



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

# Reliability Assessment of Safety Instrumented Systems: An Application Example For A Ballasting System

Pålitelighetsvurdering av instrumenterte  
sikkerhetssystemer: Med  
anvendelsesområde for et  
ballasteringsystem

**Henrik Finnema Moen**

Product Design and Manufacturing

Submission date: June 2012

Supervisor: Mary Ann Lundteigen, IPK

Co-supervisor: Marvin Rausand, IPK  
Roar Bye, Teekay Petrojarl

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



**MASTER THESIS**  
**2012**  
**for**  
**stud. techn. Henrik Finnema Moen**

**RELIABILITY ASSESSMENT OF SAFETY INSTRUMENTED SYSTEM: AN APPLICATION EXAMPLE FOR A BALLASTING SYSTEM**  
**(Pålitelighetsvurdering av instrumenterte sikkerhetssystemer: Med anvendelsesområde for et ballasteringsystem)**

Ships, including floating production, storage, and offloading (FPSO) vessels, have always required ballast to operate safely. Long back in time, ships carried solid ballast in the form of rocks, sand, or other heavy materials. Today, water is commonly used for ballasting, as water can be easily added or removed to different sections of the hull to compensate for any changes in stability or cargo load. A FPSO must, for example, adjust ballasting of water according to how it is being loaded with hydrocarbon products. Failure to ballast properly may lead to a major accident, involving multiple fatalities, release to environment, and loss of vessel. Assessments of ballasting systems are therefore needed to verify that the systems are sufficiently safe and reliable.

The main objective of this thesis is to suggest an approach for how reliability assessments of ballasting systems should be carried out, including recommendations to how reliability requirements are being set for this type of systems.

The master thesis is carried out in collaboration with Teekay, the owner and operator of several FPSO vessels worldwide.

As part of the master thesis, the candidate shall:

1. Give a thorough description of ballasting system types, their main functions, and interface with other systems onboard the FPSO.
2. Document a literature survey on reported safety and reliability challenges and incidents/accidents in relation to ballasting systems.
3. Identify and classify safety-critical functions of a ballasting system.
4. Define and discuss concepts like safe state and desired behavior upon fault conditions for ballasting systems.

5. Identify particular issues of relevance for reliability performance of ballasting systems, for example the possibility for having common cause failures (CCFs).
6. Identify and discuss relevant methods for defining reliability requirements for ballasting systems.
7. Suggest an approach for how the reliability of a ballasting system may be determined, including the analysis of CCFs.
8. Suggest an approach for preventing CCFs in relation to ballasting systems, including design related issues and operational/maintenance related issues.
9. Identify and discuss challenges in relation to reliability assessments, for which further research is needed.

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

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

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

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

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

The candidate shall follow the work regulations at the company's plant. The candidate may not intervene in the production process in any way. All orders for specific intervention of this kind should be channelled through company's plant management.

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

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

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

Deadline: June 11<sup>th</sup> 2012.

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

Responsible supervisor at NTNU: Professor Mary Ann Lundteigen  
Phone: 73 59 71 01  
Mobile phone: 930 59 365  
E-mail: [mary.a.lundteigen@ntnu.no](mailto:mary.a.lundteigen@ntnu.no)

Co-Supervisor at NTNU: Professor Marvin Rausand  
Phone: 73 59 25 42  
E-mail: [marvin.rausand@ntnu.no](mailto:marvin.rausand@ntnu.no)

Supervisor at Teekay: Roar Bye, Manager, Operations Support  
Mobile phone: 930 04 137  
E-mail: [roar.bye@teekay.com](mailto:roar.bye@teekay.com)


**DEPARTMENT OF PRODUCTION  
AND QUALITY ENGINEERING**



Per Schjølberg

Associate Professor/Head of Department

---



Mary Ann Lundteigen  
Responsible Supervisor

## **Preface**

This report documents the master thesis in RAMS at the Department of Production and Quality Engineering, Norwegian University of Science and Technology, NTNU. The master thesis was carried out the spring of 2012, in collaboration with Teekay Petrojarl, the leading operator of floating production, storage and offloading (FPSO) vessels in harsh weather environments.

Trondheim, 11.06.2012

Henrik Finnema Moen

Stud.techn.

hefimo@gmail.com

## **Acknowledgment**

I would first like to thank my main supervisor at NTNU, Professor Mary Ann Lundteigen for turning my initial idea into an interesting master thesis topic, and for helpful guidance and advice throughout the master project. I would also like to thank my co-supervisor at NTNU, Professor Marvin Rausand for providing input to the topic of the thesis.

At Teekay Petrojarl, I would like to thank several persons for their great support of the master project. First, I would like to thank my company supervisor Roar Bye for facilitating and coordinating the project, and connecting me with the right people in the organization. I would also like to thank Geir Ramsøskar, Gaute Johnsen and Henning Øverstad for a series of interesting conversations and discussions, and for valuable contributions to the project.

Finally, I would like to thank my family for supporting me throughout my entire education.

HFM

## Summary and Conclusions

Ballast systems perform important safety functions on ships and floating facilities, and failure to ballast properly may lead to a major accident, involving multiple fatalities, release to environment and loss of vessel. Assessments are therefore needed to verify that the systems are sufficiently safe and reliable. The main objective of the thesis is to suggest a reliability assessment approach for ballast systems, including recommendations to how reliability requirements should be set for this type of system.

A combination of literature surveys provide the background for the reliability assessment approach. Previous work related to reliability of ballast systems is presented, followed by a presentation of the main regulations related to the systems. The third literature survey document the reported safety and reliability challenges, incidents and accidents related to ballast systems.

As a basis for the detailed reliability assessment approach a typical ballast system on a ship shaped vessel is presented. The safety critical functions of the system are identified and the system is analyzed with regards to its role as a safety barrier system. The ballast system is subsequently classified as a safety instrumented system capable of protecting the vessel from hazards that may lead to loss of stability and draft. A hazard analysis is used to assess the adequacy of the barrier system, and the result of the analysis show that there are multiple hazards that may lead to loss of stability and draft, and that although the frequency of occurrence might be low, the associated consequences can be very high.

A comparison between different methods for assigning reliability performance requirements to ballast system functions is presented, based on two different approaches recommended by the international IEC61508 standard and the Norwegian OLF-070 guideline, respectively. A recommendation is made to assign minimum reliability performance requirements to the ballast system functions, based on the approach presented in the guideline. A proposed set of reliability performance requirements are presented.

Potential failure causes and failure modes that may influence the reliability performance of ballast system functions are identified through a safety barrier failure analysis. As part of the analysis a failure mode, effect and criticality analysis of the main components is conducted.

The proposed reliability assessment approach is presented as a practical stepwise procedure to be used when quantifying the reliability performance of the safety functions performed by a ballast system. The approach is based on a reliability block diagram technique where potential common cause failures among the components can be included in the calculations. The approach is developed to give conservative estimates for the reliability performance, and may



be used as part of a verification process of ballast system reliability, as decision support during the design phase of new systems or to quantify the effect of reliability enhancing efforts in the operational phase.

In addition to the reliability assessment approach, a defence approach against common cause failures in ballast systems is presented. The defence approach focus on the efforts that can be made in the operational phase during maintenance and testing, to reduce the influence and reoccurrence of common cause failures.

Finally, the proposed reliability assessment approach is applied to the ballast system of the Petrojarl Foinaven floating production, storage and offloading vessel as a case example of the approach. The case example show that the proposed reliability performance requirements can be achieved by performing functional tests of the ballast system components at regular intervals, and that the stepwise procedure may also identify important improvement potentials for ballast systems.

## Sammendrag

Ballastsystemer utfører viktige sikkerhetsfunksjoner ombord på skip og flytende installasjoner, og feil under ballasteringsoperasjoner kan føre til storulykker, med tap av menneskeliv, utslipp til miljøet og tap av fartøy. Det er derfor behov for pålitelighetsvurderinger for å verifisere at systemene er tilstrekkelig sikre og pålitelige. Hovedmålet med masteroppgaven er å foreslå en pålitelighetsvurderingsmetode for ballastsystemer, i tillegg til å foreslå hvordan pålitelighetskrav skal settes for slike systemer.

En kombinasjon av litteraturstudier danner bakgrunnen for pålitelighetsvurderingsmetoden. Tidligere arbeid knyttet til pålitelighet av ballastsystemer er presentert, fulgt av en presentasjon av de mest sentrale forskriftene som gjelder for ballastssystemer. Det tredje litteraturstudiet dokumenterer de rapporterte sikkerhet- og pålitelighetsutfordringene, hendelsene og ulykkene knyttet til ballastsystemer.

Som en basis for den detaljerte pålitelighetsvurderingsmetoden presenteres et typisk ballastsystem installert på et skip. De sikkerhetskritiske funksjonene i systemet er identifisert og systemet er analysert i forhold til rollen det utfører som et sikkerhetsbarriere system. Ballastsystemet er deretter klassifisert som et instrumentert sikkerhetssystem som kan beskytte fartøyet fra farekilder som kan lede til tap av stabilitet og dypgang. En farekildeanalyse er benyttet for å vurdere tilstrekkeligheten av barriere systemet, og resultatet av analysen viser at det finnes en rekke farekilder som kan lede til tap av stabilitet og dypgang, og at selv om hendelsesfrekvensen muligens er lav, så kan de tilhørende konsekvensene være veldig høye.

En sammenligning mellom forskjellige metoder for å angi ytelseskrav for pålitelighet til ballastsystemer er presentert, basert på to forskjellige metoder anbefalt av henholdsvis den internasjonale IEC61508 standarden og den norske retningslinjen OLF-070. Det er videre anbefalt at minimumskrav til pålitelighetsytelse bør angis til de forskjellige ballastsystemfunksjonene basert på metoden presentert i den overnevnte retningslinjen. Et sett med krav til pålitelighetsytelse er foreslått.

Potensielle feilårsaker og feilmodi som kan påvirke pålitelighetsytelsen til ballastsystemfunksjonene er identifisert gjennom en feilanalyse av sikkerhetsbarrieren. Som en del av analysen ble det utført en feilmodi, effekt og kritikalitetsanalyse av hovedkomponentene i systemet.

Den foreslåtte pålitelighetsvurderingsmetoden er presentert som en praktisk stegvis metode som kan benyttes for å kvantifisere pålitelighetsytelsen av sikkerhetsfunksjonene i et ballastsystem. Metoden er basert på pålitelighets blokkdiagrammer hvor potensialet for fellesfeil mellom komponentene kan inkluderes i beregningene.

Metoden er utviklet til å gi konservative estimater for pålitelighetsytelsen, og kan brukes som

en del av en verifikasjonsprosess for pålitelighet av et ballastsystem, som verktøy for beslutningsstøtte i designfasen av nye systemer eller for å kvantifisere effekten av pålitelighetsfremmende tiltak i operasjonsfasen.

I tillegg til pålitelighetsvurderingsmetoden, presenteres en forsvarmetode mot fellesfeil i ballastsystemer. Forsvarsmetoden fokuserer på tiltak som kan gjøres i operasjonsfasen under vedlikehold og testing for å redusere effekten av, og muligheten for tilbakefall av fellesfeil i systemet.

Til slutt presenteres pålitelighetsvurderingsmetoden gjennom et anvendelseksempel hvor metoden benyttes for å analysere ballastsystemet på det flytende produksjonsskipet Petrojarl Foinaven. Anvendelseksempelen viser at de foreslåtte kravene til pålitelighetsytelse kan oppnås ved å utføre regelmessige funksjonstester av komponentene i ballastsystemet, og at den stegvise metoden også kan identifisere viktige forbedringspotensialer for ballast systemer.

# Contents

Preface . . . . .	iv
Acknowledgment . . . . .	v
Summary and Conclusions . . . . .	vi
Sammendrag . . . . .	viii
<b>1 Introduction</b>	<b>2</b>
1.1 Background . . . . .	2
1.1.1 Objective . . . . .	3
1.1.2 Limitations . . . . .	3
1.1.3 Structure of the Report . . . . .	4
1.2 Literature Survey . . . . .	4
<b>2 Regulations and Standards</b>	<b>7</b>
2.0.1 PSA Regulations . . . . .	8
2.0.2 NMA Regulations . . . . .	8
2.0.3 Reliability Assessment Requirements . . . . .	9
<b>3 FPSO Ballast System and Functions</b>	<b>12</b>
3.1 Ballast System and Functions . . . . .	12
3.1.1 Ballast System . . . . .	12
3.1.2 Ballast System Functions . . . . .	16
3.1.3 Ballast System as a Safety Barrier . . . . .	17
3.1.4 Ballast System Operational Situations . . . . .	18
3.1.5 Safety Barrier Classification . . . . .	18
3.1.6 Hazard Analysis . . . . .	24
3.2 Safety Barrier Failure Analysis . . . . .	27
3.2.1 Failure Cause Classification . . . . .	28
3.2.2 Failure Mode Classification . . . . .	30
3.2.3 Failure Modes, Effects and Criticality Analysis (FMECA) . . . . .	31
3.3 Reliability Performance Requirements . . . . .	32

