific applications in the databases. The reliability data can thus not be used as general data for other applications.

Limitations included in the PFD calculations are listed in section 7.2.

1.4 Approach

Objective one will be based on reliability reports and technical reports provided by Exprosoft AS. Some information will be found in ExproBase and on vendor's web pages. Well barrier schematics and well barrier diagrams will be made for each configuration option. Based on these, advantages and disadvantages can be listed.

Objective two will be approached by the governing organisations web pages. Specific requirements regarding barriers can be found in standards such as NORSOK, OLF and IEC.

Objective three will be based on the OLF 070 guideline. Some companies have made technical reports that provide detailed and structured information of how the safety analysis report (SAR) can be made. These reports can make it easier to reach this objective.

Objective four and five can be based on reliability reports provided by ExproSoft AS. Information on how to perform such calculations can also be found in reliability theory books such as Rausand and Høyland (2004).

1.5 Structure of the Report

In agreement with supervisor, a summary in Norwegian is not included in this thesis.

Chapter two provides basic information about relevant well type, well equipment, gas lift and well barriers. This is information which is relevant for the rest of the thesis and should be used as a reference work when reading this report.

Chapter three describes the various annular barrier configurations in gas lift applications in Norway. These include a brief description of the maintenance strategy, advantages and disadvantages, well barrier schematics and well barrier diagrams. The well barrier diagrams are later used to create fault trees when performing PFD calculations.

Chapter four defines important terms regarding annular safety. These terms are safety instrumented system (SIS) and safety instrumented function (SIF) which are fundamental terms used in later chapters. The relationship between these terms and the configurations presented in chapter 3 is presented through an example.

Chapter five provides information regarding requirements for annulus barriers. Governing regulations in both the United States of America and Norway are first presented. A short interpretation of these governing regulations follows. The following requirements are then limited to Norway. The main NORSOK requirements are provided and presented through a table. OLF / IEC requirements are then provided.

Chapter six provides descriptions of the safety analysis report (SAR) both for non-proven and proven technology. This is illustrated in flowcharts and through an example which can be found in appendix. The required documentation for non-proven and proven technology is compared and differences are pointed out. Challenges when performing SAR are pointed out and potential improvements to the OLF 070 guideline and IEC are proposed.

Chapter seven provides PFD calculations for all four configurations presented in chapter 3. Reliability data are collected through various sources and used in the CARA Fault Tree software. An overall assessment of the result are provided.

Chapter 2

Well Configuration, Well Equipment and Barriers

The focus in this thesis is on annular barrier elements in offshore topside oil production wells, which uses gas lift. This chapter provides information about how these wells are configured, associated well equipment, gas lift systems and well barriers. This is basic information which is needed to fully understand the rest of the report. Note that specific requirements are provided for some components in this chapter.

2.1 Well Configuration

Oil production wells consist of the following main modules:

- **The x-mas tree (XMT**) which is a valve arrangement and an important part of the well barrier system. It is placed on top of the wellhead and can be located either subsea or topside.
- **The wellhead (WH)** which is a thick walled metal pipe attached to the surface casing. It acts as a landing arrangement for the casings, and the XMT is connected at the top.
- **The casing strings** which consists of large diameter metal pipes which are cemented in place during the drilling process.

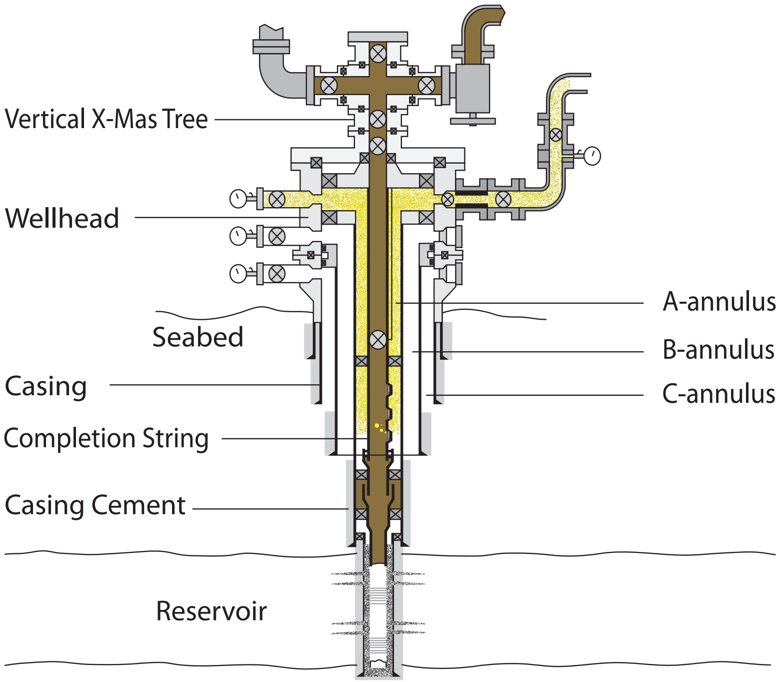


Figure 2.1: Main modules and cavities in a topside oil production well (ExproSoft, 2013)

- **The casing cement** which is used to seal between the formation and casing, and to support the casing.
- **The completion string** which consists of tubing and necessary equipment to achieve optimal flow performance and safety during production or injection.

The cavities in the well have different names:

- **The A-annulus** which is the annulus between the completion string and the production casing.
- **The B-annulus** which is the annulus between the production casing and the intermediate casing.
- **The C-annulus** which is the annulus between the intermediate casing and the surface casing.

Gas production wells, water injection wells and gas injection wells have the same configuration as oil production wells, but these are not in focus in this thesis. The main modules and cavities is illustrated in figure 2.1 (ExproSoft, 2013).

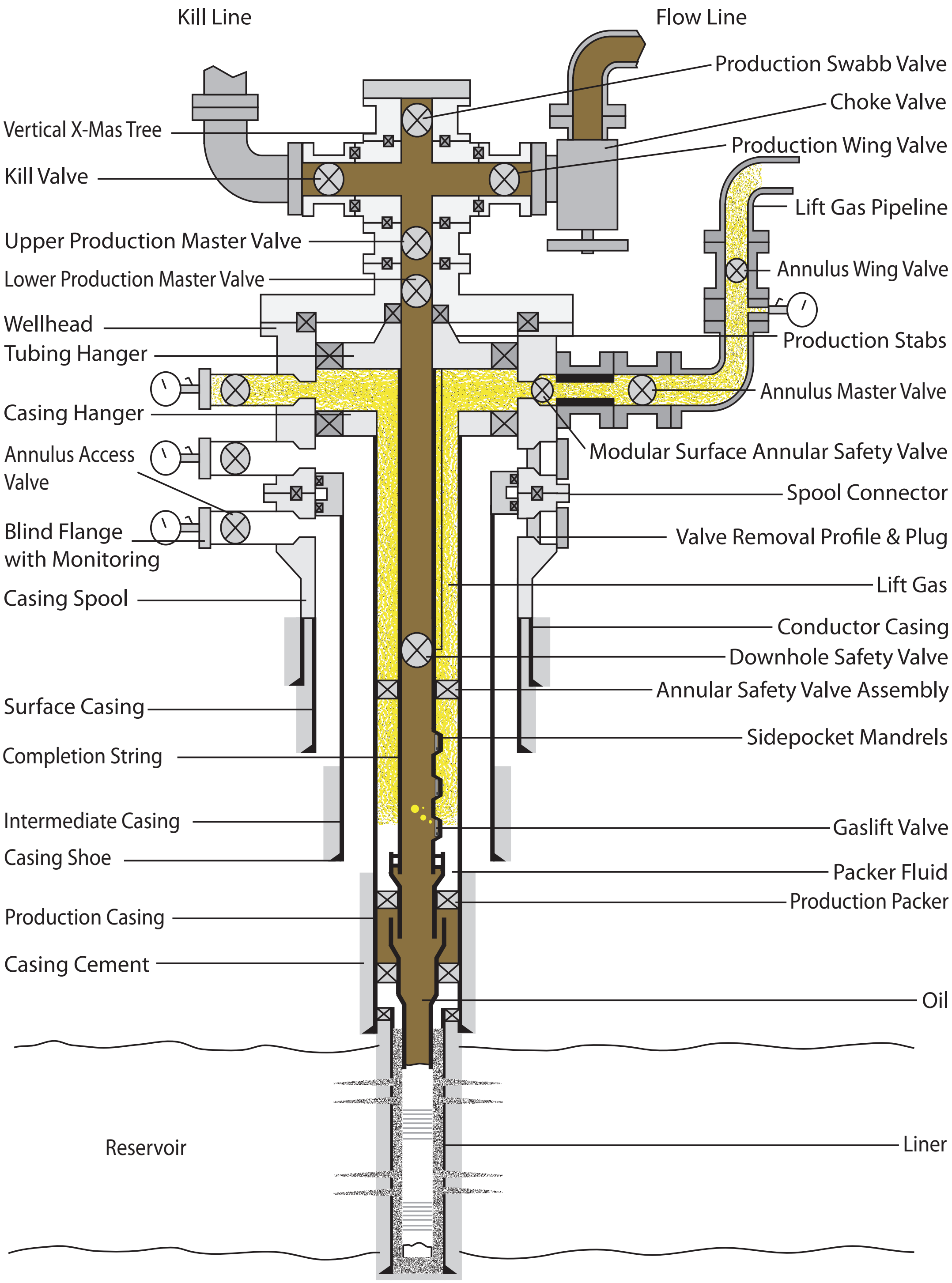


Figure 2.2: The main equipment in topside oil production wells based on (ExproSoft, 2013)

2.2 Well Equipment

The main functionality of the well equipment is:

- Supporting the wellbore
- Well barrier elements
- Enhanced well flow performance

Typical well equipment for oil production wells is listed below and illustrated in figure 2.2.

2.2.1 X-Mas Tree (XMT)

The x-mas tree (XMT), also called production tree, is a valve arrangement and an important part of the well barrier system. It is connected to the top of the WH and provides an interface from the completion string to the piping towards the process system. There are three main types of XMTs:

- Vertical topside XMT
- Vertical subsea XMT
- Horizontal subsea XMT (which contains the tubing hanger in addition to the valves)

Only vertical topside XMT is relevant in this case since this thesis focuses on gas lifted wells and since M-SAS valves (see section 2.6.3) are only applicable in topside wells. The vertical topside XMT valve arrangement consists of:

- **Production master valve (PMV)** which is an important well barrier element
- **Production wing valve (PWV)** which is located at the tree branch connected to the pipes towards the process system
- **Production swab valve (PSV)** which is located at the top of the XMT and provides access to the production bore when equipment is connected
- **Kill valve (KV)** which provides a secondary access point to the production bore

- **Production stabs** which are short tubular making a production flow path between the tubing hanger and the vertical Xmas tree. Seals on the stabs establish a cavity for testing the connection seal between the WH and the Xmas tree.

(ExproSoft, 2013)

2.2.2 Wellhead (WH)

The WH is a thick walled metal pipe attached to the surface casing. The casings are landed inside WH. Subsea and topside WH has different design. Only WHs for topside vertical XMTs are relevant for this thesis and consist of:

- **Annulus access valve (AAV)** which is an inlet/outlet valve to the various annuli used for isolation of pressure gauges or to adjusting annulus pressure
- **Annulus master valve (AMV**) which is a part of the well barrier system
- **Annulus wing valve (AWV)** which is a backup valve for the AMV and the primary valve used for gas injection shut-in
- **WH connector** which is either a API flange or a quick connector

Note that WHs for vertical XMTs accommodate the tubing hanger for the completion string, whereas for horizontal XMT the tubing hanger is located inside the XMT (ExproSoft, 2013).

Valve Removal (VR) Profile

A VR-profile is a hole in the WH wall which can be used to connect equipment such as an M-SAS valve (see section 2.6.3) to the annulus. (ExproSoft, 2013).

2.2.3 Casing String

The casing string consists of large diameter metal pipes which are cemented in place during the drilling process. The main purposes of the casing string are to:

- Prevent caving of formation wall into the wellbore

- Maintain control of drilling fluids and pressure during drilling
- Keep formation and injection fluids inside the well during operation
- Be a structural foundation to support the WH, Blowout preventer (BOP), production packer, etc.

The casing string typical consists of four types of casings:

- Conductor casing
- Surface casing
- Intermediate casing
- Production casing

Casings are sometimes extended using a liner. A liner is a casing clamped to the bottom part of the previous casing and does not extend to the surface as casings do (ExproSoft, 2013).

2.2.4 Casing Cement

The casing cement is used to seal between the formation and the casing and to structurally support the casing (ExproSoft, 2013).

2.2.5 Completion String

The completion string consists of tubing and necessary equipment to achieve optimal flow performance and safety during production or injection. (See ExproSoft (2013)).

Tubing Hanger

The tubing hanger is located at the top of the completion string. Its purposes are to enable run, hang-off, orient and lock, and seal the completion string on either inside the WH or inside a horizontal XMT (ExproSoft, 2013).

Downhole Safety Valve (DHSV)

The DHSV is a primary well barrier element located in the upper completion string. It consists of a valve unit and an actuator. The purpose of the DHSV is to prevent uncontrolled flow of well fluids from escaping though the tubing during an emergency. This is done by closing the valve and thereby seal off the well (ExproSoft, 2013).

Side Pocket Mandrel (SPM)

The SPM is a tubular conduit in the completion string with a machined or welded side pocket. The side pocket is used for housing inserted devices that require communication with the annulus. The SPM is designed to avoid the inserted device obstructing the main completion string conduit. Components are normally inserted or retrieved from the SPM by wireline using a kick-over type running tool (ExproSoft, 2013).

Gas Lift Valve (GLV)

The GLV is located in a SPM some distance below the DHSV. It enables injection of gas from the A-annulus to the completion string. Some GLVs are qualified as well barrier elements (WBE) (ExproSoft, 2013).

Annular Safety Valve Assembly

The annular safety valve assembly is a WBE in injection and gas lift applications and consists of:

- **A packer element** to seal off the annulus of the well
- **A slips element (hanger)** to lock the annular safety valve assembly to the production casing
- **An annulus safety valve (ASV)** which consist of a body, an annulus sealing element which can be activated, and control lines. Its purpose is to prevent flow of hydrocarbons or fluid up the annulus and to provide a pressure seal between the bore and the A-annulus. (See NORSOK, 2012, chapter 15.8 table 8).

2.3 Artificial Lift

Oil and gas wells are either free flowing or lifted. Artificial lift methods are used to:

- Produce wells with insufficient reservoir pressure
- Produce wells with heavy oil
- Delay water production
- Increase the production rate
- Start wells after shut-in

The two most common methods of artificial lift are:

- **Pump system** where electronic submersible pumps (ESP) are the most common type
- **Gas lift system** in form of lift gas through annulus

These two systems are illustrated in figure 2.3.

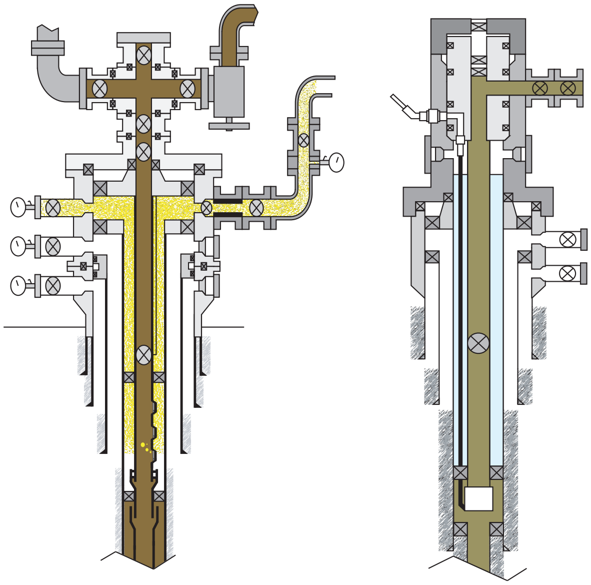


Figure 2.3: To the left: a gas lift well. To the right: a well using ESP (ExproSoft, 2013)

2.3.1 Pump System

Pumps can either be submerged into the wellbore or positioned at the top of the well. There are several categories of pumps but ESP is the most common type. Pumps create low pressure at the inlet, and high pressure at the outlet, forcing the fluid up the completion string (Rigzone, 2013).

2.3.2 Lift Gas Systems

In gas lift systems, gas is pumped into the wellbore through the A-annulus and into the well through the GLVs. The gas mixes with the fluids inside the completion string, reduces the fluid viscosity and thereby increases the flow capability. The gas also reduces the hydrostatic pressure inside the completion string and thus increases the differential pressure between the reservoir and the bottom of the well (increased drawdown). This increases the production rate and is sometimes a condition for starting the production. The mixture of oil and gas is produced to the surface where the gas is separated from the oil and re-injected though the annulus (Rigzone (2013) and ExproSoft (2013)).

2.4 Well Barrier

A well barrier is defined as an envelope of one or several WBE(s) preventing unintentional flow of fluids from the formation into the wellbore, into another formation or the external environment (NORSOK, 2012). There are at least two independent barrier envelopes forming two separate layers of protection in hydrocarbon production wells in Norway. The first layer is called the primary barrier layer (blue lines in figure 2.4). If this layer fails to control the hazard, the secondary layer (red lines in figure 2.4) takes over. This is illustrated in figure 2.4. Note that the formation is a part of both the primary and secondary well barrier envelope in addition to the well equipment.

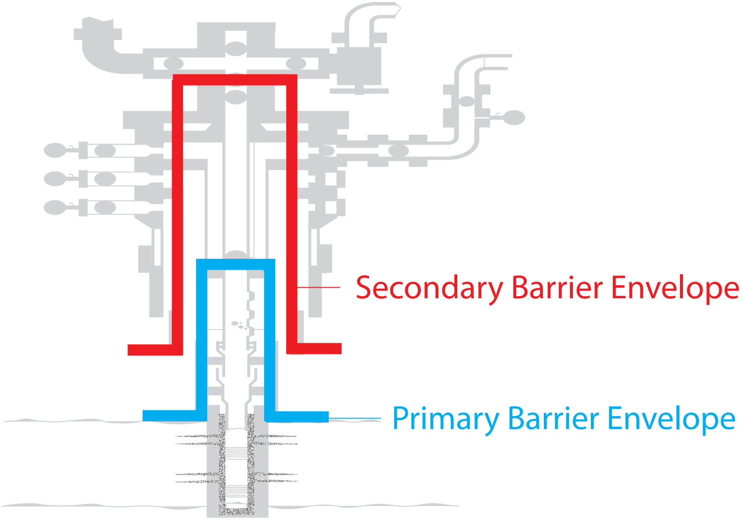


Figure 2.4: The primary (blue lines) and the secondary (red lines) well barrier envelopes

2.5 Gas Lift Barrier

A gas lift barrier is a barrier envelope that prevents flow to the environment from an artificial/injected gas lift source. Note that this is not the same as a well barrier which prevent flow to the environment from the reservoir (NORSOK, 2012). However, some WBE may be common for both well barrier and gas lift barrier. Figure 2.5 illustrate gas lift barrier envelopes.

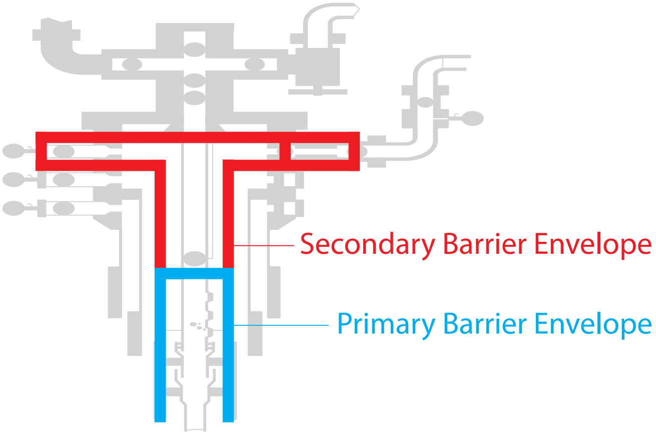


Figure 2.5: The primary (blue lines) and the secondary (red lines) gas lift barrier envelopes

2.6 Well Barrier Element (WBE)

A well barrier element (WBE) is defined as a physical element which in itself does not prevent flow but in combination with other WBEs forms a well barrier (See NORSOK, 2012, page 15). Some of the WBEs are actuating items which are controlled by a safety instrumented system (SIS) to close the barrier envelope. In conventional production wells, the primary actuating item is the DHSV. The PMV in the XMT is the secondary actuating item.

In order to enable injection of gas and to complete the well barrier envelopes, the flow path through the annulus introduced by gas lift, requires well equipment in addition to the DHSV and the PMV. This is the gas lift valve (GLV), the annular safety valve assembly, and the modular surface annular safety (M-SAS) valve.

2.6.1 Gas lift Valve (GLV)

The GLV is located in a SPM (see figure 2.6) some distance below the DHSV and enables injection of gas from the A-annulus to the completion string. GLVs are used temporary for initial or late life start-up of wells, or in continuous use in late life to compensate for reservoir depletion and increased water cut.

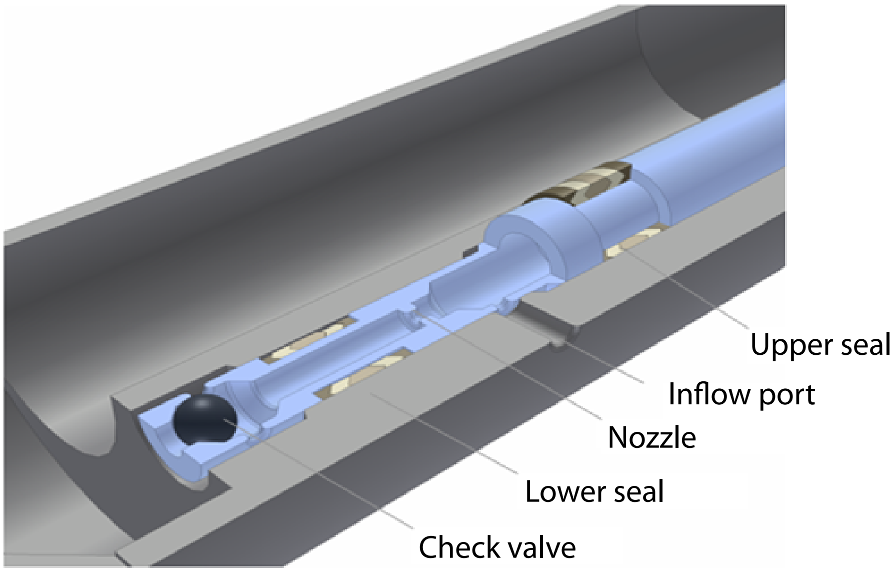


Figure 2.6: A GLV placed in a SPM (ExproSoft, 2013)

All GLVs have a check valve which prevents backflow from the completion string to the annulus when reducing the pressure in A-annulus. All GLVs also have a nozzle to regulate the maximum gas injection rate. The deepest set GLV is an operational GLV. Other GLVs above is called unloading GLVs to assist during production start-up. GLVs located between the production packer and the DHSV should be qualified as a primary well barrier. An alternative is to apply an annular safety valve. The number of GLVs installed depends on the gas injection pressure, the pressure integrity in the completion string or production casing, and the setting depth. Installation is performed by wireline intervention using a kick-over type running tool (ExproSoft, 2013). According to (NORSOK, 2012), there is no specific requirement for the GLV as it is for the ASV.

2.6.2 The Annular Safety Valve Assembly

The annular safety valve assembly is illustrated in figure 2.7 and consists of a packer element, a slips element (hanger) and an annulus safety valve (ASV). The annular safety valve assembly is integrated in the completion string and normally placed just below the DHSV to avoid the control line to the DHSV to go through the annular safety valve assembly body.

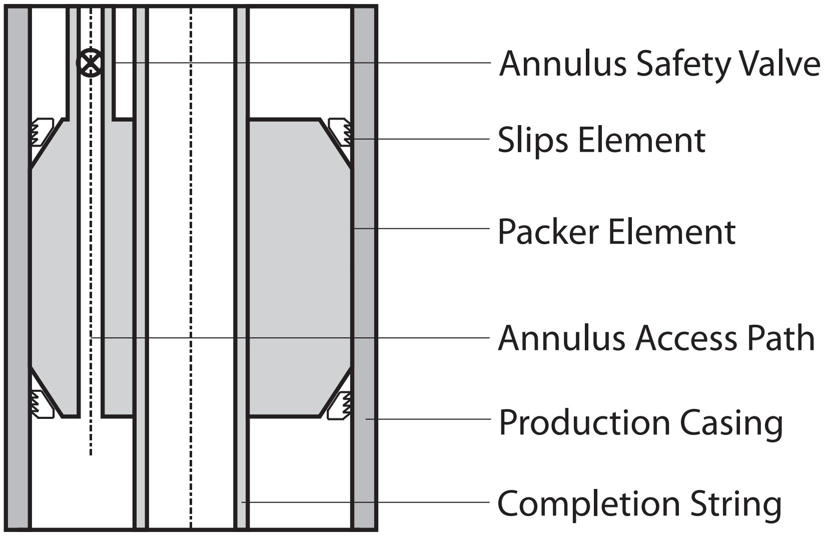


Figure 2.7: Components of the annular safety valve assembly

Packer Element

A packer element seals off the annulus of the well. It is used between the production casing and the completion string. The packer includes a flowpath for establishing fluid communication with the annulus (Schlumberger (2013) and Engineering (2013)).

Slips Element (Hanger)

The slips element is used to lock the packer element inside the production casing to prevent axial movement (Engineering, 2013). The packer and the slips elements are placed in the production casing by applying pressure trough a setting control line or by pressurizing the completion string (ExproSoft, 2013).

The Annulus Safety Valve (ASV)

The ASV is both a well barrier and a gas lift barrier that controls the flow in the flow path that bypasses the packer element. It is either located inside, below or above the packer element and can either be an integrated part of the packer and slips or a separate component. Both systems are tubing retrievable (TR). If the ASV is a separate component, a small size DHSV is normally used. The various manufacturers use different designs for ASV and typical designs are illustrated in figure 2.8 and listed below:

- Puppet
- Ball
- Flapper

Function: The ASV needs hydraulic pressure to open and to keep open. It is also a fail-safe close device which is accomplished by compressing a spring when the hydraulic pressure is applied. When the hydraulic pressure is cut or bleeds off, the spring returns to its original position and thereby closes the valve. The annulus below the ASV is sealed when the ASV is closed and it is possible to flow through the annulus and the bypass path in the packer when the ASV is open (ExproSoft, 2013).

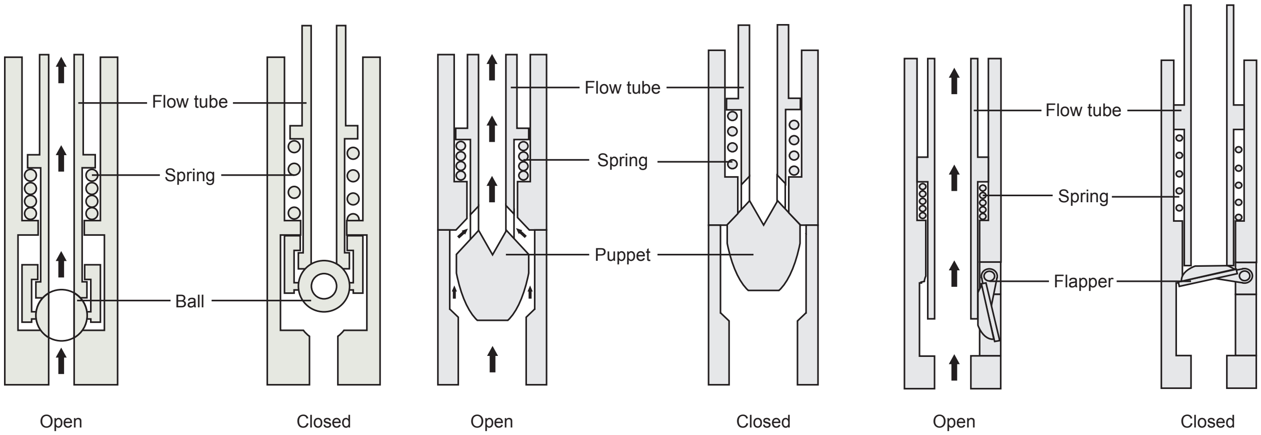


Figure 2.8: a ball valve to the left, a puppet valve in the middle and a flapper valve to the right

Installation and retrieval: The ASV is either pre-installed inside or connected to the packer element which is integrated in the tubing. This means that the whole tubing down to the packer has to be retrieved in order to retrieve the ASV. This requires costly and time-consuming workover.

Requirements: ASVs shall be designed and tested according to API RP 14B and located minimum 50m below seabed and below the well kick off point. Setting depth shall be determined by the possibility of forming hydrates and deposition of wax and scale if annulus is used for production. The maximum setting depth shall be calculated based on the highest density of fluids in the annulus.

It shall be verified for flow erosion resistance for all relevant fluids if it will be exposed to high production or injection rates. If the ASV is a part of an annulus safety system, it shall comply with ISO requirements such as for production packers.

ASVs shall have a working pressure (WP) which exceeds the maximum expected differential pressure (MEDP). It shall also be surface controlled, automatically operated, hydraulically operated, and fail safe closed.

Leak tests shall be performed in the direction of flow using low pressure (maximum 70 bar / 1000 PSI) to MEDP. Increased testing frequency shall be considered when exposed to high velocities. Leak tests shall be performed monthly until three consecutive qualified tests have been performed. Thereafter, every three months, until three consecutive qualified tests have been performed. Then every six months. Test duration shall be minimum 30 min (10 min for water). Acceptance of leak tests shall meet API RP 14B:

- 0,42 Sm3/min (25,5 Sm3/hr) (900 scf/hr) for gas
- 0,4 l/min (6,3 gal/hr) for liquid

Indirect measurement by pressure monitoring of an enclosed volume downstream of the valve shall be performed if the leak rate cannot be measured directly. The valve and the emergency shutdown function shall be periodically function tested based on reliability analysis, but as a minimum yearly. Acceptable shutdown time shall be verified as well as the valve closing on signal. The shutdown time is recorded at bleed down hydraulic system. (See NORSOK, 2012, chapter 15.8 table 8).

Innovation: All ASVs used in Norway are currently hydraulic operated but Halliburton has developed an electrical DHSV (E-DHSV) which soon will be "proven in use". When this is done, it is likely to believe that the E-DHSV will also be used as an ASV. However, much work remains in order to qualify the E-DHSV as an E-ASV ((Seime, 2012)).

2.6.3 Modular Surface Annular Safety (M-SAS) Valve

The Modular Surface Annular Safety (M-SAS) valve is a WH mounted check valve that act as a gas lift barrier. It is developed by Petroleum Technology Company (PTC) and is intended to strengthen the secondary WBE (the AMV) and thereby open up for alternative configurations to ASV. (The configurations are described in chapter 3).

Description: M-SAS comprises a valve unit and a hydraulic actuator unit. The valve unit is screwed into the VR profile inside the WH wall, and a spool flange containing the hydraulic actuator unit is bolted to the valve unit outside the WH. The Annulus Master Valve (AMV) is further bolted to the spool flange. This is illustrated in figure 2.9.

