Faculty of Science and Technology

MASTER'S THESIS

Study program/Specialization: Environmental Technology (Offshore Environmental Engineering)	Spring Semester,2014 Restricted access
Writer: Hossein Ahmadi Faryazani	…… (writer's Signature
Faculty Supervisor : R.M Chandima Ratnayaka External Supervisor : Andreas Holm	
Title of Thesis: **Safety Instrumented Functions in Workover Control Systems**	
Credit(ECTS): 30 credit points	
Key Words : none	Page: +attached CD Stavanger, June 16th 2014

Acknowledgment

This thesis work is the final part of my studies at the University of Stavanger (UIS), and it concludes my Masters of Science degree in Environmental Technology (Offshore Environmental Engineering).The study of this thesis has being executed at Akersolutions AS office in Oslo.
I would like to say a very big thank you to Anderas Holm for leading and support offered me while writing this the thesis. I also wish to thank to Ellen Lycke for the contribution she made towards making this thesis a success.
I want to also thank my supervisor, Professor R.M Chandima Ratnayaka of the University of Stavanger for his patience, support and guidance during the course of my work on this thesis.
Special thank go to Alireza Moharamzadeh , John Barry, Magnus Bårdsen for their relentless assistance and support during master's thesis work also want to thank my friends and class mate who contributed to the success of this thesis.
Finally, I want to thank my family, specially my wife, Mahtab whom were really supportive and believed in me.

Hossein Ahmadi Faryazani

.

Abstract

Those master thesis work tries to examine the maximum independency for safety system in workover and convince that the independent safety system is enough safe and comply with international and local standard. I have started by general description of workover system that be used during well intervention, then go to look the safety system and how this system prevent accident during well intervention and well testing. The aim of this thesis in the end is try to modify safety system in order to maximum independency from control system. This thesis shows a risk evaluation approach that is in line with approved standard being using to certify that the new safety system in enough safe.

TABLE OF CONTENTS

Table of Figures

List of Tables

Chapter 1

1. Introduction

1.1. Background and problem

Today it is challenging to document and verify safety integrity level in Workover systems. Particular challenges lay with the requirement to independence between process control system and safety system. For Aker's Workover system the communication line from topside to subsea and, the Subsea Electronic Modules (SEMs) are currently shared between the normal control and the safety system. According to IEC 61508 this is allowed, but requires substantial documentation of independence between the safety and non-safety systems, it is also a challenge to find sound statistical data for the verification process. Furthermore any changes to the normal control system in the SEMs needs to be evaluated from a safety point of view, and might also create a need for updating the safety documentation. This severely limits the ability to perform any changes to the non-safety software.

1.2. Scope and Objective

The main objective is to be ensuring that the non-safety system has no effect on safety system. The first goal is to identify limitations to the current system and suggest a solution by introducing a new safety system design to achieve safety integrity level (SIL 2) for the three safety instrumented functions (SIF's) PSD, ESD and EQD.

To reach main objective need to developed sub objective

- Identify the current normal control and safety system and common components in both.
- Problem and limitation that involved with this current system.
- Identify the relevant requirement of national and international standard, in this case, OLF and IEC61508/61511.
- Suggestion and developing a reasonable solution in order to ensure that the new system will be safer than the current system.
- Compare the new solution with current system and define the limitation of new system.
- Examine the new solution with scientific method like qualitative or quantitate risk reduction.
  Finally be ensured that the new system is good enough safe that will reduce the risk of hydrocarbon release and compliance with national and international standard, also will be accepted by client.

1.3. Methodology

This thesis is based on literature and document review from Aker subsea AS, and also various international and local standard such as IEC65508,IEC 65511 and NOROG .Also various journal and article , and information from world wide web have being used for this thesis. Different discussion and meeting with risk expert and

Workover expert in Aker Subsea and Aker Oilfield in order to good understanding and define general overview of Workover. Further on definition of safety and control system and other related areas for this project work.

1.4. Limitation

In this thesis the verification of safety integrity level was not possible, because the modification of new safety system are in preliminary step and not yet clear which supplier should be make the safety equipment and instrument system like safety SEM and Hydraulic DCV, so just for probability calculation of safety integrity level we use of failure data from previous supplier that will be similar to new supplier and general failure date book like OREDA and PDS handbook. The assumption that used on calculation will be followed on chapter five.

Chapter 2

2. Workover General Description

2.1. Well integrity

The workover system is designed to be used during well intervention and subsea installation activities. In detail, the equipment shall be used to perform:

Initial installation of subsea Units / Well Completion (TH/XT)
Subsea Unit and System Commissioning
Well Clean-up and Testing / Logging
Replacement of TH and XT
Well Work over (replacement of well completion strings)
Well Intervention using wireline and / or coiled tubing techniques

The main objective of the completion / workover system is to ensure the necessary integrity of the well during completion and workover operations. During completion activities the well integrity provided by the XT system is not yet in place. During workover operations, parts of the XT functionality to ensure well integrity are disabled to allow for vertical access to the well or well tubing. The intention of ensuring well integrity is to reduce risk of uncontrolled release of formation fluids. The subsea infrastructure and the C/WO system together work as a well integrity system.

The barrier philosophy on all operations using the workover system is that there shall be at least two barriers between the well and the environment at all times, primary and secondary well barriers:

- Primary well barrier - The first envelope of well barrier elements that prevents flow from a source
- Secondary well barrier - The second envelope of well barrier elements that prevents flow from a source

A well barrier consists in one or several well barrier elements. Well barrier elements can be common between primary and secondary well barrier envelope, referred to as common barrier element. To be qualified as a barrier element, the element must be tested (leak tested and or function tested) and verified prior to operation.
A key component for this Well Intervention System is the Workover Control System (WOCS) which is a generic design developed by the Akersolutions and the designated name for this WOCS is MultiWOCS^{TM}.

The MultiWOCS^{TM} will be used by the operator companies for the installation and completion of their respective subsea field developments. In some project the Contractor is not providing the subsea facilities for all of the projects, the installation and completion will be performed under a cross vendor regime. This is part of the operator companies' strategy of de-linking the dependency between Subsea Solution and Workover Systems.

For well intervention operations, the Completion/Workover system delivered by the Akersolutions will be an Open Water riser type whereby a 7-3/8" EDP and LRP stack also known as the LWRP serves the purpose for blow-out prevention.

For completion of the wells, a simplified Drill pipe Landing String (DPLS) configuration run inside a Marine Riser and BOP will be utilized.

Definition of Completion / Workover System with Subsea XT and C/WO System as stated in Table 1 below.

Statoil Categorization	ISO 13628-7 Modes of Operation	Definitions
Category A	N/A	Subsea C/WO activities (well intervention) with wireline without use of a C/WO riser to surface. Riserless Light Well Intervention (RLWI).
Category B	Well Completion (Tree Mode)	Subsea C/WO activities (completion, work over or well intervention) utilising a C/WO riser in open sea. This implies that there is a possibility to take well returns to the vessel.
	Well Intervention – Open Sea (Tree Mode)	
	Full Workover (Tree Mode)	
Category C	Well Completion (Tubing Hanger Mode)	Subsea C/WO activities (completion, work over or well intervention) utilising a C/WO riser in combination with a drilling BOP and marine riser. This includes ability to run and retrieve well completion equipment through the marine riser system. This also includes use of high pressure riser and well control equipment inside the drilling BOP and marine riser. This implies that there is a possibility to take well returns to the vessel
	Well Intervention – inside drilling riser (Tubing Hanger Mode)	
	Full Workover (Tubing Hanger Mode)	

Table 1 – Statoil categorisation of Workover Systems

2.2. Main part of Workover System

2.2.1 Shutdown panel

The PSD, ESD or EQD function is initiated by the operator pushing the PSD, ESD or EQD button.

2.2.2 LWRP Control Cabinet

The main components of the LWRP Control Cabinet are the Electrical Power Unit (EPU) and the SSCU.
The EPU supplies power to the Subsea Electronics Modules (SEM) and the SSCU. The EPU is also connected to a remote in/out unit, which allows signal to be sent from the LWRP Control Cabinet to the MCP.

The SSCU which is dual redundant, is housed in the same set of cabinets as the EPU and contains both safety and non-safety hardware. The main components of the SSCU relating to the safety system power supplies are the PLC CPU Card, Digital I/O Card and Modbus Card.
In addition the LWRP Control Cabinet also contains an Ethernet switch, AVS Relay and isolation barrier. The primary function of the LWRP Control Cabinet system with regards to the safety function is to monitor ESD, EQD and AVS hardwired input signals provided by the shutdown system,.

2.2.3 HPU

The PLC in the HPU consists of the following 3 modules.

- DI Module senses the input signal from any field installed SD-panels and safety relays. The function includes line-monitoring.
- Control Process Unit (CPU) Module re-generates the input signal from the Safety DI card into a shutdown sequence performed on Safety DO Cards. The CPU contains a separated program section for application of safety instrument functions. Programming is performed with ready-made TÜV certified blocks. Mutual interference during processing is prevented by ensuring that the standard and safety-related programs are kept strictly separate and that the data exchange takes place via special conversion function blocks. The safety functions are executed twice in different processor sections of one CPU through redundant, multi-channel command processing.
- F-DO Module provides power output to activate the Solenoid Valve (SOV) open or close solenoid. Line monitoring is provided to detect line fault.

The SOV controls the pneumatic activation of the DCV. The SOV is a 3 port 2 position valves with single coil, spring return to normally closed. The solenoid valve is FSC.

SOV coil is activated by continuous electric supply from PLC F-DO module leading to mode, Open.

A Directional Control valve (DCV) pressurizes and ventilates the hydraulic outputs.
This is a pneumatic activated 3 port 2 position balanced spool valve with spring return. This is a FSC valve.
The DCV is activated by the pneumatic pilot, controlled by SOV output. When SOV output is pressurised, DCV is activated to open. When SOV output is pressurised, DCV is activated to open. When SOV output is depressurised, DCV is spring return to closed.

2.2.4 SFT SPWV

SFT located topside, provides flow control of the production bore during flowing and CT/WL mode. The SFT features a valve block with a SPWV, connected to the testing equipment. In flowing mode, test production is produced through the wing block in the SFT and to the rig/vessel. The SFT wing valve serves as a barrier towards the rig, and the valve is directly operated from the WOCS HPU container.

2.2.5 UPS

The power supply on the workover system consists of two independent Uninterruptible Power Supply (UPS) units which are continuously receiving power from the rig, and providing power to all critical functions in the system. The UPS units are completely independent, with separate lines going from each of the UPS units to the MCU and the HPU. The UPS units are required in order to perform the PSD, ESD and EQD.

2.2.6 Workover Control Module

The WOCM consists of both hydraulic / mechanical parts and electronics.

2.2.7 WOCM hydraulics and WOCM DCVs

The umbilical transfers the signals to the WOCM, located subsea on the EDP. Hydraulic LP supply flows from topside through the umbilical, and is routed on to the hydraulic system in the WOCM.

The main components of the WOCM are the DCVs and the dual redundant SEMs (A and B), which both are regular control SEMs and Safety SEMs. The SEMs contain power supplies, a CPU, a modem and three solenoid drive cards.

The WOCM is responsible for receiving ESD or EQD activation signals from topside and processing the signals in the Safety SEM, which is mounted internally in the WOCM. The safety SEMs pulses the DCV coils in the required sequence upon activation.

DCVs located in the WOCM control the functions on the EDP and LRP. Note that each DCV has two coils on each side enabling both SEM A and B to command the valve open/close.

The WOCM also contains an electrically held fail safe valve. Upon loss of power or communication on both SEMs the fail safe valve will open a flow loop that bypasses the check valve on the fail safe close line.

2.2.8 Subsea Electronic Modules (SEMs)

The Workover Control Module (WOCM) has two SEMs (A & B), which each consists of a Safety SEM and an instrumentation SEM. The two Safety SEMs take care of user-initiated valve operations and shutdown sequence initiations. All shutdown sequences are stored in the Safety SEMs, so to initiate a shutdown or disconnect, the Safety SEMs only need a signal from the SSCU topside commanding ESD or EQD. The shutdown sequence then runs autonomously from the Safety SEMs.

Each DCV in the WOCM have dual coils, allowing parallel/redundant valve operation from both SEMs. I.e. to run a shutdown sequence, it is sufficient that only one of the Safety SEMs (A or B) run the sequence.

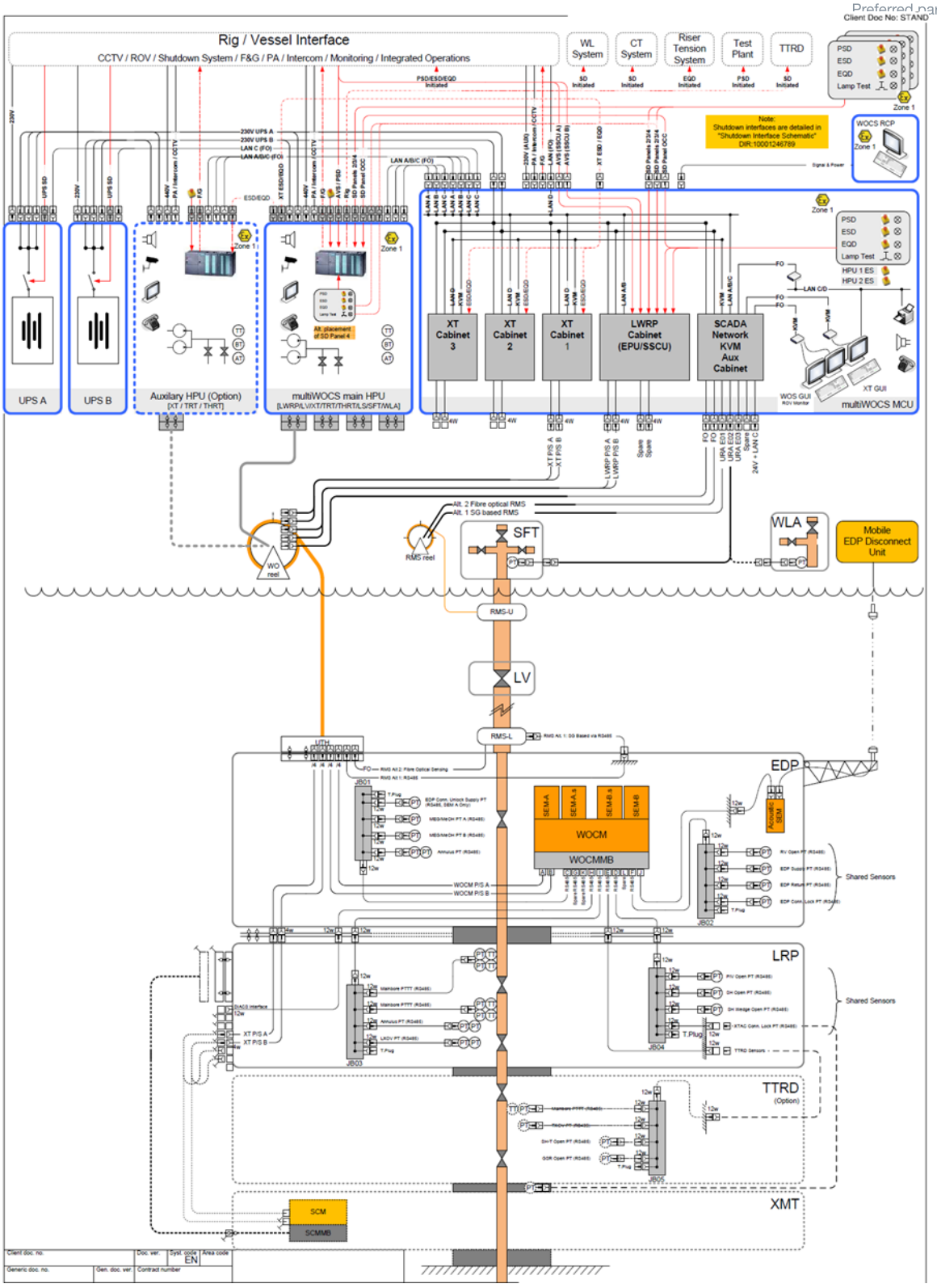


Figure - 1 Electrical top assembly sketch

2.2.9 LRP/EDP Isolation Valves

The LWRP is the lowermost equipment package in the riser string. It consists of the LRP, the EDP and the XT Adaption Connector (XTAC). The LWRP permits well control and ensures safe operation whilst performing CT, WL and well servicing operations. In other words it provides the functions of a BOP on the C/WO riser system.

The key functionality of the LWRP lies in the ability to shut in the well and cutting any WL or CT in the process. If the drilling rig drifts off location, the LWRP also provides the ability to perform an EQD. During an EQD, the EDP will be disconnected from the LRP and the drilling rig can safely drift off location.

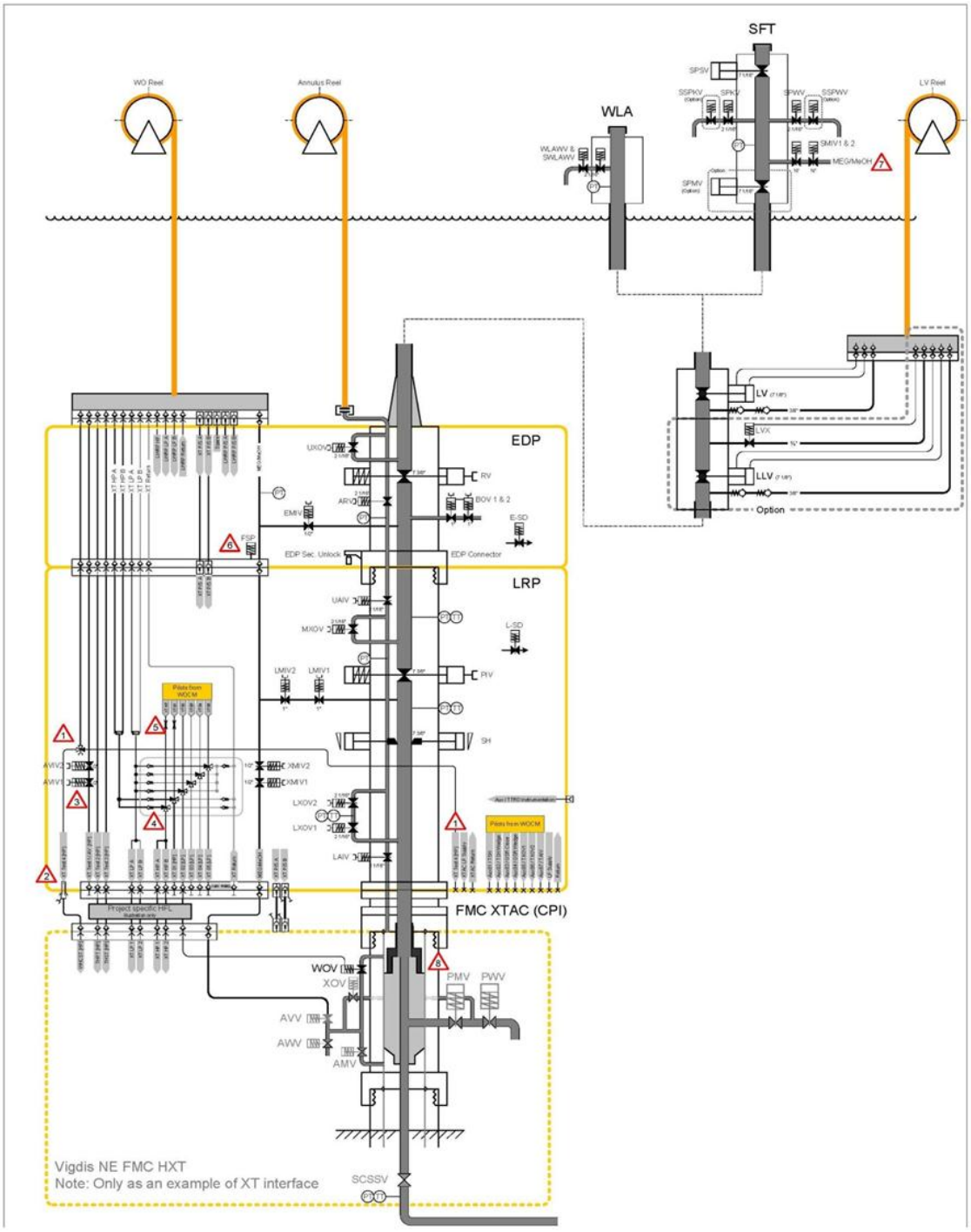
The LRP can be used on different type of XMTs from other vendors. This is made possible due to the bolt-on XTAC, which has the function of providing the interface to the specific XMT.

The main bore valves of the LWRP stack include two off Aker Solutions latest 7-3/8” cutting gate valve technology (RV & PIV) and one off 7-3/8” Texas Oil Tools shear seal ram.

For operational purposes chemical injection are enabled between all valves in the main bore and x-over between the bores allows circulation of the complete riser stack and communication between main bore and annulus. Robust guide structures facilitates for LWRP subsea and moon pool guiding and prevent damage to critical components, either from dropped object or other accidental impact loads.