<b>4 Incidents and Accidents</b>	<b>39</b>
4.1 Minor Incidents and Accidents . . . . .	40
4.2 Major Incidents and Accidents . . . . .	41
<b>5 Reliability Assessment Approach for FPSO Ballast Systems</b>	<b>47</b>
5.1 Background for the Approach . . . . .	47
5.1.1 Selection of Reliability Modeling Approach . . . . .	47
5.1.2 PFD Calculation . . . . .	48
5.1.3 Common Cause Failure Modeling . . . . .	52
5.1.4 Reliability Data . . . . .	54
5.2 Stepwise Procedure . . . . .	56
5.2.1 Step 1: Ballast System Familiarization . . . . .	57
5.2.2 Step 2: Identification of Common Cause Component Groups . . . . .	57
5.2.3 Step 3: RBD Construction . . . . .	57
5.2.4 Step 4: Determination of Reliability Data . . . . .	58
5.2.5 Step 5: PFD Calculations . . . . .	58
5.2.6 Step 6: Comparison with Reliability Performance Targets . . . . .	59
5.3 Defense Approach Against CCF in Ballast Systems . . . . .	60
5.3.1 Defence Approach . . . . .	60
<b>6 Case example: Petrojarl Foinaven FPSO</b>	<b>67</b>
6.0.2 Presentation of the Foinaven FPSO . . . . .	67
6.1 Reliability Assessment of the Foinaven FPSO Ballast System . . . . .	68
6.1.1 Step 1: Ballast System Familiarization . . . . .	69
6.1.2 Step 2: Identification of Common Cause Component Groups . . . . .	70
6.1.3 Step 2: RBD Construction . . . . .	71
6.1.4 Step 4: Determine Relevant Reliability Data . . . . .	73
6.1.5 Step 5: PFD Calculations . . . . .	75
6.1.6 Step 6: Comparison with Reliability Performance Targets . . . . .	80
<b>7 Summary and Recommendations for Further Work</b>	<b>81</b>
7.1 Summary and Conclusions . . . . .	81
7.2 Discussion . . . . .	82
7.3 Recommendations for Further Work . . . . .	83
<b>Bibliography</b>	<b>84</b>
<b>A Acronyms</b>	<b>87</b>
<b>B Additional Information</b>	<b>89</b>

# List of Figures

2.1	Main elements of a SIS	10
3.1	Sketch of the ballast system	13
3.2	Hydraulically operated butterfly valve	14
3.3	Classification of barriers	19
3.4	Ballast systems as a SIS	20
3.5	Sketch of SIF1	21
3.6	Sketch of SIF2	21
3.7	Sketch of SIF3	22
3.8	HAZID	25
3.9	Hazard-barrier matrix	27
3.10	Framework for risk reduction in IEC 61508	33
3.11	Safety integrity levels in IEC 61508	34
4.1	Petrobras P-34	42
5.1	$C_{moon}$ factors	53
5.2	$k_{\beta}$ parameters	54
5.3	Shortlist of applicable reliability data	56
5.4	Main concepts of the CCF defense approach	61
5.5	Cause defense matrix	64
5.6	Generic defense options against CCF	65
6.1	Teekay Petrojarl Foinaven	68
6.2	RBDel	72
6.3	RBDhyd	72
6.4	RBD1	73
6.5	RBD2	73
6.6	RBD3	73
6.7	Reliability data used in the case example	74

6.8 RBDelec . . . . .	75
6.9 RBDhyd . . . . .	76
6.10 RBD1 . . . . .	77
6.11 RBD2 . . . . .	78
6.12 RBD3 . . . . .	79
B.1 Hierarchical breakdown of the ballast system . . . . .	90
B.2 RABL datasheet . . . . .	91
B.3 FMECA of the ballast system valves . . . . .	92
B.4 FMECA of the ballast system pumps and control system . . . . .	93
B.5 FMECA of the ballast system utilities . . . . .	94
B.6 Calculation of minimum SIL requirements . . . . .	95
B.7 Reliability data applicable to ballast systems . . . . .	96
B.8 Reliability data applicable to ballast systems . . . . .	97
B.9 Foinaven ballast system flow diagram 2 . . . . .	101
B.10 Foinaven ballast system flow diagram 1 . . . . .	102

# List of Tables

3.1	Components subject to the FMEA . . . . .	31
3.2	Proposed minimum SIL requirements to ballast system functions . . . . .	37
4.1	Overview of tables and datasources . . . . .	40
5.1	PFD of Human performance . . . . .	52
5.2	Checklists for preparation, execution and restoration during function tests and inspections . . . . .	62
5.3	Questions for free text description during failure reporting . . . . .	62
5.4	Checklists for preparation, execution and restoration during functional tests and inspections . . . . .	66
6.1	Petrojarl Foinaven FPSO in numbers . . . . .	67
6.2	List of identified common cause component groups . . . . .	71
6.3	Description of assumptions . . . . .	74
6.4	Comparison with reliability performance targets . . . . .	80
B.1	Stability incidents reported to the PSA . . . . .	98
B.2	Stability incidents reported to the PSA . . . . .	99
B.3	Stability incidents reported to HSE (UK) 1980-2003 . . . . .	100



# Chapter 1

## Introduction

### 1.1 Background

Ballast systems perform important safety functions on ships and floating facilities, and FPSO vessels are especially dependent on their ballast systems to adjust the stability and draft according to how the vessel is loaded and unloaded with hydrocarbon products. Failure to ballast properly may lead to a major accident, involving multiple fatalities, release to the environment and loss of vessel as in the Ocean Ranger accident in 1982, and the recent incident with the Petrobras P-34 FPSO in 2002.

Despite the major accident potential of unsuccessful ballast operations, the requirements to reliability assessments and reliability performance of these systems are not regulated as strict as other systems in the offshore industry. Ballast systems are usually subject to traditional prescriptive maritime regulations, where requirements to reliability performance is limited. This may be about to change, as regulatory initiatives have been made to include ballast systems under performance based offshore regulations. The first step was taken by the [OLF070 \(2004\)](#) guideline used in the Norwegian offshore industry in 2004. The guideline assigned a reliability performance requirement to ballast systems, which to this day represent the state-of-the-art with regards to requirements for ballast system reliability performance.

This thesis is concerned with the need for improved reliability assessments methods and reliability performance requirements to verify that ballast systems are sufficiently safe and reliable for daily operation, as well as in emergency situations.

### 1.1.1 Objective

The main objective of the thesis is to suggest an approach for how reliability assessments of ballast systems should be carried out, including recommendations to how reliability requirements are being set for this type of system.

As part of the master thesis, the following shall be covered:

- Give a thorough description of ballasting system types, their main functions, and interface with other systems onboard the FPSO.
- Document a literature survey on reported safety and reliability challenges and incidents/accidents in relation to ballasting systems.
- Identify and classify safety-critical functions of a ballasting system.
- Define and discuss concepts like safe state and desired behavior upon fault conditions for ballasting systems.
- Identify particular issues of relevance for reliability performance of ballasting systems, for example the possibility for having common cause failures (CCFs).
- Identify and discuss relevant methods for defining reliability requirements for ballasting systems.
- Suggest an approach for how the reliability of a ballasting system may be determined, including the analysis of CCFs.
- Suggest an approach for preventing CCFs in relation to ballasting systems, including design related issues and operational/maintenance related issues.
- Identify and discuss challenges in relation to reliability assessments, for which further research is needed.

### 1.1.2 Limitations

The study is limited to ballast systems installed on ship shaped vessels.

### 1.1.3 Structure of the Report

The report is structured as follows

- **Chapter 1** provides the background information and problem formulation, objectives and limitations, description of the structure of the report and a presentation of previous work within the field of ballast system reliability.
- **Chapter 2** present the regulations and requirements related to ballast systems on floating facilities operating on the NCS.
- **Chapter 3** begins with a description of a typical ballast system and the functions of the system. The main components are described in detail, and the ballast system is classified as a SIS. A barrier analysis and safety barrier failure analysis is presented. The final part of the chapter is a presentation of the relevant methods that can be used to assign reliability requirements to ballast systems, and a proposed set of reliability performance requirements for the ballast system functions.
- **Chapter 4** document the reported safety and reliability challenges, incidents and accidents related to ballast systems.
- **Chapter 5** present the proposed stepwise reliability assessment method based on a reliability block diagram technique followed by a common cause failure defence approach for the operational phase of a ballast system.
- **Chapter 6** presents the reliability assessment approach through a case example conducted on the ballast system of the Petrojarl Foinaven FPSO.

## 1.2 Literature Survey

The literature survey is divided into three parts. The first part document the previous work related to reliability assessments of ballast systems, presented in the following section. The second part present the regulations governing ballasting systems on the NCS in Chapter 2. The third part present the reported safety and reliability challenges, incidents and accidents related to ballast systems in Chapter 4.

Not alot of research has been carried out within the field of reliability assessments of ballast systems. The accident reports following the Ocean Ranger accident in 1982, mark the beginning of the literature survey. These reports clearly pointed out the critical importance of ballast system integrity, and sparked an increased focus on stability and ballast system reliability in the

offshore industry. In response to the accident, the classification society DNV performed an investigation of the ballast system on a sister platform to the Ocean Ranger, and the investigation stressed the importance of improved documentation of ballast systems and how it responded to different interventions by the operator (Østby et al., 1987).

Through the *RABL-Risk Assessment Of Buoyancy Loss* (RABL) (Østby et al., 1987) research programme from 1986-87, the reliability of ballast systems on mobile platform concepts were subject to various assessments. The RABL programme was a joint industry project aimed at developing an analysis procedure for definition of accidental conditions and loads related to loss of buoyancy for mobile drilling platforms, and one of the projects focused on ballast systems. A risk assessment model for evaluation of ballast system failures and subsequent loss of buoyancy was developed, and reliability data for ballast systems were gathered. The data is presented in appendix Figure B.2.

Interestingly, the RABL project concluded that the probability of a critical accidental situation due to technical failures in the ballast system, including power supply and instrumentation, was so low that contemporary ballast system designs were in compliance with the proposed acceptance criteria, and that efforts should rather be put into detailed verification of ballast systems. The project furthermore supported the use of the mandatory Failure Mode and Effect Analysis (FMEA) technique during design, and that other methods, such as Fault Tree Analysis (FTA), should only be performed if a lack of system redundancy or possible common cause failures had been identified (Østby et al., 1987).

With the introduction of FPSOs into harsh weather environments in the North Sea, with Petrojarl 1 as the first in 1986, the requirements applicable to FPSOs, including risk analysis, reliability studies and stability evaluations became a subject of attention. The clash of the requirement regimes is described in a paper prepared by DNV, Baunan (1996). The field of FPSO safety became well represented in literature, but mostly related to collisions risks, risks associated with the topside equipment, and techniques for using risk assessments as a design tool, e.g. MacDonald et al. (1999), Nesje et al. (1999), Overfield and Collins (2000), Vinnem et al. (2000), Vinnem (2000), Leonhardsen et al. (2001), Chen and Moan (2003), OGP (2006), Chen et al. (2007), Tronstad (2009).

Following the accident with the semi-submersible production platform Petrobras P-36 in 2001, and the incident with the Petrobras P-34 FPSO in 2002, the state owned Brazilian oil company Petrobras issued an Excellency Operational Program (PEO) with a series of tasks to improve the safety and operational reliability of its platforms (Rocha et al., 2010). The effort resulted in a qualitative methodology for risk and reliability analysis of the interaction between ballast and loading systems, electric and hydraulic power systems and associated control systems on production platforms. The methodology became mandatory for all new floating production

projects in 2005. Based on one of these qualitative analysis, [Rocha et al. \(2010\)](#) presents a quantitative functional reliability study, based on a FMECA and fault tree analysis. Perhaps the most interesting result of the article is the explicit recommendation that the least reliable component from the study, the equivalent to the vessel control system, should be subject to a safety integrity level (SIL) analysis based on the IEC 61511 standard.

Safety integrity analysis has been used in the North Sea offshore petroleum industry for over a decade, and on the Norwegian Continental Shelf (NCS), the OLF-070 guideline, presented in Section 2.0.3, represent the state-of-the art when it comes to reliability requirements and verification of ballast systems on offshore facilities. Since 2004, the guideline has prescribed minimum safety integrity level requirements for ballast systems, further discussed in Section 3.3.

Risk analysis and reliability assessments are related, and [Vinnem et al. \(2006\)](#) argues that apart from analysis of ship collisions, risk analysis of maritime systems on offshore facilities, including ballast systems, are normally extraordinarily simple and superficial, compared to the comprehensive analysis performed on petrochemical process equipment and in relation to drilling operations. [Vinnem et al. \(2006\)](#) recommends the use of FTA and Event Tree Analysis (ETA) as part of a ballast system risk analysis process. In [Hansen \(2007\)](#), FTA is applied to the ballast system of a semisubmersible drilling rig from a risk analysis point of view.

The final part of the literature survey is based on reports following the Deepwater Horizon accident in 2010. As a response to the accident, the independent research organization SINTEF and the Petroleum Safety Authority Norway (PSA) issued two separate reports, [Tinmannsvik et al. \(2011\)](#) and [Askedal et al. \(2011\)](#), to highlight lessons learned from the Deepwater Horizon accident and other major accidents in the petroleum industry. The two reports provide recommendations to the industry as a part of a continuous improvement effort, and present several important findings related to stability, floatability and ballast systems on offshore facilities where improvements should be made.

# Chapter 2

## Regulations and Standards

On the Norwegian Continental Shelf (NCS), the Petroleum Safety Authority Norway (PSA) is the regulatory authority for technical and operational safety. Any floating facility conducting petroleum activities on the NCS, including FPSO vessels, must comply to the rules and regulations of the PSA in all phases of operation. An important part of the documentation of compliance to these rules and regulations is the *Acknowledgement of Compliance* (AoC), issued by the PSA.

The AoC is a decision by the PSA that express the authorities' confidence that petroleum activities can be carried out using the floating facility within the framework of the regulations (PSA, 2011). The AoC will be issued on the basis of PSAs own assessment of the condition of the facility, measured against the rules and regulations applying to the use of mobile facilities on the NCS at the time of the AoC. The practice of the AoC ensures that any floating facility operating on the NCS, is compliant to the rules and regulations of the PSA, regardless of flag or class. For FPSO vessels, holding an AoC has been mandatory since July 1st, 2006 (PSA, 2011).

Ballast systems and stability are regulated in two overlapping ways in the PSA regulations. The PSA Facilities Regulations explicitly regulate ballast systems and stability through section 39 and section 62, where reference is made to the rules and requirements issued by the Norwegian Maritime Authority (NMA). In addition, the ballasting function performed by the ballast system on a floating facility is classified by the PSA as a safety function, subject to additional regulations.

In the following, the main regulations regarding ballast systems and stability from the PSA and NMA are presented, followed by a presentation of relevant regulations and requirements concerning reliability assessments of ballast systems. Where reference is made to the Norwegian Maritime Directorate, this is the former name of the NMA, as of January 1st. 2012.