The M-SAS valve is kept in two modules to ensure that the valve closes if the hydraulic actuator unit is knocked off by an external hazard. The valve unit contains the closing mechanism which is spring loaded to ensure fail-safe closure. The hydraulic actuator unit comprises the control mechanism and consists of a hydraulic control line connection and a spring loaded

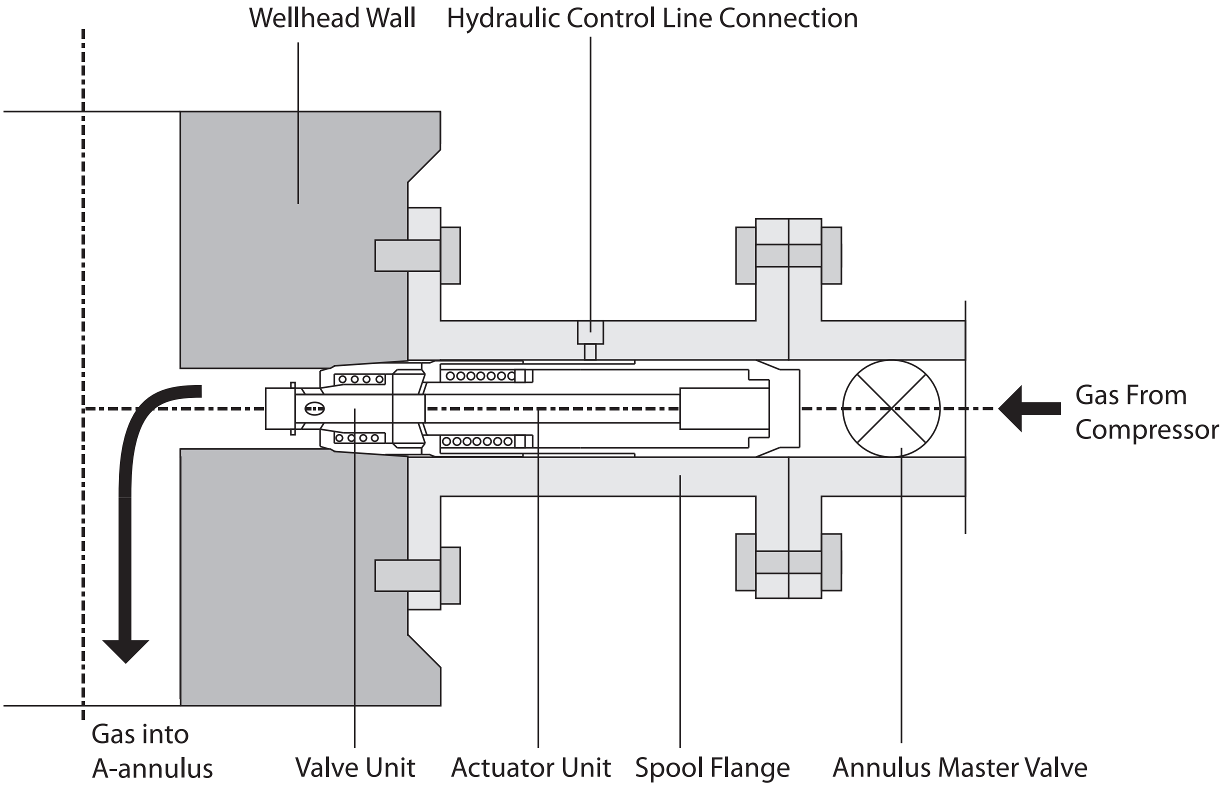


Figure 2.9: The M-SAS valve in open position mounted in a VR profile in a WH

flowtube.

Function: To open the valve, hydraulic fluid is pumped through the control line and into an opening outside the flowtube. The pressure from the fluid causes the flowtube to move towards the valve unit. This compresses the springs and the closing mechanism moves to open position. When the valve is open, gas can flow through the valve in both directions. The valve closes if the hydraulic pressure is lost or bleed off.

Installation: The M-SAS valve is installed into the VR profile using a hydraulic operated lubricator (VR-tool). The VR tool is made for pressure contained installation or retrieval of various plugs and valves through one or two gate valves. The VR tool typically replaces the AMV and acts as a barrier element during installation or retrieval of the M-SAS valve and actuator.

The installation/replacement of M-SAS valves is less risky and less complicated than retrieving the ASV, requiring only light intervention. However, M-SAS installation can be fairly complicated for existing wells where the space between the WHs or XMTs is limited (ExproSoft (2013) and Andersen (2012)).

According to (NORSOK, 2012), there are no specific requirements for M-SAS.

Chapter 3

Gas Lift Configurations

The most common annular barrier configurations in gas lift applications in Norway is described and discussed in this chapter. This includes configurations using M-SAS valve as a barrier element. General advantages and disadvantages for each option are listed. Well barrier diagram and schematics are provided for each configuration options.

3.1 Option 1: ASV + AMV

3.1.1 Strategy

An ASV and an AMV are used from day one. If the ASV fails, the AMV takes over and the ASV has to be changed in order to obtain two barriers.

3.1.2 Advantages

Table 3.1: Advantages using option 1

What	**Why**
Low installation costs	GLV (not qualified as a WBE) + ASV + AMV
Primary barrier protected against external hazards	ASV located in the well
Can be used in subsea applications	All barrier elements can be located subsea
Most used configuration	M-SAS was developed in the beginning of 21th century
Maintenance can normally take place when other well equipment is maintained	

3.1.3 Disadvantages

Table 3.2: Disadvantages using option 1

What	**Why**
Expensive, risky and time-consuming when ASV fails	ASV retrieval requires heavy workover (pulling of tubing)
Secondary barrier is not protected against external hazards	AMV is located outside WH and can be knocked off by falling objects
Large production loss when failure occurs	Because of time-consuming workover

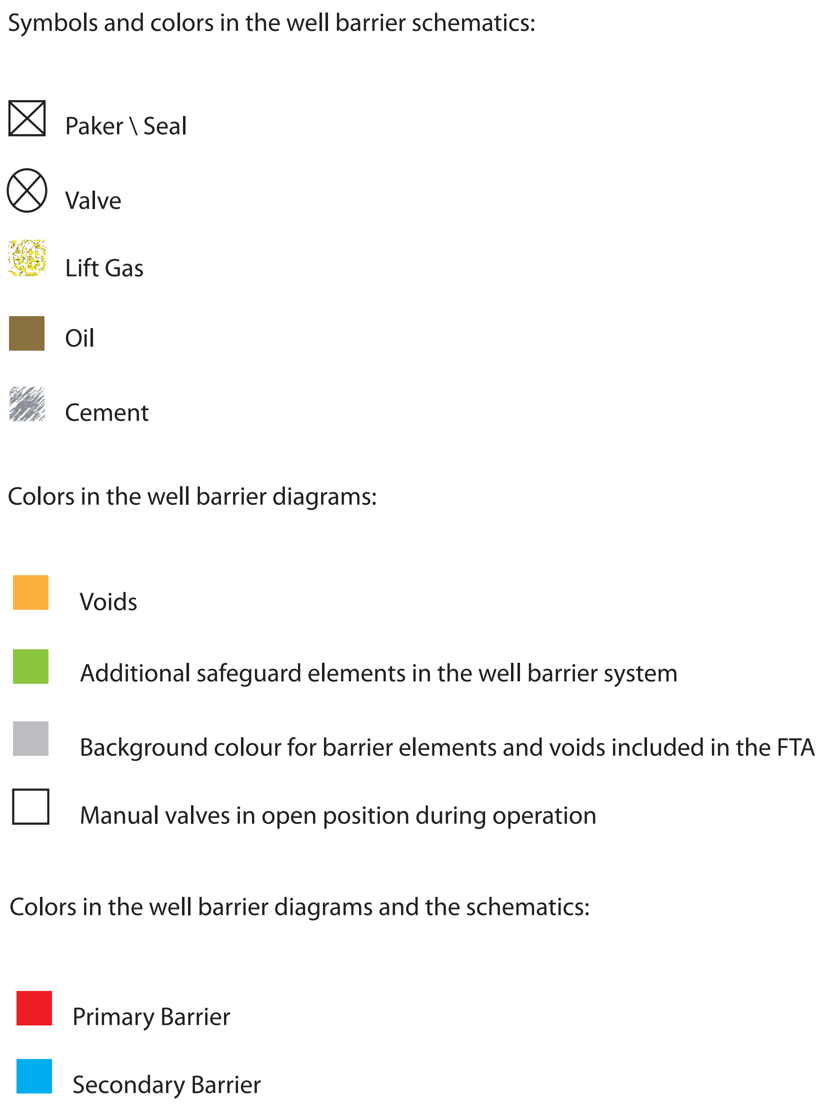

Symbols and colors in the well barrier schematics:
☒ Paker \ Seal
⊗ Valve
▨ Lift Gas
■ Oil
▨ Cement
Colors in the well barrier diagrams:
🟧 Voids
🟩 Additional safeguard elements in the well barrier system
■ Background colour for barrier elements and voids included in the FTA
□ Manual valves in open position during operation
Colors in the well barrier diagrams and the schematics:
🟥 Primary Barrier
🟦 Secondary Barrier

Figure 3.1: Symbols and color descriptions in the well barrier schematics and diagrams

Table 3.3: Barriers in option 1 (See NORSOK, 2012, page 70)

Primary Barrier Elements	Verification / Monitoring	Secondary Barrier Elements	Verification / Monitoring
ASV (Actuating item)	Periodic leak testing	AMV Wellhead annulus valve A and B (Actuating items) and control line	Periodic leak testing
Production Casing Cement	N/A after initial verification	Intermediate Casing Cement	Daily monitoring of C-Annulus
Production Casing	Continuous pressure monitoring of B-Annulus	Intermediate Casing	Daily monitoring of C-Annulus
Production Packer	N/A after initial verification	Intermediate Casing Hanger and Seal Assembly	Daily monitoring of C-Annulus / Periodic leak testing
Completion String	Periodic leak testing	Tubing Hanger	Periodic leak testing and continuous pressure monitoring of A-Annulus
DHSV (Actuating item)	Periodic leak testing	Wellhead	Periodic leak testing
In-situ Formation	N/A after initial verification	XMT	Periodic leak testing of valves
		In-situ Formation	N/A after initial verification

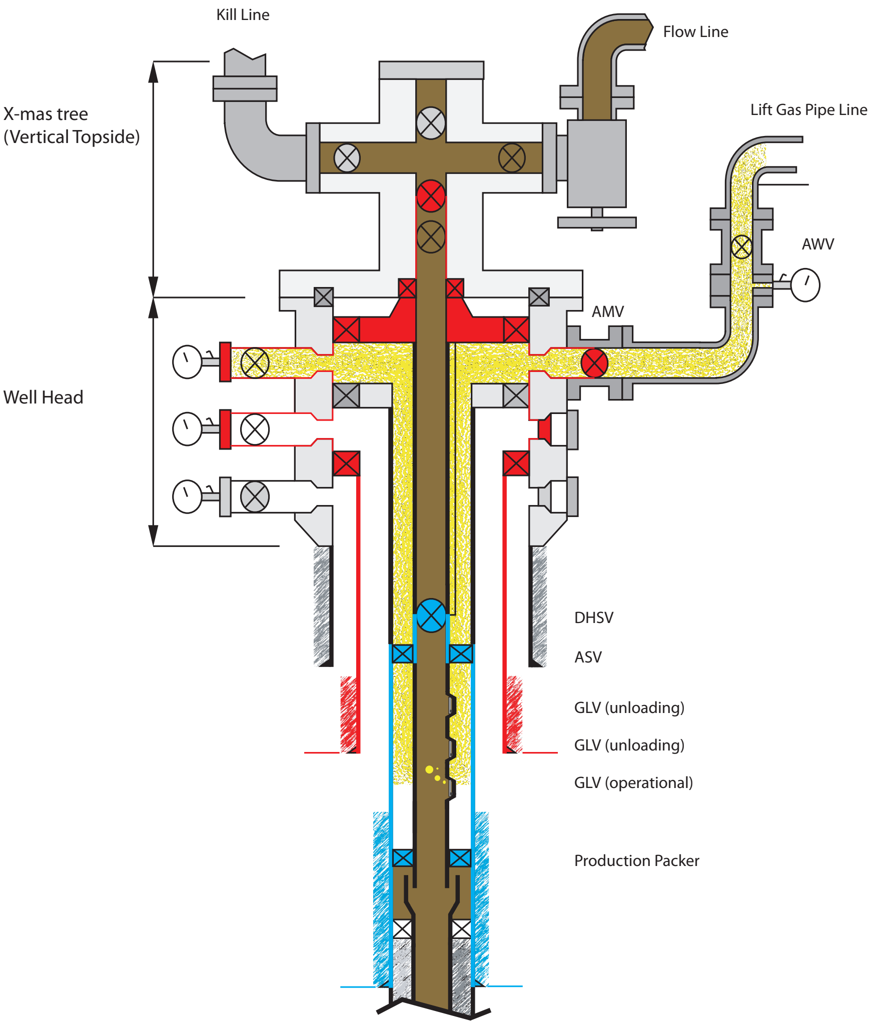


Figure 3.2: Well barrier schematics of option 1 (NORSOK (2012) and ExproSoft (2013)).

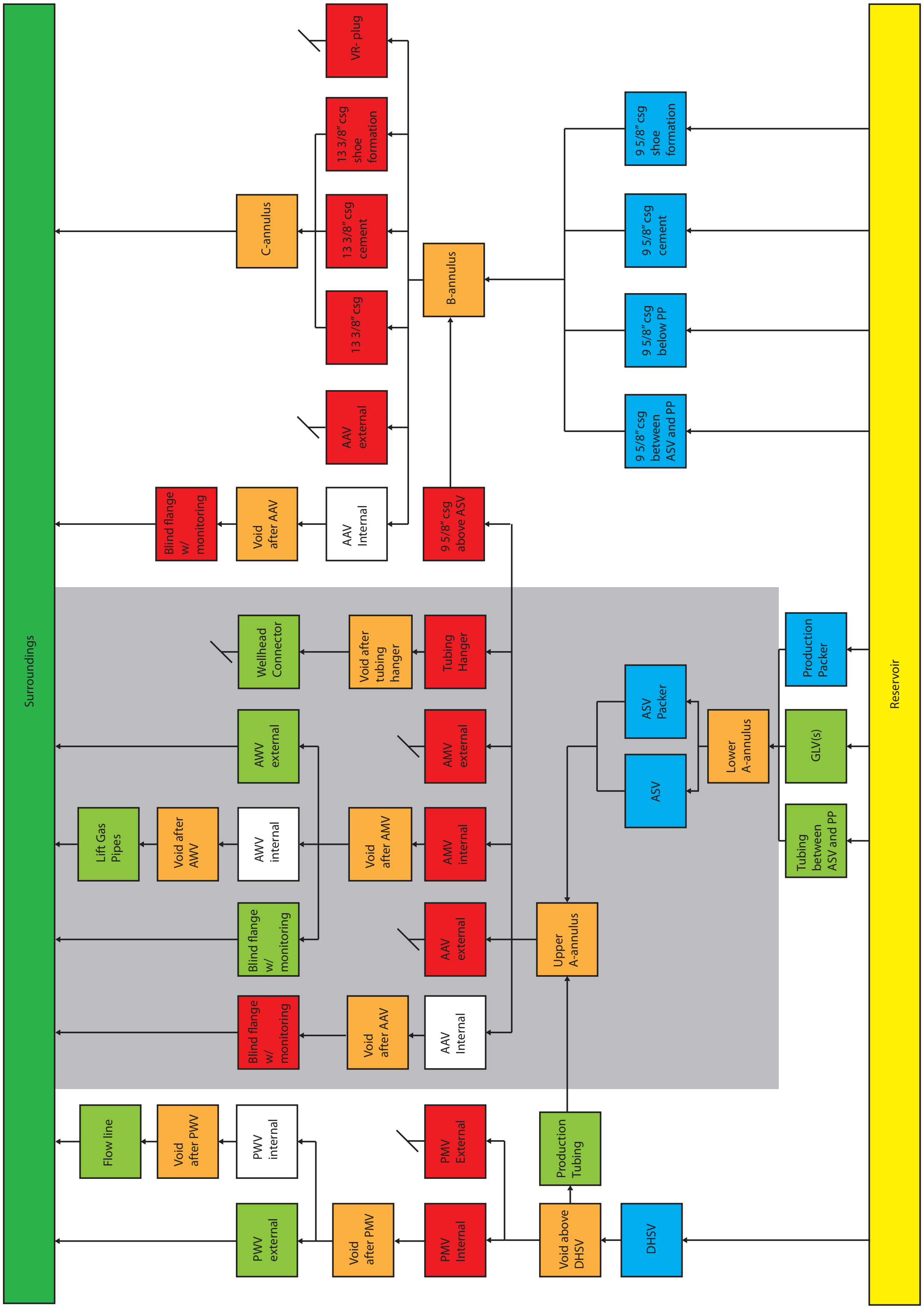


Figure 3.3: Well barrier diagram for option 1 (Will be used in chapter 7).

3.2 Option 2: AMV After ASV Failure

3.2.1 Strategy

Initially, an ASV is placed in the well and a spool flange with a protection sleeve is installed before the AMV on the WH (just like option 1 but with a spool flange for the M-SAS valve). If the ASV fails, the AMV takes over. Instead of changing ASV, the GLV(s) is qualified as primary WBE(s) and an M-SAS valve is inserted to the spool flange at the WH to strengthen the secondary barrier and to obtain two barriers.

3.2.2 Advantages

Table 3.4: Advantages using option 2

What	**Why**
Primary barrier is protected against external hazards	ASV and GLV is placed inside wellbore
Secondary barrier is protected against external hazards	M-SAS is placed inside WH wall and protected against falling objects
Low maintenance costs when ASV fails	Only light intervention is needed. M-SAS valve is inserted instead of retrieving ASV
Less risky than ASV retrieval	Pulling of tubing is not required
Small production loss when M-SAS is used compared to ASV workover	Quick maintenance compared to ASV retrieval

3.2.3 Disadvantages

Table 3.5: Disadvantages using option 2

What	**Why**
Cannot be used in subsea applications	M-SAS is only used in topside applications
Workover can be required regardless	If the ASV is stuck in closed position
Medium installation cost	GLV (qualified as WBE) + ASV + spool flange + AMV
GLV has to be qualified as WBE	In order to fulfill requirements

Table 3.6: Barriers in option 2

Primary Barrier Elements	**Verification / Monitoring**	**Secondary Barrier Elements**	**Verification / Monitoring**
ASV (Actuating item)	Periodic leak testing	AMV Wellhead annulus valve A (Actuating item) and control line	Periodic leak testing
Production Casing Cement	N/A after initial verification	M-SAS (Actuating item)	Periodic leak testing
Production Casing	Continuous pressure monitoring of B-Annulus	Production Casing Cement	Continuous monitoring of B-Annulus
Production Packer	N/A after initial verification	Production Casing (Above production packer)	Continuous monitoring of B-Annulus
Completion String	Periodic leak testing	Production Casing and Casing Hanger	Continuous monitoring of B-Annulus/ Periodic leak testing
DHSV (Actuating item)	Periodic leak testing	Tubing Hanger	Periodic leak testing and continuous pressure monitoring of A-Annulus
In-situ Formation	N/A after initial verification	Wellhead	Periodic leak testing
		XMT	Periodic leak testing of valves
		In-situ Formation	N/A after initial verification

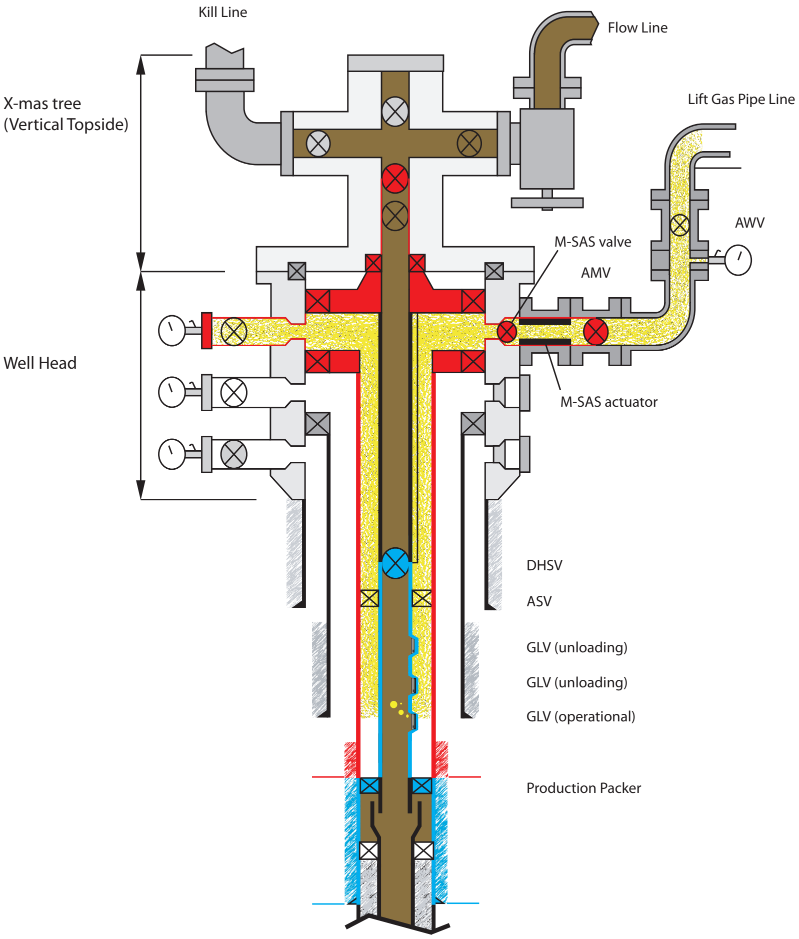


Figure 3.4: Well barrier schematics of option 2 (ExproSoft, 2013).

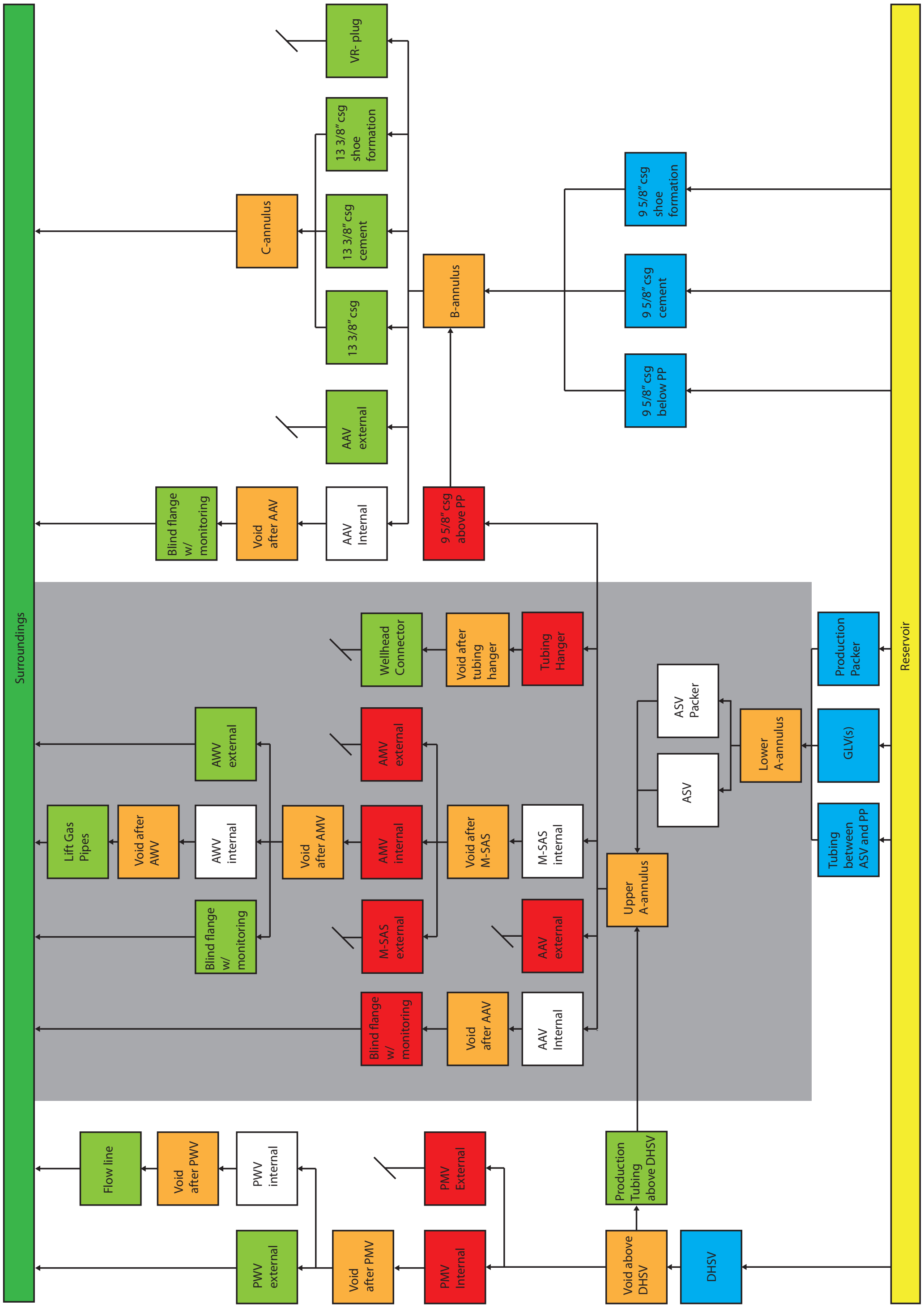


Figure 3.5: Well barrier diagram for option 2 (Will be used in chapter 7) (Based on ExproSoft (2013)).

3.3 Option 3: ASV + AMV + M-SAS

3.3.1 Strategy

An ASV, an AMV, an M-SAS valve and WBE qualified GLV(s) are installed from day one (almost the same as option 2 but an M-SAS valve is also included). If the ASV fails, the GLV(s) takes over as primary WBE(s).

3.3.2 Advantages

Table 3.7: Advantages using option 3

What	**Why**
No need for workover/ intervention when first failure occurs	M-SAS is already in place and GLV(s) is already qualified as WBE
Primary barrier is protected against external hazards	ASV and GLV is located inside wellbore
Secondary barrier is protected against external hazards	M-SAS is located inside WH wall
No production loss when initial failure occurs	No workover / intervention is needed

3.3.3 Disadvantages

Table 3.8: Disadvantages using option 3

What	**Why**
Has the highest installation cost	GLV (qualified as WBE) + ASV + M-SAS + AMV
Cannot be used in subsea applications	M-SAS is only used in topside applications
Workover can be required regardless	If ASV stuck in closed position
GLV has to be qualified as WBE	In order to fulfill requirements

Table 3.9: Barriers in option 3

Primary Barrier Elements	Verification / Monitoring	Secondary Barrier Elements	Verification / Monitoring
ASV (Actuating item)	Periodic leak testing	AMV Wellhead annulus valve A and B (Actuating items) and control line	Periodic leak testing
Production Casing Cement	N/A after initial verification	M-SAS (Actuating item)	Periodic leak testing
Production Casing	Continuous pressure monitoring of B-Annulus	Intermediate Casing	Daily monitoring of C-Annulus
Production Packer	N/A after initial verification	Intermediate Casing Cement	Daily monitoring of C-Annulus
Completion String	Periodic leak testing	Intermediate Casing Hanger and Seal Assembly	Daily monitoring of C-Annulus / Periodic leak testing
DHSV (Actuating item)	Periodic leak testing	Tubing Hanger	Periodic leak testing and continuous pressure monitoring of A-Annulus
In-situ Formation	N/A after initial verification	Wellhead	Periodic leak testing
		XMT	Periodic leak testing of valves
		In-situ Formation	N/A after initial verification

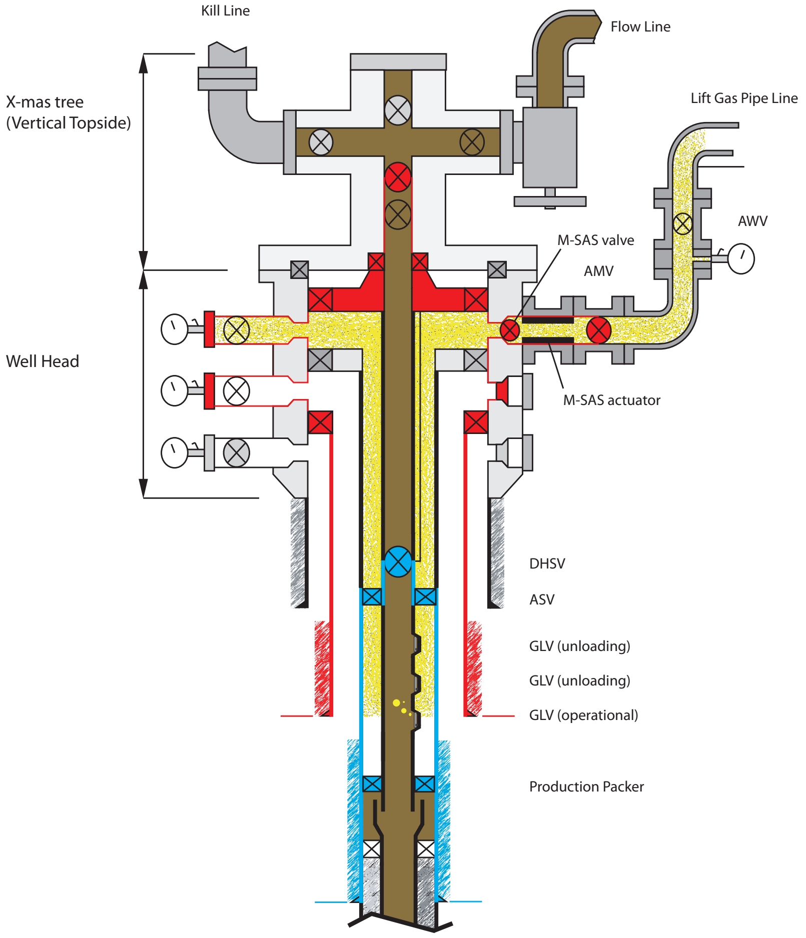


Figure 3.6: Well barrier schematics of option 3 (ExproSoft, 2013).