The valve layout sketch shows the valves relevant to the SIL rated ESD / EQD functions, and is presented in Figure 5.3 In addition to the control / pilot valves in the WOCM, there are hydraulic DCVs and accumulators located on the Lower Riser Package (LRP) and Emergency Disconnect Package (EDP). These are part of the control functionality of the EDP / LRP valves.

Doc. ref. 10001214634-CAD-000-03/ 2011.10.04 / 10:39:31 / Page 1 of 3



Client Doc No: STANDARD

Figure -2 System Valve layout sketch - LWRP

2.2.10 Cross over, annulus and methanol isolation valves

The utility isolations valves are spring return fail safe close gate valves. They are normally held in open position by hydraulic pressure directly from the WOCM. Closure of the valve is achieved by commanding the DCV in the WOCM to the vent / return position. The fail safe functionality will close the isolation valve.

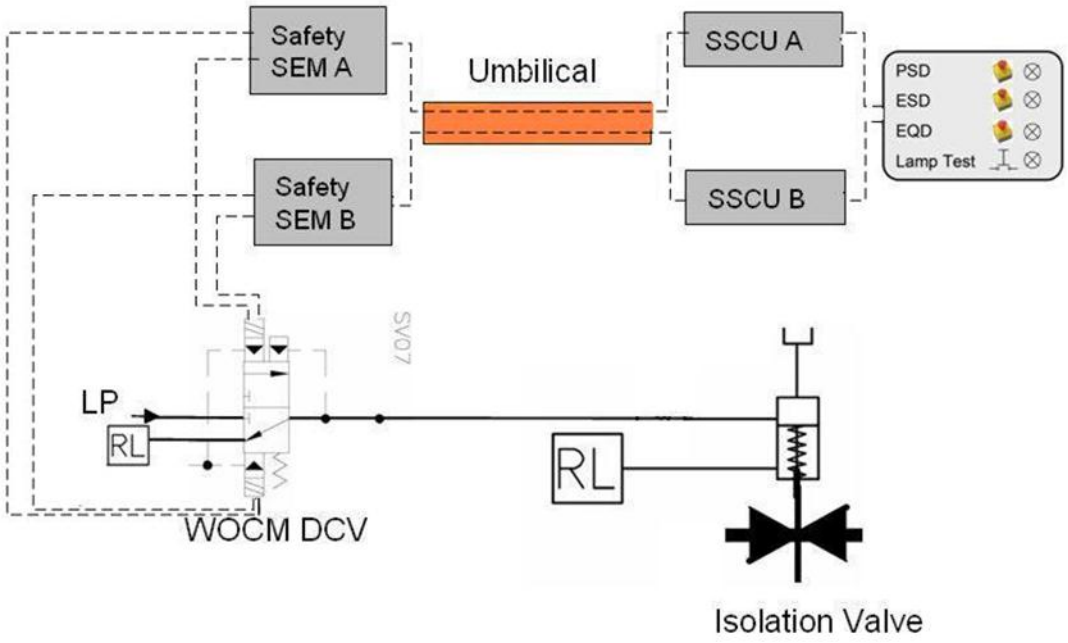


Figure -3 Utility valves control functionality

The following utility valves are bled off directly by the WOCM Directional Control Valves (DCV), and hydraulics is bled through return line(s) in the WOCM:

- UAIV
- LAIV
- LXOV 1&2
- MXOV
- LMIV 1&2
- XMIV 1&2
- AVIV 1&2

2.2.11 PIV and RV

The PIV and RV are spring return close - hydraulically operated 7 3/8” bore gate valves. The primary function of the PIV is to cut WL/CT, close off the main bore and seal towards the well. The RV has the main function of cutting WL/CT, closing-in riser content in case of EQD and to stop the flow before closing the safety head in order to protect the dynamic seal in the SHs upper blade.

The PIV and RV have additional hydraulic DCVs and need additional close assist pressure (i.e. are not directly controlled by the WOCM DCVs):

Note that in order to close, both the ‘open line hydraulic DCV’ and the ‘close line Hydraulic DCV’ needs to latch. When the WOCM DCVs latch - pressure applied to the hydraulic DCV(s) are bled-off, enabling them to latch over to return line

(open line) and/or close assist line (close). The valves will then close. Note that these valves are fail-safe close, but the close assist (cut) functionality is ensured by the close assist line pressure.

Both valves have an extra accumulator that gives pressure support in case of cutting of WL/CT. The PIV has a separate dedicated accumulator providing close assist pressure required performing cutting of WL/CT tubing. The RV gets close assist pressure from the Fail As Is (FAI) accumulator which also provides pressure to the hydraulic pilots for both primary and secondary unlock. The accumulator pressure is required and sufficient to cut and close. Topside hydraulic pressure alone will not meet response time requirements. Note that none of the accumulators have pressure detection locally, but have detection in the supply line, Pressure Transmitter (PT) in supply header.

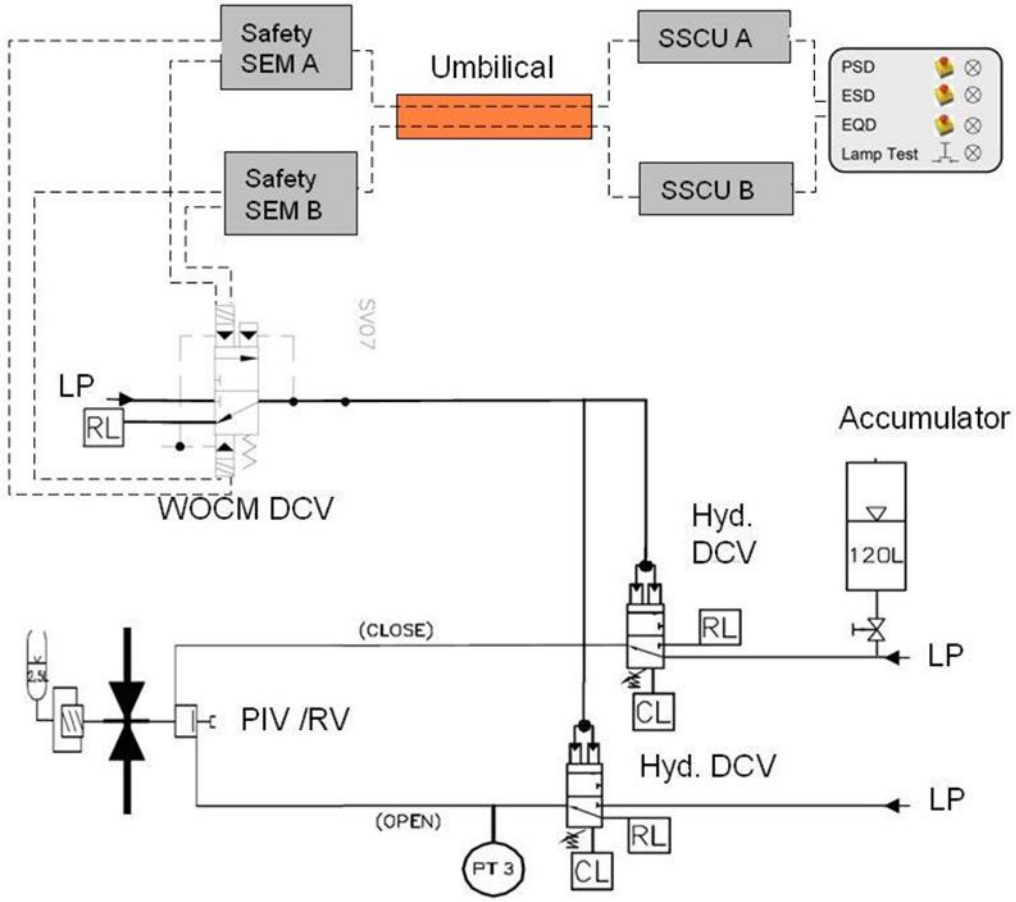


Figure -4 PIV & RV control functionality

2.2.12 Safety Head

The 7 3/8" SH is a Shear and Seal Ram located in the LRP which is a part of the LWRP. In the event of an ESD or an EQD the SH shall cut any WL/CT that might be in the bore, and also isolate the well from the environment.

After the SH has closed a wedge lock is engaged. The wedge lock locks the SH in closed position even upon loss of hydraulic pressure. This component is necessary since there is no spring to ensure that the SH remains closed. The wedge lock also has an open and a close side which needs to be bled off/pressurised in order to close it. There is one wedge lock on each of the two actuators, and the wedge lock hydraulic system is independent of the SH hydraulics.

There is on WOCM DCV controlling the hydraulic pilots on the open and close side of the safety head, and another WOCM DCV controlling hydraulic pilots on the open and close side of the wedge lock. The hydraulic pilots are normally pressurised to keep the SH and wedge lock open, and will fail safe close upon loss of hydraulic pressure in the pilot line. The control of the WOCM DCVs for the SH is the same as for the PIV and RV, illustrated in Figure 5
The SH and wedge lock close side are connected to an accumulator bank consisting of 5 accumulators, but only 4 are necessary in order to successfully cut CT/WL, seal main bore and close wedge lock.

The SH is no qualified for closing and sealing a high flow of hydrocarbons, as the dynamic seal in the upper ram will possibly be washed out by the hydrocarbon flow during closing stroke. In flowing mode it is therefore essential that the RV or PIV is closed before the SH in order for the SH to function as a barrier.
The dynamic seal in the safety head is also susceptible to wear from flowing hydrocarbons when the blades in the rams are fully subtracted. The following restrictions therefore apply to the SH:

1. Max 16 hrs. effective flow period.
2. Only one bleed down after subjected to hydrocarbons and temperature.
3. Max 15 cold closures of the ram.
4. Max 1 warm closure.
5. If a warm closure incident occurs, then max 5 subsequent cold closures.
6. Pressure differential across the shear ram must be equalised prior to opening.

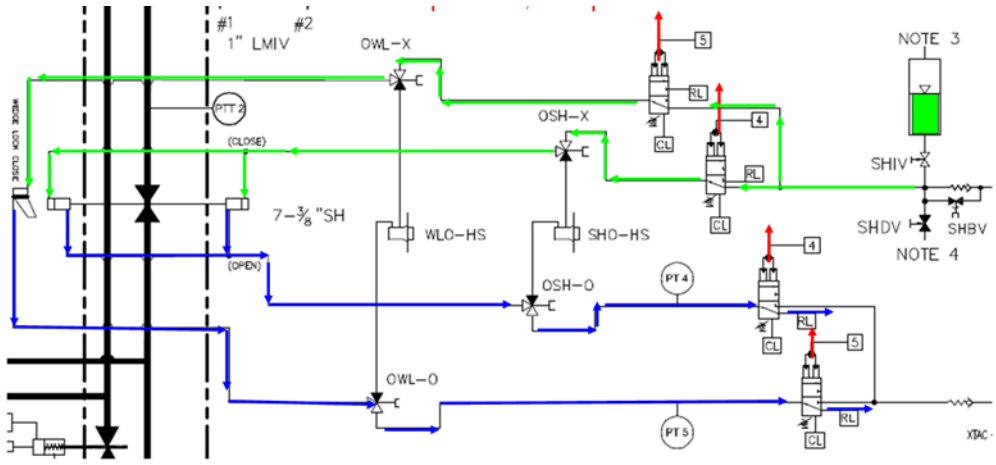


Figure -5 Safety head including wedge lock and corresponding hydraulic pilot valves.

2.2.13 EDP Connector

The EDP connector disconnects the EDP from the LRP, and needs to be pressurized during an EQD (The connector control is not of a fail-safe design). The reason for this solution is that uncontrolled "fail safe" opening of the connector

may result in a dangerous occurrence on the drilling rig (rocket effect etc.). An accumulator connected to the fail as is manifold in the WOCM ensures that sufficient hydraulic pressure is available to operate the hydraulic pilot valves that are part of a disconnection. This is the same accumulator that provides close assist pressure to the RV, and it is called the FAI accumulator. The FAI accumulator is actually an accumulator bank consisting of 3 separate accumulators with 40 l capacity each. Only 2 of these accumulators are needed for the FAI accumulator to perform its tasks, meaning that there is some redundancy built into this accumulator bank. Because of the FAI accumulator, hydraulic pressure from the HPU is not necessary to perform an EQD, and this is why only the FAI accumulator and not the HPU is included in the Reliability Block Diagram (RBD) for EQD.

Two DCVs in the WOCM control the 4 hydraulic pilot valves involved in disconnecting the EDP from the LRP. One of the WOCM DCVs controls the hydraulic pilot which pressurises the primary unlock line and one of the two hydraulic pilot which bleeds down the lock line. The other WOCM DCV controls the hydraulic pilot which pressurises the secondary unlock line and the other of the two hydraulic pilot which bleeds down the lock line. In order to disconnect the EDP from the LRP it is sufficient that one of the pilot valves bleeding down the lock line works, and that either the primary or secondary unlock function works. A failure of one of the WOCM DCVs or one of the hydraulic pilots will therefore not prevent a disconnection.

The primary and secondary unlock functions need accumulators in order to work. The primary unlock function is connected to an accumulator bank with 5 accumulators, but only 4 accumulators are necessary. The secondary unlock function is connected to an accumulator bank with 2 accumulators and both are required in order for the secondary unlock function to work. Note that the secondary unlock is, as the only element in the LWRP, operated on high pressure (690 bar).

Note that the BOV (Bleed-Off Valve) 1&2 are opened during an EQD in order to bleed off the bore pressure between the PIV and RV. Opening the BOVs requires an active hydraulic signal from the WOCM, i.e. pressurising the pilot line. This function is not deemed safety critical in terms of the relevant functions and not included in the RBD. This is supported by force calculations.

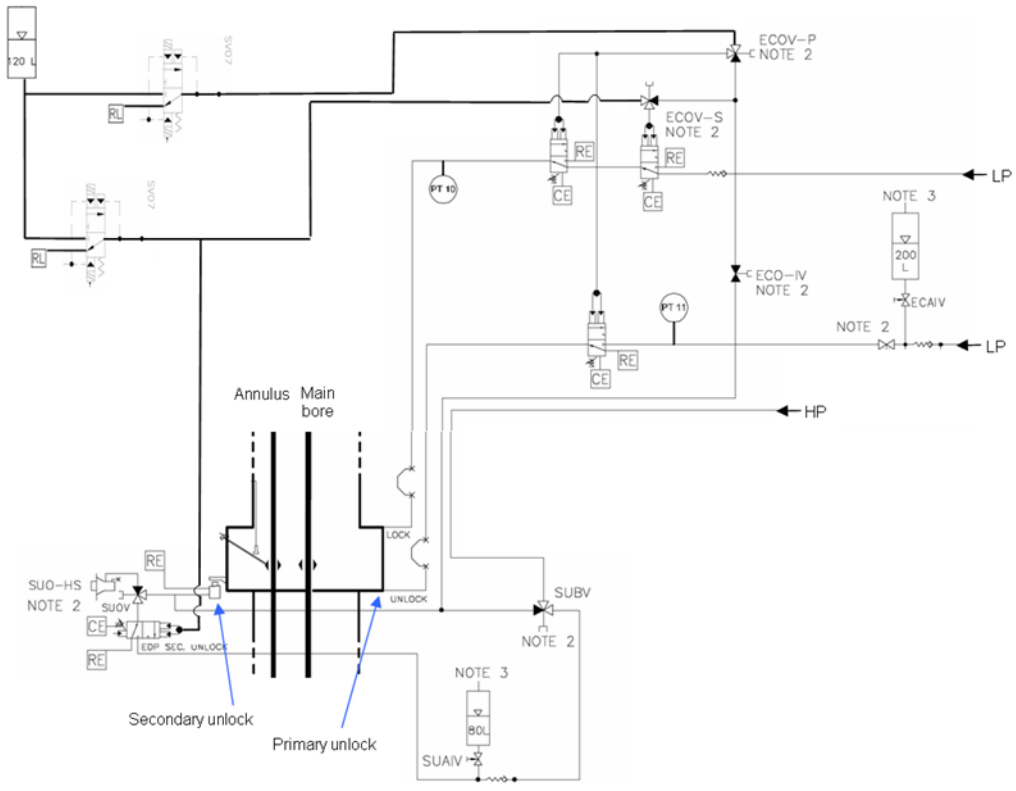


Figure -6 EDP Connector control functionality

2.2.14 Hydraulic pilot valves and return lines

The hydraulic pilot valves are 3 port 2 positions. There are three types of these valves used in the workover system: HP topside valve used in HPU, HP subsea valve used for secondary unlock function and LP subsea valve used for controlling PIV, RV, SH and EDP connector lock and primary unlock. The LP valves are double spring Fail Safe Close (FSC) valves, while the HP is a single spring FSC valve.

The hydraulic pilot valves have different functions in performing parts of the safety functions: The pilot line can either be ventilated or pressurised when safety function is initiated. This in turn will lead to the function line being either pressurised or ventilated. This gives a total of four modes of operation, and the list bellows shows which mode is applicable for the different functions.

1. Pilot line: Ventilated – Function Line: Ventilated
    - SPWV open side (HP topside valve, pneumatic pilot)
    - SH open side
    - Wedge lock open side
    - PIV open side
    - RV open side

2. Pilot line: Ventilated – Function Line: Pressurised
    - Close pressure SH
    - Close pressure Wedge Lock
    - Close Assist pressure PIV
    - Close Assist pressure RV

3. Pilot line: Pressurised – Function Line: Ventilated
    - EDP connector lock function (2 pilot valves)

4. Pilot line: Pressurised – Function Line: Pressurised
    - EDP connector primary unlock function
    - EDP connector secondary unlock function (HP subsea valve)

To run the fail safe functions the pilot lines needs to be ventilated while for the fail as is functions the pilot lines needs to be pressurised.

2.2.15 Sea dump functionality

The EDP Sea Dump and LRP Sea Dump valves (high flow DCVs) will be ventilated during ESD and / or EQD. They will then open, and vent control fluid to sea. This will make the main bore valves close faster. In an ESD or EQD, one of the sea dump valves will be fully open after 3 seconds and one after 5 seconds.
The sea dump valves are not critical for the ESD and EQD functions, as hydraulic analysis shows that the time limits of 30 seconds for ESD and EQD can be reached without opening the sea dump valves.

Chapter 3

3. Safety functional description and common components in control and safety system

The objective of the safety functions is to initiate appropriate shutdown actions to prevent escalation of abnormal conditions into a hazardous event and to limit the duration of such event when it occurs.

3.1. Three Safety functions for workover system.

3.1.1. Process Shutdown (PSD)

The objective of the PSD function is to protect the well test system and the vessel from unsafe situations arising in the well test area on the deck of the vessel and/or in the piping of the production flow from the Surface Flow Tree (SFT).

Upon initiation of the function, the circuit between the PSD push-button and the PLC in the HPU is opened (de-energized). The HPU PLC will then activate a pneumatic solenoid DCV which pilots the hydraulic DCV controlling the pressure on the function line going out of the HPU to the SPWV. As pressure drops on this function line the quick dump valve between the HPU and the SPWV actuator will de-latch and the hydraulic fluid in the open side of the PWV actuator will be vented to the return line accumulator. SPWV will then close by spring-force.

The reliability block diagram for the PSD can be seen in Appendix B01

3.1.2. Emergency Shutdown (ESD)

The objective of an ESD is to isolate the workover riser from well. This is achieved by closing a sequence of valves on the LRP and EDP.

The ESD is initiated by a manually activated push button. Upon initiation of the function, the circuits between the ESD push-button and SSCU A and B are closed (energized). SSCU A and B will send a signal through the WO umbilical to Safety SEM A and B located in the WOCM. The WOCM will then initiated a sequential valve operation of LWRP barrier valves and dump valves.

The reliability block diagram for the ESD can be seen in Appendix B02

3.1.3. Emergency Quick Disconnect (EQD)

The objective of the EQD is to isolate the rig from the riser at the seabed (against the well) by closing all barrier valves part of the ESD sequence, and disconnect the rig from the well.
The ESD is initiated by a manually activated push button. Upon initiation of the function, the circuits between the ESD push-button and SSCU A and B are closed (energized). SSCU A and B will send a signal through the WO umbilical to Safety SEM A and B located in the WOCM. The WOCM will then initiated a sequential valve operation of LWRP barrier valves and dump valves, before it disconnects the EDP from the LRP using the High Angle Release Connector.

EDP disconnect is also available in WOCM retrieval mode. This is a scenario where the WOCM is retrieved, and disconnect can be performed by pressurising the Secondary Unlock line n the WO umbilical directly from the HPU. However, this mode is not a SIL rated function, hence not considered in this document.

The reliability block diagram for the EQD Appendix B03

3.2. Normal control and safety system in workover description

The main components and relation between them for normal control and safety system schematically showed in fig 3 and 4, also the share components between these two systems. The description and rule of each component have been presented in chapter two.