### 2.0.1 PSA Regulations

The PSA Facilities Regulations regulate ballast systems and stability for floating facilities explicitly in section 39 and section 62.

#### Section 39 Ballast system

*Floating facilities shall be equipped with a system that can ballast any ballast tank under normal operational conditions. In the event of unintended flooding of any space adjacent to the sea, it shall nevertheless be possible to ballast. Ballast systems shall be in accordance with Section 2 and Sections 7 through 22 of the Norwegian Maritime Directorate's Regulations relating to ballast systems on mobile facilities (in Norwegian only).*

The regulation referred to is NMA Regulation No. 879, presented in Section 2.0.2.

#### Section 62 Stability

*Floating facilities shall be in accordance with the requirements in Sections 8 through 51 of the Norwegian Maritime Directorate's Regulations relating to stability, watertight subdivision and watertight/weathertight closing mechanisms on mobile offshore facilities (in Norwegian only). There shall be weight control systems on floating facilities, which ensure that the weight, weight distribution and centre of gravity are within the design specifications. Equipment and structure sections shall be secured against displacement that can influence stability.*

The regulation referred to is NMA Regulation No. 878, presented in Section 2.0.2.

In the PSA Guideline regarding the facilities regulations, section 3, ballasting for floating facilities is defined as a safety function. The Facilities Regulations, section 8, state that performance requirements shall be stipulated for safety functions.

#### Section 8 Safety functions

*Facilities shall be equipped with necessary safety functions that can at all times a) detect abnormal conditions, b) prevent abnormal conditions from developing into hazard and accident situations, c) limit the damage caused by accidents. Requirements shall be stipulated for the performance of safety functions. The status of safety functions shall be available in the central control room.*

### 2.0.2 NMA Regulations

The main regulations of the NMA regarding ballast systems and stability are

- Regulation 20 December 1991 No. 879 concerning ballast systems on mobile offshore units
- Regulation 20 December 1991 No. 878 concerning stability, watertight subdivision and watertight/weathertight closing means on mobile offshore units

### 2.0.3 Reliability Assessment Requirements

The PSA and NMA regulations require that the ballast system is capable of performing its function, and indirectly presents reliability assessment as a means of verification.

In the NMA regulations, the following references to reliability assessments are made

- Regulation 20 December 1991 No. 879 concerning ballast systems on mobile offshore units
  - § 8: Requirements for risk analysis: *An analysis shall be carried out to verify the ability of the ballast system to function in accordance with the provisions of these regulations*
  - The analysis may be a risk/reliability analysis (Vinnem et al., 2006)
- Regulation 20 December 1991 No. 878 concerning stability, watertight subdivision and watertight/weathertight closing means on mobile offshore units
  - § 5: Documentation: *The company shall be able to document compliance with the requirements of these regulations.*
  - This may be a risk/reliability analysis (Vinnem et al., 2006)
- Regulation 22 December 1993 No. 1239 concerning risk analysis for mobile offshore units
  - § 15: Reliability/vulnerability analysis: *In the risk analysis the company shall incorporate a reliability/vulnerability analysis from every vendor of vital operating systems and safety and emergency systems. The result of the reliability/vulnerability analysis shall be incorporated into and taken into account in the design analysis and construction analysis.*

The PSA regulations introduce reliability assessments of the ballast system through the performance requirements of safety functions. In the PSA *Guideline regarding the facilities regulations*, Re Section 8, the following applies to safety functions, including the ballasting function:

*For design of safety functions as mentioned in the first subsection, the standards NS-EN ISO 13793, NORSOK S-001 and IEC 61508 and OLF guideline No. 070 should be used.*



*In order to stipulate the performance for the safety functions as mentioned in the second subsection, the IEC 61508 standard and OLF Guideline No. 070 should be used where electrical, electronic and programmable electronic systems are used in the structure of the functions.*

The reference made to the [IEC 61508 \(2010\)](#) standard, and the [OLF070 \(2004\)](#) guideline is important. These documents will be presented in the next section, and are used throughout the thesis.

### IEC 61508 Standard

The [IEC 61508 \(2010\)](#) standard is the main international standard for developing safety requirements to electrical, electronic and programmable electronic safety related systems, also known as Safety Instrumented Systems (SIS). SISs are safety systems comprising one or more input elements, one or more logic solvers and one or more actuating units. The main parts of a SIS are illustrated in Figure 2.1, adopted from [Lundteigen and Rausand \(2007\)](#)

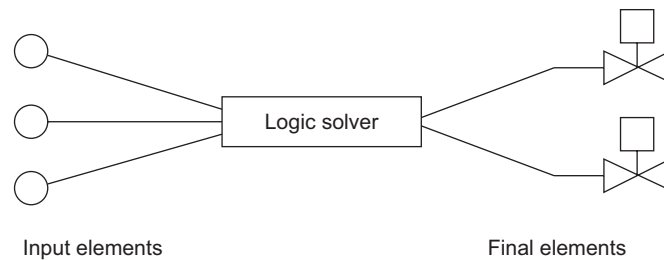


Figure 2.1: Main elements of a SIS

The [IEC 61508 \(2010\)](#) standard is a generic, performance based standard that outlines how the functional safety of a SIS should be managed, and provides guidance to the process of validation and verification of such systems. The standard is used extensively throughout the oil and gas industry, together with the application specific standard for SISs in the process industry; the [IEC 61511 \(2004\)](#) standard. In Section 3.3, the process of developing reliability requirements based on the [IEC 61508 \(2010\)](#) standard will be presented and discussed.

### OLF 070 Guideline

The [OLF070 \(2004\)](#) guideline is a document developed to adapt and simplify the use of the [IEC 61508 \(2010\)](#) and [IEC 61511 \(2004\)](#) standards in the Norwegian petroleum industry. The guideline was developed as a joint industry project between operators and suppliers of the industry, with the support of The Norwegian Oil Industry Association (OLF).

The [OLF070 \(2004\)](#) guideline has become part of the recommended standard for specification, design and operation of SISs on the NCS, and the document is closely linked to the safety func-

tions defined in the PSA regulations. The guideline presents an alternative approach to the [IEC 61508 \(2010\)](#) process of establishing reliability requirements to safety functions, and evaluates ballast systems explicitly as part of this approach. With regards to the quantification of reliability of safety functions, the guideline recommends the use of the *PDS method* ([Hauge et al., 2009b](#)). The PDS method is a reliability prediction method for SISs, in line with the main principles of the [IEC 61508 \(2010\)](#) and [IEC 61511 \(2004\)](#) standards. In Section 3.3, the process of developing reliability requirements based on the [OLF070 \(2004\)](#) guideline will be presented and discussed.

# Chapter 3

## FPSO Ballast System and Functions

### 3.1 Ballast System and Functions

#### 3.1.1 Ballast System

All shipshaped floating production vessels are equipped with a ballast system, which is used to maintain draft, stability and to keep the sheerforces and bending moments in the hull within required limits. The ballast system performs these important functions by performing ballasting and deballasting operations, whereby water is added or removed to different sections of the hull. A typical ballast system consist of the following subsystems:

- Ballast tank configuration, pumps and valves
- Electric power system
- Hydraulic power system
- Ballast control system

In the following, a base case ballast system is described. The system is described at a level of detail that provides a foundation for reliability assessments of different FPSO designs. The base case vessel is a double sided and double bottomed ship shaped FPSO.

### Ballast Tank Configuration, Pumps and Valves

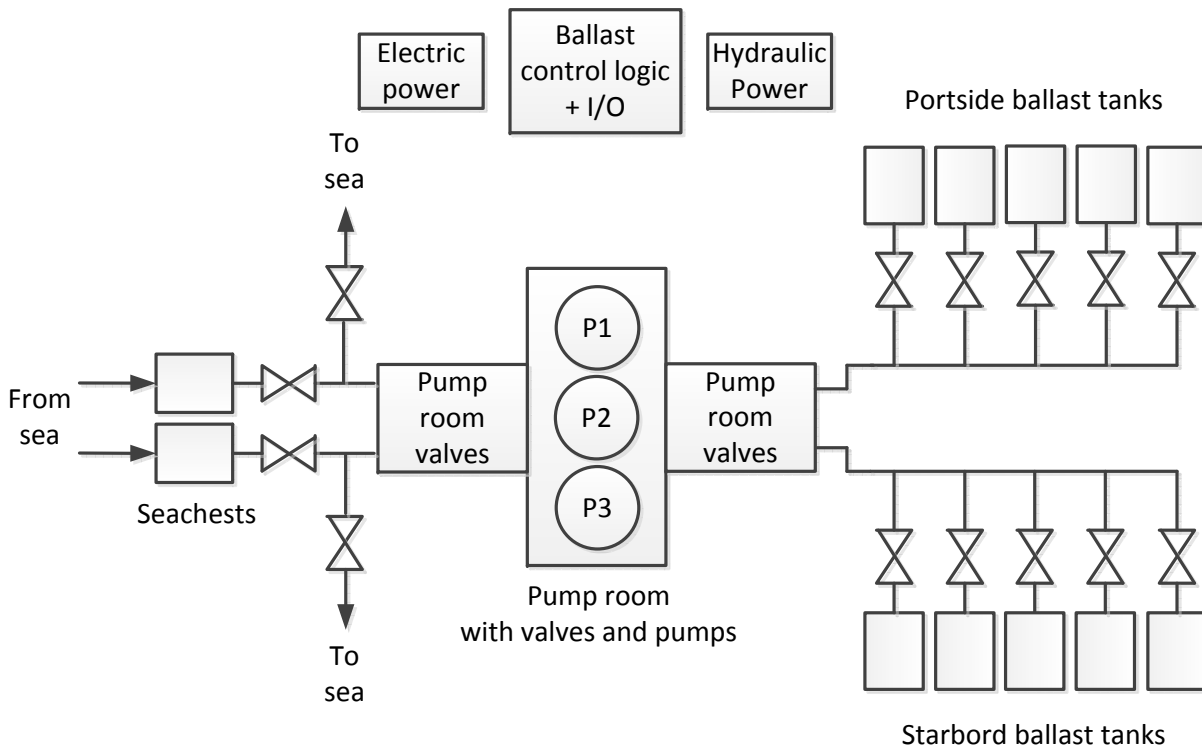


Figure 3.1: Sketch of the ballast system

### Ballast Tank Configuration

The main ballast tanks are located on the port and starboard sides of the vessel, on each side of the cargo tanks. The number of cargo and ballast tanks are usually determined based on the production capacity of the FPSO and whether a shuttle tanker will be moored to offload the produced oil. On the base case vessel, there are five main ballast tanks on each side.

The ballast tanks are connected to a ringmain line which transports ballast water between the tanks and the pump room. Ballast valves control the flow of water between the individual tanks and the ringmain line.

Through the ringmain line and pump room arrangement, ballast water can be transported between the port side and the sea, the starboard side and the sea, as well as internally between the portside and starboard ballast tanks.

Additional ballast tanks may be located in the aft and forward sections of the vessel, and are used to manipulate the trim of the vessel. Ballasting for aft trim is performed to improve inherent heading control and weathervaning, and to facilitate process pipe drainage and effective unloading of main ballast tanks. If the FPSO is equipped with an advanced turret system, an

additional turret ballast system may be present. These additional ballast tank systems are not included in the base case ballast system.

### Ballast Valves

The ballast valves are hydraulically operated butterfly valves, that fail to a closed position. The valves are normally closed, and are opened and kept open by hydraulic pressure acting through a fail safe solenoid valve. The solenoid valve is normally closed, and is opened by electric signal from the ballast control system. If the operator decides to close the valve or electric power is lost, the electric signal will stop, and the solenoid will automatically return to a closed position, closing the ballast valve. If hydraulic power is lost, the valve will return to closed position. A position feedback signal is continuously sent from the actuator to the ballast control system. In case of loss of position signal, the ballast control system will indicate a faulty signal, and close the valve. Figure 3.2 present such a valve.

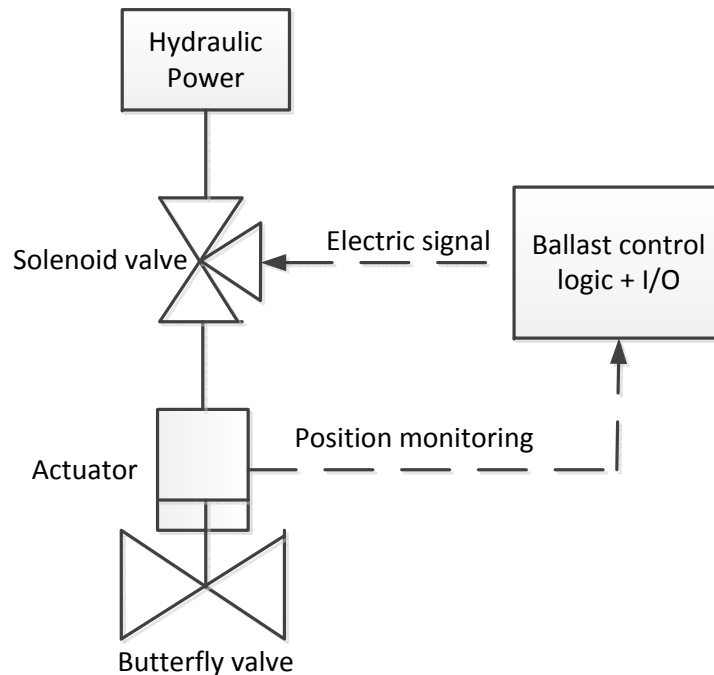


Figure 3.2: Hydraulically operated butterfly valve

### Pump room

The pump room consists of a network of pipes, pumps and pump room valves that can be brought to different configurations based on the planned ballasting operation. The ballast pumps are electric centrifugal pumps operating in one direction only. In order to switch between ballasting and deballasting operations, the water is routed around the pumps accordingly.

In the base case pump room configuration, three pumps are installed in a redundant setup,

whereby any pump can perform any ballasting operation on its own. The pumps are normally de-energized, and fail to a de-energized state. The pump room valves are hydraulically operated butterfly valves, controlled by electric signal from the ballast control system. The valves are normally closed, and are fail-to-set valves. This means that the valves do not move to a predefined position automatically upon loss of signal, but remain in the last known position. The valve is similar to the valve presented in Figure 3.2.