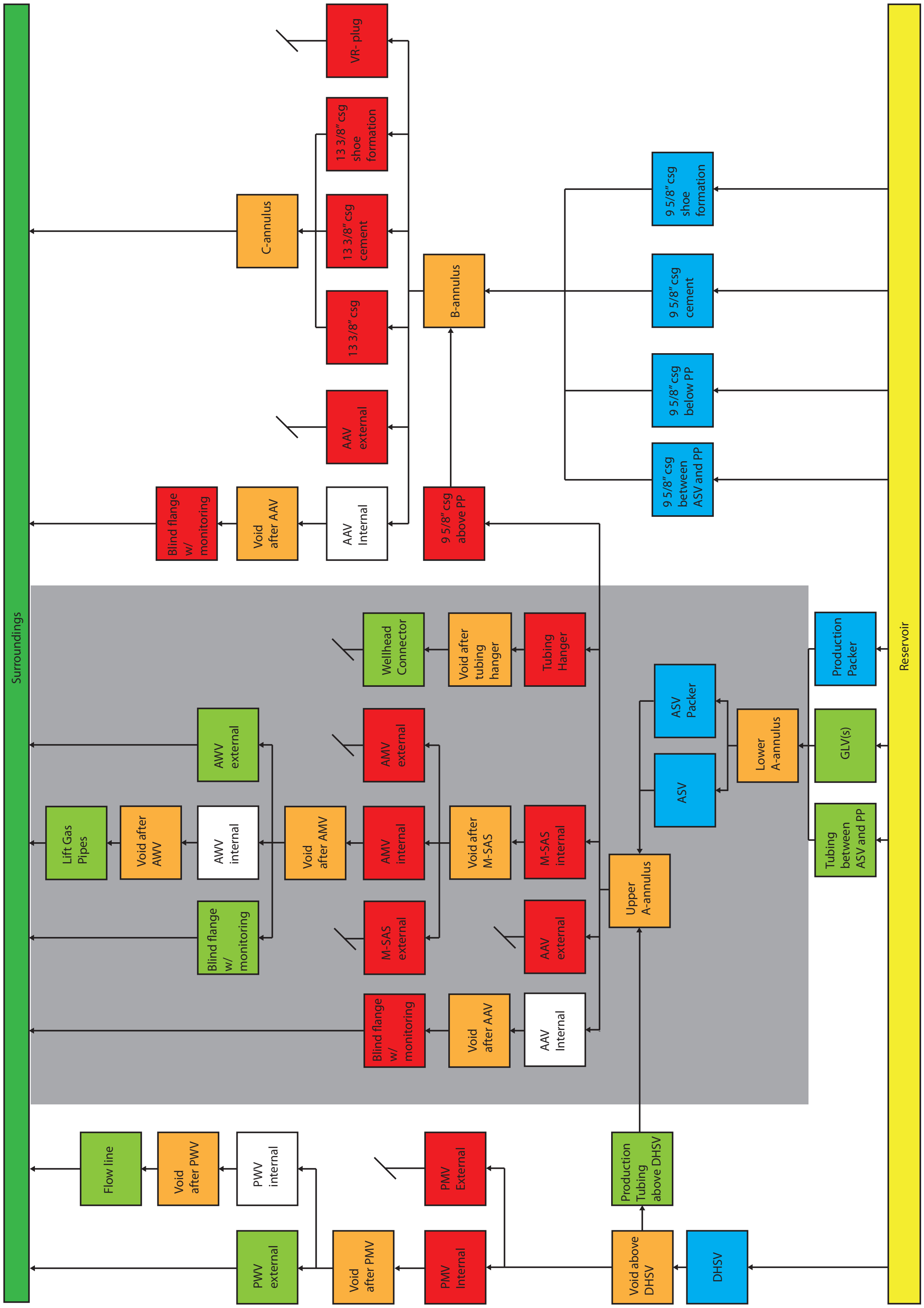


Figure 3.7: Well barrier diagram for option 3 (Will be used in chapter 7).

3.4 Option 4: AMV + M-SAS

3.4.1 Strategy

ASV is not used. Instead, WBE qualified GLV(s) is used from day one. M-SAS is used as secondary WBE from day one along with AMV to strengthen the barrier. If primary WBE (GLV) fails, it can be replaced by wireline operations.

3.4.2 Advantages

Table 3.10: Advantages using option 4

What	**Why**
Very low installation costs	GLV + M-SAS + AMV
No workover is required	Only wireline intervention for GLV. Lubricator and VR tool for M-SAS
Primary barrier is protected against external hazards	GLV is located inside wellbore
Secondary barrier is protected against external hazards	M-SAS is located inside WH wall
Low cost maintenance compared to ASV workover	Only light intervention is required in order to retrieve GLV and M-SAS
Low risk when performing maintenance compared to ASV workover	Only light intervention is required

3.4.3 Disadvantages

Table 3.11: Disadvantages using option 4

What	**Why**
Cannot be used in subsea applications	M-SAS can only be placed topside
Small production loss when intervention is performed	Intervention is quicker and less complicated than workover
GLV has to be qualified as WBE	In order to fulfil requirements

Table 3.12: Barriers in option 4

Primary Barrier Elements	**Verification / Monitoring**	**Secondary Barrier Elements**	**Verification / Monitoring**
GLV (Actuating item)	Periodic leak testing	AMV Wellhead annulus valve A (Actuating item) and control line	Periodic leak testing
Production Casing Cement	N/A after initial verification	M-SAS (Actuating item)	Periodic leak testing
Production Casing	Continuous pressure monitoring of B-Annulus	Production Casing (Above Production Packer)	Continuous monitoring of B-Annulus
Production Packer	N/A after initial verification	Casing Hanger	Continuous monitoring of B-Annulus/ Periodic leak testing
Completion String	Periodic leak testing	Tubing Hanger	Periodic leak testing and continuous pressure monitoring of A-Annulus
DHSV (Actuating item)	Periodic leak testing	Wellhead	Periodic leak testing
In-situ Formation	N/A after initial verification	XMT	Periodic leak testing of valves
		In-situ Formation	N/A after initial verification

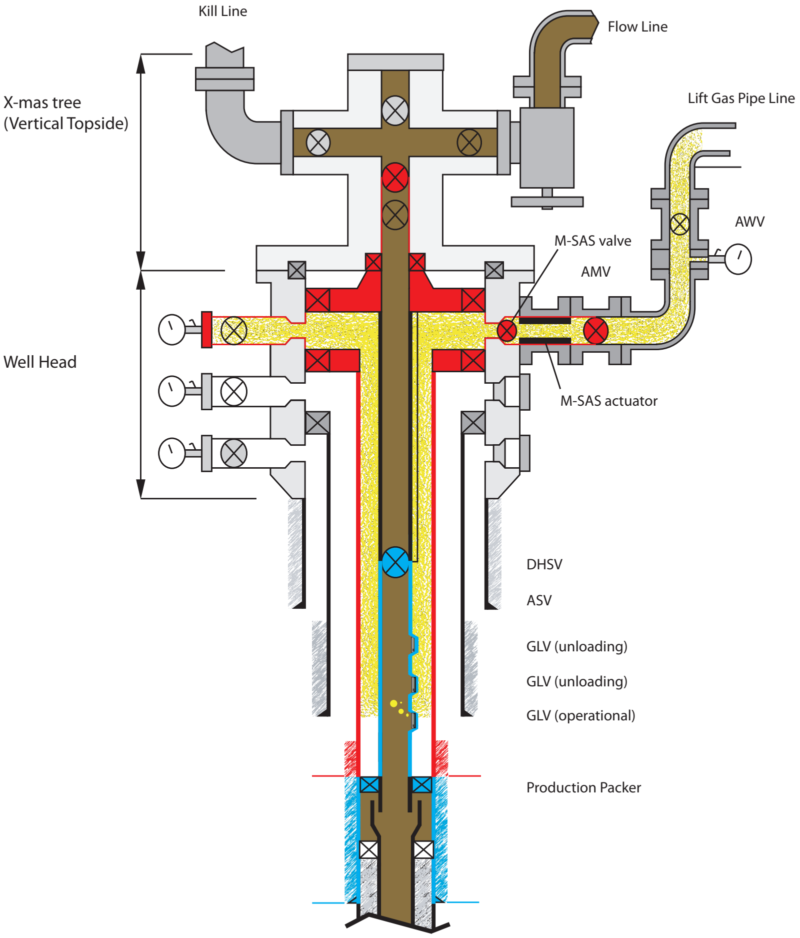


Figure 3.8: Well barrier schematics of option 4 (ExproSoft, 2013).

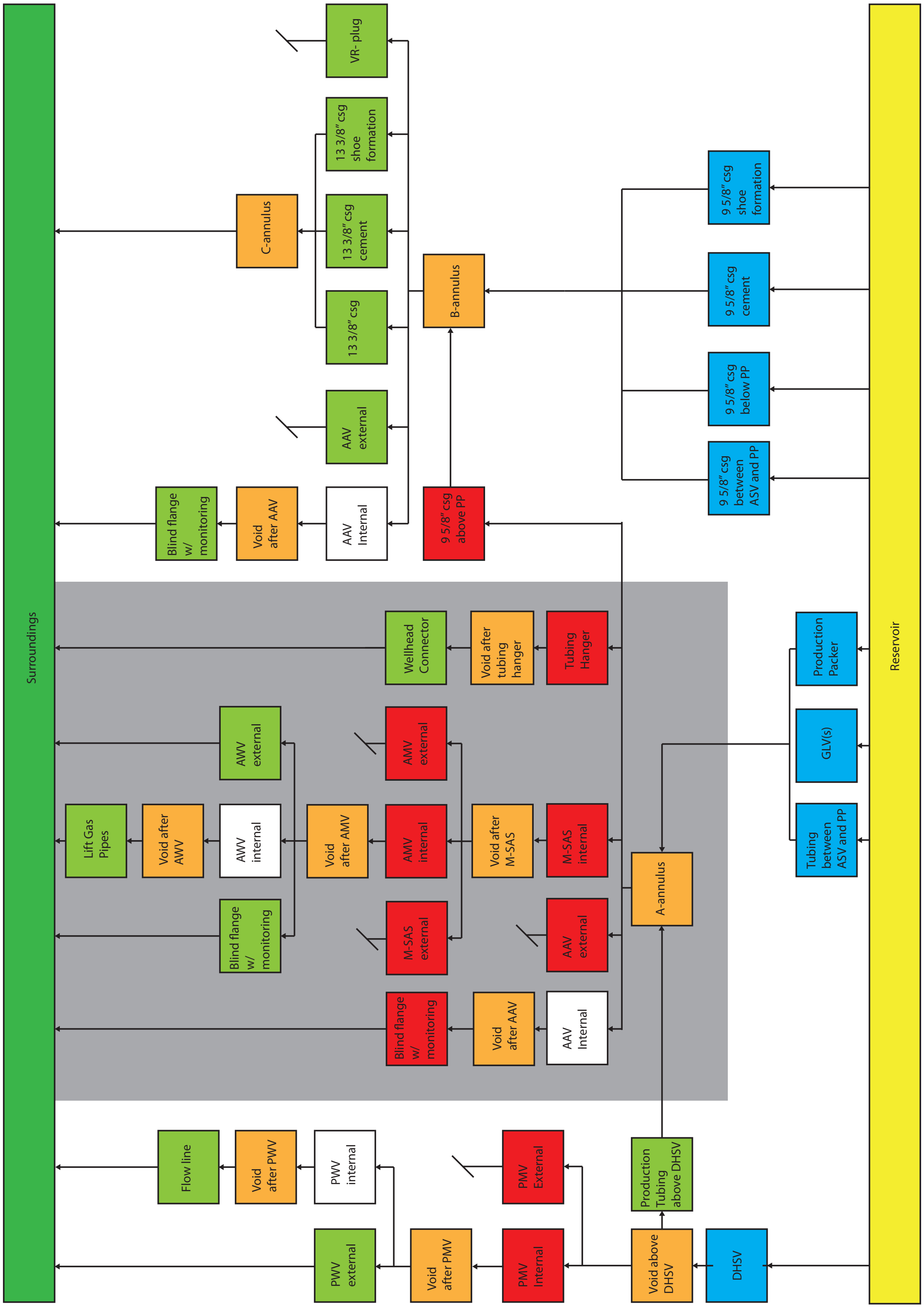


Figure 3.9: Well barrier diagram for option 4 (Will be used in chapter 7).

Chapter 4

Annular Safety

This chapter provides definitions of terms which are important in order to understand the annular safety system in lift gas applications as well as the requirements chapter (chapter 5). These terms are safety instrumented systems (SIS) and safety instrumented functions (SIF).

4.1 Safety Instrumented System (SIS)

Annular safety in lift gas applications is provided by a safety instrumented systems (SIS) which is defined as:

> "an independent protection layer that is installed to migrate the risk associated with the operation of a specified hazardous system, which is referred to as the equipment under control (EUC). An SIS is composed of sensors, logic solvers, and actuating items"

(See Rausand and Høyland, 2004, section 10.2)

4.2 Safety Instrumented Function (SIF)

A SIS has one or more safety instrumented function (SIF) where a SIF is defined as:

> "a function that is implemented by a SIS and that is intended to achieve or maintain a safe state for the EUC with respect to a specific process demand."

(See Rausand and Høyland, 2004, section 10.2)

A SIS has two main system functions:

1. When a predefined process demand (deviation) occurs in the EUC, the deviation shall be detected by the SIS sensors, and the required actuating items shall be activated and fulfil their intended functions.

2. The SIS shall not be activated spuriously, that is, without the presence of a predefined process demand (deviation) in the EUC.

A failure of the first function is referred to as fail to function (FTF), and a failure of the second function is called a spurious trip (ST) (See Rausand and Høyland, 2004, section 10.2)

4.3 Annuls Safety Systems as a Part of SIS

The annulus safety system is used as an example to illustrate the relation between the terms SIS and SIF in this case:

The annulus safety system is a part of the emergency shutdown (ESD) system in gas lift wells along with the production bore safety system. This ESD system is an example of a SIS and in this case the SIS includes:

- Sensors such as fire or heat detectors, pressure transmitters, etc.

- Actuating items which is the ASV, AMV and M-SAS valve

- Logic solver(s) which receives signals from the sensors and sends signals to the actuating items

The SIF for this SIS is to shut of the EUC which in this case is the annulus reservoir (A-annulus). This is illustrated in figure 4.1.

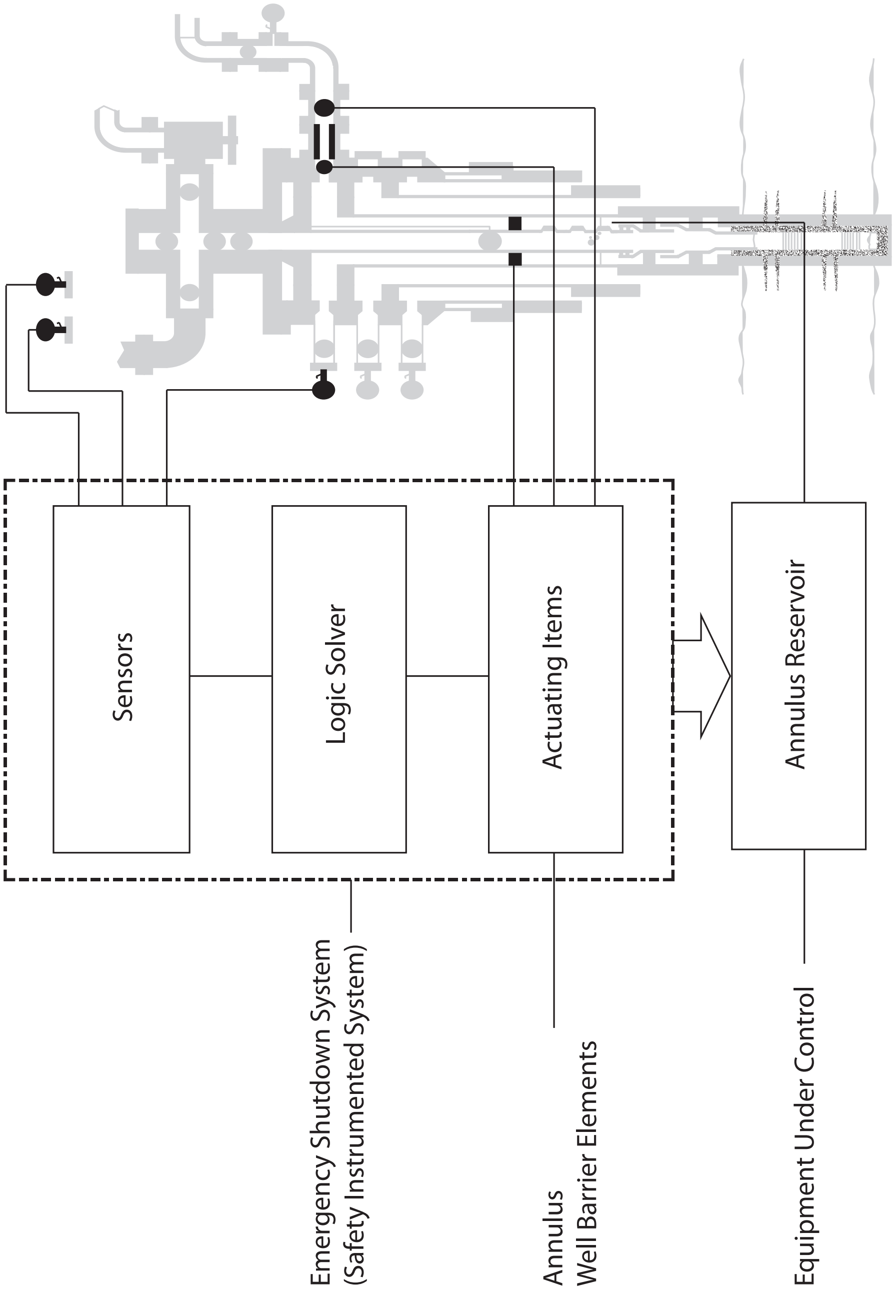


Figure 4.1: The SIS which contains sensors, a logic solver and actuating items to shut of the annulus reservoir (EUC).

Chapter 5

Annular Safety Requirements

An overview of requirements regarding annular safety systems is provided in this chapter. This includes governing regulations in the United States of America (USA) and in Norway, and Norwegian requirements regarding SIS. The main SIS project phases, SIS requirements and SIS documentation according to the OLF 070 guideline are provided.

5.1 Governing Regulations

Governing regulations for the oil and gas industry are provided by most countries. These are overall requirements which have to be interpreted. Governing regulations regarding well barriers in USA and Norway are provided and interpreted.

5.1.1 The United States of America

The oil and gas production in USA is managed by The Bureau of Safety and Environmental Enforcement (BSEE) which provides regulations regarding well barriers. According to BSEE, it is required to equip new wells or gas lift wells with at least one master valve and one surface safety valve above the master valve in the vertical run of the XMT (See BSEE, 2013a, §250.518d).

The BSEE requirement also states that all tubing installations in contact with zones containing hydrocarbon shall be equipped with subsurface safety devices that will shut off the flow from the well in the event of an emergency unless it is incapable of natural flowing. These devices can consist of e.g. a surface-controlled subsurface safety valve (SCSSV), or a tubing/annular subsurface safety device. (see BSEE, 2013b, §250.801a).

According to BSEE, gas lift or water-injection pipelines on unmanned platforms need to be equipped with an Flow Safety Valve (FSV) installed immediately upstream of each casing annulus or the first inlet valve on the XMT (see BSEE, 2013c, §250.1004 b(7)).

5.1.2 Norway

The regulatory authority for technical and operational safety for the petroleum industry in Norway is named Petroleum Safety Authority Norway (PSA) (Norway, 2013a). According to PSA regulations, barriers shall be established to reduce the probability of failures, hazard and accident situations developing, and to limit possible harm and disadvantages. There shall be sufficient independence between barriers where more than one is needed. (See Norway, 2013b, section 5). PSA also provides the following requirements regarding well barriers:

> "During drilling and well activities, there shall be tested well barriers with sufficient independence" ... "If a barrier fails, activities shall not be carried out in the well other than those intended to restore the barrier." (See Norway, 2013c, section 85).
>
> "The flow line and annulus shall be equipped with necessary downhole safety valves (SCSSV) and necessary equipment for monitoring well parameters." (See Norway, 2013d, section 53).
>
> "The christmas tree shall have at least two main valves, and at least one of them shall be automatic" (See Norway, 2013e, section 53).

5.1.3 Interpretation of Governing Regulations

The American governing regulations can be interpreted as a requirement of at least two independent barriers against reservoir and at least one barrier element against the annulus reservoir.

The Norwegian governing regulations can be interpreted as a requirement of at least two independent barriers against the reservoir. The barriers against annulus reservoir are not described directly in the Norwegian governing regulations but it is recommend using NORSOK standards to fulfil the requirements. NORSOK recommend at least two independent barriers against annuls reservoir. See section 5.2. The interpretations are illustrated in table 5.1.

Table 5.1: Interpretation of governing regulations regarding well barriers in USA and Norway

	USA	**Norway**
Primary WBE	x	x
Secondary WBE	x	x
Annulus primary WBE	x	x
Annulus secondary WBE	-	x

5.2 NORSOK

NORSOK is a national standards organization and has been approved by PSA as a provider of standards to fulfil the functional requirements in Norway. NORSOK regulations regarding barriers state that there shall be at least two independent and tested barriers available between the reservoir and the environment to prevent unintentional flow from the well during production activities. The position of the barrier shall be known at all times and the barrier shall be designed for re-establishment of a lost barrier. The XMT is defined as one barrier during normal production. The DHSV is normally the other barrier (See NORSOK, 2002, section 5.17.2).

Special requirements regarding gas lift wells are also provided by NORSOK: The volume of released hydrocarbon gas due to accidental damage to XMT, WH or surface lines shall be minimized. All gas lifted platform wells shall therefore have an ASV installed in the A-annulus. An alternative to ASV, if safety level can be documented same or better than an ASV system, is to use a WH fail safe close device in combination with WBE qualified GLV.

A WBE qualified GLV can be used as an alternative to an ASV in subsea wells if a risk analysis is conducted and shows acceptable risk. It is also required to perform a risk analysis regarding hydrocarbon gas release if barriers are lost, use tested gas tight premium connections for the production casing and completion string, constant monitoring and alarms of the B-annulus in platform wells, design B-annulus to withstand effect of thermal induced pressure in subsea wells, and to evaluate monitoring of B-annulus in subsea wells (See NORSOK, 2012, section 7.7.2). Table 5.2 shows recommended WBEs according to NORSOK. This includes alternative configurations for topside gas lift and subsea applications.

Table 5.2: Additional documentation and primary and secondary barrier elements against reservoir and against annular reservoir according to NORSOK (NORSOK, 2012).

	All wells	**Option for topside lift gas wells**	**Option for subsea wells**
Primary WBE	DHSV	DHSV	DHSV
Secondary WBE	PMV	PMV	PMV
Annulus primary WBE	ASV	GLV	GLV
Annulus secondary WBE	AMV	M-SAS + AMV	AMV
Additional documentation	-	Acceptable safety	Acceptable risk

5.3 OLF / IEC

In Norway, there are several guidelines to be followed in order to fulfil the governing regulations. Each regulation paragraph has at least one guideline. OLF 070 is an example of a guideline which is developed specific for SIS. According to the Facilities Regulations §8 provided by PSA, OLF 070 shall be used in design and performance of SIFs. IEC 61508 is the basis for specification, design and operation of SIS and IEC 61511 is the process industry's own sector specific standard for application of SIS. OLF 070 is a simplification of these international standards (OLF, 2004).

5.3.1 Safety Integrity Level (SIL)

Safety integrity is a fundamental concept in IEC 61508 and is classified into four discrete levels called Safety Integrity Levels (SIL). SIL is defined by the probability of failure on demand (PFD) which is the probability of system or component failure if a demand occurs. OLF 070 both provides SIL requirements and proposed activities to fulfil these requirements throughout the various SIS project phases.

5.3.2 SIL Requirements

According to OLF 070, there are three main requirements that need to be fulfilled in order to achieve a given SIL:

- Quantitative PFD requirements
- Quantitative architectural requirements
- Avoidance and control of systematic failures

(See OLF, 2004, section 8.5). Descriptions of the above requirements follows:

Quantitative PFD Requirements

This is a quantitative requirement expressed as PFD or alternatively as the probability of a dangerous failure per hour. This shall include:

- Random hardware failures
- Common cause failures
- If relevant, failures of any data communication systems used to support the safety function.

Table 5.3 shows the various SIL and corresponding PFD value. The table is divided into:

- Continuous demand mode, which is processes where demands occur all the time. This is applications such as exothermic reactors.
- Demand mode, which are processes where demands do not occur continuously. This is applications such as emergency shutdown (ESD) systems.

Table 5.3: The various SIL and corresponding PFD values (see OLF, 2004, table 8.1).

SIL	**Demand Mode of Operation** (Average probability of failure to perform its design function on demand - PFD)	**Continuous / High Demand Mode of Operation** (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

OLF 070 defines minimum SIL requirements for various SIS and is also a guideline of how to handle deviations from the minimum SIL requirement (See OLF, 2004, section 7.6 and 7.7).

ASV, M-SAS and AMV are not directly mentioned in table 7.1 in OLF 070 which lists the minimum SIL requirements for various safety functions. However, ASV systems in gas lift wells are a part of the ESD system for isolation of topside well which has minimum SIL requirement of SIL 3. According to table 8.1 in OLF 070, SIL 3 is defined as PFD more or equal to 10^{-4} to less than 10^{-3} for demand mode operation.

Quantitative Architectural Requirements

This is a quantitative requirement expressed in terms of architectural constraints on the subsystems constituting safety function. Architectural constrains on hardware safety integrity are given by:

- The hardware fault tolerance (HFT) of the subsystem. (The number of faults that could cause loss of safety function.)
- The safe failure fraction (SFF) (The fraction of failures which can be considered safe since they are detected, or do not cause loss of the safety function.)
- Whether the subsystem is of “A-type or B-type” where for A-type, all possible failure modes can be determined for all components and where for B-type, the behaviour under fault conditions cannot be determined for at least one component. (In practice B-type will be for systems using programmable electrical components since their behaviour under fault conditions can be hard to determine and A-type will be for systems without programmable electrical components.) (See iec, 2010b, sub clause 7.4).

Architectural requirements according to OLF 070 are shown in table 5.4 (for A-type subsystems) and in table 5.5 (for B-type subsystems).

Table 5.4: Hardware safety integrity: architectural constrains on type A safety-related subsystems (iec (2010b), Table 2 and OLF (2004) Table 8.2)

Safe failure fraction	**Hardware fault tolerance**		
	0	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3
60% - 90%	SIL 2	SIL 3	SIL 4
90% - 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Table 5.5: Hardware safety integrity: architectural constrains on type B safety-related subsystems (iec (2010b), Table 3 and OLF (2004) Table 8.3)

Safe failure fraction	**Hardware fault tolerance**		
	0	**1**	**2**
< 60%	Not allowed	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Avoidance and Control of Systematic Failures

This is requirements concerning which techniques and measures should be used to avoid and control systematic faults. These are systematic faults that are introduced during specification, design, operation or maintenance/testing, which may result in a failure of the safety function under certain conditions. (See OLF, 2004, chapter 8)

5.3.3 SIS Project Phases

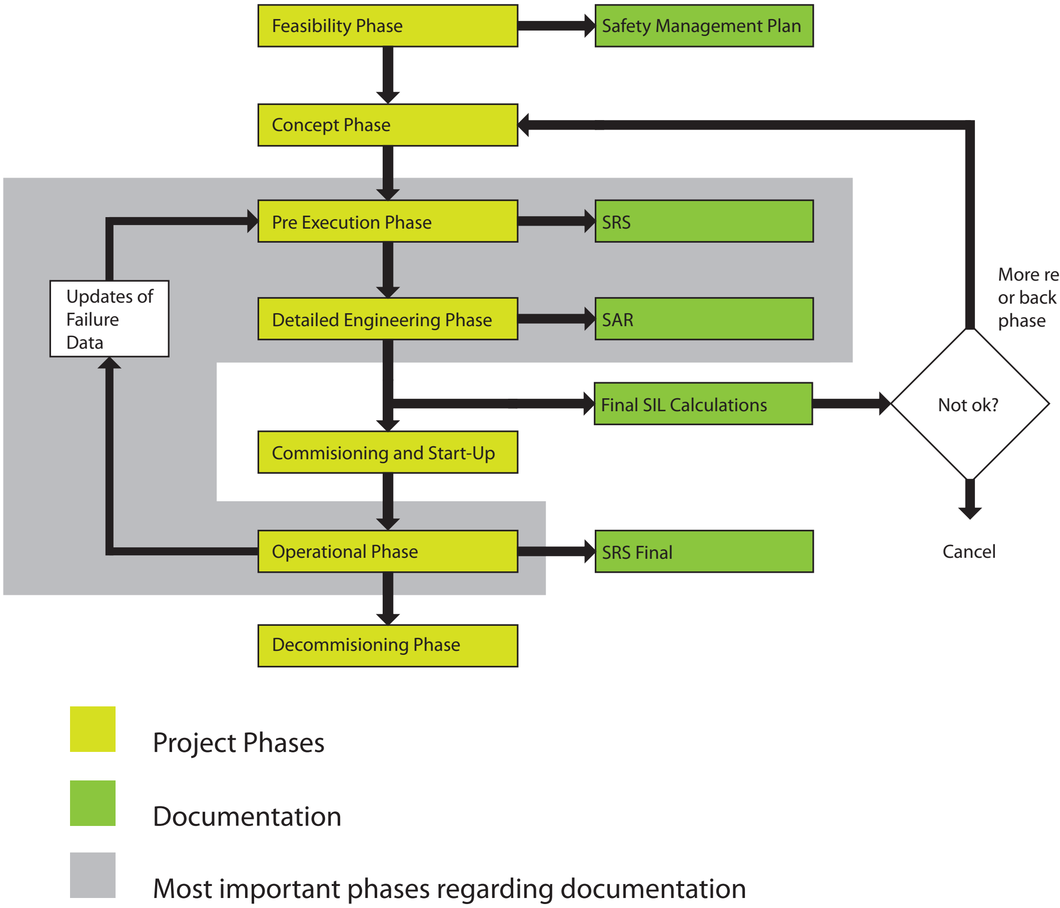


Figure 5.1: SIS phases and documentation (based on OLF, 2004, fig E1a and E1b)

Figure 5.1 shows the various project phases and the main documentation generated throughout the life cycle of a SIS. After the concept phase, the three most important phases regarding documentation are the Pre Execution Phase (in this case: Pre SIS design and engineering phase), the Detailed Engineering Phase (in this case: SIS design and engineering phase) and the Operational Phase. These three phases are highlighted in gray on figure 5.1 and briefly explained below:

- **Pre SIS design and engineering phase:** In this phase, the design basis is made for the SIS design phase. This is included in the Safety Requirement Specification (SRS). The first version of SRS is also made in this phase.

- **SIS design and engineering phase:** In this phase, the SIS is designed according to the SRS. SIS components are ordered from subcontractors. A Factory Acceptance Test (FAT) is performed and a Safety Analysis Report (SAR) is made and delivered along with each SIS component.
- **Operational Phase:** After the SIS is installed, the operational phase can begin. This implies data collection, testing, maintenance, failure data updates, and modifications which provides input to new versions of the SRS.

(OLF, 2004).

5.3.4 Required SIS Documentation

In order to qualify components as SIS components, basically two documents have to be provided in addition to manuals. This is the SRS and the SAR.