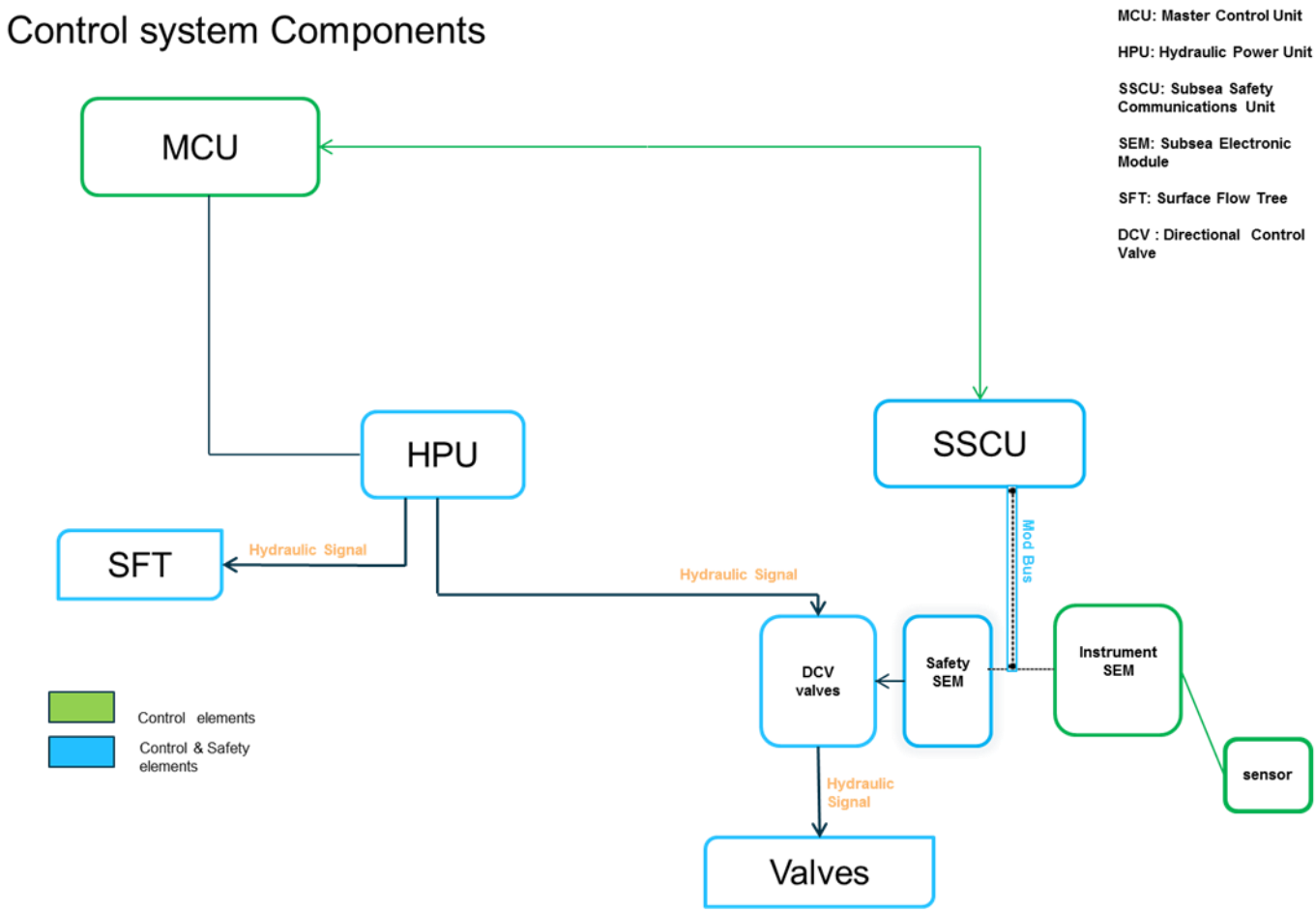


Figure - 7 Normal Control Systems

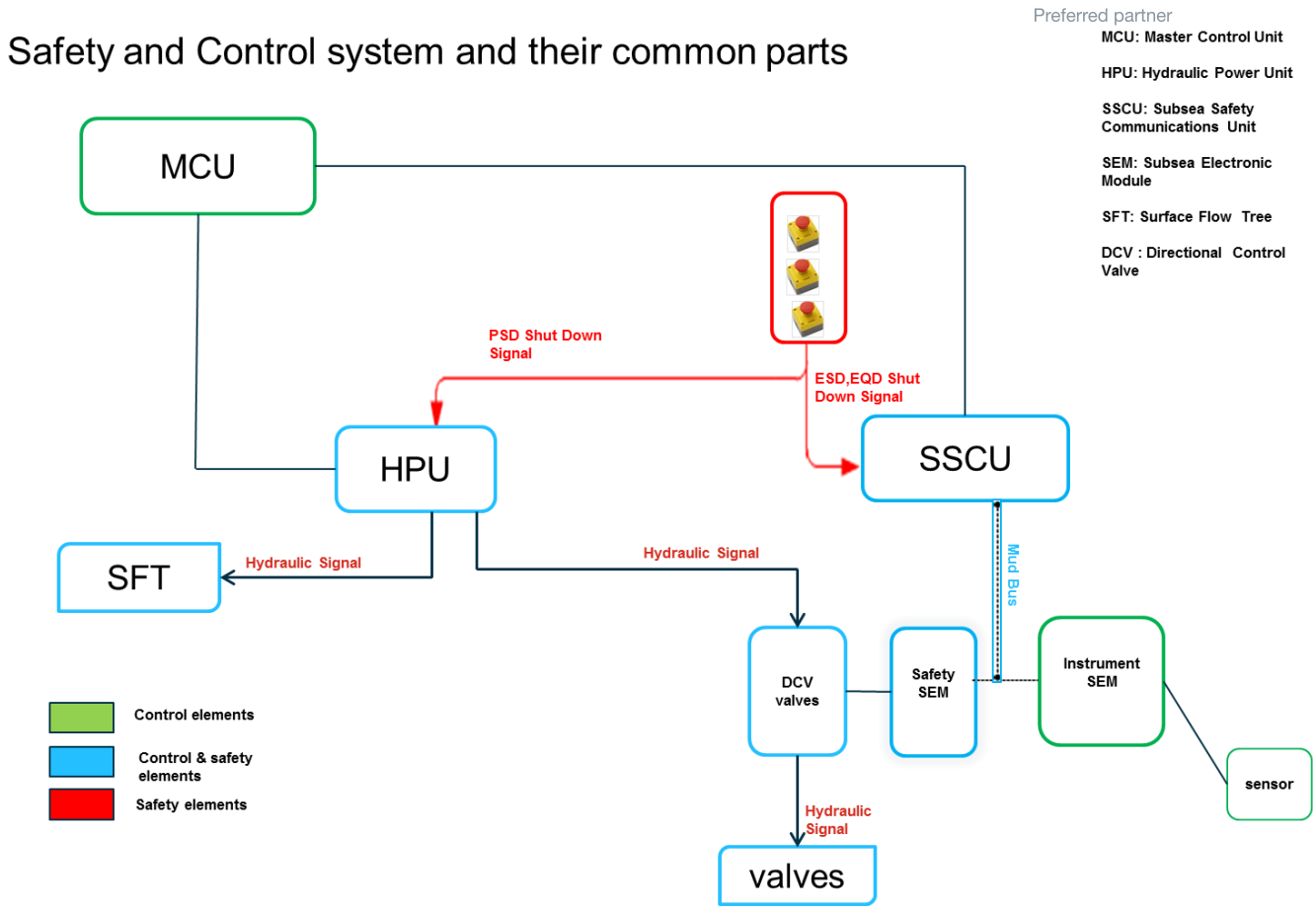


Figure -8 Safety Systems

Chapter 4

4. Safety system problem and alternative solution

Challenges lay with the requirement to independence between process control system and safety system. For Aker's Workover system the communication line from topside to subsea and, the Subsea Electronic Modules (SEMs) are currently shared between the normal control and the safety system. According to IEC 61508 this is allowed, but requires substantial documentation of independence between the safety and non-safety systems, it is also a challenge to find sound statistical data for the verification process. Furthermore any changes to the normal control system in the SEMs needs to be evaluated from a safety point of view, and might also create a need for updating the safety documentation. This severely limits the ability to perform any changes to the non-safety software.

4.1. Standard requirements

4.1.1. **IEC61508**

E/E/PE system design requirements specification
Where an E/E/PE safety-related system is to implement both safety and non-safety functions, then all the hardware and software shall be treated as safety-related unless it can be shown that the implementation of the safety and non-safety functions is sufficiently independent (i.e. that the failure of any non-safety-related functions does not cause a dangerous failure of the safety-related functions).
NOTE 1: Sufficient independence of implementation is established by showing that the probability of a dependent failure between the non-safety and safety-related parts is sufficiently low in comparison with the highest safety integrity level associated with the safety functions involved

4.1.2. **NOG – 070**

8.8 Independence between safety systems
To fulfil the requirements of the PSA and IEC 61508/61511 concerning independences between safety systems (i.e. a failure in one systems shall not adversely affect the intended safety function of another system), no communication or interaction shall occur from the PCS system to any safety system, from the PSD system to ESD, or from the PSD system to F&G. Special measures shall be implemented to avoid adverse effects between SIS and non SIS systems and applications, and between SIS nodes. If special measures are implemented, a limited degree of interconnection can be allowed. Such special measures together with examples of unacceptable and conditionally acceptable solutions are given in Appendix G.

4.2. Alternative solution

At this stage the practical solution seems to be generating new Modbus and new SEM for safety system and maintain the existing SEM and Modbus just for control system. In this solution as schematically described in figure 6 the independent SEM will be communicate through new Modbus with initiator .Simultaneously the existing SEM perform just as control task and maintain the DCV valves in open position with independent

communication way to Master control unit . In emergency case a signal comes from push bottom to new safety SEM through Modbus and shutdown signal will sent by safety SEM to DCV valve and will close the valves and finally put the system in safe state. The main advantage of new design is that we have no expected the effects from non-safety to safety components.
For PSD in order to done maximum independently for safety system the new design consist of one DCV valve that in case of emergency the hardware signal directly comes from shutdown panel on that and cut the hydraulic so consequently the bleed down the hydraulic and close surface flow tree valve, the detail will be followed in figure9. The new RBD design based of new arrangement in safety system could be followed in B .01

In ESD for maximum independency in safety system the new DCV implemented outside of WOCM in order to bleed down the hydraulic on emergency case, in this new design two redundant DCV design inside workover safety module and we don't use WOCM DCV for safety system, just the WOCM DCV's will be used for control system, these two WSM DCV's can bleed down the hydraulic pressure in LP flow and accumulator, the detail of arrangement will be followed in ESD RBD in B.02

Also for EQD two accumulators and 2 DCV implemented the detail of arrangement will be followed in EQD RBD in B.03.

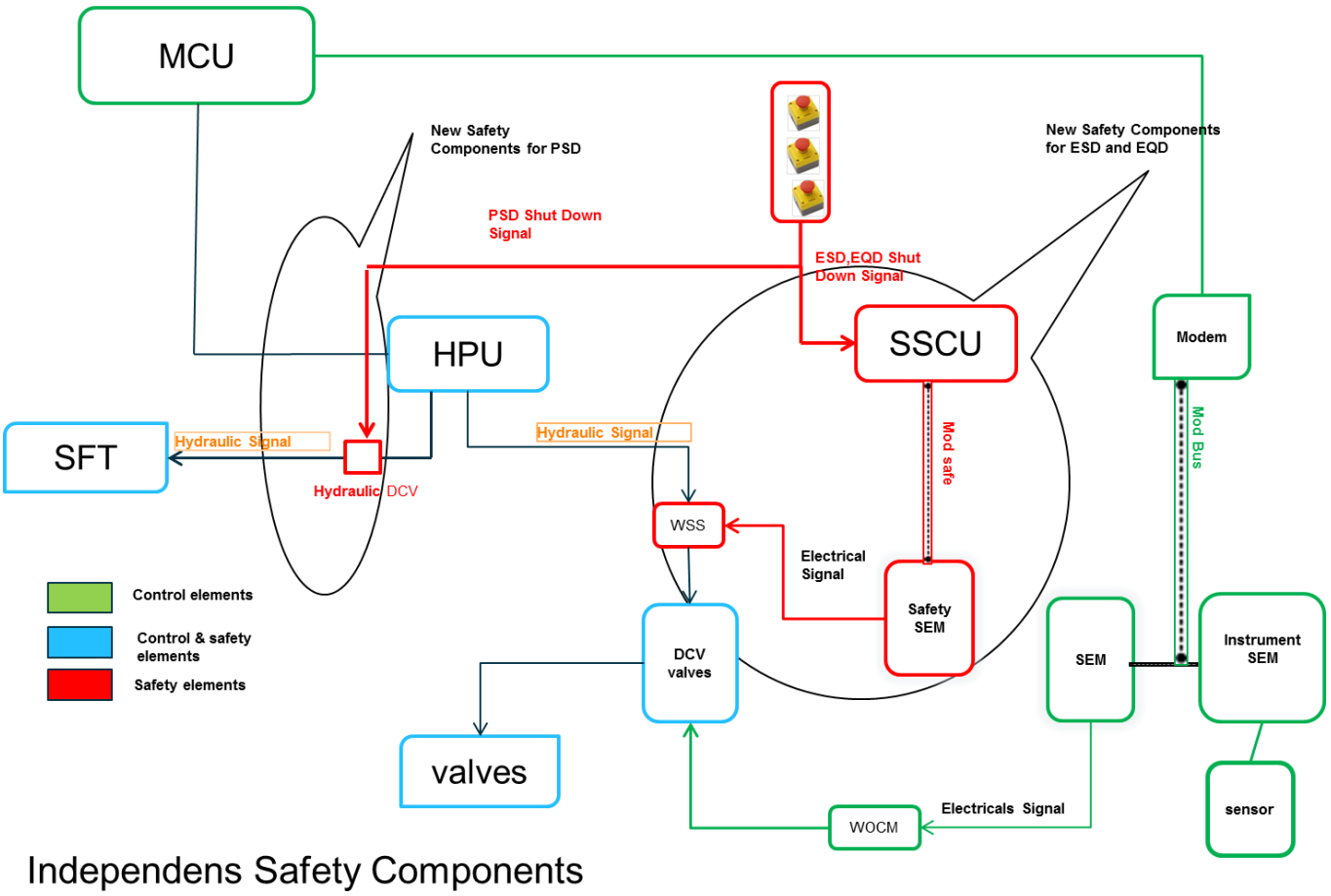


Figure - 9 New Safety Systems

4.3. Compare new system to current system

The appropriate and reasonable way for compare the new system with current system is risk reduction evaluation and probability calculation in order to assess the new safety system can meet the safety integrity level(SIL) requirement also will be enough safe

4.4. Examine the new system regarding risk reduction

There are different method for risk evaluation and show that how the new safety system will reduce the risk of hydrocarbon release during well intervention and workover.

In this thesis study I use the HAZOP Study for Qualitative risk evaluation and use of template of previous project that before have been done by Akersolution Safety and risk department, the effective and realistic way for understanding that new system is really safe and can be meet the standard requirement, also the PFD calculation done and the result shows that the new system can meet the safety integrity level requirement. The detail of PFD calculation and compare of the result for new safety system and old system could be follow in chapter six**.**

Chapter 5

5. Risk Evaluation

The risks associated with light well intervention are primarily related to uncontrolled or misdirected flow of hydrocarbons. In addition there is a risk of dropping the stack (EDP and LRP) on the X-mas tree (XT) on the well during running and retrieval of the system. There is also a risk related to vessel loss of position resulting in hydrocarbon leak and damage to equipment.
The primary concern is spill of hydrocarbons causing either fire/explosion on the vessel or spill to the environment plus financial losses associated with production loss.
The potential hydrocarbon spills can be split in three main categories based on location of the leakage. Leakages downstream the Surface Production Wing Valve (SPWV), typically associated with the well test facility, should be stopped using the well-defined Production Shutdown (PSD) function. This closes the SPWV isolating the vessel from flowing hydrocarbons.
Potential hydrocarbon spills above the LRP and for events topside where PSD is deemed insufficient, such as major fires, should be mitigated using the Emergency Shutdown (ESD) function. This function closes all LRP valves outside the vertical main bore, RV and the two cutting and sealing valves in the main bore of the LRP.
There is a risk of loss of position, in which equipment may be damaged causing spill to sea. In this situation the Emergency Quick Disconnect (EQD) should be utilized. This function is identical to the ESD. In addition the EDP connector is unlocked allowing the vessel to drift/drive off location without the risk of damaging equipment leading to hydrocarbon spill.
The RV is closed in order to prevent rocketing effects from the hydrocarbons potentially providing lift to the riser as the EDP disconnects from the LRP.

5.1. Risk **Assessment Definitions**

The term ‘’risk ‘’ is used in variety of ways in everyday speech. We frequently refer to activities such as rock –climbing or day-trading stocks as ‘’risky’’; or discuss our ‘’risky’’ of getting the flu this coming winter.in the case rock-climbing and day-trading, ‘’risky ‘’ is used to mean hazardous or dangerous.in the letter reference, ‘’risk’’ refers to the probability of a defined outcome(the chance of contracting the flu).before beginning a discussion of risk assessment, it is important to provide a clear definition of the term ‘’risk’’ and some of the other terminology used in the risk assessment field.so we need to define a number of terms:

5.1.1. **Hazards or Threats**

Hazard or threats are conditions which exist which may potentially lead to an undesirable event

5.1.2. **Controls**

Controls are the measures taken to prevent hazard from causing undesirable events. Control can be physical (emergency shutdown, redundant controls, conservative designs, etc.) procedural (written operating procedures), and can address human factors (employee selection, training, supervision).

5.1.3. **Event**

An event is an occurrence that has an associated outcome. There are typically numbers of potential outcomes from any one initial event which may range in severity from trivial to catastrophic, deepening upon other conditions and add-on events.

5.1.4. **Risk**

Now we are ready to provide a technical definition of the term risk. Risk is composed of two elements, frequency and consequence.
Risk is defined as the product of frequency with which an event is anticipated to occur and the consequence of the event's outcome.
Risk = Frequency × consequence

5.1.5. **Frequency**

The frequency of potential undesirable event is expressed as events per unit time, usually per year. The frequency should be determined from historical data if a significant number of events have occurred in the past. Often, however, risk analyses focus on events with more severe consequences (and low frequencies) for which little historical data exist.

5.1.6. **Consequence**

Consequence can be expressed as the number of people affected (injured or killed), property damaged, amount of spill, area affected, outage time, and mission delayed. Regardless of the measure chosen, the consequences are expressed ''per event''. Thus the risk equation has the units ''event/year'' times ''consequences/event'' which equals ''consequences/year'', the most typical quantitative risk measure.

5.2. Risk **Assessment Process**

To use a systematic method to determine risk levels, the Risk Assessment Process is applied. This process consists of four basic steps:

5.2.1. **Hazard Identification**

In some cases, after identifying the hazards, qualitative methods of assessing frequency and consequence are satisfactory to enable the risk evaluation. In other cases, a more detailed quantitative analysis is required. There are many different analysis techniques and models that have been developed to aid in conducting risk assessments. A key to any successful risk analysis is choosing the right method (or combination of methods) for the situation at hand.in this part I try to provide a brief introduction to some of the analysis methods available and suggest risk analysis approaches to support different types of decision.

5.2.2. **Hazard identification (HAZID) Technique**

HAZID is a general term used to describe an exercise whose goal is to identify hazards and associated events that have the potential to result in a significant consequence. For example, a HAZID of an offshore petroleum facility may be conducted to identify potential hazards which could result in consequence to personnel (e.g., production loss/delay). The HAZID technique can be applied to all or part facility or vessel or it can be applied to analyse operational procedures. Depending upon the system being evaluated and the resources available, the process used to conduct a HAZID can vary typically, the system being evaluated is divided into manageable parts, and a team is led through a brainstorming session(often with use of checklists) to identify potential hazards associated with each part of the system.

This process is usually performed with a team experienced in the design and operation of facility, and the hazards that are considered significant are prioritized for further evaluation.

5.2.2.1.What - if Analysis

What - if analysis is brainstorming approach that uses broad that uses broad, loosely structured questioning to (1) postulate potential upsets that may result in mishaps or system performance problems and (2) ensure that appropriate safeguards against those problems are in place. This technique relies upon a team of experts brainstorming to generate a comprehensive review and can be used for any activity or system. What –if analysis generates qualitative descriptions of potential problems (in the form of questions and responses) as well as lists of recommendations for preventing problems.it is applicable for almost every type of analysis application, especially those dominated by relatively simple failure scenarios.it can occasionally be used alone, but most often is used to supplement other, more structured techniques (especially checklist analysis).

5.2.2.2.Failure Modes and Effects Analysis (FMEA)

FMEA is an inductive reasoning approach that is best suited for reviews of mechanical and electrical hardware systems. This technique is not appropriate to broader marine issue such as harbour transit or overall vessel safety. The FMEA technique (1) considers how the failure mode of each system components can result in system performance problem and (2) ensures that appropriate safeguards against such problems are in place. This technique is applicable to any well-defined systems, but the primary use is for reviews of mechanical and electrical systems (e.g,fire suppression systems, vessel steering /propulsion systems).it also is used as the basis for defining and optimizing planned maintenance for equipment because the method systematically focuses directly and individually on equipment failure modes.FMEA generates qualitative descriptions of potential performance problems(failure modes, root cause, effects, and safeguards) and can be expanded to include quantitative failure frequency and /or consequence estimates.