### **Seachest/Discharge System**

The seachest/discharge system is used when performing ballasting or deballasting operations to sea. Two seachests are located below the waterline on each side of the vessel, providing primary intake of seawater for ballasting operations. The seachests are equipped with hydraulically operated valves controlled by electric signal from the ballast control system. The valves are normally closed, and fail to a closed position. The valves are similar to the valve presented in Figure 3.2.

The discharge system consist of two pipes to sea, installed above the water line on each side of the vessel. The discharge pipes are equipped with hydraulically operated ballast valves controlled by electric signal from the ballast control system. The valves are normally closed and fail to a closed position. The valves are similar to the valve presented in Figure 3.2.

### **Electrical Power System**

The electric power system consists of the main power system, the emergency backup generator and the Uninterruptible Power Sources (UPS).

Electric power is used to power the ballast control stations, pumps, the hydraulic power system and to signal and receive position feedback from all the valves in the ballast system.

The main electric power system is operating continuously. In case of loss of main electric power, UPSs will immediately provide emergency power to the ballast control stations and operator screens. Next, the emergency backup generator will turn on automatically. The emergency backup generator provides a fraction of the main electric power, but enough power to operate the ballast system.

### **Hydraulic Power System**

The hydraulic power system consists of the main hydraulic power generator and a hydraulic accumulator.

Hydraulic power is used to operate all the ballast system valves. In order to ensure consistent hydraulic pressure, the hydraulic power system is continuously energized and pressurized. In case of loss of electric power, or failure of the main hydraulic power generator, the hydraulic accumulator will automatically provide sufficient hydraulic pressure to operate the ballast valves for some time.

### **Ballast Control System**

The ballast control system consists of the ballast control logic.

The ballast system is remotely controlled by an operator from a control station on the bridge and/or from a designated ballast control room. From the control station, the various components of the ballast system are activated through a control panel. The ballast control logic translates the operator commands and the feedback from the valves and pumps into electric signals, activating the valve solenoids and ballast pumps accordingly.

The ballast operator will use various sources of information for decision support during ballasting operations. The main sources of information are the calculations performed by the load calculator, the information from level transmitters in cargo and ballast tanks and visual and physical perception of the inclination and draft of the vessel.

### **3.1.2 Ballast System Functions**

In the following section the main ballast system function is presented and split into safety functions and non-safety related functions, providing a foundation for classification of the system. The main function of the ballast system as presented in [Petrojarl \(2011a\)](#):

*The ballast system is used to maintain sufficient draft, stability and to keep the bending moments and shearforces within required limits*

#### **Safety Functions:**

- Maintain stability and draft of the vessel.

#### **Non-Safety Related Functions:**

- Keep the bending moments within required limits.
- Keep the shearforces within required limits.

These non-safety related functions are mentioned briefly in Section [3.1.4](#), but are otherwise not included. They are defined as non-safety related functions as the lack of these functions would

cause unnecessary stress to the hull of the vessel, but not loss of stability or draft and immediate danger of a hazardous situation.

### 3.1.3 Ballast System as a Safety Barrier

According to Sklet (2006), safety barriers are *physical* and/or *non-physical* means planned to prevent, control, or mitigate undesired events or accidents. Depending on when the ballast system is operated, it can prevent, control or mitigate unacceptable inclination and draft of the vessel, by ballasting or deballasting the hull. The ballast system can be regarded as a:

- *Safety barrier against unacceptable inclination and draft*

The ballast system is the second safety barrier against unacceptable inclination. The primary safety barrier against unacceptable inclination is the inherent stability and draft of the vessel design. The ballast system should furthermore be regarded as a *barrier system*. A barrier system is a system that has been designed and implemented to perform one or more *barrier functions*. A barrier function is defined as (Sklet, 2006)

- *Barrier function: A barrier function is a function planned to prevent, control, or mitigate undesired events or accidents*

If the barrier system is functioning, the barrier function is performed (Sklet, 2006). In order to assess the full functionality of the ballast barrier system, the following barrier functions are proposed:

- **Barrier function 1:** To ballast/deballast starboard ballast tank system in response to operator command (BF1)
- **Barrier function 2:** To ballast/deballast portside ballast tank system in response to operator command (BF2)
- **Barrier function 3:** To ballast/deballast between starboard and portside ballast tank system in response to operator command (BF3)
- **Barrier function 4:** Emergency stop of ballast system operation in response to operator command (BF4)

By combining ballasting and deballasting operations in the barrier function description in BF1, BF2 and BF2, the similarities between the two operations are taken into account, minimizing the number of individual barrier functions. The two operations have the opposite effect on the vessel, but utilize almost all the same components. The only difference is the routing of the water in the pump room, and the switch between using the seachest or discharge configuration to



carry out the function. The reduced number of barrier functions simplify the reliability assessment of the safety barrier. BF4 is included as a part of the barrier system, due to the fact that if an intended ballasting operation gets out of control, the ballast system will actually create unacceptable inclination and draft. Having the possibility to stop an ongoing ballast operation is therefore an important barrier function.

### 3.1.4 Ballast System Operational Situations

The ballast system functions are used in two operational situations:

1. Upon a hazardous event/situation
2. Normal operations

Upon a hazardous event/situation, any ongoing ballast operations is stopped, and the operator perform new ballasting operations to mitigate the occurrence of an undesired event. This operational situation will be intense and demanding, and rely on the operators ability to make fast decisions and perform the correct operations. During this operational situation, the ballast system perform safety barrier functions.

During normal operations the ballast system is used to perform non-safety related functions. During production of crude, the FPSO alternates between a fully loaded state and an empty state right after offloading to a shuttle tanker. Throughout these states, ballasting operations are performed with regular intervals each day to maintain the draft and stability of the vessel, and to keep the bending moments and sheerforces within required limits. These operations are part of the daily production routine, and are not conducted as a response to a hazardous event/situation.

### 3.1.5 Safety Barrier Classification

Safety barriers may be classified as either *active* or *passive*, and as *physical/technical* or *human/operational*, according to the classification by Sklet (2006), presented in Figure 3.3. An *active barrier* is defined by Sklet (2006) as:

*A barrier that is dependent on the actions of an operator, a control system, and/or some energy sources to perform its function.*

The ballast system performs its barrier functions upon demand from an operator by the means of electronic and hydraulic energy sources controlled by a specialized control system, and can be classified as an *active, physical/technical* barrier.

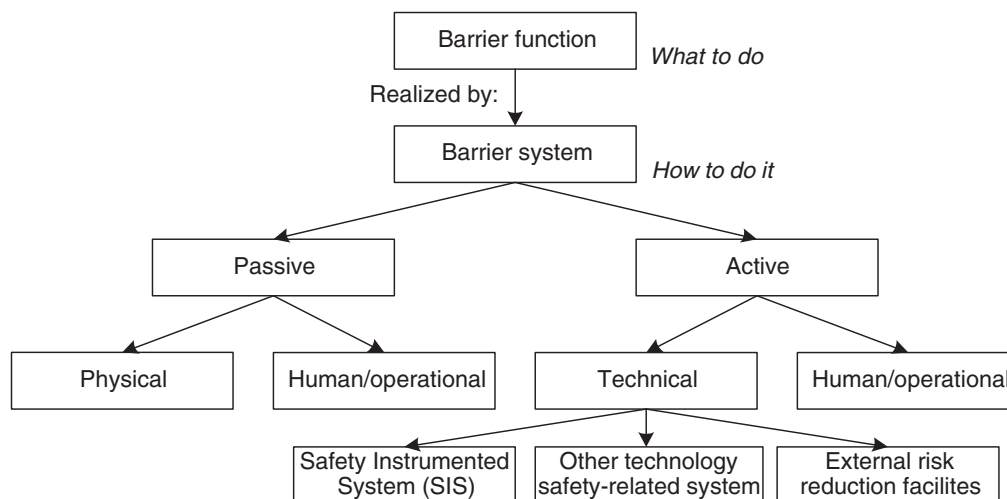


Figure 3.3: Classification of barriers

Active, technical barriers are further classified into the following three groups, in accordance with IEC 61508 (2010) and IEC 61511 (2004)

- *Safety Instrumented Systems (SIS)*
  - Safety systems comprising one or more input elements, one or more logic solvers and one or more actuating units.
- *Other technology safety-related systems*
  - Active safety systems that do not have any integrated logic (Rausand, 2011), based on technology other than electrical, electronic, or programmable electronic (Sklet, 2006).
- *External risk reduction facilities*
  - Measures to reduce or mitigate the risk that is separate and distinct from the SIS or other technology safety-related systems (Sklet, 2006).

Ballast systems should be classified as SIS, and the main parts of the ballast system SIS is presented in Figure 3.4. Upon demand, the ballast operator will provide the ballast control system with operator commands. Together with the feedback signals from the final elements, these are the main input elements to the SIS. The feedback signals are position indication signals from valves, activation signals from pumps. The ballast control logic will translate the input elements into electric signal based on the pre-programmed logic, and subsequently activate the final elements. The final elements in the ballast system are the electric pumps and various ballast system valves.

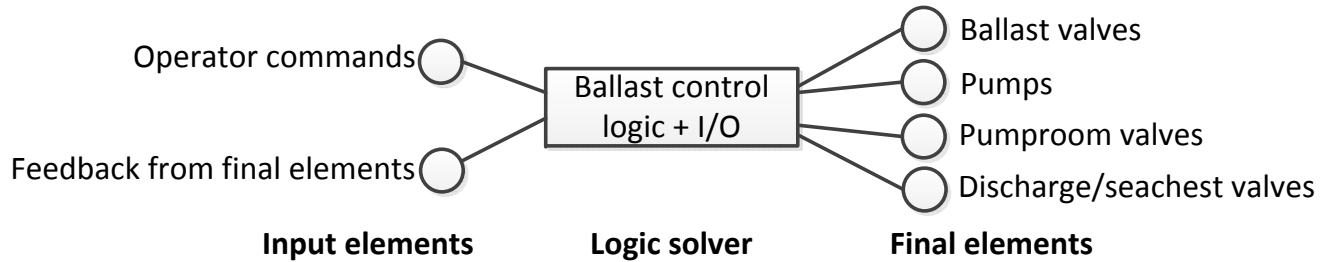


Figure 3.4: Ballast systems as a SIS

Historically, ballast systems did not involve any integrated logic, and the operator would control the ballasting operations from hardware based control stations. By physically operating switches, the final elements in the ballast system would be activated and deactivated directly. According to the classification scheme above, ballast systems were *Other technology safety-related systems*. With the introduction of integrated logic, ballast systems became *Safety Instrumented Systems*, with new inherent hazards and reliability challenges. Despite this transition, ballast systems are not regulated as SISs today. Throughout the rest of the report the ballast system will be treated according to a SIS classification.

SISs are used to implement one or more safety instrumented functions (SIF). A SIF is defined by [Rausand \(2011\)](#) as

*Safety Instrumented Function (SIF): A barrier function that is implemented by a SIS and that is intended to achieve or maintain a safe state of the EUC with respect to a specific deviation (process demand). A SIS may consist of one or more SIFs.*

The *specific deviation* or *process demand* should be regarded as the loss of stability and/or draft due to a hazardous event. The SIFs of the ballast system correspond to the barrier functions identified in Section 3.1.3. The SIFs are presented along with the defined success criteria for each SIF, and an associated sketch of the components involved in carrying out the SIF.

- **SIF 1:** To ballast/deballast starbord ballast tank system in response to operator command
  - The SIF is successful when: (1) One of the starbord ballast tanks is ballasted/deballasted to sea in response to operator command. (2) The ballasting operation stops upon operator command.

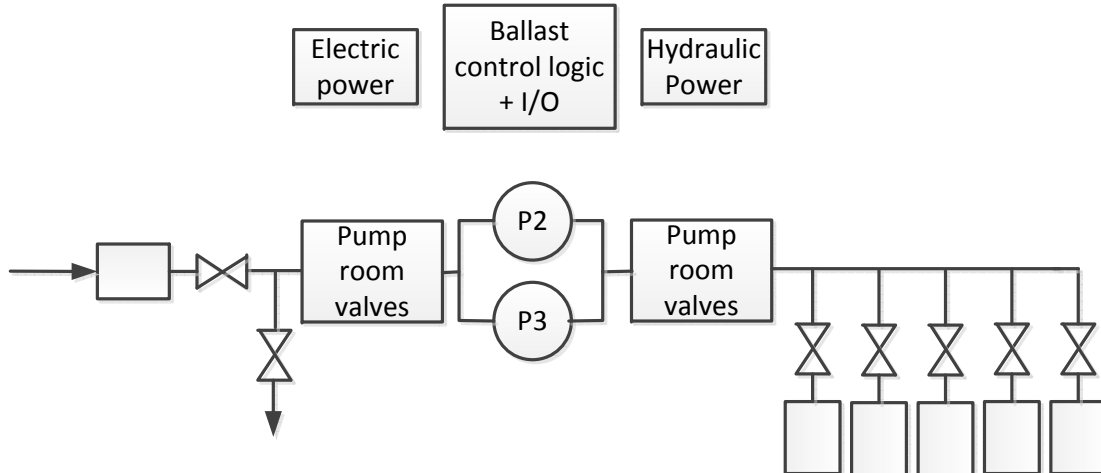


Figure 3.5: Sketch of SIF1

- **SIF 2:** To ballast/deballast portside ballast tank system in response to operator command
  - The SIF is successful when: (1) One of the portside ballast tanks is ballasted/deballasted to sea in response to operator command. (2) The ballasting operation stops upon operator command.