Safety Requirement Specification (SRS)

SRS provides the design basis for the SIS design and engineering phase. IEC 61511-1 chapter 10 describes the content of SRS in form of a series of requirements. According to OLF 070, the SRS shall contain:

- Functional requirements and descriptions such as capacities and response times
- Integrity requirements such as PFD and SIL
- Operating prerequisites and constraints

A more detailed SRS content is provided in appendix B (adopted from ConocoPhillips (2013a) and based on iec (2003), chapter 10). The SRS shall be regularly updated throughout the lifetime of the SIS in form of new versions. (See OLF (2004), section 7.8 and appendix E.2).

Safety Analysis Report (SAR)

Based on the SRS (see previous subsection), one can start the SIS design and engineering phase as described in OLF 070 chapter 8. SARs shall be a part of the final documentation in this project phase and shall document how each supplier of SIS components has implemented requirements set by IEC 61508 and IEC 61511. One SAR is typically made for each component in a SIF but several components may be documented in the same SAR. According to OLF 070 chapter 8.10, the SAR shall include:

- System description
- System topology and block diagram
- Operational description of the system
- Failure rate of the components
- Recommended time interval between functional testing
- Mean Time to Repair (MTTR)
- Diagnostic coverage
- Voting
- Common cause failures
- Behavior of system on detection of a fault
- Avoidance and control of systematic failures
- If relevant: PFD calculations

Subcontractors have various ways of structuring a SAR which is normally documented in a SAR template. An example of such a SAR template is shown in appendix C which also describes the SAR content great detail. Another example can be found in OLF (2004) appendix E.3.

There are reduced requirements for SAR documentation related to systematic failures if a SIS component is claimed to be:

- Proven in use
- Prior use
- Low complexity

However, a structure quality assurance (QA) system must be included or / and an ISO 9000 certification or better. Definitions of the above expressions follow:

Low complexity: A component is of low complexity if dependable field experience exists and if it is in accordance with definition in IEC 61508-4, clause 3.4.3: It is an Electric / Electronic / Programmable Electronic (E/E/PE) safety-related system which is defined as a designed system that both implements safety functions necessary to achieve or maintain a safe state for the EUC. It must also intend to achieve the necessary safety integrity for the required safety functions. Also two other conditions need to be fulfilled in order to achieve low complexity:

- The failure modes of each individual component are well defined
- The behaviour of the system under fault conditions can be completely determined

The behaviour of the system under fault conditions may be determined by analytical and/or test methods.

Based on the above description, a low complexity component is similar to a type A safety related subsystem which is described in section 5.3.2 under Quantitative Architectural Requirements.

If low complexity is claimed and the SAR template in appendix C is used, low complexity documentation shall be given in SAR chapter 8 - Architectural constraints (HFT and voting principles) (See iec (2010a), clause 4.2, iec (2010c), clause 3.4.3, and ConocoPhillips (2013b)).

Proven in use: A component is proven in use if in compliance with requirements in IEC 61508-2, clause 7.4.10.1 to 7.4.10.7. According to IEC 61508-2, an element shall only be regarded as proven in use when it has clearly restricted and specified functionality and when there is adequate documentary evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required SIL of the SIF that use the element is achieved. Evidence shall be based on analysis of operational experience of a specific configuration of the element together with suitability analysis and testing. (See iec, 2010b, clause 7.4.10.1))

According to ConocoPhillips (2013b), a component can be considered proven in use if the failure data can be based on:

- More than 10 inventories or more than 50 critical failures
- More than 50000 hours calendar/operational time
- More than 2 installations covered
- More than 1 operator covered

If the component is claimed proven in use and the SAR template in appendix C is used, proven in use shall be documented in SAR chapter 14 - Avoidance and control of systematic failures. QA certificates and/or procedures shall then be attached to the SAR (ConocoPhillips, 2013b).

Prior use: Requirements for claiming prior use are described in IEC 61511-1 clause 11.5. According to IEC 61511-1 clause 11.5.3.1, it is required to prove that the components and subsystems are suitable for use in SIS. According to IEC 61511-1 clause 11.5.3.2, the evidence of suitability shall include:

- Consideration of the manufacturer's quality, management and configuration management systems
- Adequate identification and specification of the components or subsystems
- Demonstration of the performance of the components or subsystems in similar operating profilers and physical environments
- The volume of the operating experience

If the component is claimed prior use, this shall be documented in SAR chapter 14 - Avoidance and control of systematic failures. QA certificates and/or procedures shall then be attached to the SAR. (See iec (2003) clause 11.5.3 and ConocoPhillips (2013b)).

5.3.5 Responsibility

According to OLF 070, it is important that an organization or a responsible person is identified for each phase of the SIS safety life cycle. When a SIS is developed, the operators order various components from different vendors. According to OLF 070 section 8.2, such vendors can be:

- Engineering contractors that is given the task to do the SIS engineering
- Systems suppliers that provide the SIS
- Control systems vendors
- Field equipment vendors

(OLF, 2004).

The vendors are responsible for making and delivering the component and a SAR to document according to requirements in the SRS. The operator qualification team is responsible for the handover to the requisitioner. The requisitioner is responsible for the final technology approval. In Norway, PSA provides regulations and ensure that the regulations are fulfilled (see OLF (2004) and ExproSoft (2013)).

Chapter 6

The Safety Analysis Report (SAR) Process

The SAR process for both proven and non-proven technology are described in this chapter. This is done by firstly interpreting the requirements of documentation for non-proven and proven technology. Flow diagrams are provided for the different documentation scenarios. Two cases are used to illustrate and exemplify the SAR processes:

- A hydraulically operated ASV (H-ASV) represents proven technology
- An electrically operated ASV (E-ASV) represents non-proven technology

Challenges when performing SAR are pointed out and improvements to the guidelines are proposed.

6.1 Reduction of SIS Documentation

According to OLF 070, the necessary documentation for non-proven technology is the SRS and the SAR. The SRS content is described in section 5.3.4 and includes the design basis which is used to create the SAR. The SRS content can thus not be reduced. However, the SAR content may be reduced by either claiming low complexity, proven in use or prior use for the component as described in section 5.3.4. This is illustrated in figure 6.1.

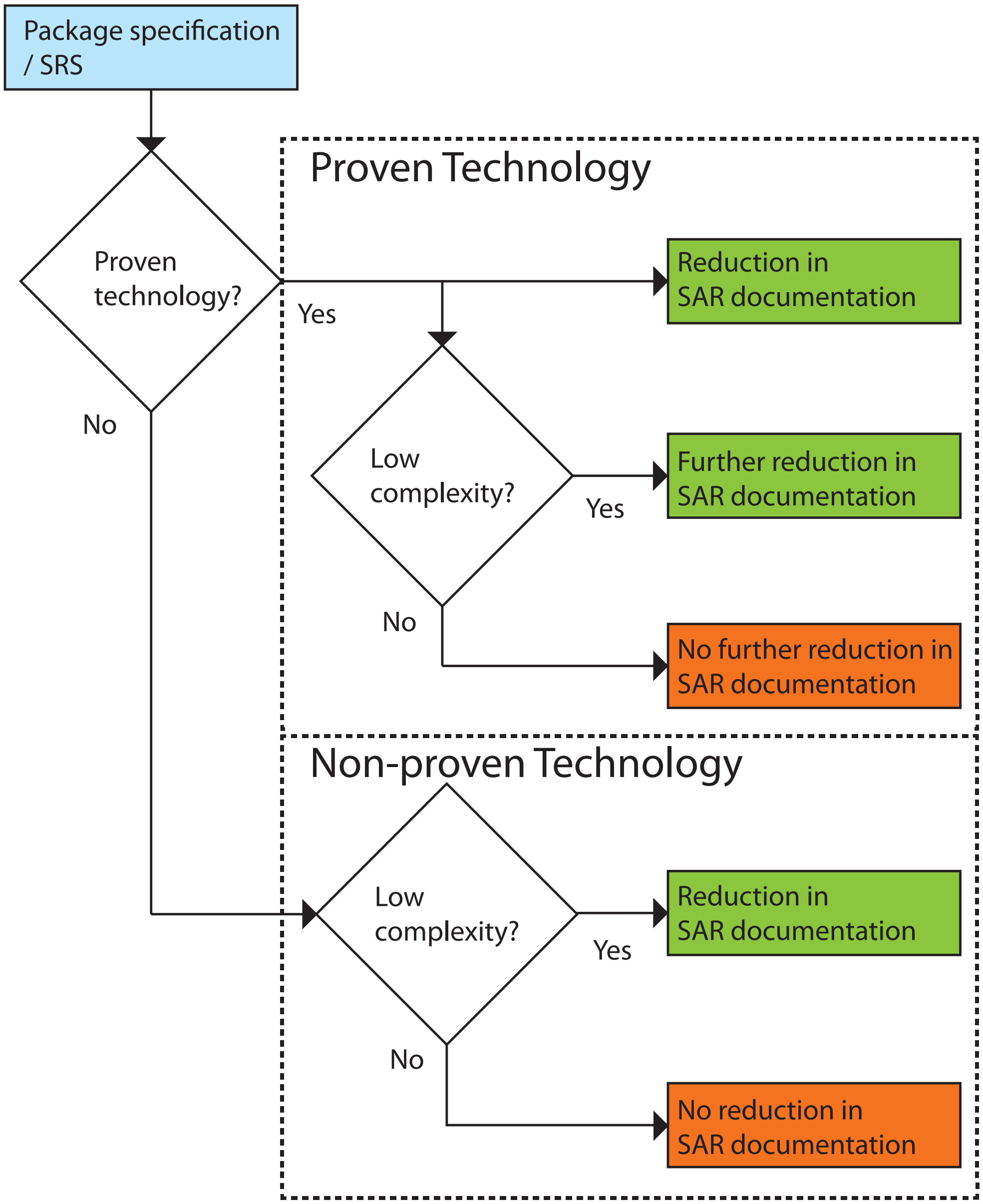

Package specification / SRS
Proven technology?
Yes
No
Proven Technology
Reduction in SAR documentation
Low complexity?
Yes
Further reduction in SAR documentation
No
No further reduction in SAR documentation
Non-proven Technology
Low complexity?
Yes
Reduction in SAR documentation
No
No reduction in SAR documentation

Figure 6.1: Possible ways of reducing SAR documentation for SIS components

The SAR content is described in accordance to OLF 070 in section 5.3.4. Each vendor or subcontractors has normally their own SAR template. An example of a SAR template is shown in table 6.1 which is the same as in appendix C.

Table 6.1: Example of a SAR template (ConocoPhillips, 2013b)

<table>
<tr><td>|</td><td>Abbrevations</td></tr>
<tr><td>||</td><td>References</td></tr>
<tr><td>|||</td><td>Summary</td></tr>
<tr><td>1.</td><td>Introduction</td></tr>
<tr><td>2.</td><td>System description</td></tr>
<tr><td>3.</td><td>System topology and block diagram</td></tr>
<tr><td>4.</td><td>Operational description of the system</td></tr>
<tr><td>5.</td><td>Assumptions</td></tr>
<tr><td>6.</td><td>Failure rate of the components</td></tr>
<tr><td>7.</td><td>Diagnostic coverage & Safe failure fraction</td></tr>
<tr><td>8.</td><td>Architectural constraints (HFT and voting principles)</td></tr>
<tr><td>9.</td><td>Common cause failures</td></tr>
<tr><td>10.</td><td>Behaviour of system/components on detection of fault</td></tr>
<tr><td>11.</td><td>Mean time to repair</td></tr>
<tr><td>12.</td><td>Factory testing</td></tr>
<tr><td>13.</td><td>Operational testing (incl. test procedures and recommended functional test interval)</td></tr>
<tr><td>14.</td><td>Avoidance and control of systematic failures</td></tr>
<tr><td>15.</td><td>Software documentation</td></tr>
<tr><td>16.</td><td>Results</td></tr>
<tr><td></td><td>Appendices</td></tr>
</table>

Note that all the chapters in table 6.1 are included in the SAR if the SAR template in appendix C is used, but the content in some of the chapters may vary and depends on whether the component is non-proven or proven.

6.2 Non-Proven Technology

Non-proven technology are components that are either under development or already developed but not used enough to be claimed proven in use or prior use. In other words, not enough field experience exists and thereby not enough proof is available for the technology to be proven suitable for its use. Non-proven technology can thus either be of low complexity or of high complexity (type A or type B subsystem). This is illustrated in figure 6.2.

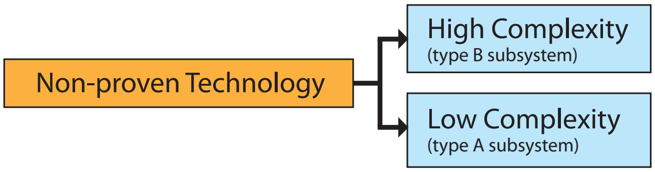


Figure 6.2: Possible claims for non-proven technology

6.2.1 Required Documentation of Non-Proven Technology

The only way of reducing SAR documentation for non-proven components is by claiming low complexity. This is illustrated in figure 6.1. The conditions for claiming low complexity are described in section 5.3.4. If low complexity is claimed, this documentation shall be given in SAR chapter 8 - Architectural constraints (HFT and voting principles) if the SAR template in table 6.1 / appendix C is used. There are then no requirements for documentation of handling of systematic failures, but QA system must be in place and be documented. If low complexity cannot be claimed for the component, it is not possible to reduce the SAR documentation.

6.2.2 SAR Process for Non-Proven Technology

If low complexity is claimed, the SAR process can be done in accordance with figure 6.3. If not, the SAR process must be done as described in figure 6.4. The differences are highlighted with blue colour in the two figures.

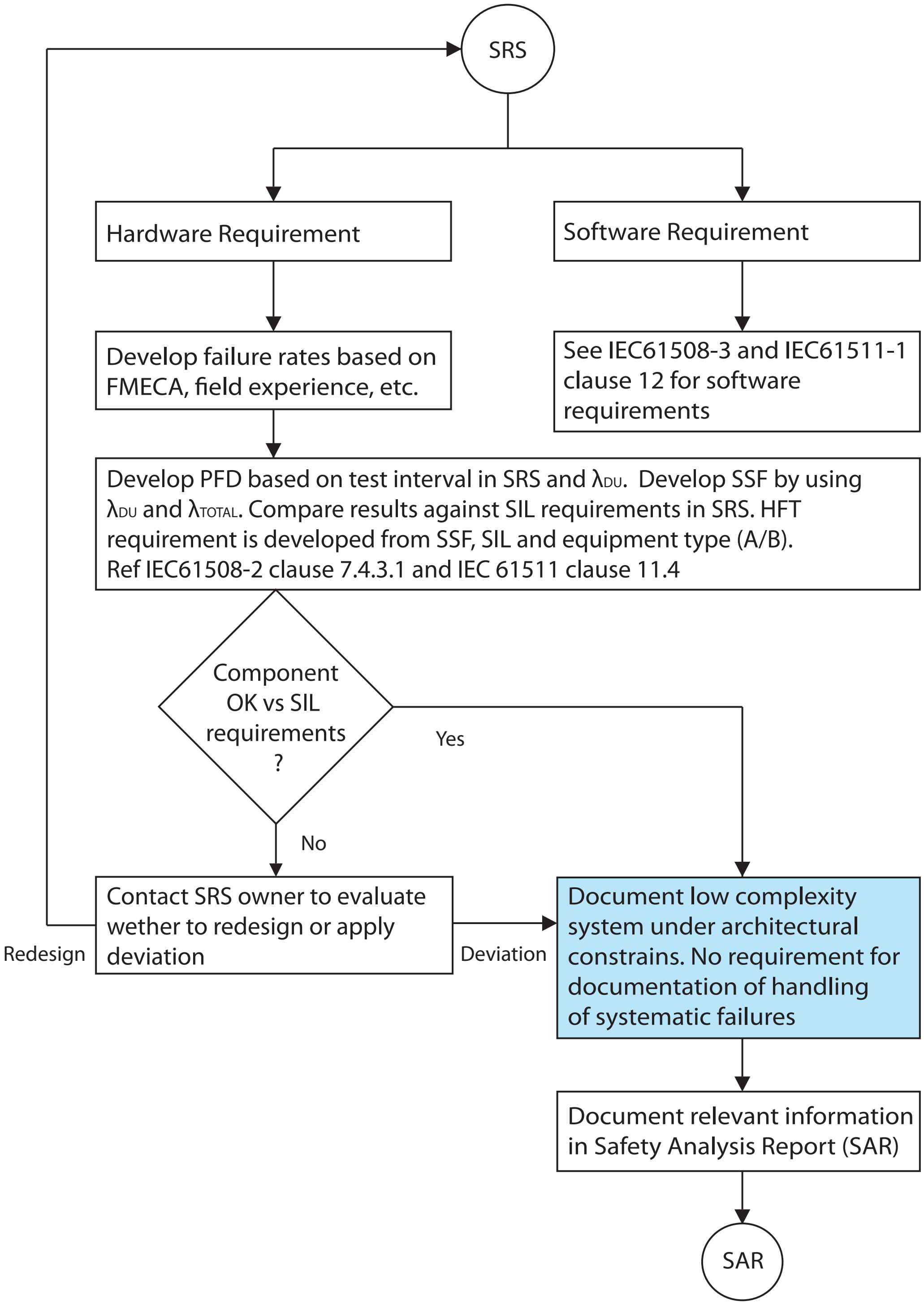

SRS
Hardware Requirement
Software Requirement
Develop failure rates based on FMECA, field experience, etc.
See IEC61508-3 and IEC61511-1 clause 12 for software requirements
Develop PFD based on test interval in SRS and λDU. Develop SSF by using λDU and λTOTAL. Compare results against SIL requirements in SRS. HFT requirement is developed from SSF, SIL and equipment type (A/B). Ref IEC61508-2 clause 7.4.3.1 and IEC 61511 clause 11.4
Component OK vs SIL requirements ?
Yes
No
Contact SRS owner to evaluate wether to redesign or apply deviation
Redesign
Deviation
Document low complexity system under architectural constrains. No requirement for documentation of handling of systematic failures
Document relevant information in Safety Analysis Report (SAR)
SAR

Figure 6.3: SAR process for non-proven low complexity claimed components. (Based on OLF, 2004, figure E2)

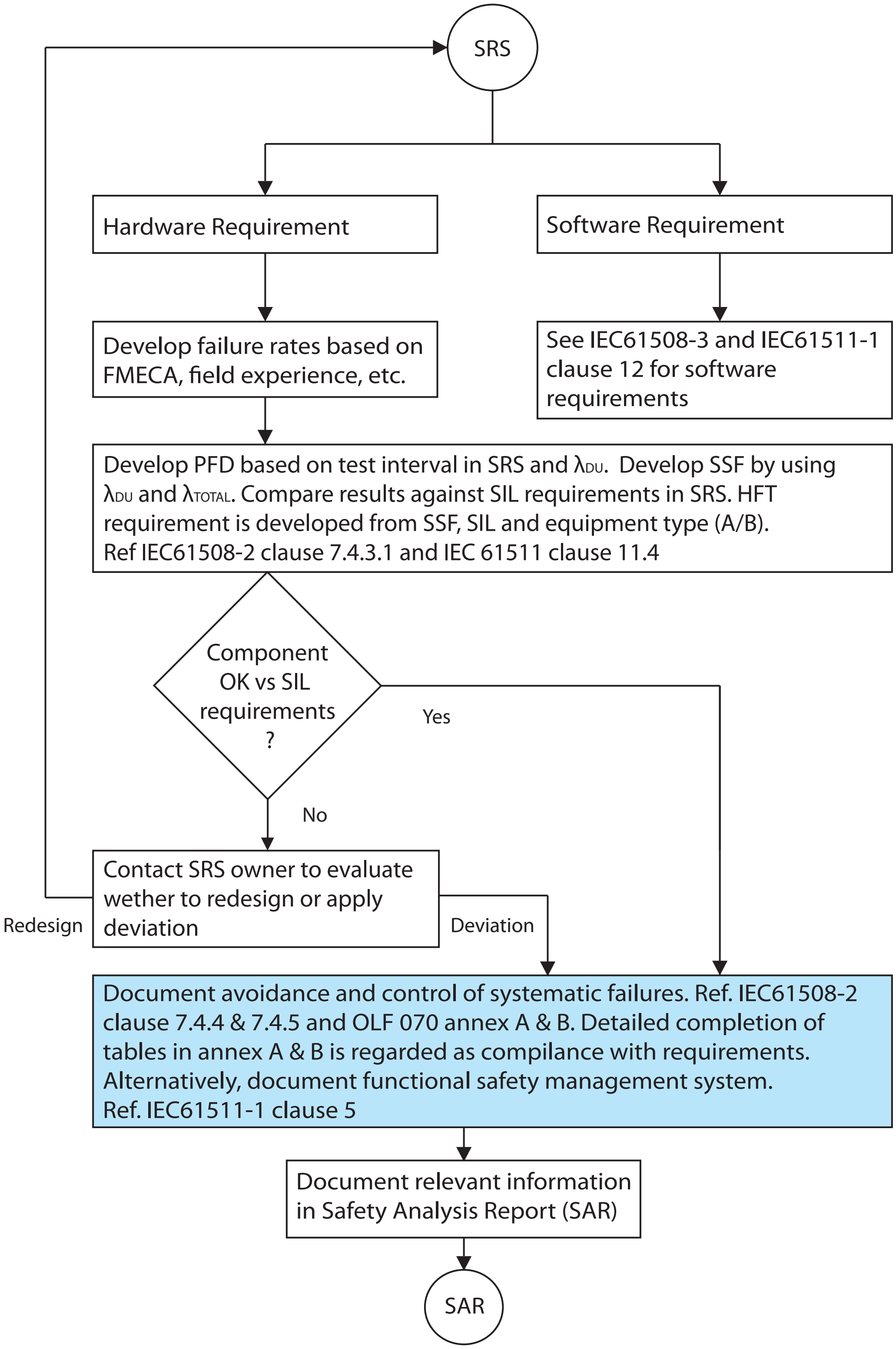

SRS
Hardware Requirement
Software Requirement
Develop failure rates based on FMECA, field experience, etc.
See IEC61508-3 and IEC61511-1 clause 12 for software requirements
Develop PFD based on test interval in SRS and λDU. Develop SSF by using λDU and λTOTAL. Compare results against SIL requirements in SRS. HFT requirement is developed from SSF, SIL and equipment type (A/B). Ref IEC61508-2 clause 7.4.3.1 and IEC 61511 clause 11.4
Component OK vs SIL requirements ?
Yes
No
Contact SRS owner to evaluate wether to redesign or apply deviation
Redesign
Deviation
Document avoidance and control of systematic failures. Ref. IEC61508-2 clause 7.4.4 & 7.4.5 and OLF 070 annex A & B. Detailed completion of tables in annex A & B is regarded as compilance with requirements. Alternatively, document functional safety management system. Ref. IEC61511-1 clause 5
Document relevant information in Safety Analysis Report (SAR)
SAR

Figure 6.4: SAR process for non-proven components that cannot claim low complexity. (Based on OLF, 2004, figure E2)

Example using an electrical ASV

An E-ASV is used as an example of non-proven technology. Such a component is considered a low complexity system if it does not contain any programmable logic solver. It may be slightly more complex than a hydraulic ASV but no new failure modes are added. The behaviour under fault condition will be possible to determine since failure modes are known. Therefore, figure 6.3 has to be used and the content of the SAR can be as described in appendix C. Reduction in documentation will be possible by documenting low complexity in SAR chapter 8 - Architectural constraints. There is also no requirement for documentation of handling of systematic failures, but QA system must be in place and be documented. See appendix D for details.

6.3 Proven Technology

Proven technology has the obvious advantage over non-proven technology because it is already proven suitable for its use. This implies available data and documentation from previous use. Proven technology can thus be defined as technology (either low or high complexity) which is already developed and verified as either proven in use or prior use as described in section 5.3.4. This is illustrated in figure 6.5.

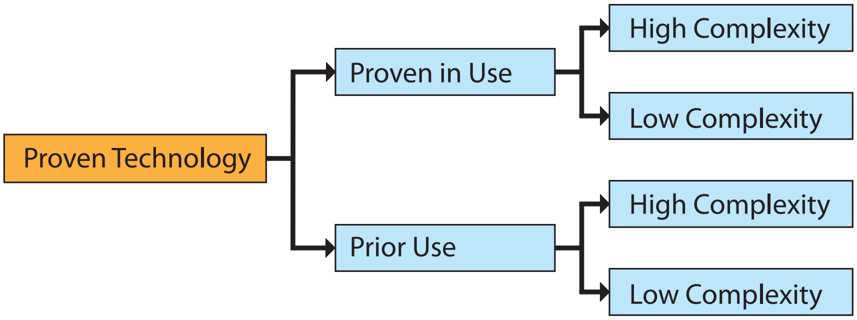


Figure 6.5: Possible verifications and claims for proven technology

6.3.1 Required Documentation of Proven Technology

The SAR content for proven technology will be reduced both for proven in use certified components and for prior use certified components. This is illustrated in figure 6.1 and implies to document proven in use or prior use in SAR chapter 14 - Avoidance and control of systematic failures if the SAR template in table 6.1 / appendix C are used. QA certificates and/or procedures shall then be attached to the SAR. In addition, proven technology can be claimed low complexity which will reduce the documentation further. This is also illustrated in figure 6.1 and implies documenting low complexity in SAR chapter 8 - Architectural constraints (HFT and voting principles) if the SAR template in table 6.1 / appendix C is used.

6.3.2 SAR Process for Proven Technology

The SAR process can be done as described in figure 6.6 for proven technology (Proven in use or prior use certified components). If the component is also considered low complexity, as described in section 5.3.4, the SAR process can be done according to figure 6.7. However, the latter may be of excess and thus unnecessary. This is because the documentation of low complexity is included in the certificate documentation of proven in use / prior use in such cases. The differences are highlighted with blue colour in the two figures.

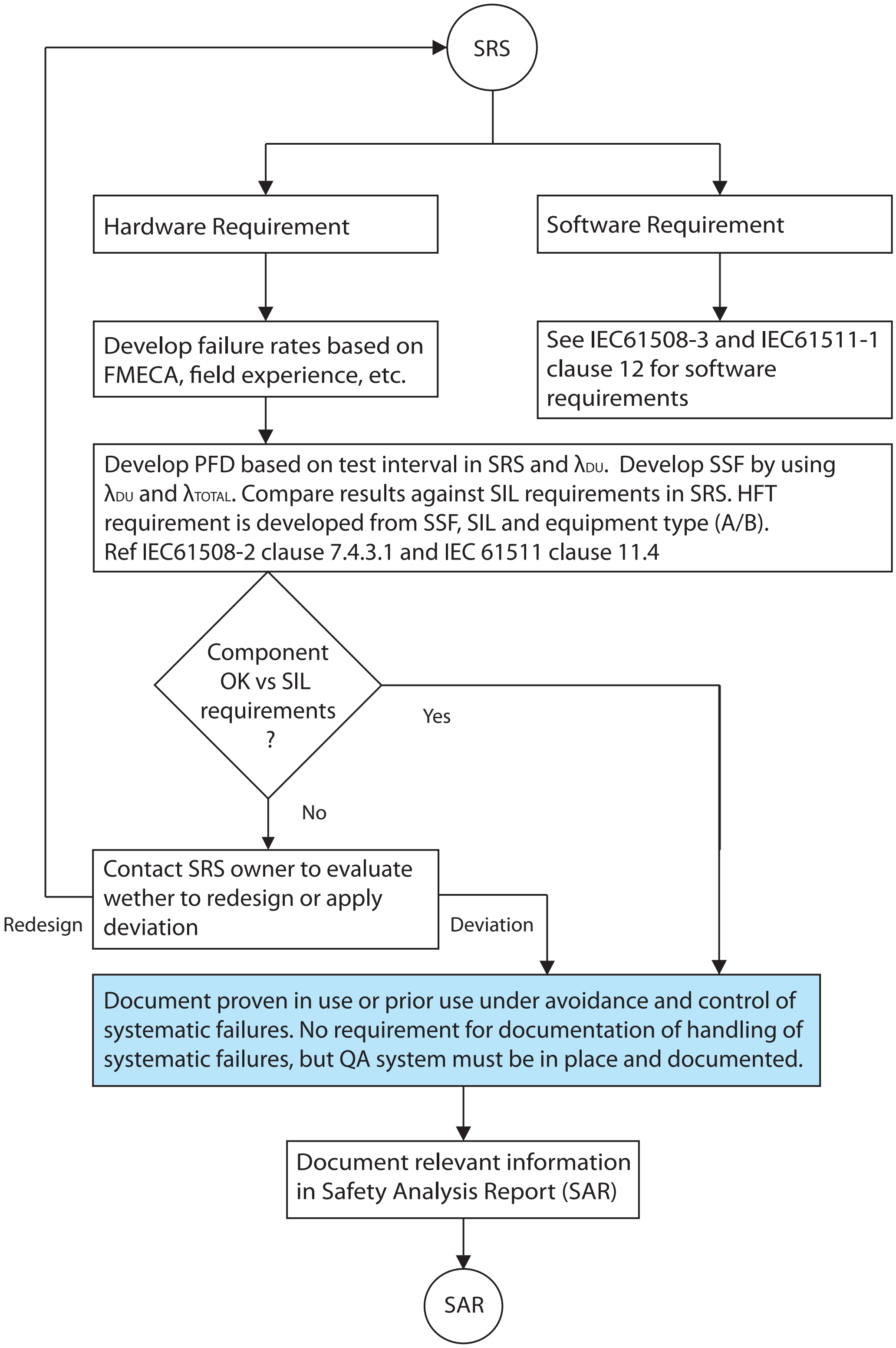

SRS
Hardware Requirement
Software Requirement
Develop failure rates based on FMECA, field experience, etc.
See IEC61508-3 and IEC61511-1 clause 12 for software requirements
Develop PFD based on test interval in SRS and λDU. Develop SSF by using λDU and λTOTAL. Compare results against SIL requirements in SRS. HFT requirement is developed from SSF, SIL and equipment type (A/B). Ref IEC61508-2 clause 7.4.3.1 and IEC 61511 clause 11.4
Component OK vs SIL requirements ?
Yes
No
Contact SRS owner to evaluate wether to redesign or apply deviation
Redesign
Deviation
Document proven in use or prior use under avoidance and control of systematic failures. No requirement for documentation of handling of systematic failures, but QA system must be in place and documented.
Document relevant information in Safety Analysis Report (SAR)
SAR

Figure 6.6: SAR process for proven components which cannot be claimed low complexity. (Based on OLF, 2004, figure E2)