5.2.2.3.Checklist Analysis

Checklist analysis is a systematic evaluation against pre-established criteria in the form of one or more checklists.it is applicable for high-level or detailed-level analysis and is used primarily to provide structure for interviews, documentation reviews and field inspections of the system being analysed. The technique generates qualitative lists of conformance and non-conformance determinations with recommendations for correcting non-conformances. Checklist analysis is frequently used as a supplement to or integral part of another method to address specific requirements.

5.2.2.4.Hazard and operability (HAZOP) Analysis

The HAZOP analysis technique uses special guidewords to prompt an experienced group of individuals to identify potential hazard or operability concerns relating to pieces of equipment or systems. Guidewords describing potential deviations from design intent are created by applying a pre define set of adjectives (i.e. high low, no, etc.) to a pre-defined set of process parameters (flow, pressure, composition, etc.). Then group then brainstorms potential consequences of these deviations and if a legitimate concern is identified, they ensure that appropriate safeguards are in place to help prevent the deviation from cccuring.This type of analysis is generally used on a system level and generates primarily qualitative results, although some simple quantification is possible. The

primary use of the HAZOP methodology is identification of safety hazards and operability problems of continuous process systems (especially fluid and thermal systems). For example this technique would be applicable for an oil transfer system consisting of multiple pumps, tanks, and process lines. The HAZOP analysis can also be used to review procedures and sequential operations.

A HAZOP study is a formal technique to systematically examine the process design of a facility, with due regard for the planned mode of operation, inspection and maintenance. A HAZOP has as aim to systematically examine a system design, to identify potential hazards and operational problems from all possible causes, and to make judgements whether planned design or operational safeguards are adequate, or if further mitigating actions are required.

A HAZOP study is performed by a HAZOP team, consisting of experienced engineers and operating personnel from appropriate disciplines, facilitated by an independent chairman experienced in the use of the HAZOP methodology. The team may include representation from both the design contractor and from their client who is to operate and maintain the facility. Typically the team may include process engineers, project engineers, electrical & instrument engineers, maintenance engineers and senior operating personnel. Other specialists may be drafted in to the meeting when appropriate.

The HAZOP review is normally based on P&IDs of the planned facility, while PFDs, Cause and Effect Diagrams, Hazardous Area Classification drawings and Layout Drawings may also be used to provide additional information. During a HAZOP, the P&IDs will be broken down in to logical sub-systems (nodes), which may be a vessel, line interconnecting equipment, or some other logical sub-system.
The HAZOP technique involves the following steps:

1. Identify the node to be studied
2. Define the design intent of the node and the normal operating parameters
3. Apply a HAZOP deviation (e.g. NO/LESS FLOW) to the node
4. Identify all possible causes for the deviation
5. Identify for each cause all possible consequences, without regard for the safeguards in place
6. Identify all available safeguards to prevent the cause or to limit the consequences
7. Recommend any new safeguards where judged necessary
8. Repeat steps 4 to 7, using the next HAZOP deviation
9. Repeat steps 3 to 8 until all HAZOP deviations have been applied to the node
10. Select the next node to be studied, repeating steps 1 to 9
11. Repeat until all nodes are studied

5.2.2.4.1. HAZOP guidewords and parameters

The guidewords and parameters used in the HAZOP are presented in the table below.

Parameter
Flow
Pressure
Temperature
Level
Operability
Maintenance
Material
Shutdown
Start-up

Guide-word
No or Not
More or Less
As well As
Part of
Reverse
Other than

5.2.3. Frequency Assessment

5.2.3.3.Frequency Assessment Methods

After the hazards of a system or process have been identified, the next step in performing a risk assessment is to estimate the frequency at which the hazardous events may occur. The following are some of the techniques and tools available for frequency assessment.

5.2.3.1.1. Analysis of Historical Data

The best way to assign a frequency to an event is to research industry databases and locate good historical frequency data which relates to the event being analysed. Before applying historical frequency data, a thoughtful analysis of the data should be performed to determine its applicability to the event being evaluated. The analyst needs to consider the source of the data, the statistical quality of the data (reporting accuracy, size of data set, etc.) and the relevance of the data to the event being analysed. For example, transportation data relating to helicopter crashes in the North Sea may not be directly applicable to gulf of Mexico operations due to significant differences in atmospheric conditions and the nature of helicopter operating practices.in another case, frequency data for a certain type vessel navigation equipment failure may be found to be based on a very small sample of reported failures, resulting in a number which is not statistically valid.
When good, applicable frequency data cannot be found, it may be necessary to estimate the frequency of an event using one of the analytical methods described below.

5.2.3.1.2. Event Tree Analysis (ETA)

Event tree analysis utilizes decision trees to graphically model the possible outcomes of an initiating event capable of producing an end event of interest. This type of analysis can provide (1) qualitative descriptions of potential problems (combinations of events producing various types of problems from initiating events) and (2) quantitative

estimates of event frequencies or likelihoods, which assist in demonstrating the relative importance of various failure sequences. Event tree analysis may be used to analyse almost any sequence of events, but is most effectively used to address possible outcomes of initiating events for which multiple safeguards are in line as protective features.

5.2.3.1.3. Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is a deductive analysis that graphically models (using Boolean Logic) how logical relationships among equipment failure, human errors and external events can combine to cause specific mishaps of interest. Similar to event tree analysis, this type of analysis can provide (1) qualitative descriptions of potential problems (combinations of events causing specific problems of interest) and (2) quantitative estimates events of failure frequencies/likelihoods and the relative importance of various failure sequences /contributing events. The methodology can also be applied to many types of applications, but is most effectively used to analyse system failures caused by relatively complex combinations of events.

5.2.3.1.4. Common Cause Failure Analysis (CCFA)

CCFA is a systematic approach for examining sequences of events stemming from multiple failures that occur due to the same root cause. Since these multiple failure or errors result from the same root cause, they can defeat multiple layers of protection simultaneously. CCFA has the following characteristics:

- Systematic, structured assessment relying on the analyst's experience and guidelines for identifying potential dependencies among failure events to generate a comprehensive review and ensure that appropriate safeguards against common cause failure events are in place
- Used most commonly as a system-level analysis
- Primarily performed by an individual working with system experts through interviews and field inspections
- Generates
  - Qualitative descriptions of possible dependencies among events
  - Quantitative estimates of dependent failure frequencies/likelihoods
  - List of recommendations for reducing dependencies among failure events
- Quality of the evaluation depends on the quality of the system documentation, the training of the analyst and the experience of the SME assisting the analyst

CCFA is used exclusively as a supplement to a broader analysis using another technique, especially fault tree and event tree analyses. It is best suited for situations in which complex combinations of errors/equipment failures are necessary for undesirable events to occur.

5.2.3.1.5. Human Reliability Analysis

Where human performance issues contribute to the likelihood of an end event occurring, methods for estimating human reliability are needed. For instance, an event tree could be constructed which includes a branch titled ‘’ operator responds to alarm and takes appropriate corrective action ’’in order to estimate a numerical frequency with which this occurs, human reliability analysis can be applied.

One of the best known approaches for assessing human errors is Human Reliability Analysis. Human reliability analysis is a general term for methods by which human errors can be identified, and their probability estimated for those actions that can contribute to the scenario being studied, be it personnel safety, loss of the system, environmental damage, etc. The estimate can be either qualitative or quantitative, depending on the information available and the degree of detail required.

5.2.4. **Consequence Assessment**

5.2.4.1.Consequence Assessment Method

Consequence modelling typically involves the use of analytical models to predict the effect of a particular event of concern. Examples of consequence models include source term models, atmospheric dispersion models, blast and thermal radiation models, aquatic transport models and mitigation models. Most consequence modelling today makes use of computerized analytical models. Use of these models in the performance of a risk assessment typically involves four activities:

- Characterizing the source of the material or energy associated with the hazard being analysed
- Measuring (through costly experiments) or estimating (using models and correlations) the transport of the material and/or the propagation of the energy in the environment to the target of interest
- Identifying the effects of the propagation of energy or material on the target of interest
- Quantifying the health, safety, environmental, or economic impacts on the target of interest

5.2.5. **Risk Evaluation**

5.2.5.1.Risk Evaluation and Presentation

Once the hazards and potential mishaps or events have been identified for a system or process, and the frequencies and consequences associated with these events have been estimated, we are able to evaluate the relative risks associated with the events. There are a variety of qualitative and quantitative techniques used to do this. Perhaps the simplest qualitative form of risk characterization is subjective prioritization. In this teqnique, the analysis team identifies potential mishap scenarios using structured hazard analysis techniques (e.g., HAZOP; FMEA). The analysis team subjectively assigns each scenario a priority category based on the perceived level of Risk. Priority categories can be:

i) Low, medium, high;
ii) Numerical assignments; or
iii) Priority levels.

5.2.5.2. Risk Categorization/Risk Matrix

Another method to characterize risk is categorization. In this case, the analyst must (1) define the likelihood and consequence categories to be used in evaluating each scenario and (2) define the level of risk associated with likelihood/consequence category combination. Frequency and consequence categories can be developed in a qualitative or quantitative manner. Qualitative schemes (i.e., low, medium, or high) typically use qualitative criteria and examples of each category to ensure consistent event classification. Multiple consequence classification criteria may be required to address safety, environmental, operability and other types of consequences. Figure 10 provide

of criteria for categorization of consequences and likelihood.

5.2.5.3.Risk Classification

Frequency	
Category	**Definition**
High	Have heard of it and its likely to occur
Medium	Have heard of, but not likely to occur, Never heard of, but likely to occur
Low	Never heard of and not likely to occur

Consequence	
Category	**Definition**
High	Death/Permanent disability Severe environmental impact. Loss of equipment
Medium	Personnel injury, Moderate environmental impact, Material damage, Time delay
Low	Never Minor impact on schedules, Minor material damage, Minor injuries heard of and not likely to occur

Risk Matrix				
Frequency / Severity		Low	Medium	High
		1	2	3
High	3			
Medium	2			
Low	1			

Figure 10 Risk Matrix

Once assignment of consequences and likelihoods is complete, a risk matrix can be used as a mechanism for assigning risk (and making risk acceptance decisions), using a risk categorization approach. Each cell in the matrix corresponds to a specific combination of likelihood and consequence and can be assigned a priority number or some other risk descriptor (as shown in figure 10). An organization must define the categories that it will use to score risks and, more importantly, how it will prioritize and respond to the various levels of risks associated with cells in the matrix

5.3. Risk Evaluation in this work

The risks associated with light well intervention are primarily related to uncontrolled or misdirected flow of hydrocarbons. In addition there is a risk of dropping the stack (EDP and LRP) on the X-mas tree (XT) on the well during running and retrieval of the system. There is also a risk related to vessel loss of position resulting in hydrocarbon leak and damage to equipment.

The primary concern is spill of hydrocarbons causing either fire/explosion on the vessel or spill to the environment plus financial losses associated with production loss.

The potential hydrocarbon spills can be split in three main categories based on location of the leakage. Leakages downstream the Surface Production Wing Valve (SPWV), typically associated with the well test facility, should be stopped using the well-defined Production Shutdown (PSD) function. This closes the SPWV isolating the vessel from flowing hydrocarbons.

Potential hydrocarbon spills above the LRP and for events topside where PSD is deemed insufficient, such as major fires, should be mitigated using the Emergency Shutdown (ESD) function. This function closes all LRP valves outside the vertical main bore, RV and the two cutting and sealing valves in the main bore of the LRP.

There is a risk of loss of position, in which equipment may be damaged causing spill to sea. In this situation the Emergency Quick Disconnect (EQD) should be utilized. This function is identical to the ESD. In addition the EDP connector is unlocked allowing the vessel to drift/drive off location without the risk of damaging equipment leading to hydrocarbon spill.

The RV is closed in order to prevent rocketing effects from the hydrocarbons potentially providing lift to the riser as the EDP disconnects from the LRP.

The workover stack design includes two Aker Solutions gate valves, RV and PIV, and a Texas Oil Tools Ram, SH. The SH is not qualified for cutting and sealing in flowing conditions. The defined source of demand for the ESD function is unintentional or uncontrolled flow of hydrocarbons causing spill above the LRP. This implies that the RV has to close and stop the flow of hydrocarbons before the PIV and SH can close in order to ensure a sealed well.

The SH is more suitable for shearing wireline and coiled tubing than the PIV, and it has previously been concluded that the SH shall close before the PIV in non-flowing conditions. This is however a complicating factor for the safety system. With the philosophy of safety through simplicity, it is concluded in the WSS Hazard Evaluation that the safety system should not include mode switches as the ESD and EQD functions will be able to reach safe state in any mode of operation provided the RV closes before the PIV and SH.

The downside to this is possible equipment damage in non-flowing conditions. As the safety functions are a last resort, equipment damage is secondary to the certainty of reaching safe state in a simple and efficient manner. A qualitative risk evaluation supports this conclusion, refer to Appendix A.

Chapter 6

6. Modelling for PFD calculation and safety integrity level

In order to check the new system to comply the SIL target (SIL) we need to calculate the probability failure on demand and so check the SIL rating of the system , the PFD calculation done by CARA Fault Tree Analysis software,
The following assumption and formula used during the PFD calculation. Also the failure rate that listed in Table 3 that comes from failure rate data book and some vendor data used for PFD calculation. The result of PFD calculation can be followed in Appendix C and Appendix D.

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	10^-5 to 10^-4	10^-9 to 10^-8
3	10^-4 to 10^-3	10^-8 to 10^-7
2	10^-3 to 10^-2	10^-7 to 10^-6
1	10^-2 to 10^-1	10^-6 to 10^-5

Table 2- probability failure on demand to meet SIL

6.1. Assumptions are made when analysing / modelling the system:

- When providing probability of failure on demand (PFD) figures it is assumed that all undetected failure modes will be identified by proof test. It is assumed that all components will be as good as new after each proof test. Testing is assumed to be performed according to procedures, and shall thus not introduce failures in the system.

- The bleed off valves (BOVs) have not been regarded as critical when performing an EQD, hence they have not been included in the PFD-calculations. The function of the BOVs is to bleed off pressure in main bore between PIV and RV before disconnecting the EDP from the LRP. However, it has been shown that the EDP connector is able to disconnect both with 690 wellhead shut-in pressures in main bore.
- Function testing of the system is assumed performed every month in the SRS. 1 month proof test interval is therefore the base case assumption for the PFD calculations.

- If a failure should occur on the safety critical components in the LRP / EDP, the riser system must be retrieved, stripped down and the component fixed (e.g. degraded operation not allowed. This is in conjunction with NPD regulations).

- Safe state: One barrier needed to establish safe state for ESD, i.e. either SH or PIV establishes safe state for the main bore on the LRP. The SH can only establish safe state given that the RV (or PIV) has stopped the flow before the SH closes.

- Leakages in the ROV operated 3-way valves are considered negligible. Small leakages are not a problem; larger leakages will be detected in the HPU for valves mounted on open and lock side. All valves are tested in correct position before deployment

- Piping is not included in the analysis. There is only hard piping, and the failure rate is deemed negligible.

- MQC failures are not included

- The umbilical and deck jumpers are assumed to have no DU-failures. Due to the accumulator's located subsea, hydraulic pressure applied from topside will not be critical in performing a shutdown as long as the WSM is pressurised. The electrical pulse / signal sent subsea is critical, but diagnostic testing will detect any failures (e.g. ping testing, MODBUS safe protocol).

- In the calculations it is assumed that the system is as good as new after each proof test.

- Components not included/not assumed critical:
    - Filter on return lines (DU failures assumed very unlikely).
    - Flow meter on return.

- DCVs in WSM assumed to have one CCF contribution

- Check valves and other points of leakage are assumed to have an insignificant impact on the overall result and are thus not included in the calculations. This may be justified by no reported leakage failures on check valves in OREDA 2009. For control valves, 1 failure due to leakage is reported among an inventory of 460.

- Secondary unlock is assumed independent and redundant to the primary unlock function.

- Dangerous detected (DD) failures are not included in the PFD calculations, as it is assumed that the system will be taken to safe state upon detection of a dangerous failure. Upon loss of PSD or ESD, the system can be taken to safe state by hydraulic bleed down in HPU. Since the EQD needs an active signal to be performed there is an acoustic backup system in place which can perform a disconnection upon loss of power. The acoustic back-up system is battery operated, and designed to have a minimum of components in common with the normal disconnect signal. An FMECA has been performed for the acoustic EQD system, where its independence from the EQD function has been verified. In case of a failure taking out both the normal EQD system and the acoustic back-up system, there is a possibility for ROV disconnect. An ROV disconnect involves turning a three-way valve, cutting the hydraulic supply line to the connector lock function and engaging the hot-stab. Assuming the ROV is already deployed, the disconnect operation is estimated to take no more than 30 minutes. Note that the ROV must have sufficient amounts of 5 kpsi hydraulic oil available to perform this operation.

- CCF modelling:

    - A Simple Beta-factor CCF model is used.
    - When a CCF occurs it will take down all the concerning components.
    - Series structures is assumed to have no effect on CCFs → e.g. 2 valves in series in parallel with one valve, is assumed to be "CCF evaluated" as 2 valves in parallel.
    - Component type and similar failure rate is used as evaluation criteria
    - If components have different failure rates, the conservative value is chosen.

- The analysis assumes constant failure rates and therefore the effects of early failures are expected to be removed by appropriate burn-in processes. It is also assumed that items included in shutdown functions are not operated beyond their useful life thus ensuring that failures due to wear-out mechanisms do not occur.

6.2. Failure data that used for PFD calculation

The failure data used in the calculations are presented in the table below.

Component	Description	Total Failure rate (10^-6)	Failure rate, Dangerous Undetected (10^-6)	β-factor	SFF	Test interval (hours)
Topside						
PSD/ ESD / EQD pushbutton	Initiator	1,11	0,2	-	82 %	720
SD-panel contact sets	Initiator	0,125	0,001	10%	99,2 %	720
Bulkhead connector	Connection between SD-panel and HPU/SSCU	0,73	0,165	4,2 %	77,4 %	720
HPU PLC, Digital input		0,011	0,0011	-	>90%	720
HPU PLC, Digital output		0,0011	0,00011	-	>90%	720
HPU PLC, CPU		0,0091	0,00091	-	>90%	720
HPU Solenoid DCV		0,37	0,063	-	83 %	720
SSCU	Single channel in the SSCU	12,19	0,19	5 %	98 %	720
SPWV incl. QEV	Surface flow tree production wing valve	2	0,8	-	60 %	720
Return accumulator	SPWV actuator fluid vented to accumulator to ensure 5 second closing time	0,093	0,0232	10 %	46 %	720
HPU Hydraulic HP DCV		0,45	0,141	-	69 %	720
Relay	Rig-initiated PSD	1,03	0,0024	-	99,8 %	720
Relay	Rig-initiated EQD	1,03	1,03	10 %	0 %	720
LRP-valves						
LAIV, UAIV, MXOV, LXOV 1&2	Annulus isolation valves and crossover valves	1,67	1,5	2 %	10%	720
LMIV 1&2	Methanol isolation valves	0,82	0,208	2 %	75 %	720
AVIV 1&2, XMIV 1&2	Annulus ventilation isolation valve and XMT methanol isolation valve	0,82	0,208	2 %	75 %	720
PIV	Production isolation valve	0,9	0,8	2%	10,9%	720
SH including wedge lock	Safety Head	6,2	6,2	-	0 %	720

EDP-valves						
RV	Retainer valve	0,9	0,8	2%	10,9%	720
EDP connector – primary unlock	Emergency disconnect package connector	1,5	1,5	10 %	0%	720
EDP connector - Secondary unlock	Emergency disconnect package connector	1,5	1,5	10 %	0%	720
UAIV	Upper annulus isolation valve	1,67	1,5	2 %	10%	720
WOCM - subsea						
WSM DCV – Fail safe close	Solenoid directional control valve for all FSC valves	1,04	0,394	10 %	62 %	720
SEM A / SEM B	Single channel in the Subsea electronic module	10,84	0,23	5 %	98 %	720
EDP/LRP DCVs & accumulators						
Hydraulic pilot valve Pilot line: Ventilate Function line: Ventilate	3 port 2 position DCV	0,47	0,158	2 %	66 %	720

Table -3 failure data for safety part of workover

6.3. Calculation Formula

Fault tree analysis model

A fault tree method is used to model the failure of a certain TOP event which depends on other basic physical components by AND-or OR -gate in a tree structure .In low demand mode, FTA provides acceptable approximations of the PFD for SIS. For each basic event is, the PFDavg is calculated in CARA Fault Tree by the approximation (equation 6.1

$$q_i \approx \frac{\lambda_{DU,i}\tau_i}{2} \qquad 6.1$$

A fault tree with m minimal cut sets can be modelled as a series structure of the m minimal cut parallel structures. The probability of failure on demand for a minimal cut set j with independent components can be expressed as:

$$Q_{MC_i} \approx \prod_{j=1}^{m_j} q_i \qquad 6.2$$

For series structure the probability failure can be expressed as:

$$Q_0 \approx 1 - \prod_{j=1}^{m}(1 - Q_{MC_j}) \quad 6.3$$

The probability of failure on demand for low demand system can be approximated with a conservative uper bound approximations:

$$Q_0 \approx 1 - \prod_{j=1}^{m}(1 - Q_{MC_j}) \quad 6.4$$

Chapter 7

7. Result, Discussion, Conclusion and Further Study

7.1. Result

This quantitative SIL compliance report is based on requirements set by IEC 61508/IEC 61511.