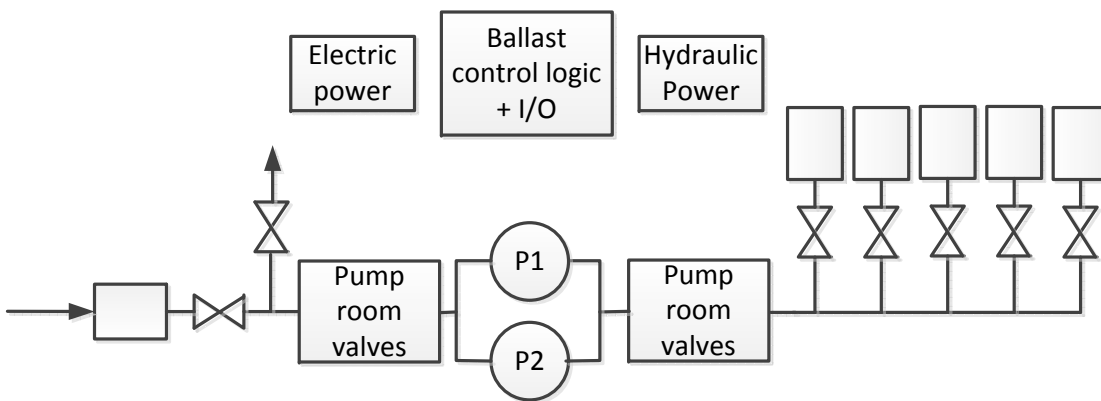


Figure 3.6: Sketch of SIF2

- **SIF 3:** To ballast/deballast between starbord and portside ballast tank system in response to operator command
  - The SIF is successful when: (1) One of the portside ballast tanks is ballasted/deballasted with one of the starbord ballast tanks in response to operator command. (2) The ballasting operation stops upon operator command.

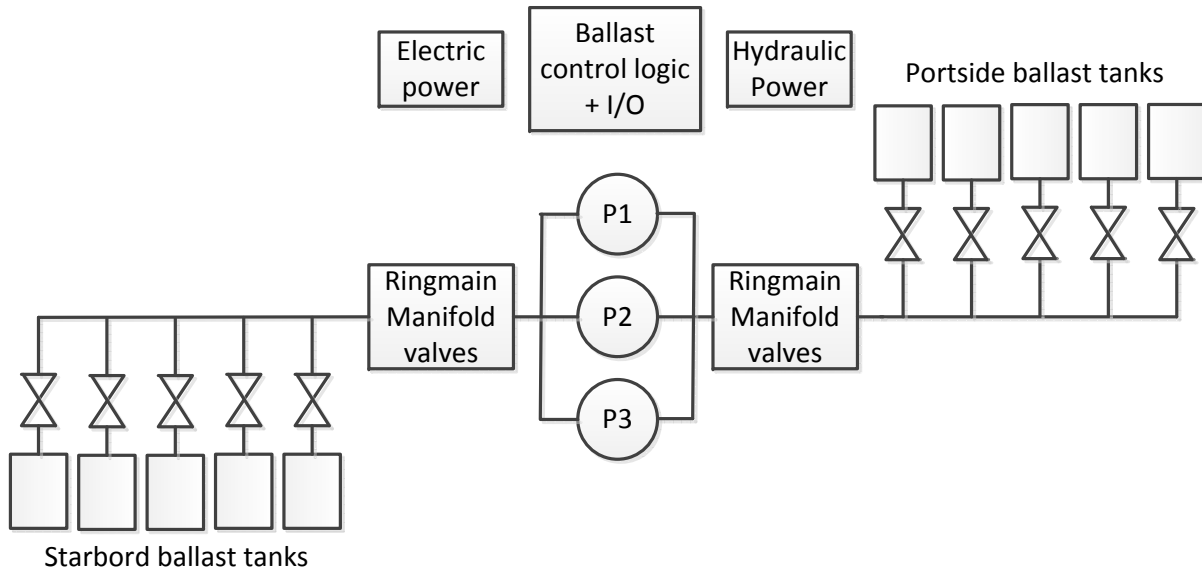


Figure 3.7: Sketch of SIF3

- **SIF 4:** Emergency stop of ballast system operation in response to operator command
  - The SIF is successful when: (1) Any ongoing ballasting operation is stopped upon operator command. (2) All active components return to safe state.

The type and amount of electrical components constituting an emergency shutdown will vary significantly. A sketch of the components is therefore not presented.

### Safe State of the FPSO

The ballast system is designed to bring the vessel into a safe state, by the use of the SIFs. The [IEC 61508 \(2010\)](#) standard defines a safe state as

*Safe state: the state of the Equipment Under Control (EUC) when safety is achieved.*

The [IEC 61508 \(2010\)](#) standard does not provide any specific rules as to how the EUC and its boundaries should be defined ([OLF070, 2004](#)), but based on the definitions in the standard, the [OLF070 \(2004\)](#) guideline has proposed that the EUC can be a piece of equipment, machinery, part of an offshore installation, or the entire installation.

With regards to the ballast system, the EUC is the entire FPSO vessel. This definition excludes any mooring, riser or offloading systems from the boundary of the EUC.

Defining the safe state of the EUC is not straightforward, as the vessel is in constant motion. With reference to the definition of safe state, safety is achieved when the FPSO has acceptable

inclination and draft. The limits for what is acceptable will vary, but the vessel must comply to the stability requirements of the flag or class, and these limits will be part of the vessel documentation. Per definition, as long as the vessel has a controlled inclination and draft within acceptable limits, safety is achieved, and the EUC is in safe state. The following definition is proposed:

- *Safe state of the vessel is the controlled state in which the vessel has acceptable inclination and draft*

This is the safe state of the FPSO, but it can not be translated directly into a requirement for fail safe design of the ballast system, because the ballast system has the capability of bringing the EUC both in and out of the safe state, depending on the actions of the operator. The same applies to any ballasting operation which is out of control. As such, the ballast system will not be able to automatically bring the EUC into safe state upon a ballast system failure.

The ballast system should be designed to fail to a state in which no escalation of a hazardous event is possible. On a system level, this implies that the ballast system should seize to perform any ballasting operations. On a component level, all components should fail to a state in which no ballasting operation is possible. The NMA regulation No. 879, presented in Section 2.0.2, define this state as the *safe position* of the system, where the valves are required to be closed and ballast pumps stopped.

### **SIS Mode of Operation**

The IEC 61508 (2010) standard differentiates between two modes of operation for SISs: *low demand mode of operation* and *high demand/continuous mode of operation*. The classification refer to the demand frequency of the SIS, and the boundary point between the modes is often taken to be once per year (Rausand, 2011). If a demand occurs more often than once per year, the SIS is operating in a high demand mode of operation. The classification of mode of operation is important, as the reliability requirements to SISs are set according to the classification.

Ballast systems on FPSOs are used extensively throughout the year. Ballasting operations are conducted daily, and the system is in high demand, but these operations are conducted as part of the daily production routine. When a ballast system SIF is used to respond to a loss of stability and/or draft due to a hazardous event, this can be looked upon as an *on demand* situation, related to systems in low demand mode of operation. In the OLF070 (2004) guideline, the low demand mode of operation is referred to as a *demand mode of operation*. The ballast system is hereby classified as a *on demand* system operating in a low demand mode of operation.

### 3.1.6 Hazard Analysis

A HAZID is carried out to identify hazards that can lead to loss of stability and draft of the vessel. The result of the HAZID is presented in Figure 3.8. The identified hazards are categorized into the following hazard categories:

- **External:** hazards originating from external forces acting on the vessel
- **Internal:** hazards originating from possible internal fault conditions in the ballast system, or during ballasting operations
- **Human error:** hazards originating from maloperation of the ballast system or vessel equipment

The hazards are ranked according to frequency and consequence based on a coarse evaluation of the hazard. The corresponding risk priority number (RPN) is the sum of the two ranking categories, ranging from 1 as the lowest, and 5 as the highest.

**Limitations** The HAZID was limited to identify only a selection of external hazards and hazards due to human errors.

**Results of the HAZID** There are multiple hazards leading to loss of stability and draft of a vessel, and although many of these hazards are rare, the consequences can be very high, and their influence on the total risk of the EUC is substantial. The hazards originating from the internal hazard category are especially important as these hazards can be practically eliminated by a robust ballast system design.

Hazard	Hazard category Internal/External/Human error	Hazardous event	Frequency class	Consequence class	RPN
Marine collision	External	Loss of stability/ draft	2	5	7
Loss of mooring			1	4	5
Loss of cargo to sea			2	4	6
Water ingress into vessel			2	3	5
Heavy weather			3	2	5
Heavy wind			3	2	5
Greenwater			2	3	5
Human error during ballasting, crane operation, offloading, production, cargo handling etc.	Human error		3	3	6
Ballast control system spurious trip	Internal		1	5	6
SIF 1 spurious trip			1	5	6
SIF 2 spurious trip			1	5	6
SIF 3 spurious trip			1	5	6
Loss of control during SIF1 operation			2	5	7
Loss of control during SIF2 operation		2	5	7	
Loss of control during SIF3 operation		2	5	7	

Figure 3.8: HAZID

### Hazard-Barrier Matrix

Based on the barriers and SIFs identified in Section 3.1.3 and Section 3.1.5, and the hazards identified in Section 3.1.6, a *hazard-barrier* matrix is used to evaluate the adequacy of the barriers. The main objectives of a hazard-barrier matrix are to (Rausand, 2011)

- Identify barriers that are (or should be) implemented as protection against a specified hazard.
- Identify barriers that are able to protect against more than one hazard.
- Identify hazards for which protection is inadequate.
- Verify the adequacy of the existing barriers and indicate where improvements are needed.

**Hazard Categories:** The hazard categories are equivalent to the hazard categories defined in the HAZID study in Section 3.1.6:

- External (hazards)
- Internal (hazards)
- Human error (hazards)



Internal hazards are assessed individually, while human error hazards and external hazards are assessed as groups of hazards.

**Barrier Categories:** Three barriers have been included in the matrix:

- Barrier 1: The inherent stability and draft of the vessel design
- Barrier 2: The ballast system
- Barrier 3: Other possible interventions

### **Results of the Hazard-Barrier Matrix**

The hazard-barrier matrix present the critical importance of the emergency stop function of SIF4, as the primary barrier against internal hazards. The inherent stability/draft of the vessel is seen to be the only barrier able to protect against all the hazards. For external hazards and human error hazards, SIF1, SIF2 and SIF3 can be used in different combinations to regain stability and draft of the vessel. Manual intervention against internal hazards is the physical override of valves and pumps by the vessel crew.

Hazard-Barrier Matrix		Barrier 1	Barrier 2				Barrier 3
Hazard category	Hazard description	Inherent stability/draft	Ballast system				Other
			SIF 1	SIF 2	SIF 3	SIF 4	
External	Loss of stability	X	X	X	X		
	Loss of draft	X	X	X	X		
Human error	Loss of stability	X	X	X	X		
	Loss of draft	X	X	X	X		
Internal	Ballast control system spurious trip	X				X	Manual intervention
	SIF 1 spurious trip	X				X	Manual intervention
	SIF 2 spurious trip	X				X	Manual intervention
	SIF 3 spurious trip	X				X	Manual intervention
	Loss of control during SIF1 operation	X				X	Manual intervention
	Loss of control during SIF2 operation	X				X	Manual intervention
	Loss of control during SIF3 operation	X				X	Manual intervention

Figure 3.9: Hazard-barrier matrix

### 3.2 Safety Barrier Failure Analysis

In order to function properly, the components constituting the various SIFs of the ballast system must be in proper condition and available on demand. This is not always so, and the ballast system may fail to operate as desired when one of its SIFs fail due to random, systematic or common cause failure. These failure causes are the main sources of system unavailability, and during ballast system design, operation and reliability verification, it is important to understand these types of failures and their influence on SIF performance.

In the following section the various failure causes and failure modes of the ballast system components are classified. Subsequently, a failure modes, effects and criticality analysis (FMECA) is carried out on the ballast system components.

### 3.2.1 Failure Cause Classification

#### Random and Systematic Failures

The IEC 61508 (2010) standard differentiate between *random hardware failures* and *systematic failures*, and based on this failure cause classification the PDS method (Hauge et al., 2009b) present a failure classification that provides a detailed classification of systematic failures. In the PDS method (Hauge et al., 2009b), **random hardware failures** are defined as failures resulting from the natural degradation mechanisms of the component. **Systematic failures** are defined as failures related to a particular cause other than natural degradation. These failures are due to errors made during specification, design, operation and maintenance phases of the component lifecycle.

In the PDS method classification (Hauge et al., 2009b), random hardware failures are consider to be *independent failures* and are assumed not to result in CCF, while systematic failures are potentially *dependent failures* which may lead to CCF. Due to the detailed breakdown of systematic failures, the PDS failure cause taxonomy has been adopted. In the PDS method, systematic failures are split into

- **Software faults:** Programming faults introduced during software design, modification or during updates. Ex: Ballast control logic programming fault.
- **Design related failure:** Failures introduced during the design phase of the equipment. Ex: Ballast valve fails to close due to insufficient actuator force.
- **Installation failure:** Failures introduced during the last phases prior to operation, during installation/commisioning. Ex: Ballast valve position sensor miscalibrated.
- **Excessive stress failure:** Failure due to stress beyond the design specification of the component. Ex: Ballast pumps operated during high pressure gravity filling.
- **Operational failure:** Failures initiated by human errors during operation or maintenance/testing. Ex: Ballast pumps operated dry.

#### Common Cause Failures

If two or more dependent failures occur simultaneously, this is referred to as a CCF, defined as

*Common cause failure (CCF): A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause.*

The definition is adopted from [Rausand \(2011\)](#), originating from the nuclear industry. As CCFs can lead to simultaneous failures of redundant components, SIFs and even different SIFs at the same time, CCFs represent a serious threat to SIS reliability performance. Ballast systems are susceptible to CCFs, and it is of critical importance to recognize the failure type and find ways to reduce the influence of CCF in design and operation of ballast systems, and to include the contribution from CCF in reliability verification calculations.

The CCF definition includes several of the attributes of CCFs, identified by [Watson and Smith \(1980\)](#), adopted from [Rausand \(2011\)](#)

- The components affected are unable to perform as required.
- Multiple failures exist within (but not limited to) redundant configurations.
- The failures are a "first in line" type of failure, not the result of cascading failures.
- The failures occur within a defined critical time period
- The failures are due to a single underlying defect or physical phenomenon
- The effect of failures must lead to some major disabling of the system's ability to perform as required.