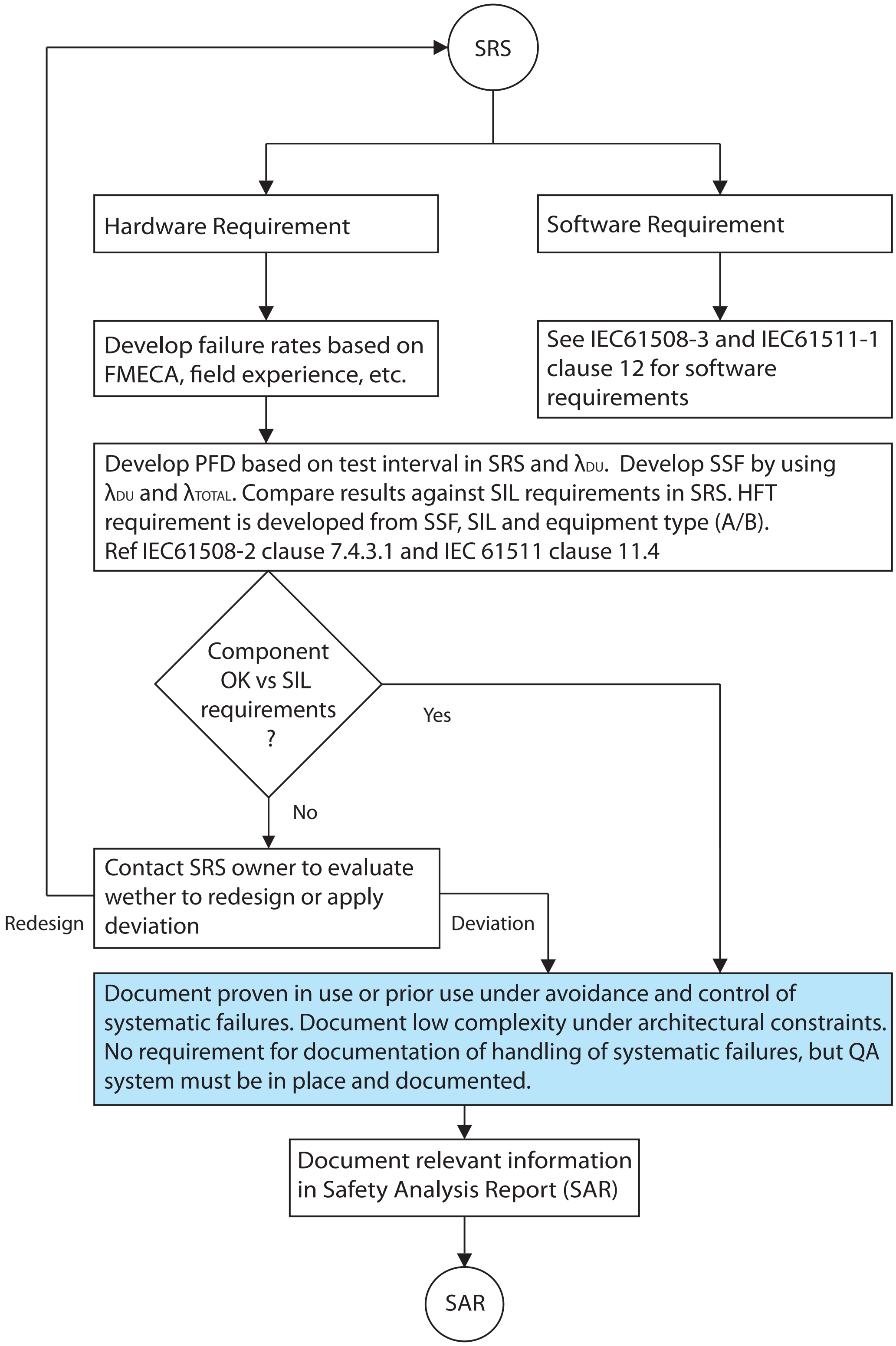

SRS
Hardware Requirement
Software Requirement
Develop failure rates based on FMECA, field experience, etc.
See IEC61508-3 and IEC61511-1 clause 12 for software requirements
Develop PFD based on test interval in SRS and λDU. Develop SSF by using λDU and λTOTAL. Compare results against SIL requirements in SRS. HFT requirement is developed from SSF, SIL and equipment type (A/B). Ref IEC61508-2 clause 7.4.3.1 and IEC 61511 clause 11.4
Component OK vs SIL requirements ?
Yes
No
Contact SRS owner to evaluate wether to redesign or apply deviation
Redesign
Deviation
Document proven in use or prior use under avoidance and control of systematic failures. Document low complexity under architectural constraints. No requirement for documentation of handling of systematic failures, but QA system must be in place and documented.
Document relevant information in Safety Analysis Report (SAR)
SAR

Figure 6.7: SAR process for proven technology which is considered low complexity components. (Based on OLF, 2004, figure E2)

Example using a hydraulic ASV

An H-ASV is used as an example for proven technology. Such a component is considered low complexity if it is pure mechanical. This is because the simplicity of the component makes it possible to foresee any failure mode and behaviour under fault condition. H-ASVs have also been used for decades and much failure data is thus available. Since many ASVs are small sized DHSVs, even more reliability data is available. It is thus assumed that an H-ASV in this case will be both a low complexity and a proven in use or prior use certified component. Figure 6.7 shall thus be used for the SAR process. If the template in appendix C is used, proven in use or prior use shall be documented in SAR chapter 14 - Avoidance and control of systematic failures and low complexity shall be documented in SAR chapter 8 - Architectural constraints. QA systems must be in place and be documented. Certificates must be included in SAR appendix. See appendix D for details.

6.4 Comparison of Proven and Non-Proven

Since both the E-ASV (non-proven) and the H-ASV (proven) are considered low complexity systems, both SARs will be quite similar even if the H-ASV is certified as proven in use or prior use. Table 6.2 and 6.3 shows the main differences in SAR documentation between the proven and non-proven technology based on the SAR example in appendix D. In addition high complexity has been added to the tables to have a wider comparison even though it may be unnecessary to make a high complexity ASV. The main differences will be between non-proven high complexity (type B systems) and all other options regardless of non-proven and proven certification.

Table 6.2: The main differences between non-proven and proven technology during SAR documentation based on the SAR example in appendix D.

	Non-proven		**Proven**	
SAR chapter	**Low complexity**	**High complexity**	**Low complexity**	**High complexity**
| Abbreviations	-	-	-	-
|| References	-	-	-	-
||| Summary	-	-	-	-
1 Introduction	It will be minor differences between non-proven and proven technology. The main differences will be between high and low complexity components where high complexity has software and maybe diagnostics coverage.			
2 System description	Minor differences between non-proven and proven. There will be differences between high and low complexity systems			
3 System topology and block diagrams	Minor differences. The main differences will be related to the complexity of the system and different designs.			
4 Operational description	Minor differences. ASVs only have minor differences in operation but each vendor has their own way of describing it.			
5 Assumptions	Minor differences.			
6 Failure rate	λ_{DD} not included	λ_{DD} maybe included	λ_{DD} not included	λ_{DD} maybe included
7 Diagnostic coverage	DC normally not included	DC included if self testing systems available	DC normally not included	DC included if self testing systems available
8 Architectural constraints	Type A subsystem	Type B subsystem	Type A subsystem	Type B subsystem
	• SIL when considering HFT and SFF will be different in most cases.			
9 Common cause failures	Similar since both E-ASV and H-ASV has the same block diagram. Dependent on the considered system.			
10 Behaviour of system/ components on detection of fault	This will require detailed documentation for high complexity systems. It is normally sufficient with FMECA in low complexity systems since it does not include software. For proven in use or prior in use certified systems, this is normally documented in certification documentation.			
11 Mean time to repair	Leak test of control line not included		Leak test of control line included	
	• Minor differences in repair time between ASV designs.			

Table 6.3: The main differences between non-proven and proven technology during SAR documentation based on the SAR example in appendix D continues.

	Non-proven		**Proven**	
SAR chapter	**Low complexity**	**High complexity**	**Low complexity**	**High complexity**
12 Factory testing	Minor differences. Each vendor has their own FAT practice.			
13 Operational testing	Minor differences. Each vendor has their own test practice.			
14 Avoidance and control of systematic failures	Normally only human errors documented. No requirement for documentation of handling systematic failures.	Software and human error documentation. Handling of systematic failures must also be included.	No requirement for documentation of handling systematic failures.	
15 Software documentation	Not included	Included	Non included	Included
16 Results	Minor differences			

The following conclusions regarding SAR documentation can be drawn from the tables 6.2 and 6.3:

- One should consider to simplify a system until it can be considered low complexity since this is the only way of reducing documentation for new technology.
- If software is included, the system will be considered high complexity (type B system) which requires additional documentation.
- If the system is a high complexity (type B) system, one shall consider certifying it as either proven in use or prior use in order to achieve reduced documentation.
- If software and a diagnostics system is included, the diagnostics coverage must be documented atleast 60% in order to be used in a SIS.
- An non-proven E-ASV does not necessarily require additional documentation compared to a proven H-ASV as long as the E-ASV can be considered a low complexity system.

6.5 Challenges and Potential Improvements

OLF 070 is a guideline made to simplify the IEC61508 and IEC61511 standards. Yet, there are challenges and room for improvement. Based on the previous sections, challenges regarding definitions and practical use are found. Improvements are proposed for both IEC and OLF.

6.5.1 Definitions

Some definitions in IEC and OLF are poorly defined. Examples are definitions of "A-type" and "B-type" systems, proven in use and prior use, etc:

Type A and type B systems: A-type is defined as a subsystem where all possible failure modes can be determined for all constituent components. B-type is described as subsystems where behaviour under fault conditions cannot be completely determined for at least one component (e.g. a logic solver). Reference is made to IEC 61508-2 clause 7.4.

These terms are presented in the IEC standards which OLF 070 refers to. IEC has the responsibility of defining these terms but they do not do this sufficiently. However, OLF is made to simplify the IEC standards and should clarify these terms so there is no doubt about the meaning.

Common practice is to define systems that contain programmable logic solvers as B-type, while any other systems which do not include programmable logic solvers are defined as A-type. This is illustrated in table 6.4 which also is a proposal of improvement to the OLF 070 guideline.

Table 6.4: Definitions of A-type and B-type subsystems in common practice

Subsystem	**Description**
A-type	Subsystems where all possible failure modes can be determined for all components. Examples are: • Mechanical components • Hydraulic components • Electronics without programmable electronic (PE) components
B-type	Subsystems where behaviour under fault conditions cannot be completely determined for at least one component. Examples are: • Any system which includes PE components

Hardware fault tolerance: Another poorly defined item is the hardware fault tolerance numbers in table 8.2 and 8.3 in OLF 070 (See table 5.4 and 5.5). Instead of explaining these numbers, reference is made to IEC 61508-2 clause 7.4. A way of explaining these numbers are e.g. to define the numbers as HFT_i where $_i$ denotes the number. $HFT_i + 1$ = number of faults that could cause loss of safety function (Lundteigen and Rausand, 2008). E.g. if $HFT_i = 0$, one fault can cause loss of safety function.

IEC terminology: An issue with the IEC 61508 and IEC 61511 standards is that they are often hard to interpret and understand. An example is the difference between the terms proven in use and prior use. Exida, which among other services provides certification of SIS components, (See `http://www.exida.com/` for details) has concluded that:

> "Both the IEC 61508 and IEC 61511 proven in use requirements lack easy practical implementation." (Exida, 2004).

It seems like there are two different comities inside the IEC organisation which has defined the same terminology:

- IEC 61508 use the term proven in use for components which is certified as suitable for its use

- IEC 61511 use the term prior use for more or less the same certification

IEC 61511 is the sector specific standard for the process industry and may implement requirements from IEC 61508. It seems unnecessary to have two definitions of the same terminology and it is thus suggested to combine them or define clear differences between them.

It will be easier to use both the IEC standards and the OLF 070 guideline if these descriptions are properly defined.

6.5.2 Safe Failure Fraction (SFF)

It is sometimes a challenge to fulfil the requirements of SFF in table 8.2 OLF 070 for non-proven technology such as mechanical safety valves (type A). The SFF is used to determine the number of redundant components that is needed in order to achieve a given SIL. An increase in redundancy above normal quantity is undesired when developing new technology since one are competing with proven technology. There is often little to none available data for newly developed components and SFF may be hard to determine. Therefore, one has to assume a value based on FMECAs, generic data, etc. In many cases, most failure modes are safety critical and SFF (based on FMECA, etc.) is thereby low (below 60%). If the collected data have insufficient value of safe failures, it is normal to use the FMECA or vendor experiences to estimate additional safe failures to achieve SFF above 60%. An example is to add minor hydraulic leakages. This will increase the total failure rate, but also the SFF. SFF between 60 and 65% is considered a normal value for new technology. Questions about the SSF value are thereby avoided.

A possible solution is to lower the requirement from <0,6 to e.g. <0,5 for new technology. This will provide more accurate SSF numbers. If not, the industry is urged to continue to perform tricks to ensure that the SFF value is kept above 60%.

6.5.3 FMEA

OLF 070 section 8.5.2 describes FMEA as a suitable method when using reliability data from generic sources (such as the data in OLF 070 Table A1). This may be a source to uncertainties in practice because generic reliability data (as in OLF 070 Table A1) are average reliability data based on the same type of equipment but from many different designs and vendors. The reliability of the newly developed technology will most likely differ from the average reliability of this equipment. Therefore, in cases when developing new technology, an FMEA alone is a poor method and should be avoided.

A possible solution is to use generic data from e.g. OREDA in combination with expert judgements to correct the failure data. Based on experience and tests of the new technology, the generic failure data can be corrected to become more suitable for the actual component or system. The comment cell in an FMEA can be used for this purpose where corrections shall be recommended. One can also add a column for suggested correction.

An FMEA is also often performed in various ways. One expert may split the failure modes more than other experts do. Differences will appear when calculating reliability data based on these FMEAs. One is thus able to reduce or increase the reliability of the component based on how the failure modes are split.

An FMEA is described as mainly a qualitative analysis in Rausand and Høyland (2004) and other methods should probably be used instead. A better method has however, not been found due to the time limit and that other objectives have been prioritized. This can thus be regarded as remaining work.

Chapter 7

PFD Calculations

This chapter provides PFD calculations for all four configurations options provided in chapter 3. These calculations are used for providing an overall assessment of the safety function configurations. The method used to perform PFD calculations is Fault Tree Analysis (FTA).

7.1 Definition of Critical Event

The critical event in these cases is lift gas release to the environment from lower A-annulus reservoir in offshore topside oil production wells that utilizes gas lift. This is because the lower A-annulus has the biggest volume compared with the upper A-annulus and thus contains most of the lift gas (see section 7.2 for details).

7.2 Boundary Conditions

The task is limited to lift gas release from A- annulus reservoir. Blowout from reservoir is not taken into account. Neither are leakage to / from B-annulus and C-annulus.

Annulus reservoir is split by the ASV. Most of annulus reservoir is contained in the volume below the ASV (lower A-annulus). A smaller volume of lift gas is also kept in the volume above the ASV (upper A-annulus). This is illustrated in figure 7.1. Leakage through B and C annulus and through completion string is not included in these analyses. This leaves us with the ASV assembly, which represent the primary barrier, and AMV, M-SAS, tubing hanger, AAV, blind flanges, etc. representing the secondary barrier. There are thus two leakage scenarios:

1. **Leakage from lower A-annulus via upper A-annulus:** Leakage from lower A-annulus through ASV assembly via upper A-annulus. From upper A-annulus to the environment through one of the secondary barrier elements.

2. **Leakage from upper A-annulus only:** Leakage from upper A-annulus to the environment through one of the secondary barrier elements.

The analyses are limited to the first leakage scenario since most of the lift gas volume is contained inside the lower A-annulus. Some of the configuration options (option 2 and 4) do not include ASV and TOP event is thus gas release from annulus reservoir (both upper and lower A-annulus).

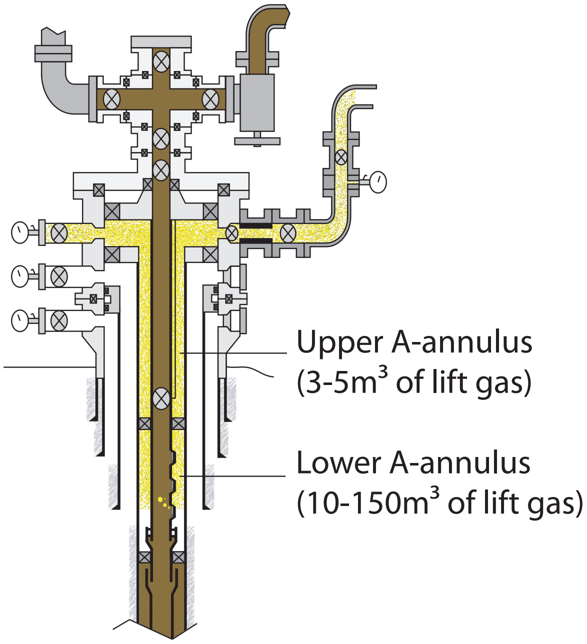


Figure 7.1: Upper and lower A-annulus volumes (Values are provided by ExproSoft AS).

The PFD calculations are performed using the A-annulus components which are needed to contain the A-annulus reservoir. Relevant components are:

- ASV packer

- ASV

- AAV
- AMV
- AWV
- M-SAS valve
- Blind flanges
- Pressure monitoring (monitoring)
- Tubing hanger
- WH connector
- Flow and gas lines (pipes)

It is assumed that the components are independent. To simplify the task and to reduce work, leak rates are not divided into levels in this study as it normally is in analysis performed by professionals. Note that some of the reliability data are provided from a database using specific filters for specific applications. These reliability data can thus not be used in other applications.

7.2.1 Scenarios

The FTAs are based on the gray area in the well barrier diagrams in chapter 3. Items outside that gray area are not taken into account. Two of the configurations in chapter 3 (option 1 and option 2) would have been almost identical if initial barriers was used in the PFD calculations. To get a wider variety in scenarios, the system PFD in option 2 (AMV after ASV failure) is calculated after failure of ASV, before M-SAS is inserted instead of ASV and AMV as in option 1. Note that since option 2 initially includes a spool flange for the M-SAS valve, M-SAS external leak has been added as a fault event.

7.3 Reliability Data

This section provides reliability data for each component in the FTAs. Reliability data are found in OREDA, OLF 070, PDS and Wellmaster Phase 5. Note that filter searches are performed for some of the data which means that the data cannot be used in other applications. Assumptions are also made for some of the components and suggested failure rates may differ from failure rates found in the databases. Note that repair times and test interval have been provided by ExproSoft AS.

The failure rate λ is calculated by equation (7.1) (Based on Rausand and Høyland, 2004, equation 2.38).

$$\lambda = \frac{\text{No.of failures}}{\text{Aggregated time in service}} = \frac{n}{t} \tag{7.1}$$

7.3.1 Gate Valves

Relevant gate valve failure modes in this study are: External leakage (EXL), Leakage in closed position (LCP) and Fail to close (FTC). LCP and FTC represent internal leakage (ITL). OREDA provides reliability data for gate valves. These are presented in table 7.1 and have a total time in service of 3 852 300 valve hours or 439,8 valve years.

Table 7.1: Reliability data for gate valves (ore, 2002)

Severity class	**Failure mode**	**No. of failures**
critical	External leak process medium	1
critical	Fail to close on demand	34
critical	Valve leakage in closed position	2
degraded	External leak process medium	8
degraded	External leak utility medium	6
degraded	Valve leakage in closed position	20
Total		71

Table 7.2 shows the failure modes and calculated failure rates from the gate valve reliability data table (table 7.1) using formula (7.1). These values are suggested to be used for relevant failure modes in the analyses.

Table 7.2: Failure modes and corresponding failure rates calculated using equation (7.1) and table 7.1.

Failure data source	**Failure mode**	**Failure rate (λ) (per 10^6 hours)**
OREDA	EXL	$3,890$
OREDA	FTC	$8,830$
OREDA	LCP	$5,710$

7.3.2 ASV

The ASV reliability data is based on WellMaster phase 5 which is provided by ExproSoft AS. A specific filter (not for general use) is used but the suggested EXL failure rate is based on table 7.2. The relevant failure modes are EXL, LCP and FTC. ASV ITL is represented by FTC and LCP together. It is assumed that EXL for ASV can be represented by 3% of the EXL for gate valves provided by OREDA. This is because it is assumed that it is a lower probability of EXL than ITL. The relevant failure modes with corresponding failure rates are given in table 7.3.

Table 7.3: Failure modes and corresponding failure rates of ASV

Failure mode	**Failure rate (λ) (per 10^6 hours)**	**Failure rate source**	**Failure observation**	**Test interval**	**Repair time**
FTC	$0,278$	WellMaster Phase 5	Testing	6 months	28 days
LCP	$0,209$	WellMaster Phase 5	Testing	6 months	28 days
FTC + LCP	$0,487$	WellMaster Phase 5	Testing	6 months	28 days
EXL	$0,117$	OREDA	Testing	6 months	28 days

7.3.3 AAV

The AAV is considered to have a ITL failure rate which is a bit better than the ASV since the flow through the AAV is less than flow through ASVs. It is thus suggested to use an ITL failure rate of 50% of ASV failure rate. EXL is assumed to be the same for both valves. The suggested failure rates for AAV is presented in table 7.4.

Table 7.4: Suggested failure rates for AAV

Failure mode	Failure rate (λ) (per 10^6 hours)	Failure rate source	Failure observation	Test interval	Repair time
ITL	$0,244$	WellMaster Phase 5	When occurring	NA	28 days
EXL	$0,117$	OREDA	Testing	NA	28 days

7.3.4 AMV and AWV

AMV and AWV failure rates are based on OREDA reliability data for gate valves (section 7.3.1). It is assumed that 2% of all EXL for gate valves are related to AMV and AWV. It is also assumed that 10% of gate valve FTC and LCP are related to AMV and AWV. The failure rates are presented in table 7.5. ITL is represented by LCP and FTC together.

Table 7.5: Failure modes and corresponding failure rates of AMV

Failure mode	Failure rate (λ) (per 10^6 hours)	Failure rate source	Failure observation	Test interval	Repair time
EXL	$0,0778$	OREDA	Testing	1 year	1 day
LCP + FTC	$1,454$	OREDA	Testing	1 year	1 day

7.3.5 M-SAS Valves

Data for the M-SAS valves has been found in WellMaster. Relevant failure modes are LCP and FTC. In addition, EXL for gate valves is used. It is assumed that EXL for M-SAS valves is the same as for AMVs and AWV. This is presented in table 7.6. ITL is represented by LCP and FTC together.

Table 7.6: Failure modes and corresponding failure rates of M-SAS valves

Failure mode	Failure rate (λ) (per 10^6 hours)	Failure rate source	Failure observation	Test interval	Repair time
EXL	$0,0778$	OREDA	Testing	1 year	7 days
LCP	$0,22$	WellMaster	Testing	1 year	7 days
FTC	$1,98$	WellMaster	Testing	1 year	7 days

7.3.6 ASV Packers

The reliability data for the ASV packer is taken from WellMaster 5. The relevant failure modes are leakage across packer (LAP) and premature release (PRL). Only LAP was found for ASV packers. The reliability data are shown in table 7.7

Table 7.7: Failure modes and corresponding failure rates for dual string ASV packers.

Failure mode	**Failure rate (λ) (per 10^6 hours)**	**Failure rate source**	**Failure observation**	**Test interval**	**Repair time**
LAP	$0,374$	WellMaster Phase 5	When occurring	6 months	28 days

7.3.7 Blind Flange and Spool Flange

There are little relevant reliability data available regarding blind flanges. The majority of such leaks are small and associated with start up. It is thus assumed that leakage from blind flanges and spool flanges can be represented by 2,5% of the EXL failure mode provided by OREDA. Suggested failure rate for use in the FTA is presented in table 7.8

Table 7.8: Suggested failure rate of blind flanges and spool flanges

Failure mode	**Failure rate (λ) (per 10^6 hours)**	**Failure rate source**	**Failure observation**	**Test interval**	**Repair time**
Leakage	$0,0973$	WellMaster Phase 5	Testing	1 year	1 day

7.3.8 Pressure Monitoring

According to the PDS handbook, pressure transmitters have a mean dangerous undetected failure rate of $0,3$ per 10^{06} hours (see Hauge and Onshus (2010)). But this is electrical equipment which provides input to a logic solver. In this case, we are looking for reliability data of also manual/analogue equipment. It is thus suggested to use 30% of the leak probability in PDS handbook. This i presented in table 7.9.

Table 7.9: Suggested failure rate of pressure monitoring

Failure mode	Failure rate (λ) (per 10^6 hours)	Failure rate source	Failure observation	Test interval	Repair time
Leakage	$0,1$	PDS Handbook	When occurring	NA	1 day

7.3.9 Tubing and Casing Hanger Seals

The relevant failure modes for tubing and casing hanger in this analysis are tubing to annulus communication (TAC) and other (OTH). WellMaster Phase 5 using a specific filter search (not for general use) is used to provide reliability data. This is shown in table 7.10.

Table 7.10: Suggested failure rates of Tubing and casing hangers

Failure mode	Failure rate (λ) (per 10^6 hours)	Failure rate source	Failure observation	Test interval	Repair time
TAC + OTH	$0,135$	WellMaster Phase 5	Testing	1 year	28 days

7.3.10 Flow and Gas Lift Line (Pipes)

It is likely that leakage through flow and gas lift lines will be different from well to well because each well has differences in line length, type of valves, number of valves, etc. It is thus hard to come up with a representative value. Based on a filter search in WellMaster Phase 5, a failure rate is suggested. This is presented in table 7.11.

Table 7.11: Suggested failure rates of flow and gas lift lines

Failure mode	Failure rate (λ) (per 10^6 hours)	Failure rate source	Failure observation	Test interval	Repair time
Leakage	$0,300$	WellMaster Phase 5	when occurring	NA	1 day

7.3.11 Wellhead Connector

OREDA (ore (2002)) has been used as a source for reliability data for WH connectors. Relevant failure mode is External leakage - process medium (ELP). OREDA does not provide detailed reliability data and mean failure rate has thus been used. Repair time is provided by Exprosoft. Suggested reliability data is presented in table 7.12.

Table 7.12: Suggested failure rates for wellhead connectors (ore (2002))

Failure mode	**Failure rate (λ) (per 10^6 hours)**	**Failure rate source**	**Failure observation**	**Test interval**	**Repair time**
ELP	$0,0857$	OREDA	Testing	1 year	7 days

7.4 Fault Tree Analysis (FTA)

A fault tree is a logic diagram that displays the connections between a potential system failure (TOP event) and the causes (Basic events) for the failure. FTAs are conducted for the four configuration options shown in chapter 3. This is done to calculate the PFD and thereby do an overall assessment of the configurations based on the results. According to Rausand and Høyland (2004), a fault tree is carried out by the following five steps:

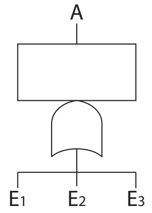
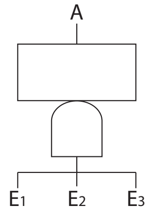
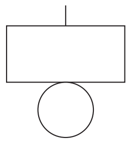
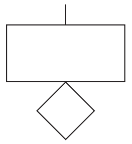
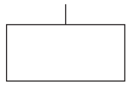
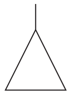
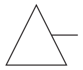
1. Definition of problem and boundary conditions
2. Construction of the fault tree
3. Identification of minimal cut sets (described further in section 7.4.3
4. Quantitative analysis of the fault tree
5. Qualitative analysis of the fault tree

Step 1 is done in section 7.1 and 7.2. Step 2 is presented in appendix E by utilizing the CARA Fault Tree software. Step 3 - 5 are performed by the software using the reliability data provided in section 7.3. The cut sets are listed in appendix E.3 and the result is presented in section 7.5 along with an overall assessment of the configurations.

7.4.1 Symbols

Table 7.13 lists and describes the symbols used in the FTAs.

Table 7.13: Fault tree symbols (Rausand and Høyland, 2004)

Type	Symbol	Description
Logic gates	OR-Gate 	The OR-gate indicates that the output event A occurs if any of the input events Ei occur.
	And-Gate 	The AND-gate indicates that the output event A occurs only when all the input events Ei occur simultaneously.
Input events	Basic event 	The basic event represents a basic equipment fault or failure that requires no further development into more basic faults or failures.
	Undeveloped event 	The undeveloped event represents an event that is not examined further because information is unavailable or because of insignificant consequences.
Description	Comment rectangle 	The comment rectangle is for supplementary information.
Transfer symbols	Transfer out  Transfer in 	The transfer out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer in symbol.

7.4.2 Basic Events

According to the CARA Fault Tree software, there are four types of basic events which can be used in the FTA:

- Test interval
- Repairable
- Non-repairable
- On demand

All basic events in this thesis are of either test interval or repairable basic events since both test intervals and repair times are available or assumed for most components. Some of the components such as AAV, pressure monitoring equipment, and the gas and flow lines are not tested regularly. Since test interval is not available for these components, they are assumed repairable. Information about the relevant basic events are provided by ExproSoft AS and listed below:

Test Interval

Test interval is used to describe components that are tested periodically with test interval t. A failure may occur anywhere in the test interval. The failure will, however, not be detected until the component is needed or the test is carried out. The failure rate λ (expected number of critical failures per hour), the test interval t (in hours) and the repair time τ (in hours) are the entered reliability parameters. CARA Fault Tree calculates the PFD by the formula (7.2).

$$q_i(t) \approx \frac{\lambda t}{2} + \lambda \tau \tag{7.2}$$

Note that formula (7.2) is only valid if independent testing of each component is performed. Therefore, this formula will not be correct if components are tested simultaneously or if staggered testing is done. The result will then be too optimistic. Since the test-interval and time of tests generally are known parameters and not independent, this restriction in the program is compensated for by re-defining the tested barriers as repairable items with an increased critical repair time of half the test interval (shown in formula (7.3)).

$$q_i(t) \approx \frac{\frac{t}{2} + MTTR}{\frac{t}{2} + MTTR + MTTF} \tag{7.3}$$

The mean safety critical downtime will in this case be the sum of half of the test interval and mean time to repair ($MTTR$).

Repairable

Repairable is used for components that are repaired when failure occurs. The components are tested periodically with the test interval t (in hours). A failure may occur anywhere in the test interval. The failure will, however, not be detected until the test is carried out or the component is needed. The probability $q_i(t)$ is in this situation often referred to as the PFD or unavailability. The failure rate (λ) is the expected number of critical failures per hour. The mean time to repair (MTTR) is denoted τ (in hours). MTTR is also the mean repair time. $q_i(t)$ may be calculated by the formula (7.4).

$$q_i(t) = \frac{\lambda\tau}{1+\lambda\tau}(1 - e^{1-\frac{(1+\lambda\tau)t}{\tau}}) \tag{7.4}$$

By letting t tend to infinity, we obtain the well-known approximation which is shown in equation (7.5).

$$q_i(t) = \frac{\text{MTTR}}{\text{MTTR} + \text{MTTF}} \tag{7.5}$$

where

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

The reliability parameters entered to the CARA software are λ (expected number of failures per hour) and MTTR (in hours).

7.4.3 Cut Set

A combination of fault events that will lead to a TOP event is called a cut set. In FTAs, a cut set is defined as:

> "...a set of basic events whose occurrence (at the same time) ensures that the TOP event occurs." (Rausand and Høyland, 2004).

The CARA Fault Tree software can analyse and present the cut sets in fault trees. However, the cut sets presented are called minimal cut sets. A minimal cut set is defined as a cut set that cannot be reduced without losing its status as a cut set. The order of the cut set is defined as the number of the basic events in a minimal cut set.

In small fault trees, it is possible to identify the minimal cut sets by inspection. In larger fault trees, this is not possible without an efficient algorithm (see Rausand and Høyland, 2004, section 3.6.4).