Reliability-expressed in terms of PFD or failure rate per hour.

The Safety Integrity Level (SIL) is a statistical representation of the integrity of the SIS when a process demand occurs. The purpose of the SIS is to reduce risk, so SIL levels can be defined in terms of the risk reduction factor (RRF). The inverse of the RRF is the probability of failure on demand (PFD).

Risk reduction factor / Probability of failure on demand

Table shows the PFD for the three SIFs for current safety system. It can be seen that all three functions are well within the SIL 2 requirement.

Function	PFD calculated	PFD required	Safety Integrity Level	Proof test interval (hours)
PSD	$5{,}63*10^{-4}$	10^{-2}	2	720
ESD	$1{,}21*10^{-4}$	10^{-2}	2	720
EQD	$1{,}76*10^{-4}$	10^{-2}	2	720

Table -4 Summary table PFD-results for current safety system

Table shows the PFD for the three SIFs for new safety system. It can be seen that all three functions are well within the SIL 2 requirement. Details on the failure rates used as input in the PFD calculations can be found in chapter 6, table

Function	PFD calculated	PFD required	Safety Integrity Level	Proof test interval (hours)
PSD	$5{,}40*10^{-4}$	10^{-2}	2	720
ESD	$1{,}16*10^{-4}$	10^{-2}	2	720
EQD	$1{,}70*10^{-4}$	10^{-2}	2	720

Table -5 Summary table PFD-results for new safety system

7.2. Discussion

The qualitative risk assessment for workover system with new safety design shows, the maximum independency in safety system dramatically decreases the potential risk of hydrocarbon release. This risk reduction is because we design the new DCV on the flow of hydraulic to the SFT and this system is completely independent of HPU that is part of control system so with this arrangement our safety system will be reliable .In addition the risk of dropping the stack (EDP and LRP) on the X-mas tree (XT) on the well during running and retrieval of the system will be decrease and main reason for this risk reduction is new design DCV for ESD system and independent of that from control system.

There is also a risk reduction related to vessel loss of position resulting in hydrocarbon leak and damage to equipment. That is related to EQD safety function and with new design and maximum independency in safety function from control part; we will achieve the risk reduction in vessel loss of position.

In the case of PFD calculation and SIL Rating, the compare between the current system and new system shoes the slightly better achievement in PFD calculation and so on SIL rating, in fact the new system has been achieved better SIL rating.

7.3. Conclusion

Well intervention and workover system are very important in different phase of oil and gas reservoir life time, and in this operation the safety issue and suitable barrier is vital, so the safety system for workover should be protect personnel and facilities. The key component in this safety system is instrument safety function that I discussed in this thesis work. The main problem in this safety system as I mentioned in chapter 3 is some common part in safety and control system that maybe effect on safety system and made potential hazard like hydrocarbon release. so the solution that have been presented in this work is the roadmap to develop the maximum independency in safety system in order to confirm that the workover and well intervention is enough safe and meet all international and national standard .the examination of this solution done by risk assessment in term of qualitative and quantitative and two approaches shoes that this new safety design not only be safer than current system but comply with SIL target and have been achieve better PFD calculation .

7.4. Further Studies

In this work I have done a general assessment for Safety system in workover and some independency in safety system .I would have loved to this study continued with detail design of new safety components and specification of them, also there is a good opportunely to further work and depth analysis to develop the safety system in workover until to achieve complete independency in safety and control system. The result of future studies with focus to enhance safety system will promote the more safe work in well intervention and definitely decrease the risk of hydrocarbon release and accidents during workover.

APPENDIX A. RISK ASSEEMENT SHEETS

Light Well Intervention							
ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
PSD_1	Flowing/ Well Testing	Flow	Uncontrolled flow with no tools in bore	HC leak topside	Fire/explosion/ oil spill	Close SPWV	SPWV is in PDS handbook accepted for use in SIL2 without redundancy - only need to close one valve. (SFF = 60 %) SPWV shall be FSC (NORSOK D-010 15.34 Table 34 item C.) It should be noted that the SPWV is normally closed when not flowing the well

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
ESD_1	Flowing/ Well Testing	Flow	HC leak / fire topside	Uncontrolled flow with no tools in bore	HC spill to sea, explosion, fire	Close main bore valves. RV or PIV before SH. RV may be safer due to erosion.	in process systems it is common practice to close valves further away from hazard to help the valves closer to hazard (i.e. close RV before PIV and SH) If SH closes first in flowing conditions, we lose redundancy due to loss of sealing capability - NOT SIL2! If RV closes first, then PIV and SH last, we have redundant means to help SH be able to cut and seal - SIL2 is ok. VNE hydraulic set-up today indicates that PIV and RV will close before SH is exposed to flow if hydraulic supply is dumped (if sequence in hydraulic not in electric)

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
ESD_2	Flowing/ Well Testing	Flow	HC leak / fire topside	Uncontrolled flow with no tools in bore, We now have Integrity or third gate valve, not TOT ram SH	HC spill to sea, explosion, fire	No foreseen change to the sequence. It will reach safe state with RV and PIV before third valve	Sea dump needs to be part of safety system to avoid pressure build-up in return system triggering an unintentional disconnects. Annulus, crossovers and chemical injection needs to be closed. Hydraulic lock in annulus indicates that another valve has closed and sealed. No sequencing in annulus required
EQD_0	Coiled Tubing	Barrier	Loss of position	Rupture of well head, XT connection	Major HC spill to sea, subsea equipment damage	Previously discussed function (RV-PIV-SH) will reach safe state in this scenario as well	Worst case scenario for EQD demand is drive-off with coiled tubing in bore and well flowing. All other scenarios for EQD are considered safe with the recommendations for flowing condition included in the function.

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
EQD_1	Flowing/ Well Testing	Barrier	Loss of position	Rupture of well head, XT connection	Major HC spill to sea, subsea equipment damage	No foreseen change to the sequence. It will reach safe state with RV and PIV before third valve for systems with the TOT RAM	Integrity and SH are not qualified for cutting moving objects. Advantage to "sacrifice" RV.
EQD_2	Flowing /Well Testing	Barrier	Loss of position	Rupture of well head, XT connection	Major HC spill to sea, subsea equipment damage	For systems with SH qualified for closing in flowing, all valves can be closed simultaneously to save time. Given hydraulic delay, this timing can be modified separately in each project	Time is essential in EQD. Important to be disconnected before something breaks. For EQD the connector can be disconnected after PIV is closed, relying on hydraulic FSC of SH Wedge lock on SH has to be pressurized to ensure closed and sealing SH when pressure in bore is lower than pressure outside bore and when high-flow DCVs latch due to accumulator depressurization. Wedges are FSC, pressure is applied to hold the wedge open and away from the stem of the valve. Testing can be simpler than actual operation. The aim of testing is to uncover all failures in the system.

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
EQD_3	Flowing/ Well Testing	Barrier	Loss of position	Rupture of well head, XT connection	Major HC spill to sea, subsea equipment damage	Include a function in the Workover Safety Module for opening Annular Retainer Valve or BOVs for projects where this may be necessary to avoid hydraulic lock in the connector.	Hydraulic lock on annulus side of TULIP/MOHO connector (13 5/8) is solved by opening annulus retainer valve in the EDP. New connector has lower area of annulus sealing, thus reduced force. Should not be a problem. For high angle connector, this should not be a problem
EQD_4	Flowing/ Well Testing	Barrier	Loss of position	Rupture of well head, XT connection	Major HC spill to sea, subsea equipment damage	Weigh time criticality with risk of damaging equipment (and possibly loosing ability to reconnect without repair)	Female stab plate might be destroyed if not lifted in EQD, this is not safety critical. It is however a requirement to be able to reconnect after an EQD

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
EQD_5	Running/ Retrieval	Mechanical failure	spurious trip of EQD	stack dropped on well head/XT	damage to equipment and spill to sea	Evaluate current solution with respect to DU failure. PT monitors pressure, not sufficient flow. How to verify that the inhibit valve is fully open?	Connector unlock is inhibited by an ROV operated valve with downstream PT to monitor re-activation. This valve does not protect against pressure build up in return line leading to spurious trip of connector

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
EQD_6						Could include a possibility to delay the safety system to allow for the WOCS to run its SD sequence first on deep water / in situations this is acceptable. Check procedures and situations with regards to error in delay vs. SIL	This might not be a good solution as operator would typically increase the operating window on deeper water, making the EQD equally time critical.
Gen_1		Non-sharable item	spurious trip of ESD/EQD	Valves closing on perforating guns	explosion in stack, damage to equipment, potential loss of well control	For running of non-sharable (e.g. perforation gun) no inhibit of safety system should be included. Procedure to ensure safe running.	The risk of spuriously tripping ESD/EQD while running non-sharable is lower than the risk of forgetting to reactivate WSS after running non-sharable. note scenarios in SRS, allow projects to implement mitigating actions in procedures, Qualitative reasoning for suggested solution shall be included in SRS XT plug tool can block LRP, procedure to include sharable spacer

ID	Operational Mode	Guide word	Cause	Hazard	Consequence	Recommendations	Comments
Gen_2							The guidewords and operational modes not listed in this sheet were deemed covered by the recommendations and comments made above. All operational modes for all guidewords are the same; worst case scenario is flow with coiled tubing in bore.
Gen_3	Flowing/Well Testing	Barrier	ESD or EQD demand	HC leak, fire/explosion topside, loss of position	Spill to sea, escalation fire, damage to subsea equipment	Use RV for redundant means of stopping flow in ESD or EQD prior to closing SH	Need to have a second PIV/RV in order to have redundancy when TOT SH is the safety head due to lack of qualification for sealing in flowing conditions

APPENDIX B.

B.01 PSD RBD

B.02 ESD RBD

B.03 EQD RBD

PSD RBD

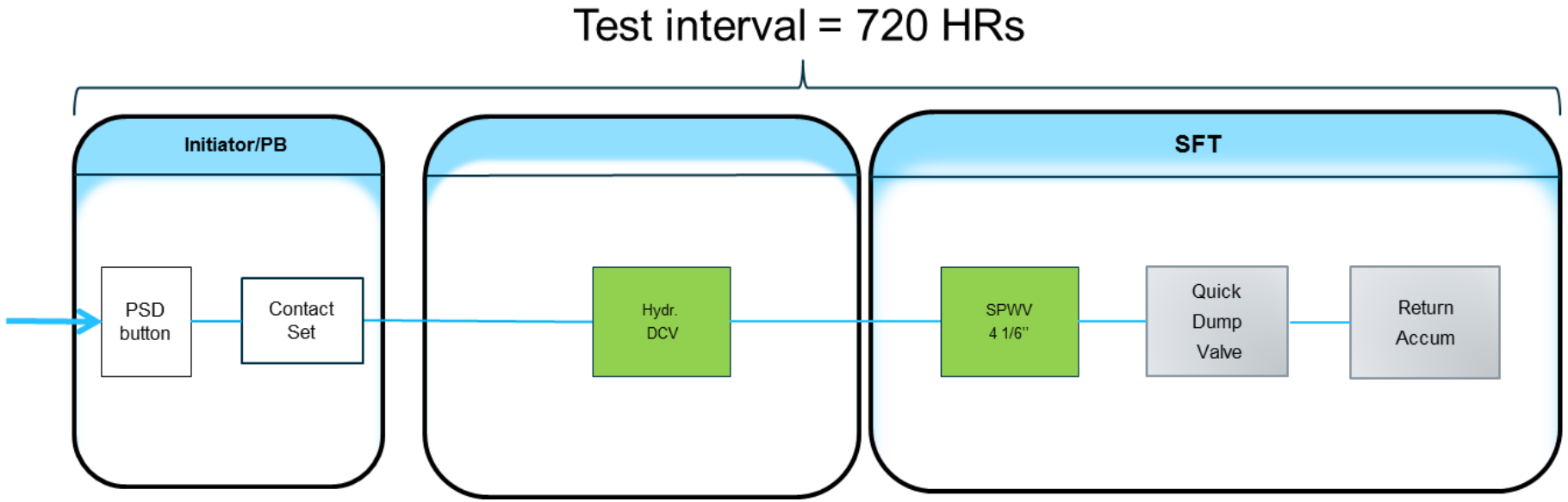
Legend:

Controls (initiator/ Logic)

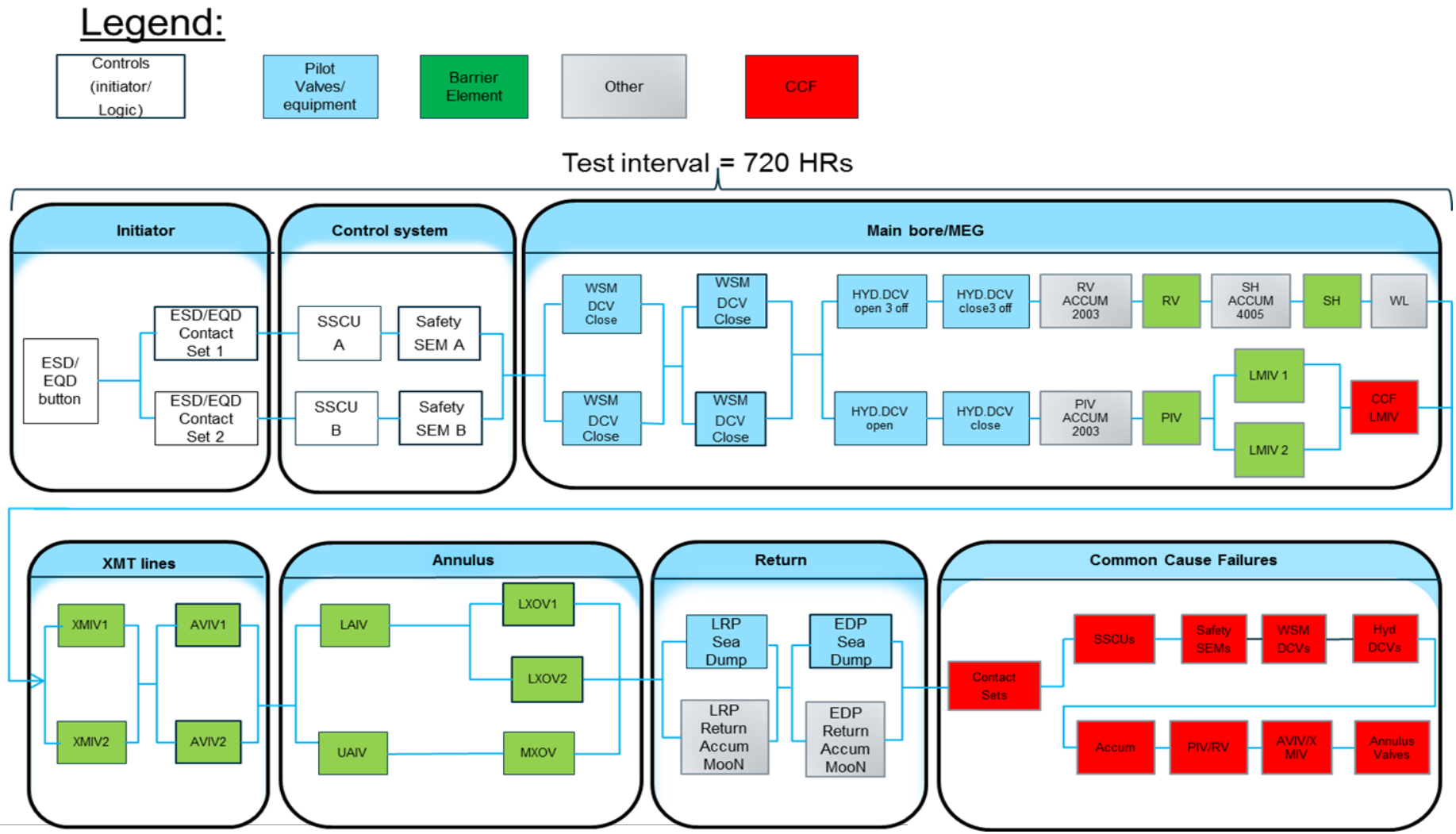
Pilot Valves/ equipment

Barrier Element

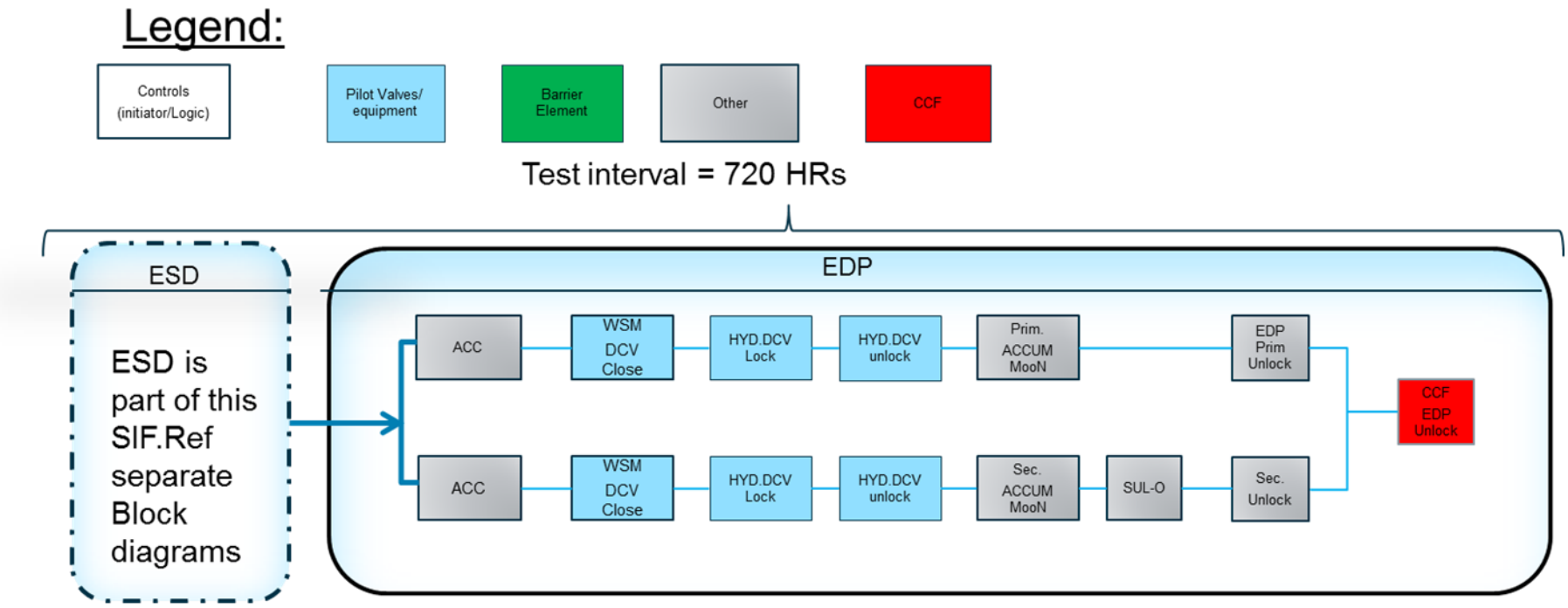
Other



ESD RBD


Legend:
Controls (initiator/ Logic)
Pilot Valves/ equipment
Barrier Element
Other
CCF
Test interval = 720 HRs
Initiator
ESD/ EQD button
ESD/EQD Contact Set 1
ESD/EQD Contact Set 2
Control system
SSCU A
SSCU B
Safety SEM A
Safety SEM B
Main bore/MEG
WSM DCV Close
WSM DCV Close
WSM DCV Close
WSM DCV Close
HYD.DCV open 3 off
HYD.DCV close3 off
RV ACCUM 2003
RV
SH ACCUM 4005
SH
WL
HYD.DCV open
HYD.DCV close
PIV ACCUM 2003
PIV
LMIV 1
LMIV 2
CCF LMIV
XMT lines
XMIV1
XMIV2
AVIV1
AVIV2
Annulus
LAIV
UAIV
LXOV1
LXOV2
MXOV
Return
LRP Sea Dump
LRP Return Accum MooN
EDP Sea Dump
EDP Return Accum MooN
Common Cause Failures
Contact Sets
SSCUs
Safety SEMs
WSM DCVs
Hyd DCVs
Accum
PIV/RV
AVIV/X MIV
Annulus Valves