The emphasis on dependent failure in the definition is important, and explains why CCF causes are often identical to the systematic failure causes. To clarify when dependent failures are defined as CCF, the following attributes from [Lundteigen and Rausand \(2007\)](#) may be used as a guideline: (1) the CCF event comprises multiple (complete) failures of two or more redundant components or two or more SIFs due to a shared cause, (2) the multiple failures occur within the same inspection or function test interval, (3) the CCF event leads to failure of a single SIF or loss of several SIFs.

CCF failures reduce the effect of redundancy in SIS design, and the number of components failing at the same time is only limited to the severity of the common cause, and the strength of the dependency between the components. It should be noted that a CCF may lead to just one component failing, if the other components have not yet failed within the critical time period.

An important element of failure classification of CCF is to identify the basic causes of component failure and the reason why several components are affected by the same basic cause. One way to do this, is by splitting CCFs failure causes into to *root causes* and *coupling factors*. A root cause of a failure is defined by [Rausand \(2011\)](#) as

*Root cause: The root cause of a specified failure is the most basic cause that, if corrected, would prevent recurrence of this and similar failures.*

A coupling factor is defined by [Rausand \(2011\)](#) as

*Coupling factor: A property that makes multiple components susceptible to failure from a single shared cause.*

A CCF is always the result of a root cause and a coupling factor, and knowledge of root causes and coupling factors among the components in a SIS will provide a basis for corrective actions and defenses aimed at minimizing the influence of CCF on the system. In Section 5.3, a defence approach against CCF in ballast systems is presented.

### 3.2.2 Failure Mode Classification

In [IEC 61508 \(2010\)](#), failure modes are split into Dangerous (D) and Safe (S) failures, based on the effect the failure mode has on the function of the SIS, the SIS subsystem or the SIS element. Dangerous failures *"prevent the safety function from operating when required, or decreases the probability that the safety function operates correctly when required"*([IEC 61508, 2010](#)), while Safe failures *"result in the spurious activation of the safety function to put the EUC (or part thereof) into a safe state, or increases the probability of the spurious operation of the safety function into a safe state."* ([IEC 61508, 2010](#))

Based on the definitions above, and the descriptions in [Rausand \(2011\)](#) the following classification and subclassification is used:

- **Dangerous (D)**. The SIS/SIS subsystem/SIS element does not fulfill its required safety-related functions upon demand. These failures may be split further into:
  - **Dangerous Undetected (DU)**: Dangerous failures that prevent activation on demand and are revealed only by testing or when a demand occurs.
  - **Dangerous Detected (DD)**: Dangerous failures that are detected immediately when they occur.
- **Safe failure (S)**. The SIS/SIS subsystem/SIS element has a nondangerous failure. These failures may be split further into:
  - **Safe Undetected (SU)**: Non-dangerous failures that are not detected by automatic self-testing or incidentally by personnel.
  - **Safe Detected (SD)**: Non-dangerous failures that are detected by automatic self-testing or incidentally by personnel.

### 3.2.3 Failure Modes, Effects and Criticality Analysis (FMECA)

A FMECA is carried out to identify failure modes, failure causes and failure effects among the main components of the ballast system. The main objective of the FMECA is to identify the dangerous undetected (DU) failure modes of the ballast system components. The dangerous undetected failure modes are hidden failures that will only be revealed by a real demand or a function test. The final FMECA worksheets are presented in appendix Figure B.1. A description of the method can be found in [Rausand \(2011\)](#) or the [IEC 60812 \(2006\)](#) standard.

#### System Breakdown

The FMECA is based on the system description from Section 3.1.1, and the system breakdown presented in appendix Figure B.1. The system breakdown provides an overview of the relevant components, but does not reflect the system functionality. The components included in the FMECA analysis are:

Ballast tank configuration, ballast valves and pumps	Ballast valves Pumproom valves Seachest valves Discharge valves Ballast pumps
Electric power system	Main electric power generator Emergency backup generator UPS
Hydraulic power system	Main hydraulic power generator Hydraulic accumulator
Ballast control system	Ballast control logic

Table 3.1: Components subject to the FMEA

#### System Functions and Operational Modes

The components are analysis in accordance to how they function as part of the barrier functions presented in Section 3.1.3. The operational modes are based on the typical modes of the specific component. The failure modes are ranked according to frequency and consequence based on a coarse evaluation. The corresponding risk priority number (RPN) is the sum of the two ranking categories, ranging from 1 as the lowest, and 5 as the highest.

#### Assumptions and Limitations

- During the FMECA analysis, it is assumed that only one component fails at a time.
- The identified failure causes should be regarded as examples, not the result of a full assessment.
- Regarding detection of failure, failures are assumed to be either *hidden* or *evident*. Evident failures are detected the moment they occur. Hidden failures are detected during testing or during actual demand. Function testing or on-demand situations are assumed to be the only methods for detecting errors.
- Only the main failure modes of the components have been analyzed.

### 3.3 Reliability Performance Requirements

The PSA requires that the IEC 61508 (2010) standard and the OLF070 (2004) guideline is used when stipulating the performance of safety functions when electrical, electronic and programmable electronic systems are inherent in the structure of the function. The IEC 61508 (2010) standard and the OLF070 (2004) guideline determine reliability requirements in two different ways. In the following the two approaches are presented and discussed, and the proposed reliability requirements for ballast systems on FPSOs will be presented.

#### The IEC 61508 Approach for Setting Reliability Requirements

The IEC 61508 (2010) is based on a *Safety Life Cycle* concept, which represent the necessary steps towards achieving functional safety for an EUC in a systematic way. Central to the safety life cycle concept is the structured and thorough approach to hazard and risk analysis, and the objective of the process is to identify the risk associated with the EUC and the EUC control system. If the risk is found to be above the upper level of tolerability, the standard requires that one or more *safety functions* should be put in place to reduce the risk to a tolerable level. The concept is illustrated in Figure 3.10, adopted from OLF070 (2004) based on the original figure from IEC 61508 (2010) standard.

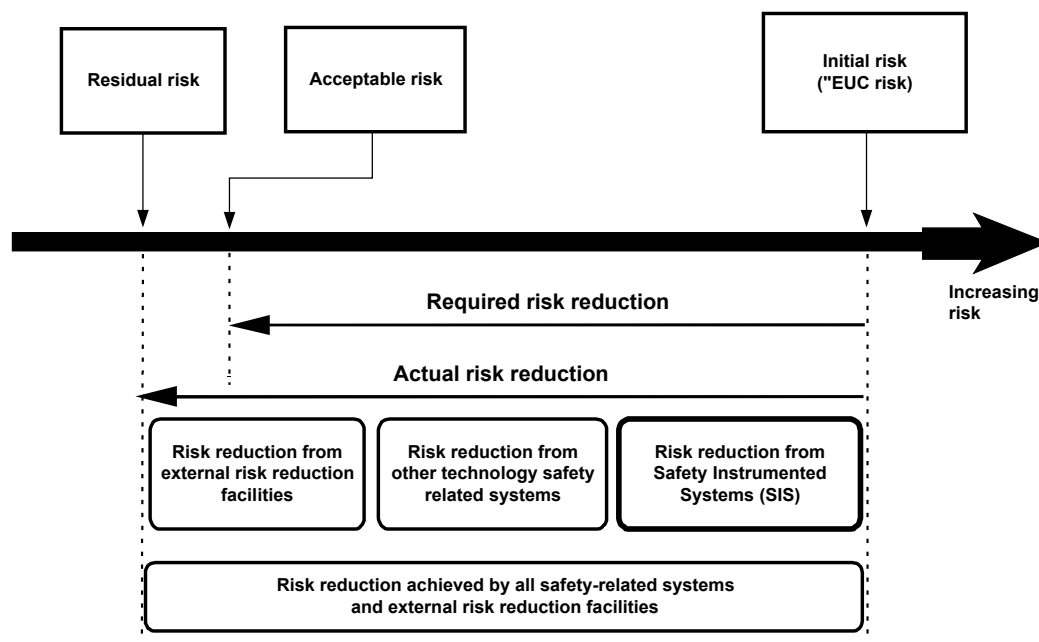


Figure 3.10: Framework for risk reduction in IEC 61508

The level of tolerable risk for an EUC will vary, and is often derived from

- Regulations and guidelines from regulatory authorities
- Industry standards
- Expert, industry or scientific advice

The safety function will then be assigned a safety integrity requirement, which will be a measure of the risk reduction associated with the safety function. The [IEC 61508 \(2010\)](#) approach ensures that all requirements are *risk based*, and that all decisions shall be taken based on tolerability of risk and in the effort of risk reduction.

The standard requires that the risk reduction achieved by the function should be quantified and expressed as a *safety integrity level (SIL)*, which will be the primary reliability requirement for the safety function. Safety integrity level (SIL) is defined by [Rausand \(2011\)](#) as

*Safety integrity level (SIL): the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period of time.*

The [IEC 61508 \(2010\)](#) standard defines four discrete safety integrity levels, where each level corresponds to an interval in the average probability of failure on demand,  $PFD_{avg}$ , and the probability of a dangerous failure per hour,  $PFH$ , as shown in Figure 3.11, adopted from the [OLF070 \(2004\)](#) guideline.



SIL 4 is the highest safety integrity level, and SIL 1 the lowest. The  $PF_{D_{avg}}$  applies to SISs operating in on demand/low demand mode of operation, and the  $PFH$  applies to SISs in high demand mode of operation. For the rest of the thesis,  $PF_{D}$  is the equivalent to  $PF_{D_{avg}}$ .

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

Figure 3.11: Safety integrity levels in IEC 61508

By using the “top-down” [IEC 61508 \(2010\)](#) approach, the obtained SIL requirement for each SIF will be directly related to the total risk reduction needs of the EUC. For each SIS introduced to protect the EUC, the initial EUC risk will be reduced towards the acceptable risk level. The process of assigning SIL requirements to various SIFs based on the identified risk reduction goal is called *SIL allocation*. A number of qualitative and quantitative methods for SIL allocation exist and several are presented in [IEC 61508 \(2010\)](#), such as

- Layers of protection analysis (LOPA)
- Risk graph method
- Event tree method

### The OLF 070 Approach for Setting Reliability Requirements

The [OLF070 \(2004\)](#) guideline presents a different approach to setting reliability requirements for safety systems than the risk based approach of the [IEC 61508 \(2010\)](#). The guideline make use of the same reliability performance metric, the SIL concept, but rather than allocating the requirements to the SIFs "top-down", a set of *minimum SIL requirements* have been established for the most common safety functions, as defined by the PSA.

As presented in the guideline, the rationale behind predefining the SIL requirements is

- To ensure a minimum safety level
- To enhance standardisation across the industry
- To avoid time-consuming calculations and documentation for more or less standard safety functions.

The minimum SIL requirements have been developed by combining simplified loop diagrams of the safety functions with reliability data based on industry experience. As such, if the reliability experienced in the industry is low, the minimum SIL requirement can turn out low. To cope with this issue, the guideline has stipulated the stricter performance requirement in cases where the calculated requirement turn out between two reliability levels, and emphasises that the requirements are *minimum* requirements.

In the guideline, the ballast system is defined as a safety system with two safety functions, with individual SIL requirements. The minimum requirements are established based on two simplified loop diagrams, and a number of assumptions.

- OLF070 Subfunction 1: Start of ballast system for initiation of rig re-establishment
  - SIL1 minimum requirement
- OLF070 Subfunction 2: Emergency stop of ballast system
  - SIL2 minimum requirement

### **Proposed Reliability Performance Requirements**

The proposed reliability requirements to FPSO ballast systems are based on the OLF 070 approach for setting reliability requirements. Although the risk based approach of the [IEC 61508 \(2010\)](#) standard may lead to an adequately strict requirement, the process of assigning reliability performance targets for ballast systems based on the overall EUC risk is not preferred, for several reasons:

- The level of detail of QRAs as they are performed today, make them less appropriate for stating absolute criteria. ([OLF070, 2004](#))
- The requirements should be absolute, and applicable to all FPSOs, regardless of the risk profile of the vessel.
- By assigning requirements directly to the systems, a minimum safety level is achieved, regardless of any modification to the vessel.

The minimum SIL requirement approach is therefore adopted as the most effective way to ensure adequate reliability performance of ballast system functions.

With regards to the specific SIL requirements proposed by the [OLF070 \(2004\)](#) guideline, these are not adopted without a proper discussion.

As presented above, the SIL requirements are the result of calculations based on a combination of simplified loop diagrams and reliability data from the industry. In addition to the data, a range of assumptions are made with regards to the test interval of the various components.

A review of the data used in the calculation in OLF070 (2004) showed that some of the data had changed since the calculations were performed. More specifically, the failure rate data used to represent the failure rate of the valves had actually reduced significantly. To verify if the SIL requirements would have been stricter if the calculations were performed today, a series of case calculations are performed on the *OLF070 Subfunction 1: Start of ballast system for initiation of rig re-establishment*. The result of the calculations are presented in appendix Figure B.6. The findings of the calculations are presented:

- Case1: The calculations are identical to the calculations in OLF070 (2004). The result is a SIL1 minimum requirement.
- Case2: The calculations are performed based on the same assumptions as in Case1, but with the new valve failure rates. The PFD of the function result in a SIL1 minimum requirement.
- Case3: The calculations are performed based on the same assumptions as in Case1, but with the new valve failure rates and a 2190h test interval instead of a 4380h from Case 1. The PFD of the function result in a SIL1 minimum requirement.
- Case4: The calculations are performed based on the same assumptions as in Case1, but with the new failure rates and a 730h test interval instead of a 4380h from Case 1. The PFD of the function result in a SIL2 minimum requirement.

The main result of the calculations show that if the calculations were performed today with the same assumptions, same test interval, but new failure rates (Case2), the resulting minimum SIL requirement would turn out the same. If the calculations were performed today with the same assumptions, new failure rates and a test interval for valves less than every sixth week (1011h) as in Case4, the PFD of the function would correspond to a SIL 2 minimum requirement.