7.4.4 Upper Bound Approximation

The CARA Fault Tree software uses upper bound approximation to calculate the unavailability of the system (TOP event). Upper bound approximation is considered to be a conservative method since it uses the minimal cut sets of the fault tree to calculate unavailability. If the basic events are assumed to be independent, the upper bound approximation can be expressed by the formula (7.6) (See Rausand and Høyland, 2004, equation 4.47), where $q_i(t)$ denote the probability that basic event i occurs at time t and $\overset{\vee}{Q}_j(t)$ denote the probability that minimal cut set j fails at time t.

$$\overset{\vee}{Q}_j(t) = \prod_{i \in K_j} q_i(t) \tag{7.6}$$

The CARA Fault Thee software uses another formula which is used when all the $q_i(t)$s are small. This is formula (7.7). Note that $Q_0(t)$ denote the system failure.

$$Q_0(t) \approx 1 - \prod_{j=1}^{k} (1 - \overset{\vee}{Q}_j(t)) \tag{7.7}$$

Formula 7.7 has to be used with care when atleast one of the $q_i(t)$s is of order 10^{-2} or larger (Rausand and Høyland (2004)).

7.5 Overall Assessment of Safety Function Configurations

The fault trees in appendix E are used to quantify the probability of lift gas release from annulus reservoir for all configurations options in chapter 3. Limitations are listed in section 7.2. Option 1, which is the conventional annulus safety configuration using ASV and AMV as barrier elements, is used as base case. This means that the other configurations are compared to option 1. The various configurations are listed in table 7.14.

Table 7.14: List of the various configuration options

Option:	**Components:**	**Description:**
1 (Base case)	ASV + AMV	Initial barrier elements
2	AMV	After ASV failure before M-SAS is inserted
3	ASV + AMV + M-SAS	Initial barrier elements
4	AMV + M-SAS	Initial barrier elements

7.5.1 FTA Results

The result from the FTAs are presented in table 7.15 and in figure 7.2, and act as a base line for further analyses. Note that logarithmic scale is used in figure 7.2.

Table 7.15: Overall assessment of the safety configurations **(Base line)**

Well design	**PFD**	**Relative base case**	**Relative option 2**
Option 1: ASV + AMV **(Base case)**	$2,40E^{-06}$	1,00	
Option 2: AMV after ASV failure	$8,52E^{-04}$	355,32	1,00
Option 3: ASV + AMV + M-SAS	$1,45E^{-06}$	0,60	
Option 4: AMV + M-SAS	$5,17E^{-04}$	215,44	0,61

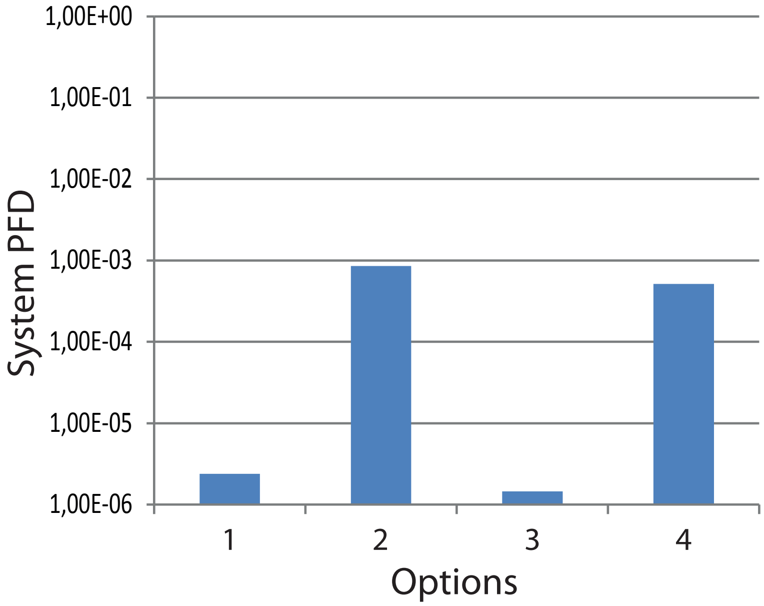


Figure 7.2: The result of the PFD calculations for each option **(Base line)**

The result shows that the configuration, which includes three barriers (option 3), is the most reliable. The second most reliable configurations are the ones that include two barriers (option 1 and 4). The option that only includes one barrier has the poorest reliability (option 2). This was as expected.

The result also shows that the configurations using M-SAS valves (option 3 and 4) are slightly more reliable than the configurations without (option 1 and 2). This indicates that the M-SAS valve does not contribute significantly to the reliability of the system. When comparing option 2 (AMV) with option 1 (ASV + AMV) and option 4 (AMV + M-SAS) the result shows minor differences between option 2 and 4 compared to option 2 and 1. This is another indication of low system reliability contribution for the M-SAS valve.

The low system reliability contribution is hard to believe since configurations that utilize M-SAS valves are approved by OLF as alternative to ASV configurations. Further investigation is thus performed (see subsection 7.5.2).

If the result in figure 7.2 and table 7.15 is final, the following recommendations can be drawn from the result:

- All configuration options except for option 4 are recommended to be used in offshore topside gas lift applications. Note that option 2 initially includes an ASV and can therefore be recommended. Option 4 is not recommended since it represents almost the same system PFD as option 2 (AMV after ASV failure).

- An configuration using only AMV as barrier element (represented by option 2) should be avoided because of high system PFD compared to option 1 and 3.
- ASVs are preferred before M-SAS valves

7.5.2 Sensitivity Analysis

The result (base line) showed a low system reliability contribution from the M-SAS valve. This is hard to believe due to approval of the configuration from OLF. Sensitivity analyses are conducted for further investigation:

A series of assumptions was made when developing reliability data and this can be a source to uncertainties. A sensitivity analysis is conducted for M-SAS valves, AMV and ASV for base line to compare the criticality of the barrier elements. This is presented in table 7.16.

Table 7.16: System PFD when using different failure rates for M-SAS, AMV and ASV

	2 · M-SAS failure rate		**20 · M-SAS failure rate**	
Option:	**PFD**	**Relative base line**	**PFD**	**Relative base line**
1 ASV + AMV	$2,40E^{-06}$	1,00	$2,40E^{-06}$	1,00
2 AMV	$4,69E^{-03}$	5,51	$4,70E^{-03}$	5,51
3 ASV + AMV + M-SAS	$1,48E^{-06}$	1,03	$5,03E^{-06}$	3,48
4 AMV + M-SAS	$5,30E^{-04}$	1,03	$1,80E^{-03}$	3,48
	2 · AMV failure rate		**20 · AMV failure rate**	
Option:	**PFD**	**Relative base line**	**PFD**	**Relative base line**
1 ASV + AMV	$3,37E^{-06}$	1,41	$2,08E^{-05}$	8,66
2 AMV	$1,19E^{-03}$	1,40	$7,33E^{-03}$	8,60
3 ASV + AMV + M-SAS	$1,45E^{-06}$	1,01	$1,63E^{-06}$	1,13
4 AMV + M-SAS	$5,20E^{-04}$	1,01	$5,82E^{-04}$	1,13
	2 · ASV failure rate		**20 · ASV failure rate**	
Option:	**PFD**	**Relative base line**	**PFD**	**Relative base line**
1 ASV + AMV	$4,79E^{-06}$	2,00	$4,74E^{-05}$	19,78
2 AMV	$8,52^{-04}$	1,00	$8,52E^{-04}$	1,00
3 ASV + AMV + M-SAS	$2,89E^{-06}$	2,00	$2,86E^{-05}$	19,78
4 AMV + M-SAS	$5,17E^{-04}$	1,00	$5,17E^{-04}$	1,00

Table 7.16 shows that the ASV contribute much more to the system reliability than the M-SAS valve and the AMV. If the failure rate of the ASV is doubled, the system PFD is doubled, and if the failure rate of the ASV is multiplied with 20, the system PFD is multiplied with almost 20. The M-SAS valve and AMV makes minor changes to the system PFD when the failure rates are changed. A higher system PFD contribution is expected from the M-SAS valve since it is recommended as an alternative configuration to the conventional configuration (option 1). The reason for the result may be that the M-SAS valve is located on the same branch as the AMV in the fault trees. There are also alternative leakage paths (through the tubing hanger or via AAV) to the leakage path through the M-SAS valve. It is suspected that the alternative leakage paths contribute so much to the system PFD that changes in M-SAS valve failure rate, only brings minor changes to system PFD.

7.5.3 Suggested System Improvements

It is expected to be more similarity between the options using two barrier elements (option 1 and 4). Two reasons are suspected to be the cause of the unexpected result.

- There are errors (either in the fault trees or in the failure rates used).
- The M-SAS valve does not contribute significantly due to low reliability in a nearby fault tree branch.

The cut sets for each tree (listed in appendix E) indicate that the open AAV can be a source to the low contribution of system reliability by the M-SAS valve. This is because the AAV is included in many of the lowest order minimal cut sets. By looking at the well barrier schematics in chapter 3 or the fault trees in appendix E, one can see that the path through the AAV has only one barrier in addition to the primary, while the others have two.

M-SAS Valve as AAV

The AAV is a manual valve which is kept open all the time except for when the blind flange or pressure monitoring is replaced. It has to be kept open in order to monitor the annulus pressure. A solution can be to close the AAV when a demand occurs in order to increase the system reliability. This may be hard to do in practice since the AAV is manual. It is thus instead suggested to use an M-SAS valve as an AAV. The additional M-SAS valve can be connected to the SIS and automatically close on demand. New fault trees are developed (see appendix E.4) and the result is presented in table 7.17 and in figure 7.3. Note that logarithmic scale is used in figure 7.3.

Table 7.17: Overall assessment of the safety configurations when M-SAS valve is used as AAV

Well design	**PFD**	**Relative base case**	**Relative option 2**
Option 1: ASV + AMV **(Base case)**	$9,95E^{-07}$	1,00	
Option 2: AMV after ASV failure	$7,09E^{-04}$	712,97	1,00
Option 3: ASV + AMV + M-SAS	$4,21E^{-08}$	0,04	
Option 4: AMV + M-SAS	$1,50E^{-05}$	15,12	0,02

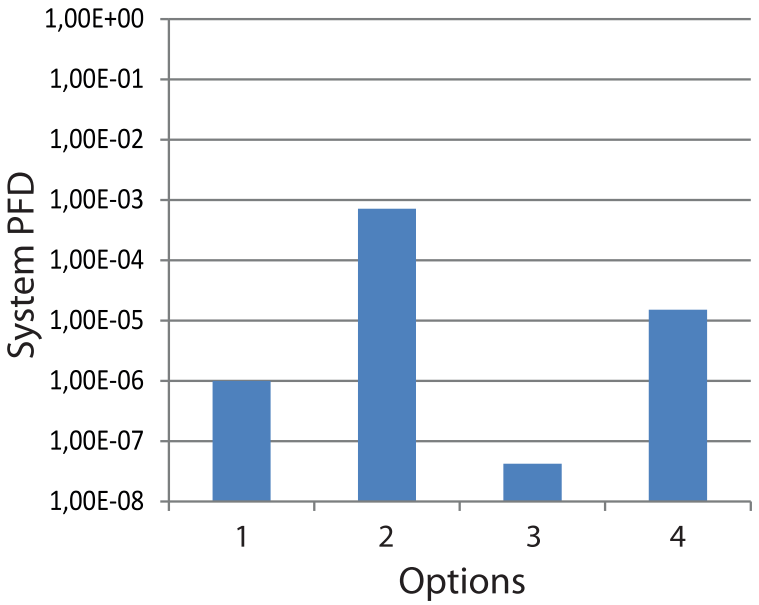


Figure 7.3: The result of the PFD calculations for each option when M-SAS valve is used as AAV

The result shows a significant improvement compared to base line: If option 2 (AMV after ASV failure) is compared to option 4 (AMV + M-SAS), option 2 is almost 50 times worse than option 4. Option 1 and 4 has become more similar as well. The results are good, but the suggested improvement can probably not be used in practise since the pressure monitoring has to be used all the time. If the suggested improvement was used regardless of the pressure monitoring, the following recommendations can be drawn from the results:

- All four configuration options (represented by option 1, 3 and 4) are recommended to be used in offshore topside gas lift applications. Note that option 2 initially includes an ASV and can therefore be recommended.

- A configuration using only AMV as barrier element (represented by option 2) should be avoided because of high system PFD compared to the other configuration options.
- Option 4 provides high system availability compared to option 2 and is considered an alternative to option 1 if 15,12 times higher unavailability is sufficient.
- Option 3 will improve system availability compared to the conventional configuration (option 1).
- Option 2, 3 and 4 provides advantages such as reduced risk, cost and time-consumption (see chapter 3 for details) when performing maintenance since the M-SAS valve is used.

Improvement of Failure Rates

The small system PFD contribution of the M-SAS valve can probably be caused by the small differences in reliability between the basic events in the "Release via AAV" fault tree branch (Blind flange, pressure monitoring and AAV external leak) and the other components (M-SAS, AMV, ASV, etc.). This leaves us with three options:

1. **Change failure rates** Prove either lower failure rate on blind flange, pressure monitoring and AAV, or higher failure rate on the other components in the tree.
2. **Change the system** Change the system by adding or reducing components. The highest effect in this option will probably be to include an and-gate in the "Release via AAV" fault tree branch so the failure rates below will be multiplied with each other (This is done when an M-SAS is used as AAV).
3. **A combination of the above**

A change in the basic event failure rates in the "Release via AAV" fault tree branch is done since the second option is already tried. The failure rates of AAV external leak, blind flange and pressure monitoring are multiplied with 0,1. The result is presented in table 7.18 and in figure 7.4. Note that logarithmic scale is used in figure 7.4.

Table 7.18: Overall assessment of the safety configurations when failure rates of AAV external leak, blind flange and pressure monitoring are multiplied with 0,1

Well design	PFD	Relative base case	Relative option 2
Option 1: ASV + AMV **(Base case)**	$1,11E^{-06}$	1,00	
Option 2: AMV after ASV failure	$3,94E^{-04}$	355,21	1,00
Option 3: ASV + AMV + M-SAS	$1,63E^{-07}$	0,15	
Option 4: AMV + M-SAS	$5,82E^{-05}$	52,47	0,15

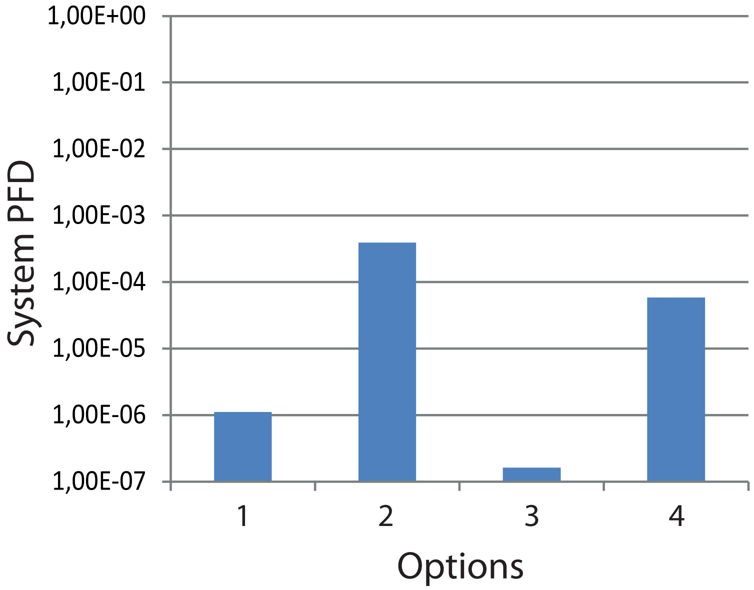


Figure 7.4: The result of the PFD calculations for each option when failure rates of AAV external leak, blind flange and pressure monitoring are multiplied with 0,1

The result is not as good as the result when using M-SAS as an AAV, but it improved the system PFD contribution of M-SAS valve compared to base line for option 4. It will however be hard to prove lower failure rates than done in this case and this is thus not suggested as a good solution to the problem. This problem has not been investigated further due to lack of time and higher priority of other topics. It can thus be regarded as remaining work.

Chapter 8

Summary and Recommendations for Further Work

This final chapter sums up what is done and what the result shows. The result is discussed and recommendations for future work are given.

8.1 Summary and Conclusions

The overall objective was to describe the steps components need to go through in order to be a part of a safety function. All the objectives stated in section 1.2 are more or less answered.

Basic information about relevant well type, well equipments, gas lift and well barriers is provided in chapter 2. Special requirements are provided for some of the WBEs in this chapter.

Four annulus barrier configurations for gas lift systems are found and described in chapter 3. Their maintenance strategies are briefly described and general advantages and disadvantages are listed. Well barrier diagrams and well barrier schematics are also provided for each configuration. The well barrier diagrams are used in the PFD calculations in chapter 7.

Important terms regarding annular safety are briefly explained in chapter 4. This includes safety instrumented system (SIS) and safety instrumented function (SIF). An example is used to illustrate the relation between these terms and annulus safety.

Requirements regarding annulus safety systems are provided in chapter 5. This chapter starts off with governing regulations regarding barriers in both Norway and the United States of America. The main difference between these governing regulations is that Norway requires two WBEs in annulus, while USA requires only one. Norwegian requirements open up for alternative configurations to the conventional one if acceptable risk and safety can be documented. Requirements regarding SIS for annulus well barriers in Norway follow. According to OLF, there are three main requirements that need to be fulfilled in order to achieve a given SIL. Required documentation for SIS components is described. This includes the SRS and the SAR. The SAR content varies from whether the component is proven or non-proven. Recommendations for SIS project phases and information regarding responsibility according to OLF are also provided in this chapter.

Descriptions of the safety analysis report (SAR) processes are provided both for non-proven and proven technology in chapter 6. This is also the third objective. This is done by making flowcharts based on the OLF 070 guideline. A hydraulically operated ASV is used as proven technology and an electrically operated ASV is used as non-proven technology. SAR examples for proven and non-proven technology are made and used for comparison. Challenges regarding the SAR process are pointed out and discussed. Potential improvements to the OLF 070 guideline and to the IEC standards are also proposed. Examples are poor definitions of terms and practical problems regarding SFF and methods for acquiring reliability data.

PFD calculations for the safety configuration options are performed in chapter 7. These are provided by using reliability data found in OREDA, WellMaster and other databases, and the well barrier schematics and diagrams given in chapter 3. The PFD calculations were performed using the CARA fault three analysis software.

An overall assessment of the safety function configurations is performed in chapter 7. This is done based on the PFD calculation results. The result was unexpected and shows that only three of the options can be recommended. The result indicates poor reliability for the alternative configuration compared to the conventional. This was also unexpected since the alternative configuration is recommended by OLF 070. Another unexpected feature with the result is that the option with three barrier elements has slightly better reliability than the most used gas lift configuration which only includes two barriers. A significant difference is expected here.

Sensitivity analyses was conducted and showed low system reliability contribution of the M-SAS valve. The blind flange, pressure monitoring and AAV are reviled as system weaknesses. An improvement is proposed involving replacing the AAV with an M-SAS valve to improve the secondary barrier. The suggested improvement proves increased system reliability which results in recommendation of all four configurations options. A specified configuration is recommended not to be used. However, the suggested improvement may not be used in practise due to blocking of a monitoring device. Another improvement is suggested and analysed. This involves improving the components that is included in the weak part of the system. The suggested improvement shows minor changes in system PFD compared to the first suggestion and is thus discarded.

8.2 Discussion

In chapter 3 the various gas lift configuration options are listed. In option 2 and 3, ASV retrieval (workover) may be required regardless if the ASV is stuck in closed position. If this happens, the whole intention with the M-SAS valve will be wasted since the main advantage is to do a light intervention (inserting the M-SAS valve) and thus avoid risky and time-consuming workover. It is, however, possible to force the ASV open by pumping gas down towards the flapper or by lowering a pipe down to the flapper and thereby push it open. The SIS will be functioning as long as the A-annulus can be closed by the M-SAS and AMV. Gas lift during production will also be possible as long as the ASV is kept open.

Whether or not the ASV has to be retrieved if it is stuck in closed position, has not been investigated any further due to limited time. This can thus be added to remaining work. The possibility of having the ASV stuck in closed position is most likely very small. Such an event can be caused by control line leakage or severe mechanical damage. The latter may result in a mandatory retrieval of the ASV if the ASV is not possible to force open.

The PFD calculations were performed by making fault trees in the CARA fault tree analysis software. The result shows small improvements to the system when the M-SAS valve is used. There are also major differences when ASV and AMV (option 1) is used compared to when an AMV and an M-SAS (option 4) is used. A low contribution to the system PFD is found for the M-SAS valve. The improvements proposed helped but was disregarded due to practical problems. Other suggestions such as larger changes in the system are not investigated any further due to lack of time.

The reason for the result can be related to lack of experience if the fault trees include errors. The system could have been misunderstood and thereby caused faulty fault trees. It is possible that an expert would have done the FTAs differently. However, experts had a look at the fault trees and provided tips, but without major improvements.

The reliability data which was used in the FTAs may be a source of uncertainty and can also be the reason for the problem. These were mainly found in old OREDA versions and in WellMaster Phase 5. Newer versions of these databases are available but were not used due to restricted access. Different results may have been obtained if these newer databases were used.

Some of the reliability data were assumed due to lack of relevant data. These data may be available elsewhere and could have changed the result. If errors in reliability data are the cause to the problem, the result in chapter 7 is a good example of why quality assurance of the reliability data is important.

8.3 Recommendations for Further Work

This thesis was carried out within a limited period of time and it is recommended that the findings are explored further. Remaining work are mainly PFD calculations and overall assessment of the configurations. There are also more challenges and potential improvements that can be done in OLF 070.

PFD Calculations

The PFD calculations performed in chapter 7 are based on databases such as OREDA and WellMaster. These are old databases and newer reliability data would be better to use and would probably enhance the result. Some of the reliability data used was assumed since no data was available. This may be obtained if more time and other databases were available. The fault trees may also be a source to uncertainties since they have been performed by a student.

The task is also limited to gas release from annulus reservoir. This could be extended to include blowout from reservoir. More components must then be included and the analysis will be more extensive. Problems regarding the PFD calculation can be regarded as anywhere from short to long term work classification.

Improvements to the System

Work can be done in order to improve the annulus safety systems, especially if the fault trees in chapter 7 are found without errors. Good improvements may require a lot of work but suggestions may not. Further work regarding system improvement is considered short to medium term work classification.

Challenges and Improvements of OLF 070

Only a few challenges related to OLF 070, IEC and the safety analysis report (SAR) process were pointed out due to limited time and lack of experience. More potential improvements to the OLF 070 can be found if one or several more experienced person(s) are available. Interviews with experienced persons can be arranged to obtain more proposals of improvements to the OLF 070 guideline. One can also study IEC and OLF further to acquire the knowledge needed. Working with these standards is difficult and requires a lot of time. This work is thus considered as long term work.

Improving OLF and IEC

The challenges and improvements regarding OLF and IEC presented in this thesis can be developed further. Clear definitions of the various terms shall be defined and there are many which are interested in simplified standards. More knowledge and experience are then required. This is considered short to long term work, dependent on how much improvement that should be done.

Failure Rates for New Technology

Alternative ways of developing failure rates for new technology can be suggested. FMEA, FMEDA, expert judgements and other methods can be investigated in order to find the best method. This will require knowledge about the various methods available today. This is considered medium to long term work classification.

Retrieval of ASV in M-SAS Configurations

Potential future work is to investigate the likelihood of a mandatory retrieval of the ASV in configurations that utilizes M-SAS valves. This is also discussed in section 8.2. If the likelihood of having the ASV stuck in closed position is high, the M-SAS configurations may not be recommended regardless of system reliability. This is considered short term work.

Appendix A

Acronyms

AAV Annulus access valve

AMV Annulus master valve

API American Petroleum Institute

ASV Annulus safety valve

AWV Annulus wing valve

BSEE Bureau of Safety and Environmental Enforcement

BOP Blowout preventer

DHSV Downhole safety valve

E-ASV Electrically operated annulus safety valve

E-DHSV Electric operated downhole safety valve

E/E/PE Electric/Electronic/Programmable Electronic

ELP External leakage - process medium

ESD Emergency shutdown

ESP Electronic submersible pump

EUC Equipment under control

EXL External leakage

FMEA Failure mode and effect analysis

FMECA Failure mode, effect and criticality analysis

FTA Fault Tree Analysis

FTC Fail to close

FSN Fail to set in nipple

FSV Flow safety valve

FTA Fault tree analysis

FTC Fail to close on command

GLV Gas-lift valve

H-ASV Hydraulically operated annulus safety valve

HAZOP Hazard and operability study

HFT Hardware fault tolerance

IEC International Electrotechnical Commission

ITL Internal leakage

KV Kill valve

LAP Leakage across packer

LCP Leakage in closed position

M-SAS Modular surface annular safety

OLF Oljeindustriens Landsforening

OREDA Offshore Reliability Data

OTH Other

PFD Probability of failure on demand

PMV Production mater valve

P & ID Piping and identification

PE Programmable Electronic

PSA Petroleum Safety Authority Norway

PSV Production swab valve

PTC Petroleum Technology Company

PWV Production wing valve

QA Quality assurance

QRA Quantitative risk assessment

SAR Safety analysis report

SCSSV Surface-controlled subsurface safety valve

SIF Safety instrumented function

SIL Safety integrity level

SIS Safety instrumented system

SPM Side pocket mandrel

SRS Safety requirement specification

SSF Safe failure fraction

TAC Tubing to annulus communication

TR Tubing retrievable

USA The United States of America

VR Valve removal

WBE Well barrier element

WH Wellhead

WP Working pressure

MEDP Maximum expected differential pressure

XMT X-mas tree or production tree

Appendix B

Detailed SRS Content

This is a detailed description of the SRS content (adopted from ConocoPhillips, 2013a, table 1-2).

ID	Reference to IEC 61511, Chapter 10.3	Comments	SRS version
1	A description of all the safety instrumented functions necessary to achieve the required functional safety	Identified safety functions are listed in SIL identification and allocation report /6/. Detailed description of each function is described in the system SRSs.	Version 1
2	Requirements to identify and take account of common mode failures	General description in OLF 070 to be used generally in all SRS'S	Version 2
3	A definition of the safe state of the process for each identified safety instrumented function	Evaluated in SIL identification and allocation report /6/. Further details in system SRS.	Version 1
4	A definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system)	Planned included as a check point for HAZOP. Possible feedback to be documented in SRS.	Version 2
5	The assumed sources of demand and demand rate on the safety instrumented function	The assumed source of demand and demand rate are based on OLF 070 i.e. assuming low demand mode of operation. For functions not covered by OLF 070 further details are found in system SRS.	Version 1

ID	Reference to IEC 61511, Chapter 10.3	Comments	SRS version
6	Requirement for proof-test intervals	As specified in COP document TCD 5048/9/. A review of test interval in order to optimize could be performed in compliance calculations indicate compliance with SIL requirements.	Version 1
7	Response time requirements for the SIS to bring the process to a safe state	Information found in various data sheets as well as design philosophy documents. The requirements are more detailed in the system SRS. Documents specifying fulfilment of requirement is referred to in the system SRS.	Version 2
8	The safety integrity level and mode of operation (demand/continuous) for each safety instrumented function	Found in SIL allocation Report and specified for each function in the system SRS. The default mode of operation is default low demand if not otherwise specified in system SRS.	Version 1
9	A description of SIS process measurements and their trip points	Information found on P& ID, SCD or data sheets. Relevant information referred to in system SRS.	Version 3
10	A description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves	Information found in Cause & Effect sheets, SCD, and ESD Block Logic. Relevant information referred to in system SRS.	Version 3
11	The functional relationship between process input and outputs, including logic, mathematical functions and any required permissive	Information found in Cause & Effect sheets, SCD, and ESD Block Logic. Relevant information referred to in system SRS and illustrated with reliability block diagram for function "typical" in system SRS.	Version 2
12	Requirements for manual shutdown	Information found in general design philosophy documents. Will be referred to in SRS if relevant.	Version 2

ID	Reference to IEC 61511, Chapter 10.3	Comments	SRS version
13	Requirements relating to energise or deenergise to trip	To be evaluated case by case. Fail-safe principles to be evaluated (e.g. deluge valve).	Version 2
14	Requirements for resetting the SIS after a shutdown	Information found in operations manual. Specific requirements are identified in system SRS.	Version 2
15	Maximum allowable spurious trip rate	To be evaluated case by case. Important with logging of statistics during operations. As a guideline parts of a SIF should have a MTTFST > 5 years.	Version 2
16	Failure modes and desired response of the SIS (for example, alarms, automatic shutdown)	Information found in SAR and Operation manuals	Version 2
17	Any specific requirements related to the procedures for starting up and restarting the SIS	Information found in operations manual. Will be referred to in system SRS.	Version 2
18	All interfaces between the SIS and any other system (including the control system and operators)	To be considered in connection with manual systems. Information found in System Engineering Manual... Relevant system interfaces are specified in system SRS.	Version 2
19	A description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode	Information found in Operations manual. The identified safety functions shall be designed to function in all modes of operation, unless otherwise specified.	Version 3

ID	Reference to IEC 61511, Chapter 10.3	Comments	SRS version
20	The application software requirements	All software to be documented in accordance with check lists in IEC 61508 Part 3. It shall also be documented as part of the SAR to be issued by relevant Suppliers. Documentation of compliance to software requirements to be referred to in the final SIL compliance documentation (i.e. in the relevant system SRS) to be issued prior to end of detail engineering phase.	Version 2
21	Requirements for overrides/inhibits/bypasses including how they will be cleared	Information found on P & ID and SCD. As a general requirement the safety functions shall not be bypassed unless risk reducing measures that equal the risk reduction by the SIF are implemented.	Version 2
22	The specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors	Information found in test procedures and operations manuals and on SCD	Version 2
23	The mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints	Information found from maintenance program and spare part program. However the assumption as that in a bypass/override of a safety function for maintenance, compensating measures are implemented that equals the risk reduction performed by the SIF.	Version 3
24	Identification of dangerous combinations of output states of the SIS that need to be avoided	Included as a checkpoint for HAZOP to be included in system SRS if identified.	Version 2

ID	Reference to IEC 61511, Chapter 10.3	Comments	SRS version
25	The extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radio frequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lighting, and other related factors	Information found in Design basis and COP specifications. To be referred to in system SRS.	Version 2
26	Identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (e.g. equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions maybe required to support these modes of operation	Information based on Design basis and specifications	-
27	Definition of the requirements for any safety instrumented function necessary to survive a major accidental event, for example, time required for a valve to remain operational in the event of a fire	Information found in vulnerability considerations in connections with the risk analysis (QRA). Specific requirements for survivability to be specified in system SRS. In general all SIFs shall be designed according to the design accidental loads.	Version 2

Appendix C

Detailed SAR Content

This is a description of detailed SAR content taken from ConocoPhillips (2013b). (See ConocoPhillips, 2013b, Chapter 4.2)

| Abbreviations List of all abbreviations used

|| References List of all relevant references with data, time, revision no., document no., document owner etc.

||| Summary Shall include conclusion of whether the SIL requirements are met or not, suggestions of potential improvements to achieve better performance vs. IEC61508 and IEC61511

1 Introduction Shall contain general information, presentation of the suppliers process work with respect to "Management of functional safety" e.g. how the requirements have been implemented in the package delivery.