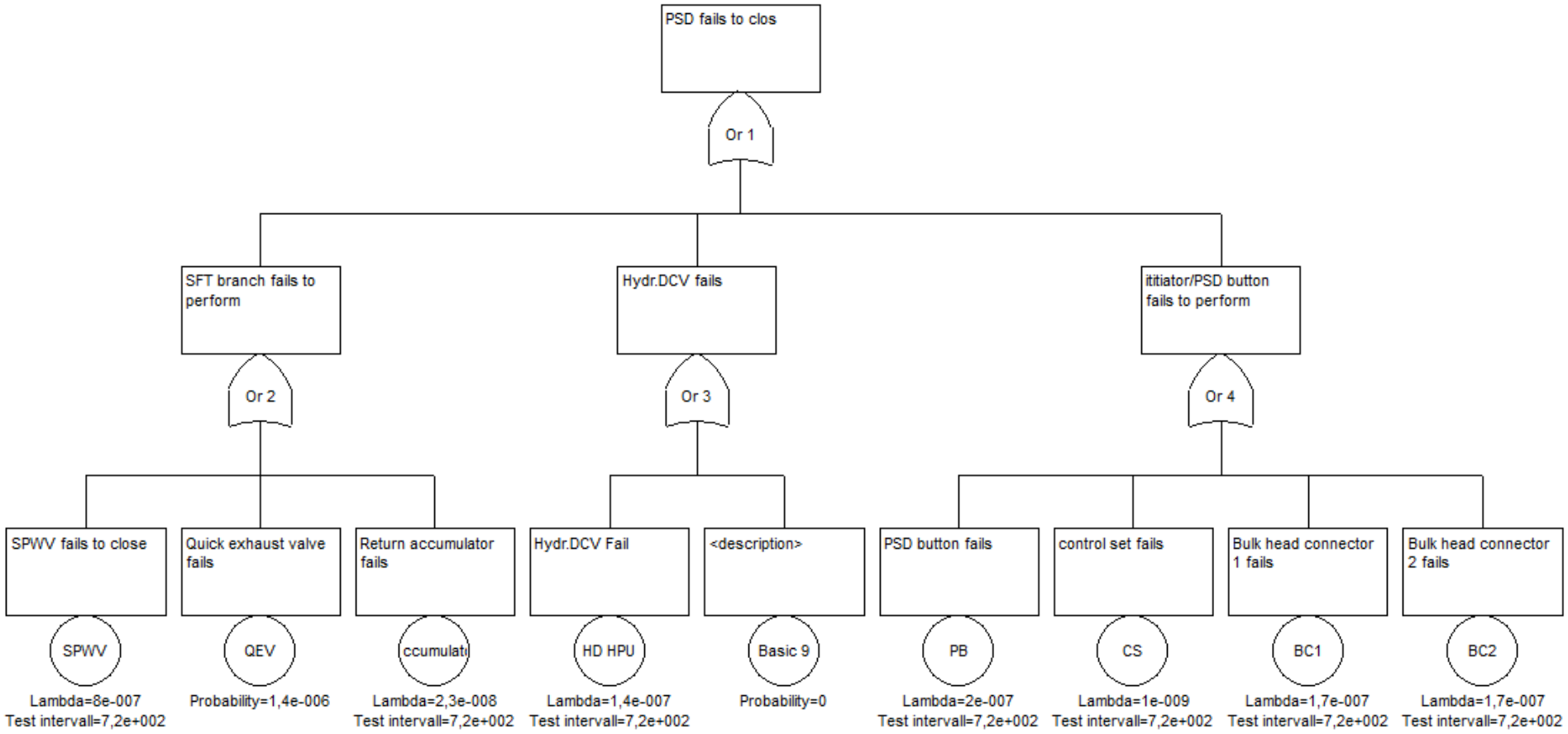
EQD RBD


Legend:
Controls (initiator/Logic)
Pilot Valves/ equipment
Barrier Element
Other
CCF
Test interval = 720 HRs
ESD
ESD is part of this SIF.Ref separate Block diagrams
EDP
ACC
WSM DCV Close
HYD.DCV Lock
HYD.DCV unlock
Prim. ACCUM MooN
EDP Prim Unlock
ACC
WSM DCV Close
HYD.DCV Lock
HYD.DCV unlock
Sec. ACCUM MooN
SUL-O
Sec. Unlock
CCF EDP Unlock

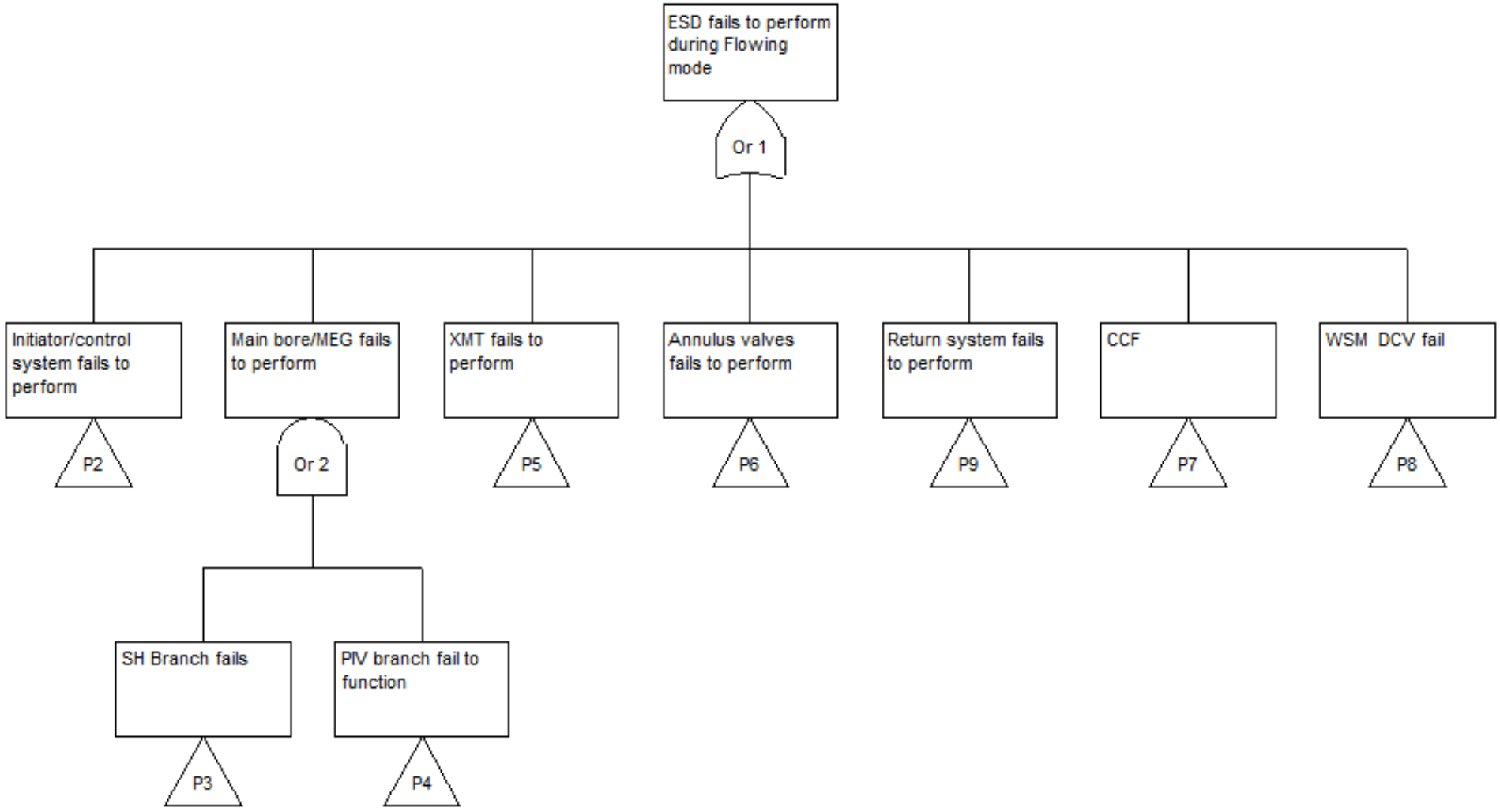
APPENDIX C.

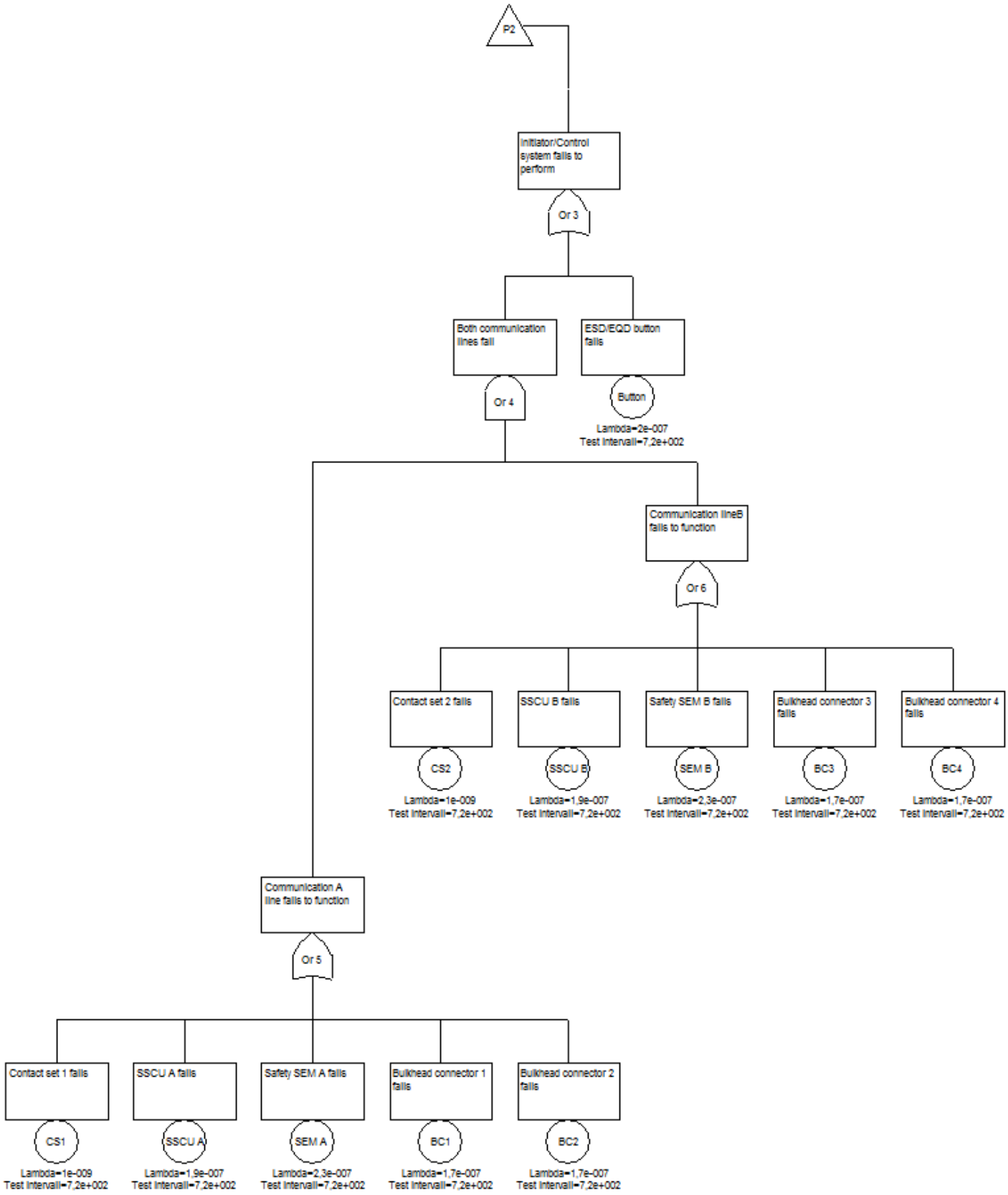
C.01 PSD FAULT TREE

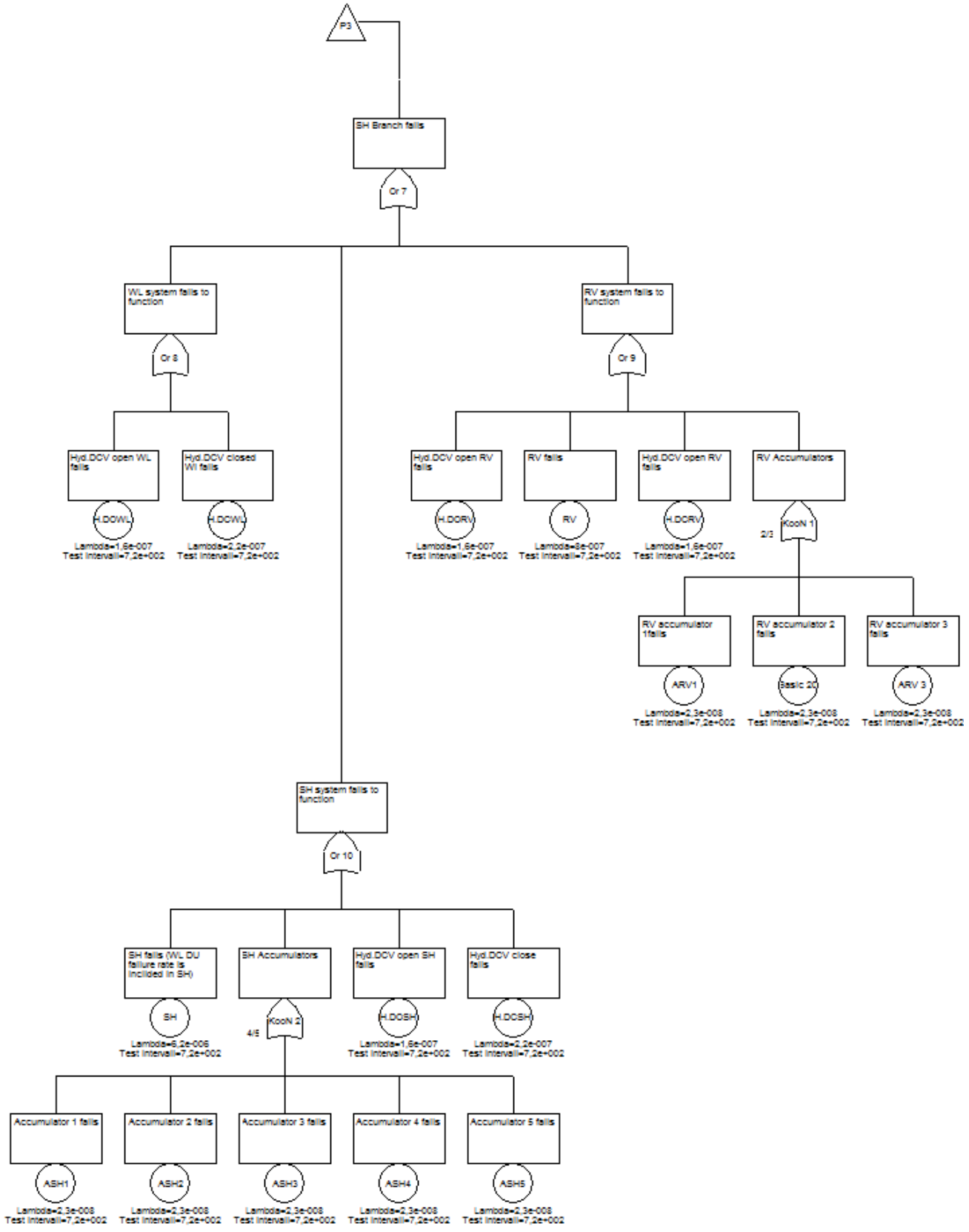
CARA Fault Tree version 4.1(c) Sydvest Software 1999Licensee:
Aker Kværner Norway