Since the ballast valves on a FPSO are used every day, one could argue that they are actually "tested" all the time, but an important assumption when performing function tests are that the valves are assumed to be *as good as new* when they have been function tested. To carry out such a test, a more thorough test approach is conducted. Due to resource constraints, these function tests are performed less frequently.

To conclude on the specific requirement of the OLF070 (2004), the requirements for *OLF070 Subfunction 1: Start of ballast system for initiation of rig re-establishment* could have been increased to a SIL2 minimum requirement to ensure continuous improvement of reliability performance of ballast system functions. On the other hand, as the guideline stress the fact that these requirements are *minimum requirements*, the SIL1 performance requirement is found adequate.

For ship-shaped floating facilities, including FPSOs, the following reliability performance requirements are proposed, based on the SIFs and the success criteria identified in Section 3.1.5:

Safety Instrumented Function	Proposed minimum SIL requirement
SIF1	SIL1
SIF2	SIL1
SIF3	SIL1
SIF4	SIL2

Table 3.2: Proposed minimum SIL requirements to ballast system functions

The requirements for SIF1 and SIF2 are based on the calculations conducted in Case3, where the minimum SIL requirement calculations from OLF070 (2004) are performed with new failure rates and a 2190h test interval. The requirement for SIF3 is based on the calculations from Case5 in appendix Figure B.6. In Case5, minimum SIL requirement calculations are performed according to the OLF070 (2004) approach, but based on 1oo3-voting for pumps, 2190h test interval, and a *tank valve+solenoid/pilot* instead of a *discharge valve+ solenoid/pilot* to account for the configuration necessary to carry out SIF3. The result is a PFD within the SIL1 interval. The requirement for SIF3 is adopted from the OLF070 Subfunction 2: *Emergency stop of ballast system*.

With regards to the OLF070 (2004) guideline, there should be different requirements to different floating facilities. By assigning only one requirement, covering all facilities with a ballast system, important differences between the systems are overlooked. An important function of a ballast system on a shipshaped vessel is the possibility to ballast internally between the port- and starbord side, presented through SIF3. This is an important function of a shipshaped vessel's ballast system, and should be given a unique reliability requirement as in the proposed requirements. As a minimum, different requirements should be made to ship-shaped vessels and semi-submersible rigs, to account for the differences in design.

### **Reliability Performance Achieved**

According to IEC 61508 (2010), three main types of requirements have to be fulfilled in order to claim that a specific SIF have the potential to actually *achieve* a given SIL upon system startup: (OLF070, 2004)

- A quantitative analysis must verify that the required failure probability can be achieved for the SIF.
- A qualitative requirement must be met, expressed in terms of architectural constraints on the subsystem constituting the safety function.
- Requirements concerning which techniques and measures should be used to avoid and

control systematic faults.

The requirements to the SIL *achieved* will not be looked further into. More information on the subject can be found in the [IEC 61508 \(2010\)](#) standard and the [OLF070 \(2004\)](#) guideline.

# Chapter 4

## Incidents and Accidents

The following chapter presents the findings of the literature survey into the reported safety and reliability challenges, incidents and accidents related to ballast systems. Incidents to both ships and other floating facilities are presented. The major incidents and accidents are presented below, and the minor incidents are summarized and presented in Appendix B.

Rather than reproducing a full description of the incidents and accidents, the incident descriptions are primarily concerned with the specific findings related to the ballast systems.

The findings show that failures related to ballast system can have a severe impact on the chain of events in an accident. The Ocean Ranger accident is one of the worst accidents ever in the off-shore industry, and the investigations revealed the vulnerability of ballast control system failure. Using reliability assessment terminology, the control system, indicators and operator panels on the Ocean ranger were subject to a severe CCF, where the root cause was electric failure due to water ingress, and the coupling factor between the different components was the same location.

The Petrobras P-34 FPSO incident is highly relevant for the topic of the thesis. The incident represent a typical systematic software failure where the control logic of the ballast system lacked the proper fail safe functionality upon valve position feedback failure. The incident stress the importance of proper manual intervention and emergency plans in case of loss of control of the ballast system, and the need for proper reliability assessments of ballast systems.

The Gjøa and Thunder Horse accidents represent systematic failures inherent in the design of the ballast systems. Although the Gjøa platform was under modification work, the systematic programming errors in the valve control systems had been made prior to installation. The same applies to the hydraulic power unit installed on the Thunder Horse production facility.

The minor incidents present a series of spurious trip incidents, valve leakage failures and other

incidents causing a range of problems in the daily operation.

## 4.1 Minor Incidents and Accidents

Minor incidents and accident where ballast systems have caused or contributed to unwanted events are documented in a set of tables in Appendix B. The tables and their associated data sources are presented in Table 4.1

Table 4.1: Overview of tables and datasources

Table	Description	Source
<a href="#">B.1</a>	Stability incidents reported to the PSA (Source 1)	<a href="#">Vinnem et al. (2006)</a>
<a href="#">B.2</a>	Stability incidents reported to the PSA (Source 1)	<a href="#">Vinnem et al. (2006)</a>
<a href="#">B.3</a>	Stability incidents reported to HSE (UK) 1980-2003 (Source 2)	<a href="#">Vinnem et al. (2006)</a>

## 4.2 Major Incidents and Accidents

<h1>Petrobras P-34</h1>
<p><b>Date and time:</b> 13.10.2002</p>
<p><b>Accident type and severity:</b> Critical list of the FPSO due to ballast system failure. Potential major accident. Evacuation.</p>
<p><b>Accident location:</b> Barracuda field, Campos Basin Brazil</p>
<p><b>Description of system involved:</b> FPSO converted from a tanker. L.W.H: 240x26x17m. Displacement 62000tons. Storage capacity: 58000m<sup>3</sup>. Production capacity: 45000 bopd. Owned and operated by Petrobras.</p>
<p><b>Context of accident:</b> Weather was not a contributing factor to the event.</p>
<p><b>Accident description in relation to the ballast system:</b> The incident occurred during maintenance of a battery charger. The electric circuits fed by the particular battery charger became de-energized, among them the intrinsic safety panel connecting the ballast and cargo control system with the electric position feedback from the ballast and cargo valves. The main electric power generation shut down, and the hydraulic power system, ECOS and PLC relay cards in the valve control system were de-energized. Emergency backup generator started within 40 sec, PLC relay cards energized, ECOS starts booting operating systems but remain down in 11min. The PLC receives no position feedback from any valve (0mA). The PLC logic was not failsafe and started immediate actions to open all valves in order to reach the (4mA) electric feedback signal corresponding to a closed valve (20mA=Open). All 66 ballast and cargo tanks were opened by hydraulic pressure available in the hydraulic accumulators. Crude oil in the cargo tanks and ballast water in the ballast tanks gravity drained to the portside tanks. The FPSO reached a critical 34 degree list before control was regained and salvaging operations could begin. Crew were abandoned in lifeboats throughout the incident. No injuries to personnel.</p>
<p><b>Source of information:</b> <a href="#">Tinmannsvik et al. (2011)</a> <a href="#">Petrobras (2002)</a>. Figure 4.1 adopted from <a href="#">Petrobras (2002)</a></p>



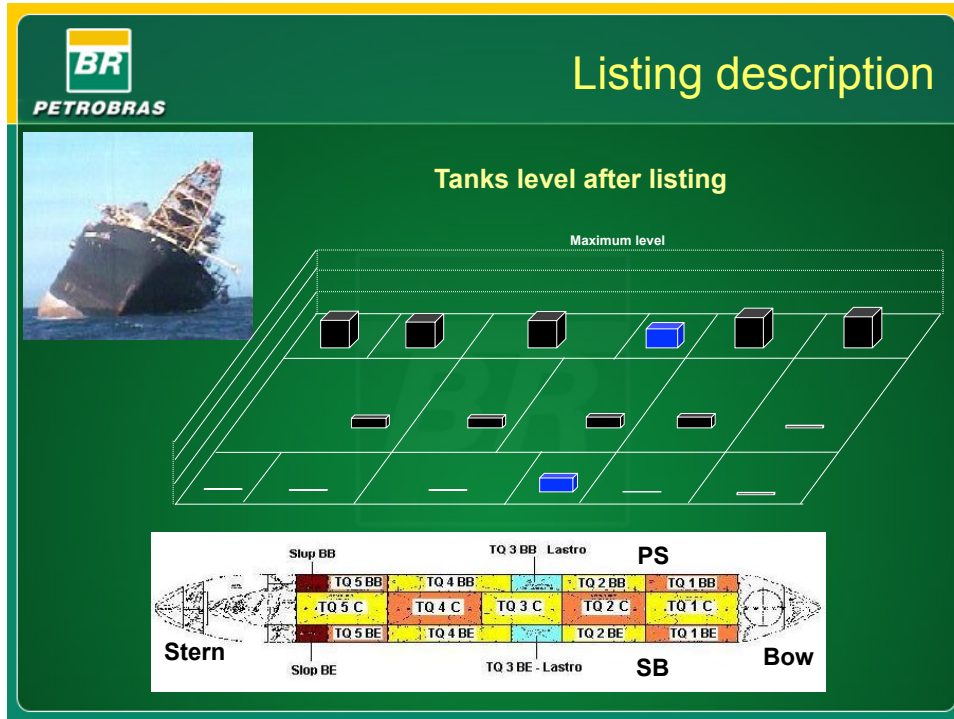


Figure 4.1: Petrobras P-34

## Ocean Ranger

**Date and time:** 15.02.1982

**Accident type and severity:** Major accident. Rig capesizing. Loss of all 84 crewmembers. Loss of semisubmersible drilling rig.

**Accident location:** Canadian waters outside Newfoundland

**Description of system involved:**

Semisubmersible drilling rig owned by ODECO, drilling for Mobil Exploration. L.W.H: 121x80x103m. Weight: 25000tons. Designed for harsh weather operations.

**Context of accident:** An incoming storm had a direct effect on the accident. The rig was preparing to abandon drilling operations and prepare for the storm when the accident occurred. The rig had not yet been brought to safe draft.

**Accident description in relation to the ballast system:**

A large wave hit the Ocean Ranger as the rig was preparing for the storm. The wave broke 2 of the 4 portlights in the ballast control room located in a vulnerable position in a column below the main deck. Water ingress through the portlights caused the ballast control station to malfunction, and ballast valves to open and close in an uncontrolled way.

*"As a direct or indirect result of the malfunction, several valves in the ballast control system opened or were opened allowing seawater to enter the forward ballast tanks and/or on-board ballast water to gravitate forward, either of which would have caused a substantial forward list." (U.S. Coast Guard, 1983)*

The combination of the electric malfunction, ineffective initial response from the ballast operators and lack of training in emergency operation of the ballast control system caused the Ocean Ranger to assume a forward list allowing the unprotected forward chain lockers to be filled with seawater, causing increased list. The ballast system pump and piping design and arrangement was inadequate for deballasting at excessive heel or trim angles under emergency operating conditions. Efforts to abandon the rig was unsuccessful, and the rig eventually capesized and sank. All 84 crewmembers died in the accident.

## Ocean Ranger

### **Accident description in relation to the ballast system: (Continued)**

All the ballast valves on the Ocean Ranger, except two manually operated sea inlet gate valves were pneumatically operated butterfly valves located in the ballast pump rooms and propulsion rooms of each pontoon. The valves were designed to fail to a closed position in case of an electrical or air pressure failure. Investigations showed that the crew had attempted to manually operate the system by using brass control rods designed to manually operate the systems air control solenoids, which in turn controlled the opening and closing of the ballast valves. Since all valve indication lights were out, this was most likely done completely in the blind. It normally took approximately 40 seconds to open a valve and 20 seconds to close a valve.

Another feature was the main electric power cut off installed inside the ballast control console. The cut off circuit breaker was not marked, and testimonies from former crewmembers indicated that operators were unaware of the location of this circuit breaker. The investigations of the accident confirmed that a series of mitigating actions could have been initiated by the operators if they had been sufficiently trained to operate the ballast system in an emergency situation.