2 System Description Shall contain a description of the component(s) which have SIL requirements and is delivered as part of the package. It may be sufficient to refer to the SRS or other documents which covers the intent of this chapter, but the SRS will normally not cover this chapter in sufficient detail.

3 System Topology and Block Diagram Shall contain a description of the arrangement of the system vs. the other elements in the SIF and interfaces with other systems (in particular with other electrical/electronic/programmable electronic systems). Shall also include a description of how the components in the SIF are linked together.

4 Operational Description of the System Shall contain a description of how the component(s) shall be operated to fulfil the SIL requirements.

5 Assumptions Shall include a list of all essential assumptions made regarding the performance of the component(s). Essential assumptions can be assumptions regarding operational environment, maintenance, performance of other components in the SIF (e.g. ability to discover dangerous failures by the automatic system), and analytical assumptions (i.e. related to calculations).

6 Failure Rate of the Components Shall contain the failure rate(s) of the component(s) covered by the SAR. As a minimum, the failure rates shall be given as total failure rate and dangerous undetected failure rate for each component. This chapter shall also document how the failure rates are found and the information shall be traceable. If generic failure data are used there shall be documentation of why generic failure data can be used for the supplied components (i.e. why the supplied components are as good as or better than, the historic generic failure data). Generic failure databases that can be used are Offshore Reliability Data (OREDA), Electronic Parts Reliability Data (EPRD), Non-electronic Parts Reliability Data (NPRD), or similar high quality databases. Failure data can also be developed through FMECA (ref. IEC 61508-2, Annex C) or by in-house data (i.e. estimates based on number of delivered components and reported number of failures. Note that for in-house data to be approved it is required that the vendor has pro-actively gathered failure data from use. The classification of dangerous/safe detected/undetected failures may be documented through use of e.g. FMECA. The applied reliability data shall be traceable.

The rate of spurious trips shall also be documented in this chapter.

7 Diagnostic Coverage and Safe Failure Fraction Shall contain calculations of SFF for each component. Diagnostic coverage (DC) can also be calculated and documented. DC and SFF are calculated as follows:

$$DC = \frac{\lambda_{DD}}{\lambda_D} \tag{C.1}$$

$$SFF = \frac{\lambda_{TOTAL} - \lambda_{DU}}{\lambda_{TOTAL}} \tag{C.2}$$

Ref. IEC 61508-2, annex C and IEC 61508-6, annex C. λ_D = probability of dangerous failures λ_{DD} = probability of dangerous detected failures λ_{DU} = probability of dangerous undetected failures λ_S = probability of safe failures

$$\lambda_{TOTAL} = \lambda_{DD} + \lambda_{DU} + \lambda_S \tag{C.3}$$

Note: No-effect and no-part failures shall not play any part in the calculations of the diagnostic coverage or the safe failure fraction, ref IEC 61508, annex C.

8 Architectural Constraints (HFT and Voting Principles) Shall document that the component(s) comply with the requirements for HFT as given in tables 2 and 3 in IEC 61508-2, clause 7.4.4.2.2. The component must be classified into type A or B (see IEC 61508, clause 7.4.4.1.2 and 7.4.4.1.3), and by using the required SIL from the package specification and the calculated SFF from chapter 7, verify that the component can operate with the suggested HFT in the SIF (and its associated SIL) without increasing the HFT. The reasoning behind classification into either type A or B shall be properly documented. This is particularly important if a type A component is claimed.

9 Common Cause Failures Shall document the probability of common cause failures. This chapter is only relevant for SIFs involving two or more components in parallel (i.e. where more than one failure is required to result in critical failure in a SIF). The β-fraction model shall be used unless otherwise agreed with Company. It is recommended that the methodology suggested in IEC 61508-6, annex D is used for developing the β-fraction unless field experience data is available.

10 Behaviour of System / Components on Detection of Fault Shall describe how the system or component will behave on detection of a fault in the system/component. Ref. IEC 61508-2, clause 7.4.8 and IEC 61511-1, clause 11.3.

11 Mean Time to Repair Shall describe the estimated average time spent for repair of the component(s). Only the active repair time is required to be given, as the administrative and logistic delays as well as time for ramp up etc. cannot be properly estimated by the component supplier.

12 Factory Testing Shall describe how Factory Acceptance Test (FAT) shall be performed and documented. This chapter may refer to other documents.

13 Operational Testing Shall describe how testing shall be performed on the component(s) to be able to achieve the failure rates and SFF described in the chapters 6 and 7. This chapter shall give requirements related to operational testing to minimize the probability for failures not discovered by the test (referred to as independent failure or probability for systematic failures). A minimum recommended functional test interval can also be given in this chapter if different from the required minimum test interval given by the package specification. If the required PFD is not met for the component(s) covered by the SAR, this chapter shall give the required minimum test interval to achieve the required PFD. If the PFD is met with some margin, the suggested increased minimum test interval should be given.

14 Avoidance and Control of Systematic Failures Shall describe how the component supplier has ensured that systematic failures are minimized. As a minimum, the tables A.15-A.19 and B.2-B.6 in IEC 61508-2, annex A.3 and B shall be completed. If documentation of proven in use is available, reference is made to chapter x section x (proven in use).

15 Software Documentation Shall describe how the component supplier has ensured that the software development is performed within sufficiently controlled forms. As there are no software safety requirement specifications made in the project, the minimum requirement is that the component supplier completes the tables A.2-A.10 and B.1-B.9 in IEC 61508-3, annex A and B. The response can be non-compliant vs. the requirements in the standard, but it is expected that the component supplier can document what has been done for each topic covered by these tables. In the vendor comments/method columns it is expected that the software supplier gives a brief description of how the software supplier has executed the relevant technique/measure in his software realization. It is required to have a response to all columns, but for "—" and "NR" this response can be short, e.g., "not implemented". If "HR" recommendations have not been implemented this can be acceptable, provided the alternative method is equal or better than the recommended approach. IF "NR" recommendations have been implemented, this can be acceptable, provided reasonable argument for implementing this measure can be given and the same time assuring that the performance of the software will not be negatively affected by implementing this not recommended technique/measure.

16 Results This chapter shall give the main results from the report and indicate whether the SIL requirement is complied with or not. If required, propose measures for fulfilling the SIL requirements. A summary of the results documented in the SAR shall be in the following format:

Table C.1: SAR Results

Component name:	
Component identification (e.g. Tag no.)	
Test interval	Hours
Failure rate (10-6 / hour) (λ_{TOTAL})	Failures / hour
Dangerous undetected failure (λ_{DU})	Failures / hour
Safe failure fraction (SFF)	-
Mean Time to Repair (MTTR)	Hours
Calculated PFD	-
Common cause failure (CCF) (β-factor)	%
Within Allocated PFD (Y/N)	
Source	
Assumptions	
Comments	

Appendices E.g. Certificates, test documentation, FMECA, Failure reports.

Appendix D

SAR Example for Non-Proven and Proven Technology

This is an example of the SAR content for ASVs for the two cases in chapter 6. An E-ASV represent non-proven technology and an H-ASV represent proven technology. The examples are based on information found in ExproSoft (2013) and technical reports provided by ExproSoft AS.

| Abbreviations List of all abbreviations used:

ASV Annulus Safety Valve

E-ASV Electrically operated Annulus Safety Valve

H-ASV Hydraulically operated Annulus Safety Valve

etc.

|| References Document references:

No	Document	Date	Rev	Doc no	Made by
1	Safety Requirement Specification (SRS)				Operator
2	Safety Analysis Report requirements				Operator
3	Industry standards such as IEC 61508-2	2013	2		IEC
5	Product Description	2011	5		Vendor

||| Summary The summary shall include:

- Conclusion of whether the valve meets the SIL requirements or not
- A copy of the result table in section 16
- Recommendations to achieve high performance

1 Introduction The introduction shall present the vendors work process with respect to management of functional safety. The following steps are typically included:

- How to achieve technology readiness
- How to achieve operational readiness
- How to collect and learn from experience data

2 System Description The system description shall include the following issues related to the component:

- Intention
- Location
- What does it look like
- Installation and retrieval
- How it works
- Independence
- Configuration
- FMECA
- Closing time

3 System Topology and Block Diagram Shall describe the SIF by words and by illustration (a reliability block diagram). The block diagram may be similar for both H-ASV and E-ASV and may look like figure D.1.

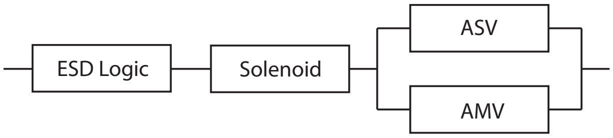


Figure D.1: Example of a block diagram for both E-ASV and H-ASV

4 Operational Description of the System Shall describe how the component(s) shall be operated to fulfil the SIL requirements. It is normal to refer to operational procedure.

5 Assumptions This is normally provided as a list of all essential assumptions made regarding the performance of the component(s). E.g. operational environment, maintenance and analytical assumptions (i.e. related to calculations).

6 Failure Rate of the Components This section shall have the following sub sections:

- Data sources
- Dangerous undetected failure rate (λ_{DU})
- Dangerous detected failure rate (λ_{DD})
- Non-safety critical (safe) failure rate (λ_S)
- Total failure rate (λ_{TOT})
- Probability of failure on demand (PFD)

Failure rates are typically based on failure data from field experience for the specific equipment. When experience data are not available there are two options:

- Utilize generic data
- Use FMECA to develop failure rates

If generic data is used there shall be documentation of why generic failure data can be used for the supplied component. If it is claimed that the component is better than or as good as the generic data, this must also be documented. Only high quality databases can be used as sources for the generic data. Failure data can also be developed through a FMECA (ref IEC 61508-2, Annex C).

The various failure rates are calculated using the formula (D.1):

$$\lambda = \frac{\text{No.of failures}}{\text{Aggregated time in service}} = \frac{n}{\tau} \tag{D.1}$$

λ_{TOT} is calculated using the formula (D.2):

$$\lambda_{TOT} = \lambda_{DD} + \lambda_{DU} + \lambda_S \tag{D.2}$$

Note that dangerous detected failure rates are based on safety critical failure modes detected by self testing or operating personnel. The failure rate λ_{DD} is not relevant for ASVs since such equipment normally does not include automatic self testing equipment. The failure rate λ_{DD} is thus set to 0.

The probability of failure on demand (PFD) shall be calculated for the component with the test interval given in the SRS.

Also note that only failures related to the component itself shall be registered as component failures. Cascading failures caused by e.g. a solenoid valve in the hydraulic system causing a safety valve failure shall not be included in the data set.

7 Diagnostic Coverage and Safe Failure Fraction Diagnostic coverage (DC) is only required for equipment with automatic self test or for failures detected by operating personnel. DC will thus not be included for either of the ASV designs in this case.

The safe failure fraction (SFF) is calculated using formula (D.3).

$$SFF = \frac{\lambda_{TOT} - \lambda_{DU}}{\lambda_{TOT}} \tag{D.3}$$

For the ASV cases, SFF can be calculated as shown in formula D.4 since $\lambda_{DD} = 0$ and since λ_{TOT} is calculated as shown in formula (D.2).

$$SFF = \frac{\lambda_S}{\lambda_{DU} + \lambda_S} \tag{D.4}$$

8 Architectural Constraints (HFT and Voting Principles) The first step is to determine whether the component is of A-type or B-type. The component is A-type if all possible failure modes can be determined for the component. All safety valves without software are A-type components. Since both ASV designs in this case are assumed without software and thus low complexity both will be categorized as type A components.

The second step is to use OLF 070 guideline, table 8.2 to determine the maximum SIL the component can be applied for, which is determined by the safe failure fraction (SFF) calculated in section 7 and the hardware fault tolerance (HFT).

- HFT = 0 means that the subsystem is used as a stand-alone component
- HFT = 1 means that the subsystem is used together with 1 redundant component
- HFT = 2 means that the subsystem is used together with 2 redundant components

An ASV is HFT = 1 because it is redundant with the annulus master valve (AMV). Examples from table 8.2 in OLF 070 with different SFF values:

- An ASV with SFF = 66% and HFT = 1 can be used for a SIL 3 system
- An ASV with SFF = 59% and HFT = 1 can be used for a SIL 2 system
- An ASV with SFF = 59% and HFT = 2 can be used for a SIL 3 system

9 Common Cause Failures In practice, this section is only relevant for systems with two or more components in parallel. If the vendor is responsible for these two components in parallel, the vendor shall also suggest a beta factor. If the vendor only is responsible for one of the components in parallel, the vendor shall only discuss internal and external hazards that may cause common cause failures (CCF). For ASVs, such hazards can e.g. be:

- Deposits
- Hydrate formation

10 Behaviour of System / Components on Detection of Fault This item is not applicable for ASVs which are systems without software and failure detection systems. Reference is made to IEC61511-1, clause 11.3. for systems which includes software and failure detection. This requirement is probably made to ensure that such systems covers at least 60% of its safe failures.

11 Mean Time to Repair This chapter shall describe the average time spent on repair of the component. Only the active repair time shall be provided, as administrative and logistic delays as well as time for ramp up etc. cannot be properly estimated by the component supplier. The repair time normally includes pull, replace and install. Longer repair time is normal for components related to topside wells compared to subsea wells.

12 Factory Testing This chapter shall describe how FAT shall be performed and documented. Only a short summary of the test procedure shall be included in the SAR. Reference shall be made to FAT documents which shall be included in the reference list. A description of how the test results are stored shall also be included.

13 Operational Testing This chapter shall describe how the operational testing is performed. The following items shall be included:

- Initial testing
- Regular testing
- Recommended regular test interval
- Test interval described in the operator SRS
- Recommendations to avoid systematic failures

Systematic failures are failures that are undetected during the regular testing. Such failures are assumed to be the same for both ASV designs and shall be documented in this chapter.

14 Avoidance and Control of Systematic Failures Shall describe how the component supplier has ensured that systematic failures are minimized. As a minimum, the tables A.15-A.19 and B.2-B.6 in IEC 61508-2, annex A.3 and B shall be completed. There are reduced requirements for documentation related to avoidance and control of systematic failures if the component can be classified as either:

- Proven in use

- Prior us
- Low complexity

If one of these items can be documented, the only additional requirement will be to document a structured quality assurance (QA) system, preferably ISO 9000 certified. This can be done by attaching a copy of QA certificates or a copy of the procedures. This will be the practice for the ASV designs since both are considered low complexity and the H-ASV can be certified as proven in use or prior use.

15 Software Documentation Shall describe how the component supplier has ensured that the software development is performed within sufficiently controlled forms. There is nothing to document for either ASV designs since there is no software included in these systems.

16 Results This chapter shall summarize the main results in a table. An example is provided in table D.1 (example data) :

Table D.1: SAR Results

Component name:	H-ASV
Component identification	-
Test interval	6 months
Failure rate (λ_{TOT})	$2,0$ per 10^6 hours
Dangerous undetected failure (λ_{DU})	$0,5$ failures per 10^6 hours
Safe failure fraction (SFF)	68%
Mean Time to Repair (MTTR)	144 hours
Calculated PFD, $\tau = 6$ months	$2,3 \cdot 10^{-3}$
Common cause failure (β)	NA
Within Allocated PFD (system)	To be calculated by operator or contractor
Source	Data is collected from OREDA
Assumptions	See section 5
Comments	NA

Appendices E.g. Certificates, test documentation, FMECA, Failure reports.

Appendix E

Fault Tree Analyses

This chapter includes fault trees with input data and minimal cut sets used in chapter 7.

E.1 Input Data

Table E.1: List of input data (from reliability data in chapter 7 section 7.3) which is used in the FTAs

Hazard	**Basic event name**	**Failure rate**	**Mean time to repair (MTTR)**		**Test interval** (τ)	
		per 10^6 **hour**	**days**	**hours**	**months**	**hours**
ASV internal leak	ASVI	0,487	28	672	6	4380
ASV external leak	ASVE	0,117	28	672	6	4380
ASV packer leak	ASVP	0,374	28	672	6	4380
M-SAS internal leak	MSASI	2,2	7	168	12	8760
M-SAS external leak	MSASE	0,0778	7	168	12	8760
AAV external leak	AAVE	0,117	28	672	NA	NA
AAV internal leak	AAVI	0,244	28	672	NA	NA
Leak through tubing hanger	TH	0,135	28	672	12	8760
Leak through WH connector	WHC	0,0857	7	168	12	8760
AMV external leak	AMVE	0,0778	1	24	12	8760
AMV internal leak	AMVI	1,454	1	24	12	8760
Leak through pressure monitoring	M	0,1	1	24	12	8760
Leak through blind flange	BF	0,0973	1	24	12	8760
Leak through pipes	P	0,300	1	24	NA	NA
AWV external leak	AWVE	0,0778	1	24	12	8760
AWV internal leak	AWVI	1,454	1	24	12	8760

E.2 FTA (Base Line)

This section includes fault trees for the base line.

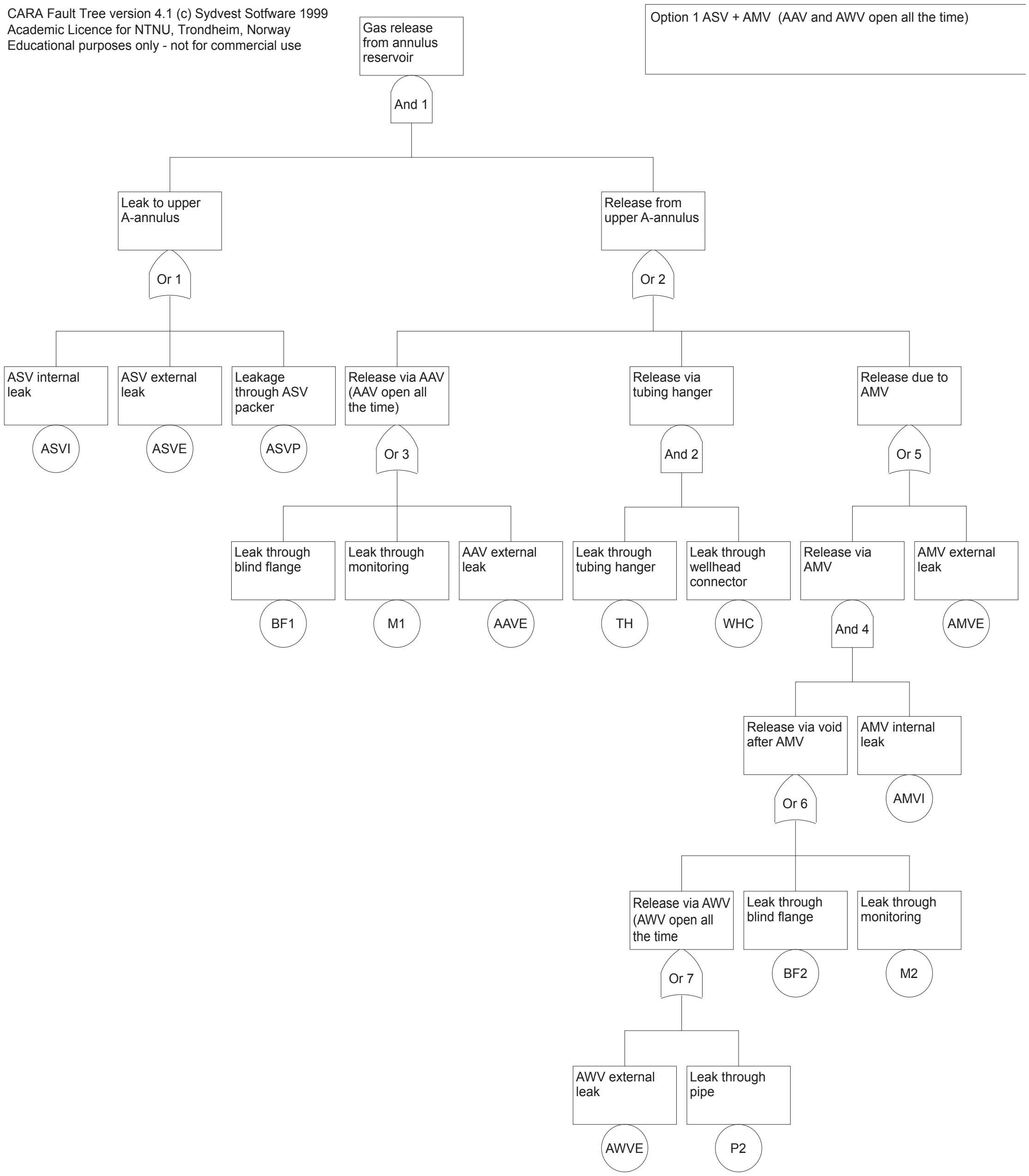

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 1 ASV + AMV (AAV and AWV open all the time)
Gas release from annulus reservoir
And 1
Leak to upper A-annulus
Or 1
Release from upper A-annulus
Or 2
ASV internal leak
ASVI
ASV external leak
ASVE
Leakage through ASV packer
ASVP
Release via AAV (AAV open all the time)
Or 3
Release via tubing hanger
And 2
Release due to AMV
Or 5
Leak through blind flange
BF1
Leak through monitoring
M1
AAV external leak
AAVE
Leak through tubing hanger
TH
Leak through wellhead connector
WHC
Release via AMV
And 4
AMV external leak
AMVE
Release via void after AMV
Or 6
AMV internal leak
AMVI
Release via AWV (AWV open all the time
Or 7
Leak through blind flange
BF2
Leak through monitoring
M2
AWV external leak
AWVE
Leak through pipe
P2

Figure E.1: Fault tree analysis for option 1 ASV + AMV

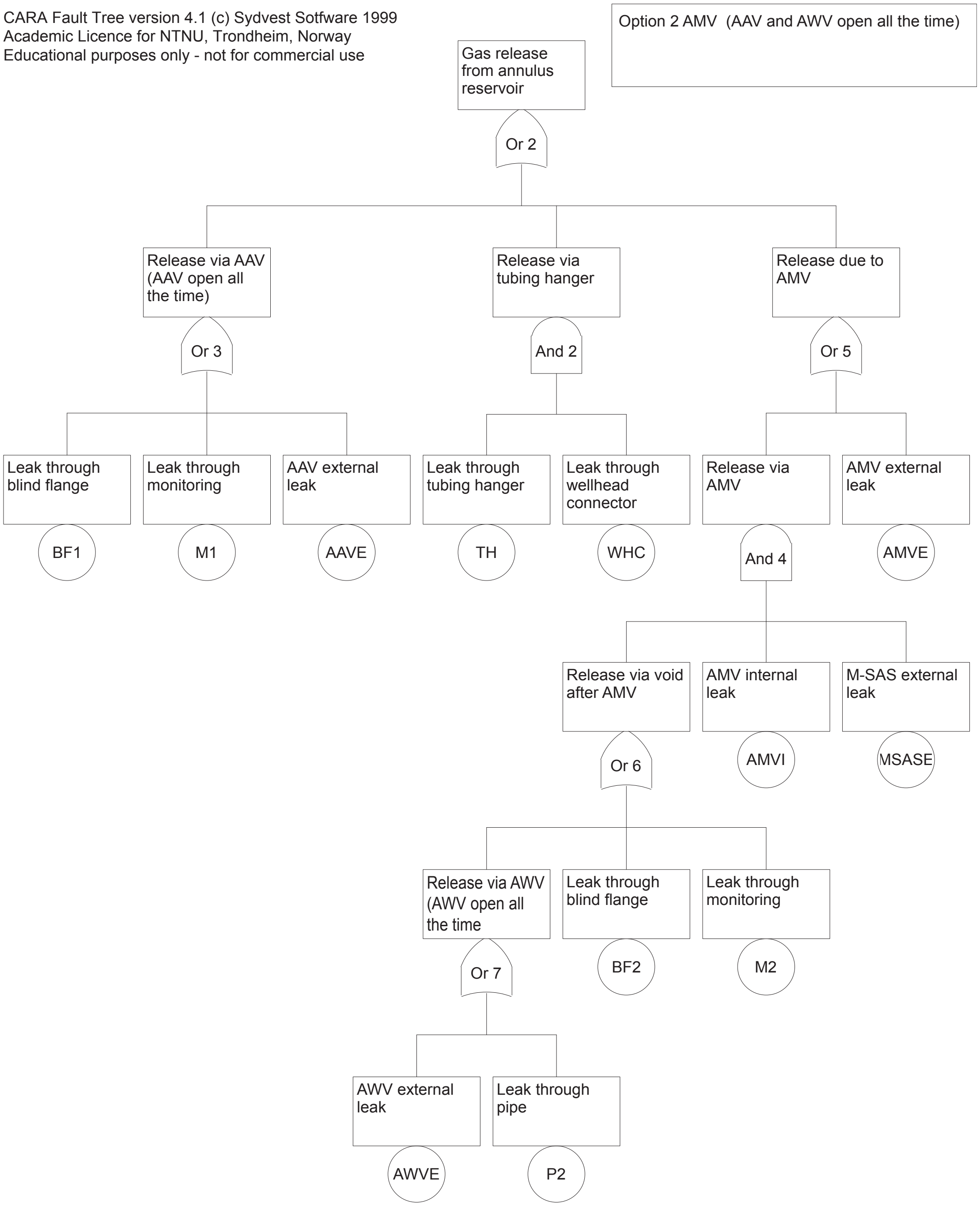

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 2 AMV (AAV and AWV open all the time)
Gas release from annulus reservoir
Or 2
Release via AAV (AAV open all the time)
Release via tubing hanger
Release due to AMV
Or 3
And 2
Or 5
Leak through blind flange
Leak through monitoring
AAV external leak
Leak through tubing hanger
Leak through wellhead connector
Release via AMV
AMV external leak
BF1
M1
AAVE
TH
WHC
And 4
AMVE
Release via void after AMV
AMV internal leak
M-SAS external leak
Or 6
AMVI
MSASE
Release via AWV (AWV open all the time
Leak through blind flange
Leak through monitoring
Or 7
BF2
M2
AWV external leak
Leak through pipe
AWVE
P2

Figure E.2: Fault tree analysis for option 2 AMV

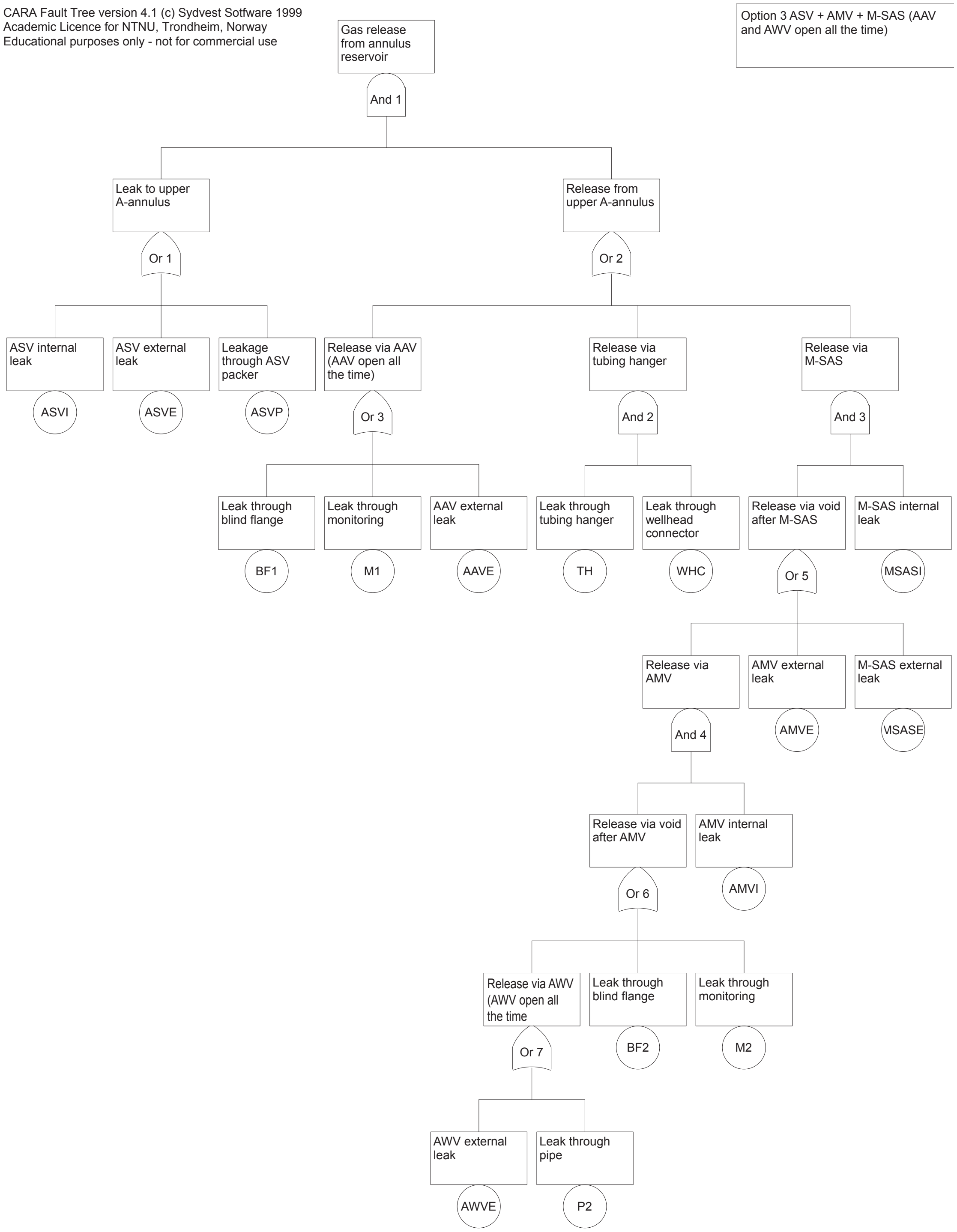

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Gas release from annulus reservoir
Option 3 ASV + AMV + M-SAS (AAV and AWV open all the time)
And 1
Leak to upper A-annulus
Release from upper A-annulus
Or 1
Or 2
ASV internal leak
ASV external leak
Leakage through ASV packer
Release via AAV (AAV open all the time)
Release via tubing hanger
Release via M-SAS
ASVI
ASVE
ASVP
Or 3
And 2
And 3
Leak through blind flange
Leak through monitoring
AAV external leak
Leak through tubing hanger
Leak through wellhead connector
Release via void after M-SAS
M-SAS internal leak
BF1
M1
AAVE
TH
WHC
Or 5
MSASI
Release via AMV
AMV external leak
M-SAS external leak
And 4
AMVE
MSASE
Release via void after AMV
AMV internal leak
Or 6
AMVI
Release via AWV (AWV open all the time
Leak through blind flange
Leak through monitoring
Or 7
BF2
M2
AWV external leak
Leak through pipe
AWVE
P2