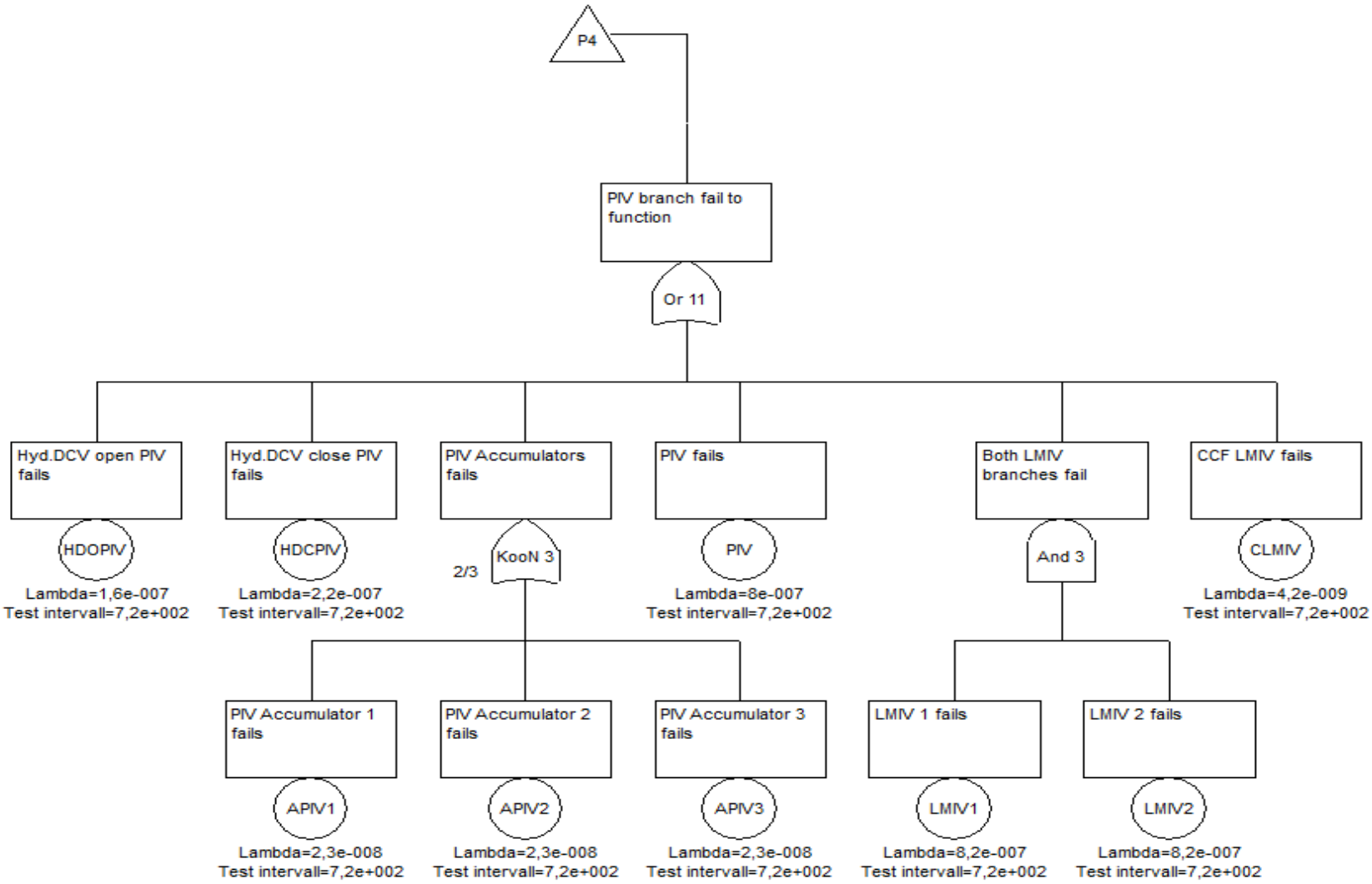


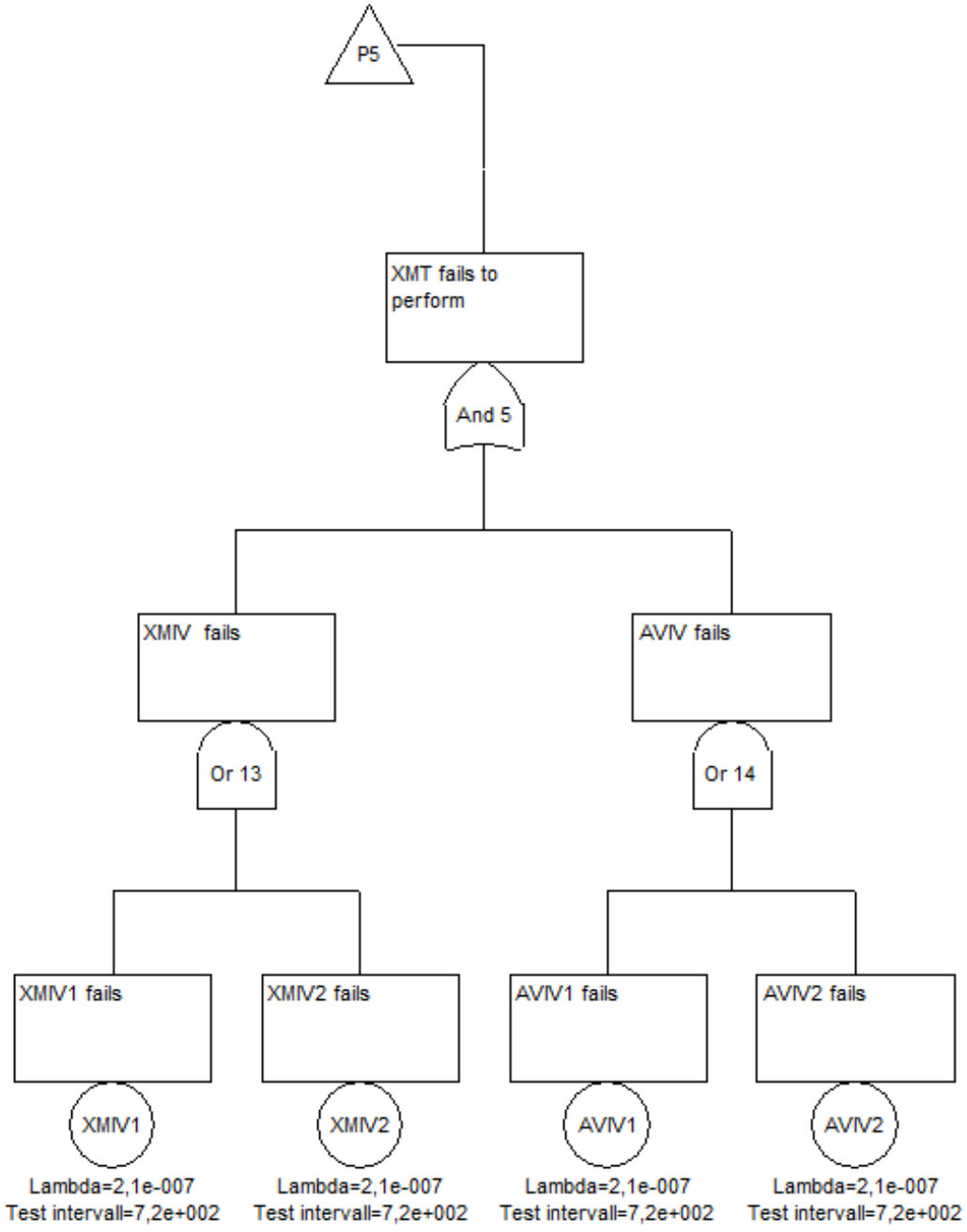
C.02 ESD FAULT TREE

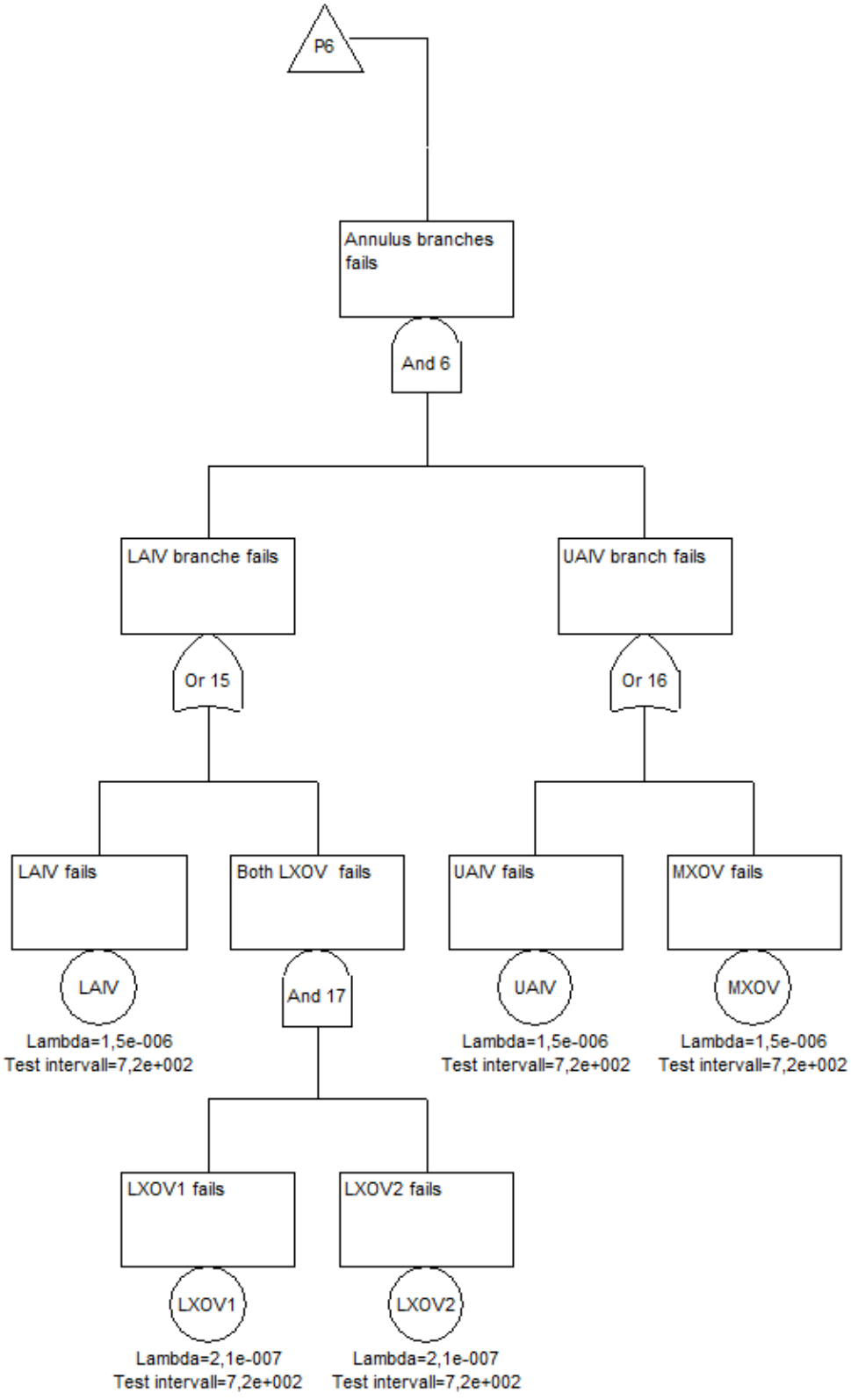


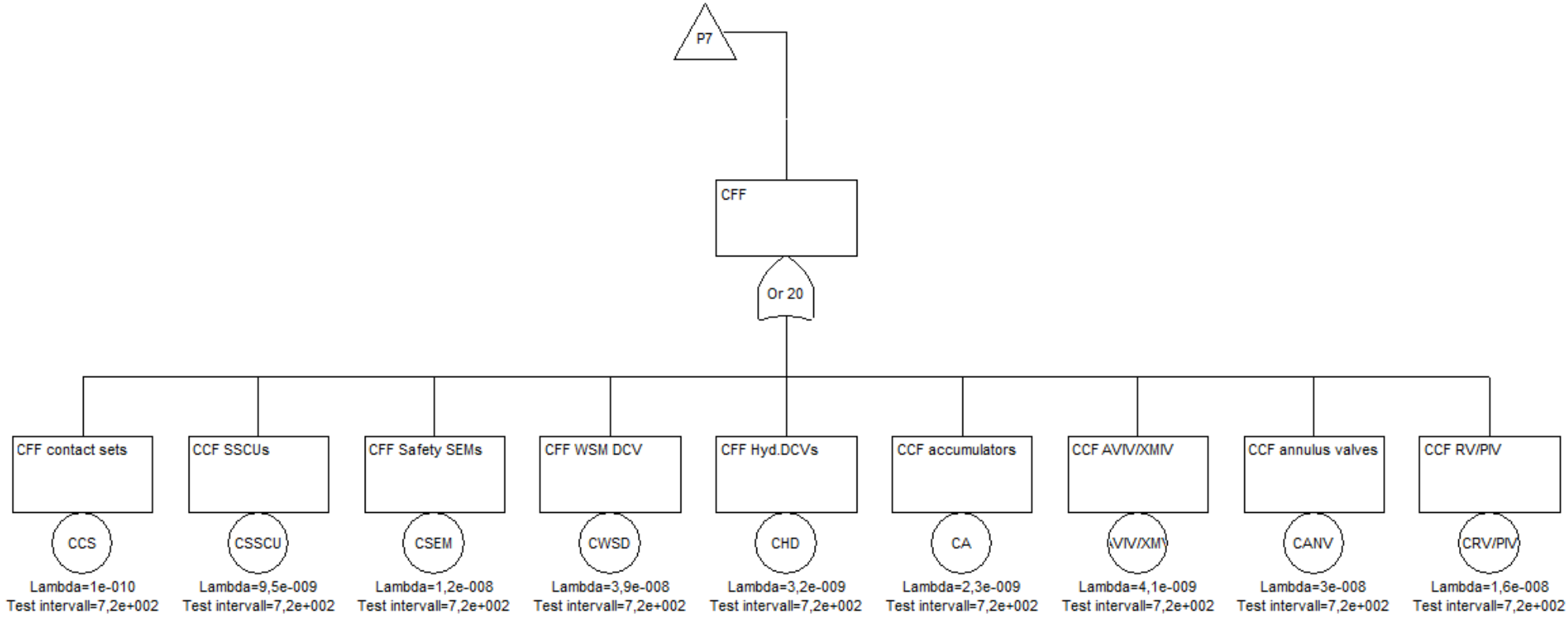

P2
initiator/Control system fails to perform
Or 3
Both communication lines fail
Or 4
ESD/EQD button fails
Button
Lambda=2e-007
Test Intervall=7,2e+002
Communication lineB fails to function
Or 6
Contact set 2 fails
CS2
Lambda=1e-009
Test Intervall=7,2e+002
SSCU B fails
SSCU B
Lambda=1,9e-007
Test Intervall=7,2e+002
Safety SEM B fails
SEM B
Lambda=2,3e-007
Test Intervall=7,2e+002
Bulkhead connector 3 fails
BC3
Lambda=1,7e-007
Test Intervall=7,2e+002
Bulkhead connector 4 fails
BC4
Lambda=1,7e-007
Test Intervall=7,2e+002
Communication A line fails to function
Or 5
Contact set 1 fails
CS1
Lambda=1e-009
Test Intervall=7,2e+002
SSCU A fails
SSCU A
Lambda=1,9e-007
Test Intervall=7,2e+002
Safety SEM A fails
SEM A
Lambda=2,3e-007
Test Intervall=7,2e+002
Bulkhead connector 1 fails
BC1
Lambda=1,7e-007
Test Intervall=7,2e+002
Bulkhead connector 2 fails
BC2
Lambda=1,7e-007
Test Intervall=7,2e+002

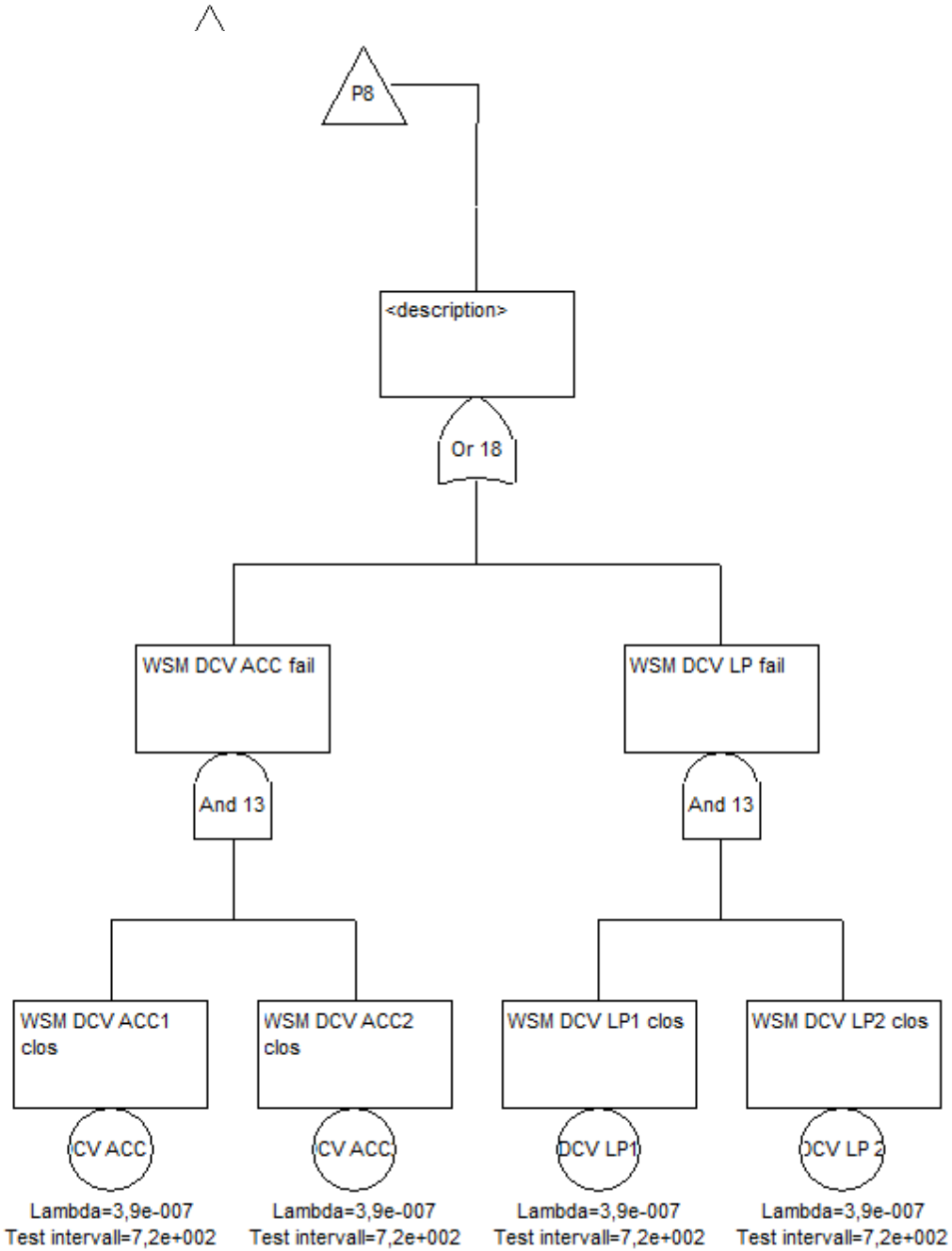

P3
SH Branch fails
Or 7
WL system fails to function
Or 8
Hyd.DCV open WL fails
H.DOWL
Lambda=1,6e-007
Test Interval=7,2e+002
Hyd.DCV closed WI fails
H.DCWL
Lambda=2,2e-007
Test Interval=7,2e+002
RV system fails to function
Or 9
Hyd.DCV open RV fails
H.DORV
Lambda=1,6e-007
Test Interval=7,2e+002
RV fails
RV
Lambda=8e-007
Test Interval=7,2e+002
Hyd.DCV open RV fails
H.DORV
Lambda=1,6e-007
Test Interval=7,2e+002
RV Accumulators
2/3
KooN 1
RV accumulator 1fails
ARV1
Lambda=2,3e-008
Test Interval=7,2e+002
RV accumulator 2 fails
basic 20
Lambda=2,3e-008
Test Interval=7,2e+002
RV accumulator 3 fails
ARV 3
Lambda=2,3e-008
Test Interval=7,2e+002
SH system fails to function
Or 10
SH fails (WL DU failure rate is incided in SH)
SH
Lambda=6,2e-006
Test Interval=7,2e+002
SH Accumulators
4/5
KooN 2
Hyd.DCV open SH fails
H.DOSH
Lambda=1,6e-007
Test Interval=7,2e+002
Hyd.DCV close fails
H.DCSH
Lambda=2,2e-007
Test Interval=7,2e+002
Accumulator 1 fails
ASH1
Lambda=2,3e-008
Test Interval=7,2e+002
Accumulator 2 fails
ASH2
Lambda=2,3e-008
Test Interval=7,2e+002
Accumulator 3 fails
ASH3
Lambda=2,3e-008
Test Interval=7,2e+002
Accumulator 4 fails
ASH4
Lambda=2,3e-008
Test Interval=7,2e+002
Accumulator 5 fails
ASH5
Lambda=2,3e-008
Test Interval=7,2e+002


P4
PIV branch fail to function
Or 11
Hyd.DCV open PIV fails
HDOPIV
Lambda=1,6e-007
Test intervall=7,2e+002
Hyd.DCV close PIV fails
HDCPIV
Lambda=2,2e-007
Test intervall=7,2e+002
PIV Accumulators fails
2/3
KooN 3
PIV fails
PIV
Lambda=8e-007
Test intervall=7,2e+002
Both LMIV branches fail
And 3
CCF LMIV fails
CLMIV
Lambda=4,2e-009
Test intervall=7,2e+002
PIV Accumulator 1 fails
APIV1
Lambda=2,3e-008
Test intervall=7,2e+002
PIV Accumulator 2 fails
APIV2
Lambda=2,3e-008
Test intervall=7,2e+002
PIV Accumulator 3 fails
APIV3
Lambda=2,3e-008
Test intervall=7,2e+002
LMIV 1 fails
LMIV1
Lambda=8,2e-007
Test intervall=7,2e+002
LMIV 2 fails
LMIV2
Lambda=8,2e-007
Test intervall=7,2e+002

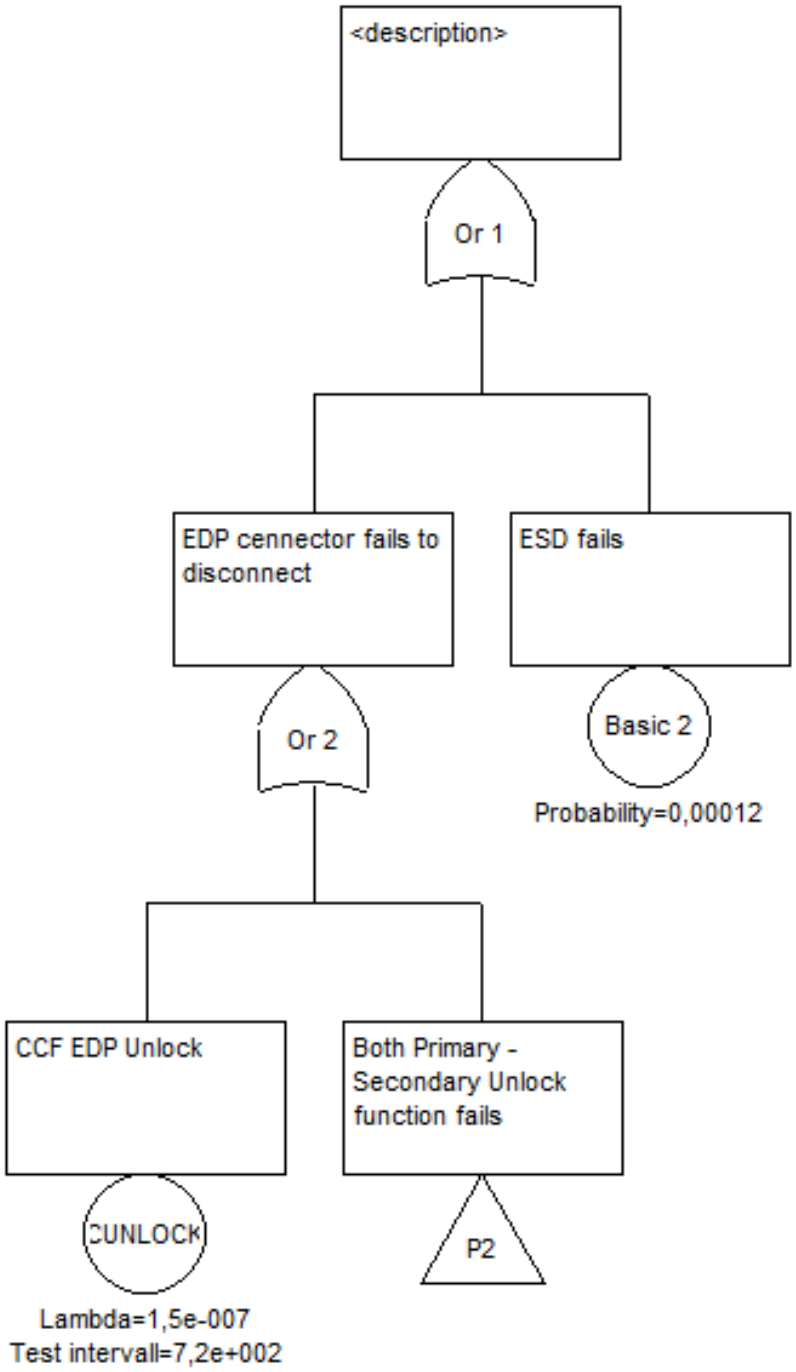

P5
XMT fails to perform
And 5
XMIV fails
AVIV fails
Or 13
Or 14
XMIV1 fails
XMIV2 fails
AVIV1 fails
AVIV2 fails
XMIV1
XMIV2
AVIV1
AVIV2
Lambda=2,1e-007
Test intervall=7,2e+002
Lambda=2,1e-007
Test intervall=7,2e+002
Lambda=2,1e-007
Test intervall=7,2e+002
Lambda=2,1e-007
Test intervall=7,2e+002

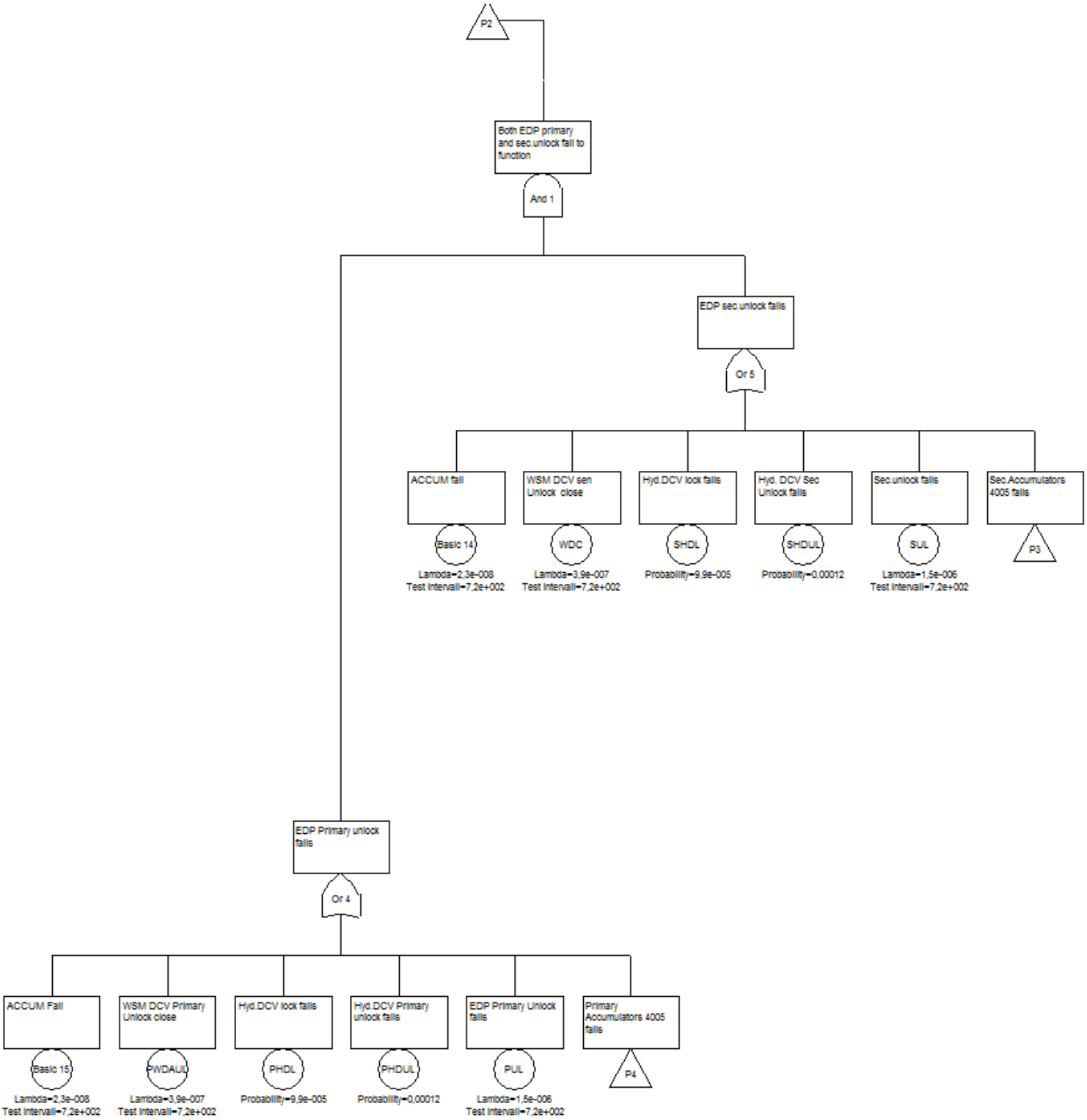

P6
Annulus branches fails
And 6
LAIV branche fails
UAIV branch fails
Or 15
Or 16
LAIV fails
Both LXOV fails
UAIV fails
MXOV fails
LAIV
And 17
UAIV
MXOV
Lambda=1,5e-006
Test intervall=7,2e+002
Lambda=1,5e-006
Test intervall=7,2e+002
Lambda=1,5e-006
Test intervall=7,2e+002
LXOV1 fails
LXOV2 fails
LXOV1
LXOV2
Lambda=2,1e-007
Test intervall=7,2e+002
Lambda=2,1e-007
Test intervall=7,2e+002

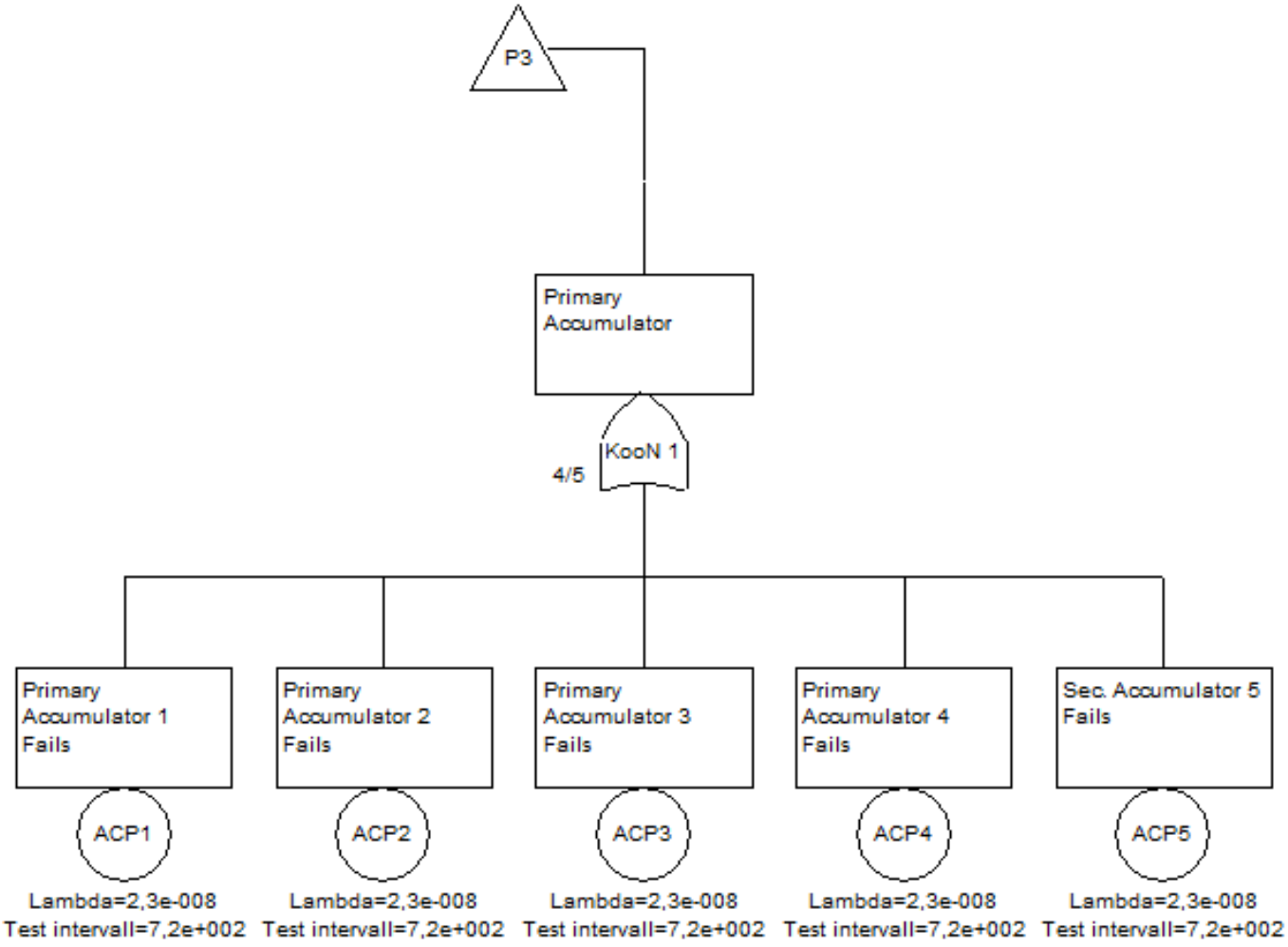

P7
CFF
Or 20
CFF contact sets
CCS
Lambda=1e-010
Test intervall=7,2e+002
CCF SSCUs
CSSCU
Lambda=9,5e-009
Test intervall=7,2e+002
CFF Safety SEMs
CSEM
Lambda=1,2e-008
Test intervall=7,2e+002
CFF WSM DCV
CWSD
Lambda=3,9e-008
Test intervall=7,2e+002
CFF Hyd.DCVs
CHD
Lambda=3,2e-009
Test intervall=7,2e+002
CCF accumulators
CA
Lambda=2,3e-009
Test intervall=7,2e+002
CCF AVIV/XMIV
AVIV/XMV
Lambda=4,1e-009
Test intervall=7,2e+002
CCF annulus valves
CANV
Lambda=3e-008
Test intervall=7,2e+002
CCF RV/PIV
CRV/PIV
Lambda=1,6e-008
Test intervall=7,2e+002

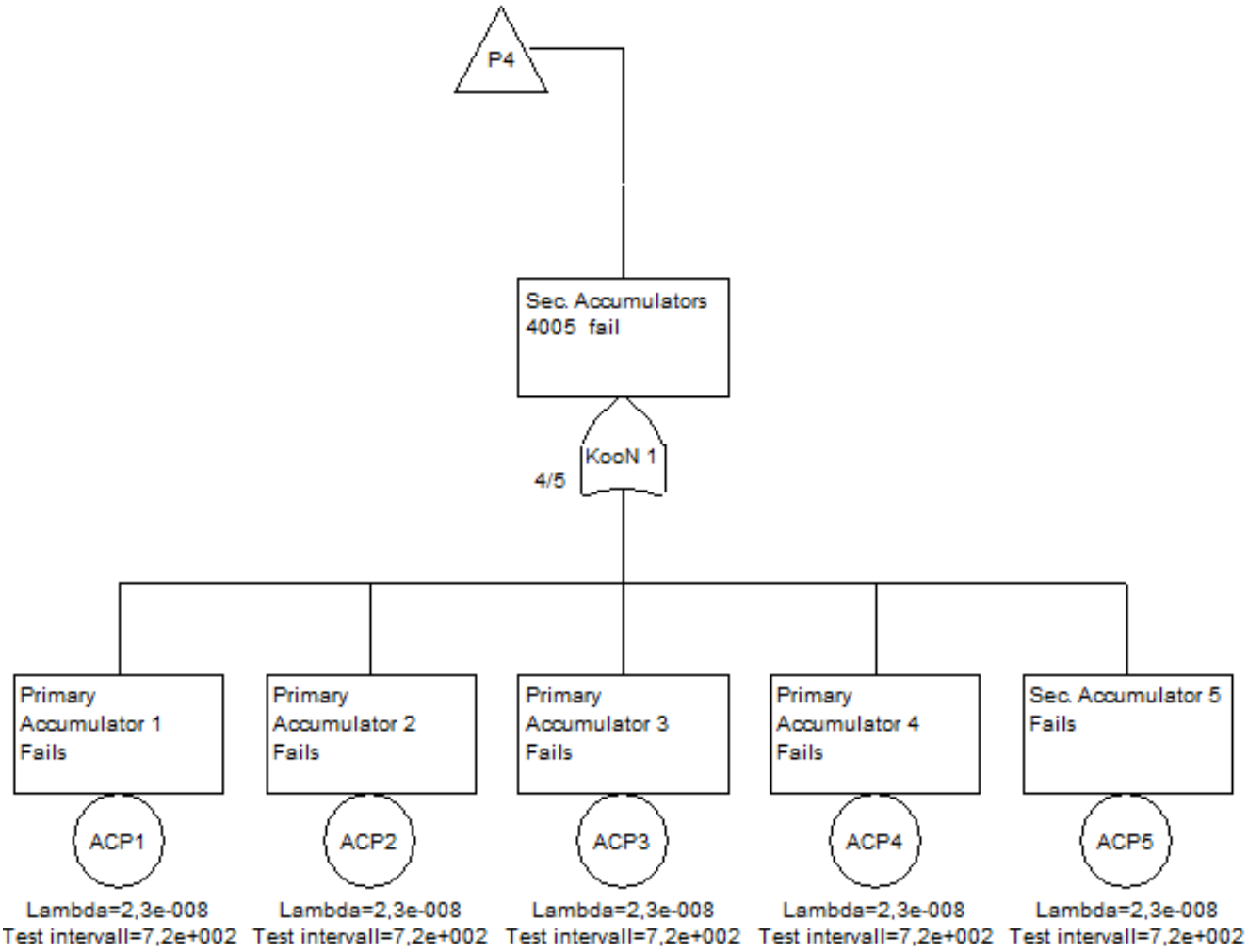

P8
<description>
Or 18
WSM DCV ACC fail
WSM DCV LP fail
And 13
And 13
WSM DCV ACC1 clos
WSM DCV ACC2 clos
WSM DCV LP1 clos
WSM DCV LP2 clos
CV ACC
CV ACC
DCV LP1
DCV LP 2
Lambda=3,9e-007
Test intervall=7,2e+002
Lambda=3,9e-007
Test intervall=7,2e+002
Lambda=3,9e-007
Test intervall=7,2e+002
Lambda=3,9e-007
Test intervall=7,2e+002

C.03 EQD FAULT TREE


<description>
Or 1
EDP cennector fails to disconnect
ESD fails
Or 2
Basic 2
Probability=0,00012
CCF EDP Unlock
Both Primary - Secondary Unlock function fails
CUNLOCK
P2
Lambda=1,5e-007
Test intervall=7,2e+002


P2
Both EDP primary and sec.unlock fail to function
And 1
EDP sec.unlock fails
Or 5
ACCUM fail
Basic 14
Lambda=2,3e-008
Test Intervall=7,2e+002
WSM DCV sen Unlock close
WDC
Lambda=3,9e-007
Test Intervall=7,2e+002
Hyd.DCV lock fails
SHDL
Probability=9,9e-005
Hyd. DCV Sec Unlock fails
SHDUL
Probability=0,00012
Sec.unlock fails
SUL
Lambda=1,5e-006
Test Intervall=7,2e+002
Sec.Accumulators 4005 fails
P3
EDP Primary unlock fails
Or 4
ACCUM Fail
Basic 15
Lambda=2,3e-008
Test Intervall=7,2e+002
WSM DCV Primary Unlock close
PWDAUL
Lambda=3,9e-007
Test Intervall=7,2e+002
Hyd.DCV lock fails
PHDL
Probability=9,9e-005
Hyd.DCV Primary unlock fails
PHDUL
Probability=0,00012
EDP Primary Unlock fails
PUL
Lambda=1,5e-006
Test Intervall=7,2e+002
Primary Accumulators 4005 fails
P4


P3
Primary Accumulator
4/5
KooN 1
Primary Accumulator 1 Fails
Primary Accumulator 2 Fails
Primary Accumulator 3 Fails
Primary Accumulator 4 Fails
Sec. Accumulator 5 Fails
ACP1
ACP2
ACP3
ACP4
ACP5
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002


P4
Sec. Accumulators
4005 fail
KooN 1
4/5
Primary
Accumulator 1
Fails
Primary
Accumulator 2
Fails
Primary
Accumulator 3
Fails
Primary
Accumulator 4
Fails
Sec. Accumulator 5
Fails
ACP1
ACP2
ACP3
ACP4
ACP5
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002
Lambda=2,3e-008
Test intervall=7,2e+002

APPENDIX D.

D.01 PSD REPORT

CARA Fault Tree version 4.1 (c) Sydvest Software 1999
Licensee: Aker Kværner, Norway

Date: 20.05.2014 Time: 15:33:01

File: Fault tree for new work over PSD.CFT

New fault tree

Qo (t) - Unavailability

Method: Upper bound approximation

Maximum cut size: 4 Mod. Level: 0 Top events: Or 1

Unavailability [Qo(t)]:

t	Est. Value
0	5,3951e-004
76	5,3951e-004
152	5,3951e-004
228	5,3951e-004
304	5,3951e-004
380	5,3951e-004
456	5,3951e-004
532	5,3951e-004
608	5,3951e-004
684	5,3951e-004
760	5,3951e-004

D.02 ESD REPORT

CARA Fault Tree version 4.1 (c) Sydvest Software 1999
Licensee: Aker Kværner, Norway

Date: 20.05.2014 Time: 15:36:45

File: Fault tree for new work over ESD.CFT

New fault tree

Qo (t) - Unavailability

Method: Upper bound approximation

Maximum cut size: 4 Mod. Level: 0 Top events: Or 1

Unavailability [Qo(t)]:

t	Est. Value
0	1,1572e-004
76	1,1572e-004
152	1,1572e-004
228	1,1572e-004
304	1,1572e-004
380	1,1572e-004
456	1,1572e-004
532	1,1572e-004
608	1,1572e-004
684	1,1572e-004
760	1,1572e-004

D.03 EQD REPORT

CARA Fault Tree version 4.1 (c) Sydvest Software 1999
Licensee: Aker Kværner, Norway

Date: 20.05.2014 Time: 15:37:30

File: Fault tree for new work over EQD.CFT

New fault tree

Qo (t) - Unavailability

Method: Upper bound approximation

Maximum cut size: 4 Mod. Level: 0 Top events: Or 1

Unavailability [Qo(t)]:

t	Est. Value
0	1,7058e-004
76	1,7058e-004
152	1,7058e-004
228	1,7058e-004
304	1,7058e-004
380	1,7058e-004
456	1,7058e-004
532	1,7058e-004
608	1,7058e-004
684	1,7058e-004
760	1,7058e-004

APPENDIX E.

E.01 TERMS AND ABBREVIATIONS

Abbreviation	Description
AKSO	Aker Solutions, represented by Aker Subsea
AVIV	Annulus Ventilation Isolation Valve
BOP	Blow-Out Preventer
CCF	Common Cause Failure
DCV	Directional Control Valve
DHSV	Down-Hole Safety Valve
DU	Dangers Undetected
EDP	Emergency Disconnect Package
EQD	Emergency Quick Disconnect
ESD	Emergency Shutdown
FSC	Fail Safe Close
FCV	Fail Safe Valve
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode and Critical Analysis
HAZID	Hazard Identification (study)
HAZOP	Hazard and Operability (study)
HC	Hydrocarbon
HCR	Hydrocarbon Return (line)
HPU	Hydraulic Power Unit
LLP	Lower Lubricator Package
LMIV	LRP Methanol Injection Valve
LP	Low Pressure
LRP	Lower Riser Package
LS	Landing String
LWI	Light Well Intervention
MCU	Master Control Unit
MXOV	Middle Crossover Valve
NPD	Norwegian Petroleum Directorate
P&ID	Piping and Instrumentation (Diagram)
PCH	Pressure control Head

PFD	Probability of Failure on Demand
PFD	Process Flow Diagram
PIV	Production Isolation Valve
PSD	Production Shutdown
PWV	Production Wing Valve
RBD	Reliability Block Diagram
RLWI	Riserless Light Well Intervention
RV	Retainer Valve
QDV	Quick Dump Valve
SAR	Safety Analysis Report
SAS	Safety and Automation System
SBOP	Submerged Surface BOP
SEM	Safety Electronic Module
SFT	Surface Flow Tree
SH	Safety Head
SIL	Safety Integrity Level
SIF	Safety Instrument Function
SIS	Safety Instrument System
SPCU	Subsea Power Communications Unit
SSCU	Subsea Safety Communicationl Unit
SPWV	Surface Production Wing Valve
SSTT	Subsurface Test Tree
TTHP	Through Tubing High Pressure
TTRD	Through Tubing Rotary Drilling
UAIV	Upper Annulus Isolation Valve
ULS	Upper Lubricator Section
UTH	Umbilical Termination Head
WCP	Well Control Package
WSS	Workover Safety System
WSM	Workover Safety Module
WOCM	Workover Control Module
WOCS	Workover Control System
XMIV	XT Methanol Injection Valve
XTAC	Xmas Tree Adaption Connector

Referencies

1 - Control System Safety Evaluation and Reliability ,William M. Goble, third edition, International Society of Automation
2 - SIL REQUIREMENT, PSD, ESD & EQD / Statoil Safety Requirement Specification, Rev. 1.
3 - IEC 61508, Functional safety of electrical/ electronic/programmable electronic safety-related systems.
4 - IEC 61511, Functional safety – Safety instrumented systems for process industry sector. Part 1-3
5 - ISO 13628-7:2006, Petroleum and natural gas industries – Design and operation of subsea production systems Part 6 Completion/Workover riser system
7- PDS Handbook (2013) SINTEF Reliability Data
8 - Rausand & Høyland; System Reliability Theory – Models, Statistical Methods and Applications, 2nd edition.
9 - OREDA handbook (2009) Reliability Data
10 - OREDA SSDAS Database Aker Solutions Database
11 - GL-070 rev.2, Application of IEC 61508 and IEC 61511 in Norwegian petroleum industry.
12 - Subsea XT and C/WO Systems, Vigdis project, AKSO 2012
13 - HAZOP analysis report – Workover System, Vigdis project, AKSO 2012
14 - Calculation and Data Dossier for workover safety instrument function,Aasta Hansteen Project,AKSO,2013
15 - Shutdown Interface Schematic MultiWOCS, Aasta Hansteen Project,AKSO,2013
16 - Safety Analysis Report (SAR)– workover system
17 - FMECA, Safety Head, Vigdis project, AKSO 2012
18 - FMECA, SSCU, Vigdis project, AKSO 2012
19 - FMECA, SIL 2 WOCM, Vigdis project, AKSO 2012
20 - FMECA 7 3/8” workover valve, Vigdis project, AKSO 2012
21 - FMECA 2 1/16” Annulus valve , Vigdis project, AKSO 2012
22 - FMECA & SIL Audit, ½” Rotating Disc Valve, Vigdis project, AKSO 2012
23 - FMECA & SAR, Subsea Accumulators, Vigdis project, AKSO 2012
24 - FMECA, SPWV 4 1/16” Gate Valve, Vigdis project, AKSO 2012