Figure E.3: Fault tree analysis for option 3 ASV + AMV + M-SAS

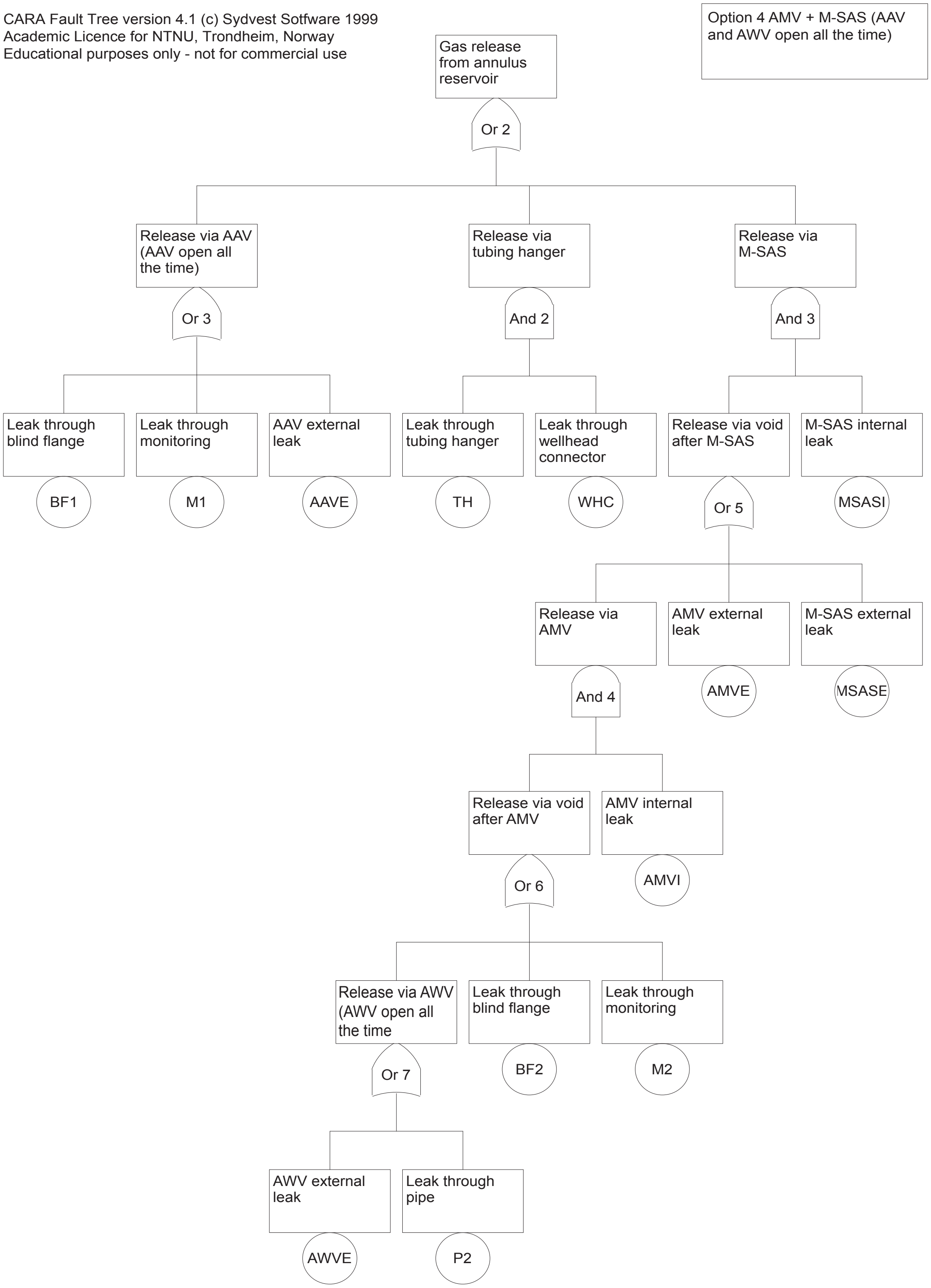

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 4 AMV + M-SAS (AAV and AWV open all the time)
Gas release from annulus reservoir
Or 2
Release via AAV (AAV open all the time)
Release via tubing hanger
Release via M-SAS
Or 3
And 2
And 3
Leak through blind flange
Leak through monitoring
AAV external leak
Leak through tubing hanger
Leak through wellhead connector
Release via void after M-SAS
M-SAS internal leak
BF1
M1
AAVE
TH
WHC
Or 5
MSASI
Release via AMV
AMV external leak
M-SAS external leak
And 4
AMVE
MSASE
Release via void after AMV
AMV internal leak
Or 6
AMVI
Release via AWV (AWV open all the time
Leak through blind flange
Leak through monitoring
Or 7
BF2
M2
AWV external leak
Leak through pipe
AWVE
P2

Figure E.4: Fault tree analysis for option 4 AMV + M-SAS

E.3 Minimal Cut Sets (Base Line)

Table E.2: List of minimal cut set for option 1: ASV + AMV

Option:	Cut set order	Cut set
1	1	NA
Total amount: 0		
1	2	ASVI,BF1
1	2	ASVI,M1
1	2	ASVI,AAVE
1	2	ASVI,AMVE
1	2	ASVE,BF1
1	2	ASVE,M1
1	2	ASVE,AAVE
1	2	ASVE,AMVE
1	2	ASVP,BF1
1	2	ASVP,M1
1	2	ASVP,AAVE
1	2	ASVP,AMVE
Total amount: 12		
1	3	ASVI,TH,WHC
1	3	ASVI,AMVI,AWVE
1	3	ASVI,AMVI,P2
1	3	ASVI,AMVI,BF2
1	3	ASVI,AMVI,M2
1	3	ASVE,TH,WHC
1	3	ASVE,AMVI,AWVE
1	3	ASVE,AMVI,P2
1	3	ASVE,AMVI,BF2
1	3	ASVE,AMVI,M2
1	3	ASVP,TH,WHC
1	3	ASVP,AMVI,AWVE
1	3	ASVP,AMVI,P2
1	3	ASVP,AMVI,BF2
1	3	ASVP,AMVI,M2
Total amount: 15		

Table E.3: List of minimal cut set for option 2: AMV after ASV failure

Option:	**Cut set order**	**Cut set**
2	1	BF1
2	1	M1
2	1	AAVE
2	1	AMVE
Total amount: 4		
2	2	TH,WHC
Total amount: 1		
2	3	AMVI,MSASE,AWVE
2	3	AMVI,MSASE,P2
2	3	AMVI,MSASE,BF2
2	3	AMVI,MSASE,M2
Total amount: 4		

Table E.4: List of minimal cut set for option 3: ASV + AMV + M-SAS

Option:	**Cut set order**	**Cut set**
3	1	NA
Total amount: 0		
3	2	ASVI,BF1
3	2	ASVI,M1
3	2	ASVI,AAVE
3	2	ASVE,BF1
3	2	ASVE,M1
3	2	ASVE,AAVE
3	2	ASVP,BF1
3	2	ASVP,M1
3	2	ASVP,AAVE
Total amount: 9		
3	3	ASVI,TH,WHC
3	3	ASVI,MSASI,AMVE
3	3	ASVI,MSASI,MSASE
3	3	ASVE,TH,WHC
3	3	ASVE,MSASI,AMVE
3	3	ASVE,MSASI,MSASE
3	3	ASVP,TH,WHC
3	3	ASVP,MSASI,AMVE
3	3	ASVP,MSASI,MSASE
Total amount: 9		
3	4	ASVI,MSASI,AMVI,AWVE
3	4	ASVI,MSASI,AMVI,P2
3	4	ASVI,MSASI,AMVI,BF2
3	4	ASVI,MSASI,AMVI,M2
3	4	ASVE,MSASI,AMVI,AWVE
3	4	ASVE,MSASI,AMVI,P2
3	4	ASVE,MSASI,AMVI,BF2
3	4	ASVE,MSASI,AMVI,M2
3	4	ASVP,MSASI,AMVI,AWVE
3	4	ASVP,MSASI,AMVI,P2
3	4	ASVP,MSASI,AMVI,BF2
3	4	ASVP,MSASI,AMVI,M2
Total amount: 12		

Table E.5: List of minimal cut set for option 4: AMV + M-SAS

Option:	**Cut set order**	**Cut set**
4	1	BF1
4	1	M1
4	1	AAVE
Total amount: 3		
4	2	TH,WHC
4	2	MSASI,AMVE
4	2	MSASI,MSASE
Total amount: 3		
4	3	MSASI,AMVI,AWVE
4	3	MSASI,AMVI,P2
4	3	MSASI,AMVI,BF2
4	3	MSASI,AMVI,M2
Total amount: 4		

E.4 FTA (M-SAS as AAV)

This section includes fault trees when M-SAS valve is used as AAV.

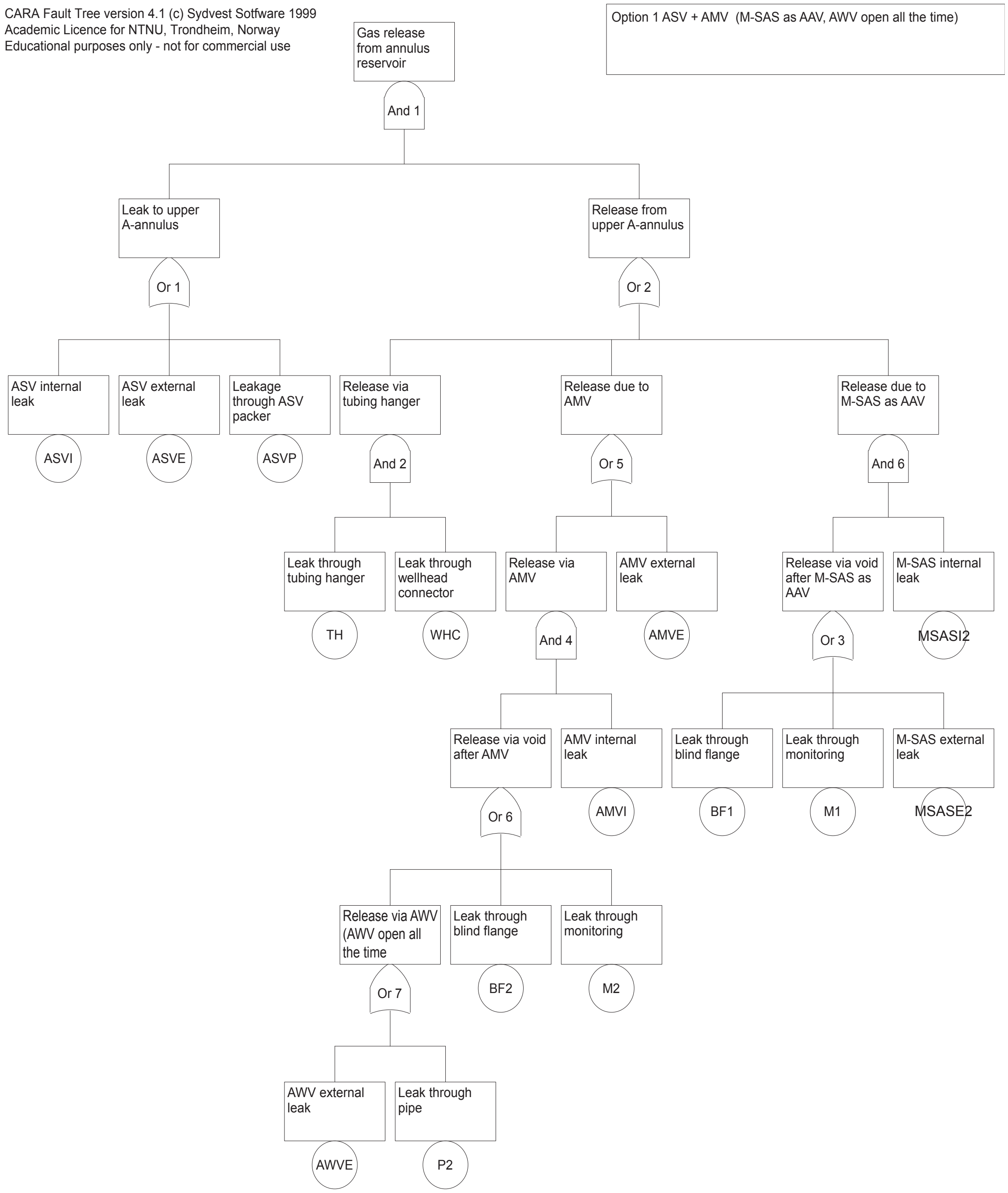

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 1 ASV + AMV (M-SAS as AAV, AWV open all the time)
Gas release from annulus reservoir
And 1
Leak to upper A-annulus
Or 1
Release from upper A-annulus
Or 2
ASV internal leak
ASVI
ASV external leak
ASVE
Leakage through ASV packer
ASVP
Release via tubing hanger
And 2
Release due to AMV
Or 5
Release due to M-SAS as AAV
And 6
Leak through tubing hanger
TH
Leak through wellhead connector
WHC
Release via AMV
And 4
AMV external leak
AMVE
Release via void after M-SAS as AAV
Or 3
M-SAS internal leak
MSASI2
Release via void after AMV
Or 6
AMV internal leak
AMVI
Leak through blind flange
BF1
Leak through monitoring
M1
M-SAS external leak
MSASE2
Release via AWV (AWV open all the time
Or 7
Leak through blind flange
BF2
Leak through monitoring
M2
AWV external leak
AWVE
Leak through pipe
P2

Figure E.5: Fault tree analysis for option 1 ASV + AMV using M-SAS valve as AAV

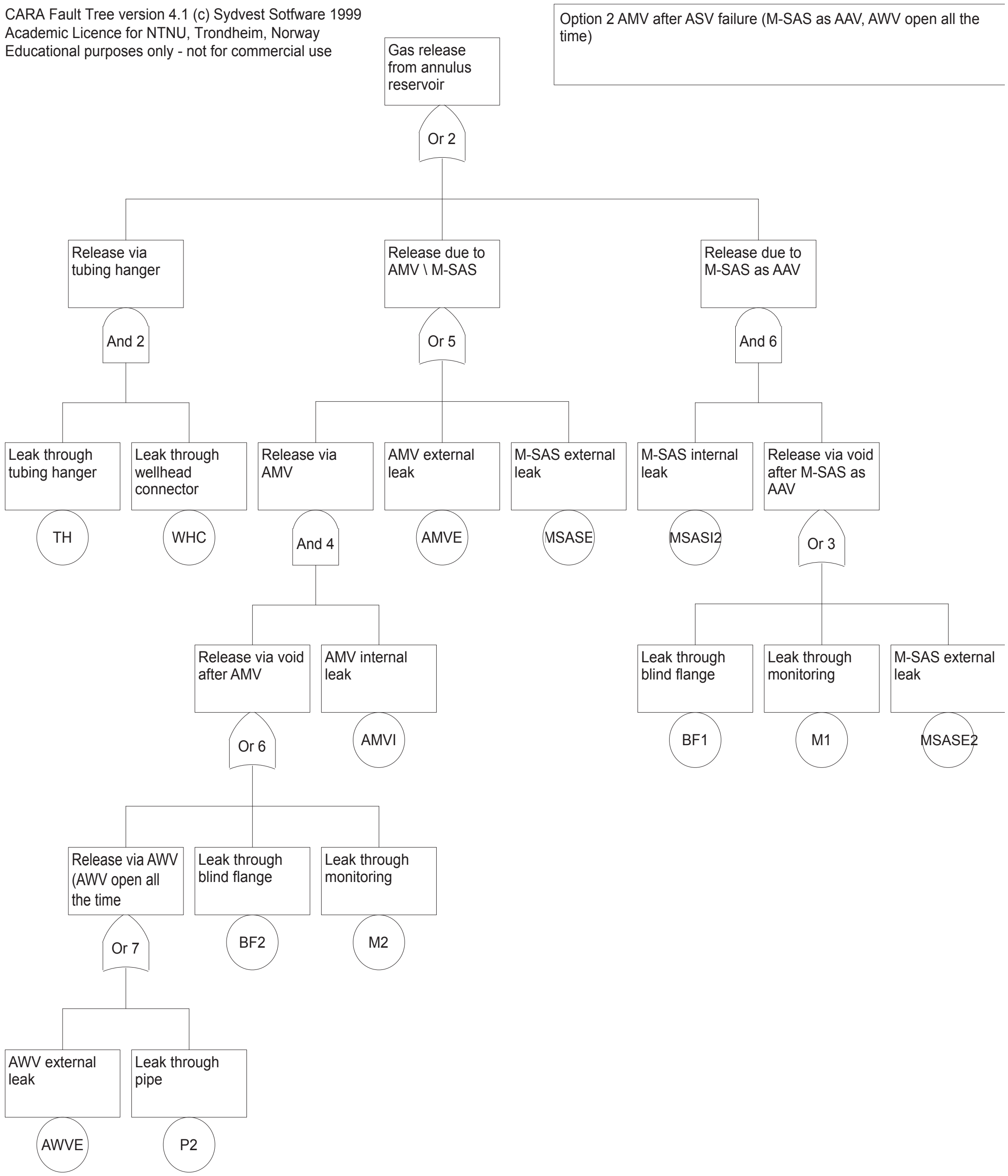

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 2 AMV after ASV failure (M-SAS as AAV, AWV open all the time)
Gas release from annulus reservoir
Or 2
Release via tubing hanger
Release due to AMV \ M-SAS
Release due to M-SAS as AAV
And 2
Or 5
And 6
Leak through tubing hanger
Leak through wellhead connector
Release via AMV
AMV external leak
M-SAS external leak
M-SAS internal leak
Release via void after M-SAS as AAV
TH
WHC
And 4
AMVE
MSASE
MSASI2
Or 3
Release via void after AMV
AMV internal leak
Leak through blind flange
Leak through monitoring
M-SAS external leak
Or 6
AMVI
BF1
M1
MSASE2
Release via AWV (AWV open all the time
Leak through blind flange
Leak through monitoring
Or 7
BF2
M2
AWV external leak
Leak through pipe
AWVE
P2

Figure E.6: Fault tree analysis for option 2 AMV using M-SAS valve as AAV

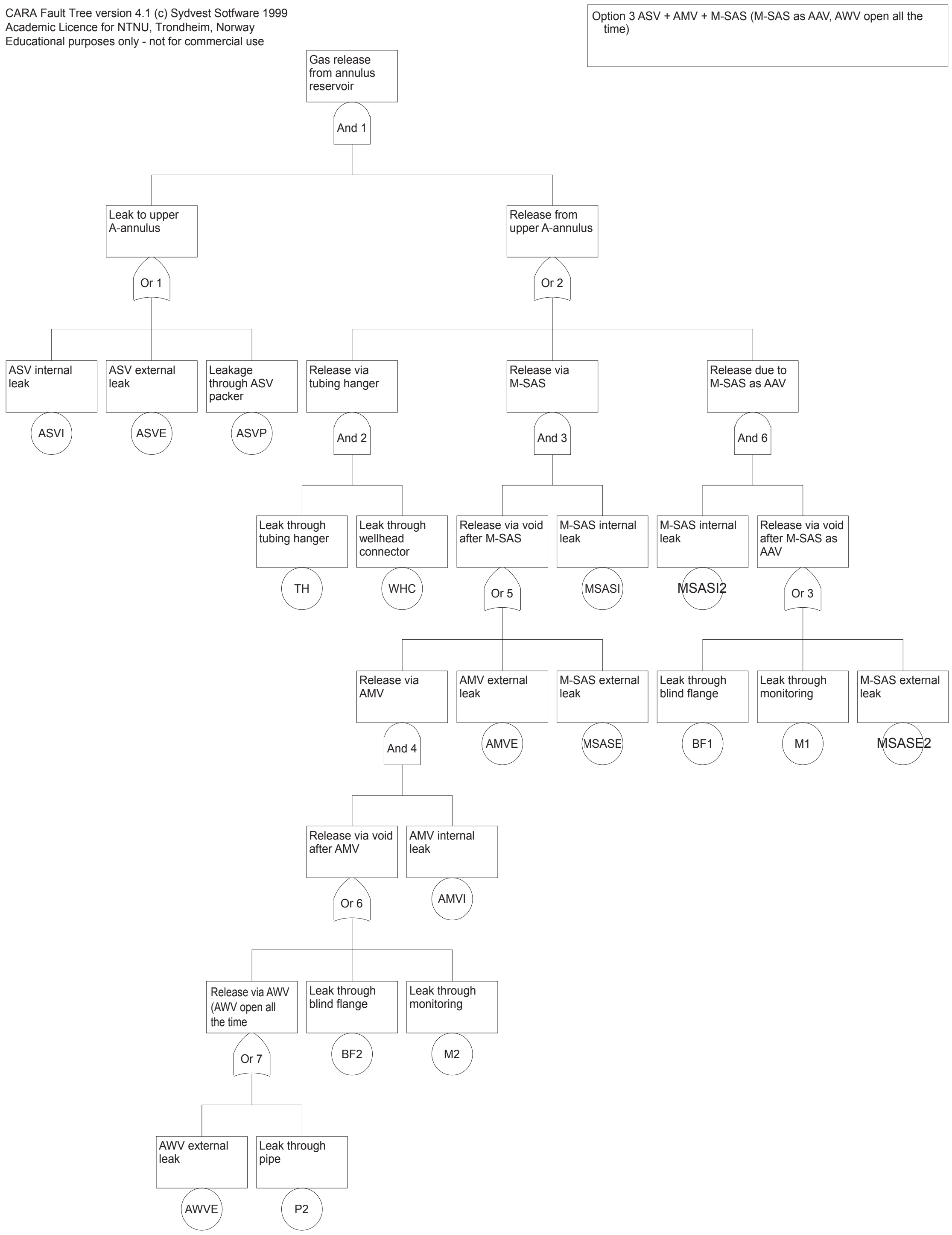

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 3 ASV + AMV + M-SAS (M-SAS as AAV, AWV open all the time)
Gas release from annulus reservoir
And 1
Leak to upper A-annulus
Release from upper A-annulus
Or 1
Or 2
ASV internal leak
ASV external leak
Leakage through ASV packer
Release via tubing hanger
Release via M-SAS
Release due to M-SAS as AAV
ASVI
ASVE
ASVP
And 2
And 3
And 6
Leak through tubing hanger
Leak through wellhead connector
Release via void after M-SAS
M-SAS internal leak
M-SAS internal leak
Release via void after M-SAS as AAV
TH
WHC
Or 5
MSASI
MSASI2
Or 3
Release via AMV
AMV external leak
M-SAS external leak
Leak through blind flange
Leak through monitoring
M-SAS external leak
And 4
AMVE
MSASE
BF1
M1
MSASE2
Release via void after AMV
AMV internal leak
Or 6
AMVI
Release via AWV (AWV open all the time
Leak through blind flange
Leak through monitoring
Or 7
BF2
M2
AWV external leak
Leak through pipe
AWVE
P2

Figure E.7: Fault tree analysis for option 3 ASV + AMV + M-SAS using M-SAS valve as AAV

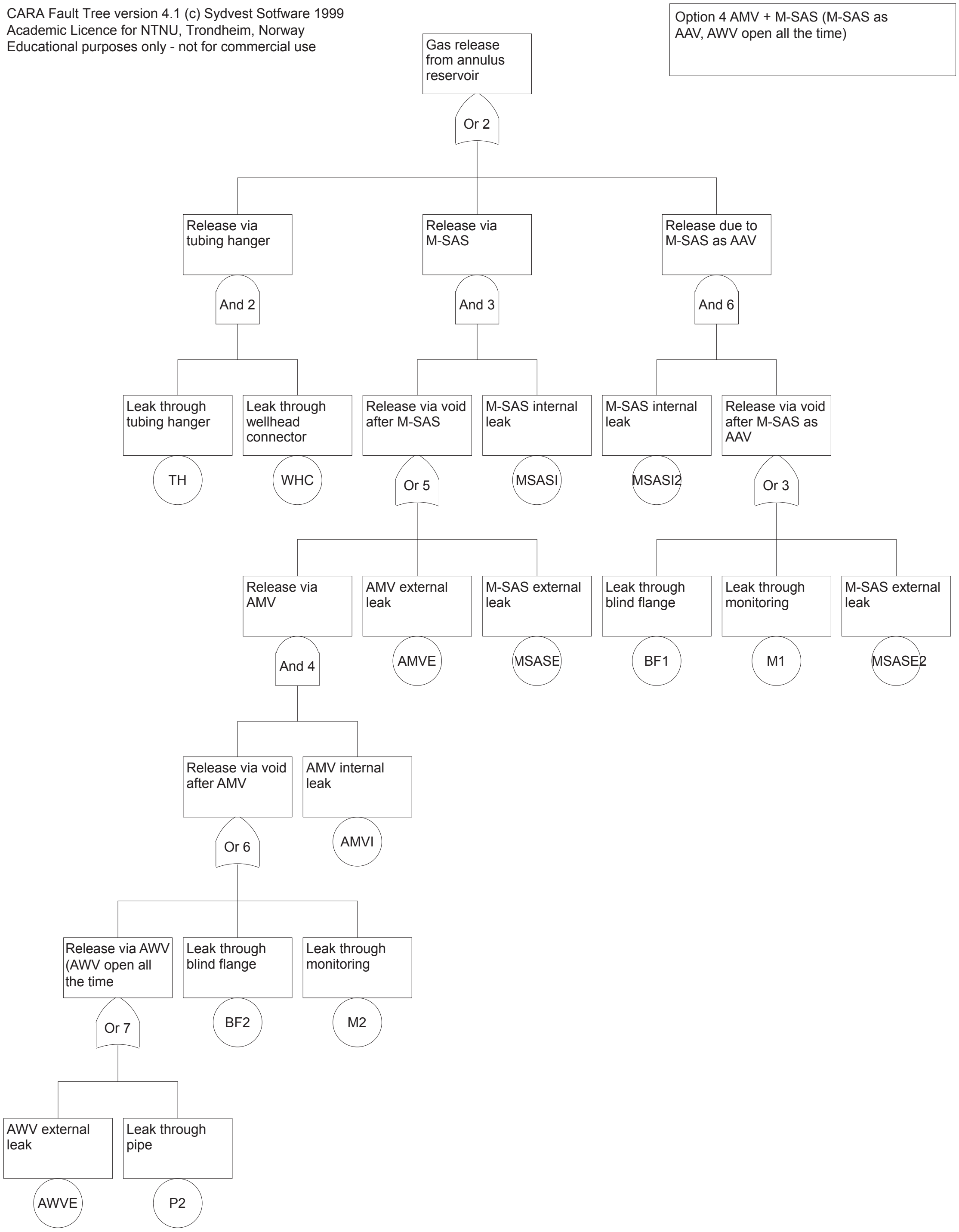

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Academic Licence for NTNU, Trondheim, Norway
Educational purposes only - not for commercial use
Option 4 AMV + M-SAS (M-SAS as AAV, AWV open all the time)
Gas release from annulus reservoir
Or 2
Release via tubing hanger
And 2
Release via M-SAS
And 3
Release due to M-SAS as AAV
And 6
Leak through tubing hanger
TH
Leak through wellhead connector
WHC
Release via void after M-SAS
Or 5
M-SAS internal leak
MSASI
M-SAS internal leak
MSASI2
Release via void after M-SAS as AAV
Or 3
Release via AMV
And 4
AMV external leak
AMVE
M-SAS external leak
MSASE
Leak through blind flange
BF1
Leak through monitoring
M1
M-SAS external leak
MSASE2
Release via void after AMV
Or 6
AMV internal leak
AMVI
Release via AWV (AWV open all the time
Or 7
Leak through blind flange
BF2
Leak through monitoring
M2
AWV external leak
AWVE
Leak through pipe
P2

Figure E.8: Fault tree analysis for option 4 AMV + M-SAS using M-SAS valve as AAV

Bibliography

(2002). *OREDA Offshore reliability Data.* OREDA Participants.

(2003). *IEC 61511-1 Functional safety Safety instrumented systems for the process industry sector Part 1: Framework, definitions, system, hardware and software requirements.* IEC, 3, rue de Varembè, CH-1211 Genova 20, Switzerland.

(2010a). *IEC 61508-1 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements.* IEC, 3, rue de Varembè, CH-1211 Genova 20, Switzerland.

(2010b). *IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safetyrelated systems.* IEC, 3, rue de Varembè, CH-1211 Genova 20, Switzerland.

(2010c). *IEC 61508-4 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations.* IEC, 3, rue de Varembè, CH-1211 Genova 20, Switzerland.

Andersen, A. (2012). Safety analysis report (sar) for m-sas. Technical report, ExproSoft AS.

BSEE (2013a). http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=0007751dbdd2715fe217f2c3a426fa4d&ty=HTML&h=L&r=SECTION&n=30y2.0.1.2.2.5.73.18.

BSEE (2013b). http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=6a5bdd4d122d596563e2ba549b089110&rgn=div8&view=text&node=30:2.0.1.2.2.8.74.2&idno=30.

BSEE (2013c). http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=177b7f750de705e77e77e7b2768fdab6&rgn=div5&view=text&node=30:2.0.1.2.2&idno=30#30:2.0.1.2.2.10.78.5.

ConocoPhillips (2013a). *SAFETY REQUIREMENT SPECIFICATION (SRS)*.

ConocoPhillips (2013b). *SAR SUPPLIER REQUIREMENTS*.

Engineering, G. (2013). http://gekengineering.com/Downloads/Free_Downloads/Packer.pdf.

Exida (2004). http://www.exida.com/articles/prove.pdf.

ExproSoft (2013). http://www.exprobase.com.

Hauge, S. and Onshus, T. (2010). Reliability data for safety instrumented systems pds handbook. Technical report, SINTEF Technology and Society.

Lundteigen, M. A. and Rausand, M. (2008). Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering and System Safety*, page 521.

NORSOK (2002). *NORSOK U-001 Subsea production systems*. Norwegian Technology Centre, Oscarsgt. 20, Box 7072 Majorstuen, N-0306 Oslo.

NORSOK (2004). *NORSOK STANDARD S-001 Technical safety*. Standards Norway, Strandveien 18, P.O. Box 242, N-1326 Lysaker, 4th edition.

NORSOK (2012). *NORSOK STANDARD D-010 Well integrity in drilling and well operations*. Standards Norway, Strandveien 18, P.O. Box 242, N-1326 Lysaker.

Norway, P. S. A. (2013a). http://www.ptil.no/about-us/category89.html?lang=en_US.

Norway, P. S. A. (2013b). http://www.ptil.no/management/category401.html#_Toc280619391.

Norway, P. S. A. (2013c). http://www.ptil.no/activities/category399.html?lang=en_US#_Toc345662871.

Norway, P. S. A. (2013d). http://www.ptil.no/facilities/category400.html#p53.

Norway, P. S. A. (2013e). http://www.ptil.no/facilities/category400.html#_Toc345671563.

OLF (2004). *OLF 070 APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY*. Standards Norway, 2th edition.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition.

Rigzone (2013). http://www.rigzone.com/training/insight.asp?insight_id=315&c_id=4.

Schlumberger (2013). http://www.freepatentsonline.com/6186227.html.

Seime, O. J. (2012). Reliability assessment of an electrical downhole safety valve. http://frigg.ivt.ntnu.no/ross/stud/project/2012/seime.pdf.