### **Source of information:**

[Tinmannsvik et al. \(2011\)](#)

[U.S. Coast Guard \(1983\)](#)

<h2>Gjøa</h2>
<b>Date and time:</b> 03.03.2010
<b>Accident type and severity:</b> Minor stability incident, spurious trip of ballast system
<b>Accident location:</b> Dockside at Aker Stord Norway
<b>Description of system involved:</b> Semisubmersible drilling rig
<b>Context of accident:</b> No weather effects.
<b>Accident description in relation to the ballast system:</b> The rig was under construction and outfitting when a power failure caused a number of control units to stop and restart. Due to a programming error in the ballast control logic, all the ballast valves in a specific quadrant were spuriously opened, causing 700-900tons of ballast water to migrate internally, causing a 3 degree list of the rig. The power failure also caused a series of local failures where systems had to be manually restarted. The emergency shut-down button for the ballast system had not yet been installed. Controlled evacuation of the rig. Control of the situation after restarting systems.
<b>Source of information:</b> <a href="#">Tinmannsvik et al. (2011)</a> <a href="#">Vinnem et al. (2006)</a>

<h2>Aban Pearl</h2>
<b>Date and time:</b> 13.05.2010
<b>Accident type and severity:</b> Semisubmersible sinking
<b>Accident location:</b> Off the coast of Venezuela
<b>Description of system involved:</b> Semisubmersible gas production platform from 1977. Newly refurbished.
<b>Context of accident:</b> No weather effects.
<b>Accident description in relation to the ballast system:</b> The floating devices on the rig started to take in water during transit. The rig eventually sank. Probable cause is leakage, maloperation or other error with the ballast system ( <a href="#">Tinmannsvik et al., 2011</a> ).
<b>Source of information:</b> <a href="#">Tinmannsvik et al. (2011)</a> <a href="#">Vinnem et al. (2006)</a>

<h1>Thunder Horse</h1>
<b>Date and time:</b> 08.07.2005
<b>Accident type and severity:</b> Severe and uncontrolled heel of floating production platform.
<b>Accident location:</b> US Gulf of Mexico
<b>Description of system involved:</b> Semisubmersible production platform.
<b>Context of accident:</b> The platform was under commissioning, and the incident happened during evacuation before Hurricane Dennis.
<b>Accident description in relation to the ballast system:</b> The rig had been evacuated due to the passage of Hurricane Dennis. When the crew returned to the rig they found it listing 20 degrees with the top deck in the water on the port side. Findings indicate that failures associated with the hydraulic control system and the isolation of the system during evacuation led to the partial opening of multiple hydraulically operated valves in the ballast and bilge systems of the vessel, allowing water migration to take place. The ballast water migration led to the initial listing of around 16 degrees. The subsequent water migration into manned spaces in the lower hull via faulty check valves in the integrated ballast and bilge system increased the degree of listing. Downflooding of seawater, and possible wave action associated with the hurricane increasing the list up to 21 degrees. The platform was restored.
<b>Source of information:</b> <a href="#">Tinmannsvik et al. (2011)</a>
<h1>Jupiter</h1>
<b>Date and time:</b> 12.04.2011
<b>Accident type and severity:</b> Semisubmersible flotell partial sinking.
<b>Accident location:</b> Gulf of Mexico
<b>Description of system involved:</b> Semisubmersible flotell
<b>Context of accident:</b> Weather was not a contributing factor.
<b>Accident description in relation to the ballast system:</b> The semisubmersible flotell started to take in large amounts of seawater through a faulty valve in one of the pontoons. The 713 workers onboard were evacuated. The affected side eventually sank to the bottom of the shallow water.
<b>Source of information:</b> <a href="#">Tinmannsvik et al. (2011)</a>

# Chapter 5

## Reliability Assessment Approach for FPSO Ballast Systems

In the following chapter, a stepwise reliability assessment approach for ballast systems is presented. The reliability assessment approach can be used to quantify the reliability performance of the safety functions of a ballast system, and identify the contribution from CCFs on the reliability performance of these functions. The results of the assessment can be used as part of a verification process of reliability performance, as decision support during the design phase of new ballast systems or to quantify reliability enhancing efforts performed on an existing design.

In addition, a defence approach against CCFs in ballast systems is presented. The approach can be used to improve the operators ability to identify and avoid the reoccurrence of CCF in the operational phase.

### 5.1 Background for the Approach

#### 5.1.1 Selection of Reliability Modeling Approach

In order to verify compliance to reliability targets of SIFs, the [IEC 61508 \(2010\)](#) and [IEC 61511 \(2004\)](#) standards suggest the use of FTA, Reliability Block Diagrams (RBD) or Markov methods to calculate reliability performance ([Lundteigen and Rausand, 2009](#)). FTA and RBD are methods that model the system failures and functions in a static way, with binary states. The system components and functions are assumed to be either available or not. With Markov methods, the components may have more than one state, and Markov methods is preferred when modeling

dynamic systems that are switching between different states. As the ballast system components may be adequately modeled as either available or not, Markov methods are not included as part of the modeling approach.

Both FTA and RBD are applicable methods for reliability modeling of the ballast system, and if the models are established on the same basis, the two approaches will give the same result. The FTA method is considered to be more comprehensive than the RBD method, due to the failure oriented approach, and is often preferred for modeling complex SIFs with a large number of components.

The RBD method provides a different approach to modeling. Rather than focusing on how a function may fail, the approach focuses on how a function may be achieved, and the sequence of reliability blocks in the RBD may be set up similar to the sequence the SIF is activated. This is a benefit, as components can then be easily added and removed to the RBD when modeling different ballast system designs. Generic RBDs for the different SIFs can easily be changed to represent the ship specific configuration of a safety function. Identified CCF among redundant components can easily be included in the RBD. Due to the flexibility of the RBD method, it is found to be the most appropriate modeling approach for the ballast system reliability assessment.

### 5.1.2 PFD Calculation

The quantitative reliability performance measure for a SIS operating in low demand mode of operation is the average probability of failure on demand,  $PFD_{avg}$  (PFD), which is only related to DU-failures. The PFD can be calculated for individual items and complete systems as long as the following basic assumptions hold:

- The item is subject to a regular functional test at test interval  $\tau$
- All hidden failures are revealed by the functional test and repaired immediately.
- The time required to test and repair the item is considered to be negligible
- After a test/repair the item is "as good as new"
- The item is not subject to diagnostic self-testing
- The item is functioning as a safety barrier only if a DU failure mode is not present

For practical calculations of PFD, approximation formulae are used. For detailed derivations leading to these formulae, see [Rausand and Høyland \(2004\)](#). The following approximation formulae can be used in the assessment:

**PFD Single Item:**

For a single item, tested at regular intervals of length  $\tau$ , with constant failure rate  $\lambda_{DU}$  with respect to  $DU$ -failures, and where  $\lambda_{DU}\tau$  is small, (*i.e.*  $< 10^{-2}$ ) (Lundteigen and Rausand, 2009), the following formula can be used:

$$PFD \approx \frac{\lambda_{DU}\tau}{2} \quad (5.1)$$

The approximation is conservative, which means that the approximated value is greater than the correct value obtained by detailed calculations.

**PFD Parallel Items:**

For two independent items of the same type operated as a *1oo2*-system, tested simultaneously at regular intervals of length  $\tau$ , with constant failure rates  $\lambda_{DU}$  with respect to  $DU$ -failures, and where  $\lambda_{DU}\tau$  is small (*i.e.*  $< 10^{-2}$ ), the following formula can be used:

$$PFD \approx \frac{1}{3}(\lambda_{DU}\tau)^2 \quad (5.2)$$

A *1oo2*-system will only fail when both components fail. The probability  $Q(t)$  that the system is in failed state at time  $t$  is

$$Q(t) = q_1(t) \cdot q_2(t) \quad (5.3)$$

Where  $q_i(t)$  is the probability that component  $i$  is in failed state at time  $t$ , for  $i=1,2$ . This relationship is sometimes wrongfully interpreted in PFD software calculations, where  $PFD_{1oo2}$  is calculated by

$$PFD_{1oo2} = \Pi_1^n PFD_n \quad (5.4)$$

The approximation does not give accurate results, and should not be used directly. The reason it does not hold is because PFD is the average unavailability of the system, and the average of a product is not the same as the product of averages. This is known as the *Schwartz inequality*.

Interestingly, 5.4 can be used successfully to calculate PFD of more complex *1oo $n$* -configurations comprising different types of components if coupled with the correction factor presented in Lundteigen and Rausand (2009):

$$CF_{1oo2} = \frac{2^n}{n+1} \quad (5.5)$$

For complex *1oo $n$* -configurations that comprise different types of components, the approach is as follows: (1) Calculate PFD of each redundant channel. (2) Calculate the non-conservative PFD by using 5.4. (3) Reduce the non-conservative error by multiplying with the appropriate correction factor from 5.5.



**PFD Series System:**

For two independent items with individual constant failure rates  $\lambda_{DU_1}$  and  $\lambda_{DU_2}$  with respect to  $DU$ -failures, tested simultaneously at regular intervals of length  $\tau$ , where both items have to function for the system to function, and where  $\lambda_{DU_i}\tau$  is small (*i.e.*  $< 10^{-2}$ ) for  $i=1,2$ , the following formula can be used:

$$PFD \approx \frac{(\lambda_{DU_1} + \lambda_{DU_2})\tau}{2} = \frac{\lambda_{DU_1}\tau}{2} + \frac{\lambda_{DU_2}\tau}{2} \quad (5.6)$$

The approximation shows that for series systems, the PFD of a series system is approximately the sum of the PFDs of the individual items (Rausand and Høyland, 2004).

**PFD *koon*-Systems:**

For a system of independent components of the same type operated as a *koon*-system, tested simultaneously at regular intervals of length  $\tau$ , with constant failure rates  $\lambda_{DU}$  with respect to  $DU$ -failures, and where  $\lambda_{DU}\tau$  is small (*i.e.*  $< 10^{-2}$ ), the following formula can be used:

$$PFD_{koon} \approx \binom{n}{n-k+1} \frac{(\lambda_{DU}\tau)^{n-k+1}}{n-k+2} \quad (5.7)$$

**PFD of Components in Continuous Operation:**

In order to calculate PFD of component in continuous operation, a simplification can be made. These items are in continuous operation with occasional unexpected downtime. They are not function tested or needed "on demand". The suggested approach for modeling these components is presented through the main electric power system.

Consider the main electric power system as an item, which is either functioning or not. By functioning, the item is in active operation, delivering electric power. By not functioning, the item is unavailable due to any failure cause, as opposed to a planned shutdown. When the main electric power is repaired, it is assumed to be "as good as new", with sufficient power.

The *average unavailability* of the item,  $\bar{A}_{av}$ , denotes the mean proportion of time the item is not functioning (Rausand and Høyland, 2004)

$$\bar{A}_{av} = \frac{MTTR}{MTTF + MTTR} \quad (5.8)$$

Where MTTR (*mean time to repair*) denotes the mean downtime after a failure, and MTTF (*mean time to failure*) denotes the mean functioning time of the item. MTTF may be written as

$$MTTF = \frac{1}{\lambda} \quad (5.9)$$

Where  $\lambda$  denotes the failure rate of the item. Equation 5.8 becomes

$$\bar{A}_{av} = \frac{MTTR}{\frac{1}{\lambda} + MTTR} = \frac{\lambda \cdot MTTR}{1 + \lambda \cdot MTTR} \quad (5.10)$$

The second term in the denominator is negligible for practical calculations and the final term becomes

$$PFD \approx \bar{A}_{av} \approx \frac{\lambda \cdot MTTR}{1} \approx \lambda \cdot MTTR \quad (5.11)$$

Where  $\lambda$  denotes how often the main electric power is not functioning due to an unexpected failure, and the MTTR is the time required to get the main electric power functioning again.

#### **PFD of Human Interventions:**

If any human interventions are necessary to successfully execute a ballasting function, the possible non-fulfilment of that task should be included in the PFD calculations. The planning and initiation of the ballast functions should not be included in the calculations, only possible extraordinary human interventions identified through the shipspecific ballast system familiarization.

As with structured *Human Reliability Analysis* (HRA) methods, some of the benefits of including human errors during reliability modeling are that the process (Rausand, 2011): (1) Identifies weaknesses in operator interfaces with the system (2) Demonstrates quantitative improvements in human interfaces (3) Supports the development of preventive or mitigating measures to reduced the influence of human errors on the system reliability.

If sufficient data is available, the probability of a human error can be represented by the *Human Error Probability* defined as

*Human error probability (HEP): The probability that an error will occur when a given task is performed.*

Estimated by

$$HEP = \frac{\text{number of errors}}{\text{number of opportunities for error}}$$

Alternatively, the HEP may be based on expert judgement or by using tabulated values for human performance. The *LOPA* technique, presented in the IEC 61511 (2004) standard provide the

suggested PFD values for operator intervention in Table 5.1, adopted from IEC 61511 (2004).

Protection layer	PFD
Human performance (trained, no stress)	$1,0 \times 10^{-2}$ to $1,0 \times 10^{-4}$
Human performance (under stress)	0,5 to 1,0
Operator response to alarms	$1,0 \times 10^{-1}$

Table 5.1: PFD of Human performance

### 5.1.3 Common Cause Failure Modeling

The IEC 61508 (2010) and IEC 61511 (2004) standards require that the effect of CCFs are included in reliability performance calculations, and recommend the use of the  $\beta$ -factor model.

The  $\beta$ -factor model is the most commonly used model for CCF modeling, but it is not the only option for modeling CCFs.

The model assigns a fraction,  $\beta$  of the failures of a component to be CCF, and assumes that when a CCF occurs, all components in that component group will fail due to the same cause. In a redundant setup, with  $n$  identical components in parallel, each with a constant failure rate  $\lambda$ , this means that given a component failure, this failure will cause all the  $n$  other components to fail with probability  $\beta$ , and involve only the single component with probability  $(1 - \beta)$  (Rausand, 2011).

The implications of the simplicity of the  $\beta$ -factor model, is that the contribution from CCFs will dominate the results of PFD calculations, regardless of voting configuration (Rausand, 2011). This can be illustrated by an example:

Consider a system of 5 ballast tank valves configured as 1oo5-system, which is functioning as long as at least one of the five channels is functioning. The critical failure rate of the valves is estimated to  $\lambda_{DU}$ , and the valves have been found to be exposed to CCFs. The system is tested at regular intervals of length  $\tau$ , and one can assume that the testing is perfect and that the valves are as good as new after each test.

The PFD is calculated by using 5.7 for a koo $n$ -system of identical and independent components, with CCFs modeled by the  $\beta$ -factor model

$$PFD_{1oo5} \approx \frac{((1 - \beta)\lambda_{DU}\tau)^5}{6} + \frac{\beta\lambda_{DU}\tau}{2} \quad (5.12)$$

The first term in the answer is the contribution from independent failures, while the last term is from CCFs. The contribution from CCFs will by far outweigh the contribution from the indepen-

dent failures, and this dominance will not be affected significantly by any change in voting. As one may expect to have CCFs where not all the redundant components fail with probability  $\beta$ , the  $\beta$ -factor model will be rather pessimistic for redundant systems with many channels.

This has been taken into consideration in the OLF070 guideline, which recommend the CCF model developed as part of the PDS method (Hauge et al., 2009b) when quantifying PFD. The model argues that there should be different  $\beta$  factors for different voting configurations, and presents a configuration factor,  $C_{MooN}$ , which takes into account the specific voting configuration. The result is a CCF modeling approach which is more sensitive to the specific voting configuration in the reliability model. The modified  $\beta$ -factor of a system with  $MooN$  voting configuration equals:

$$\beta_{MooN} = C_{MooN} \cdot \beta \quad (5.13)$$

The numerical values for the  $C_{MooN}$  factor can be extracted from figure 5.1, adopted from Hauge and Onshus (2009). Note that for 1oo2 systems the  $C_{1oo2}=1$ , resulting in  $\beta_{1oo2}=\beta$ .

<b>M \ N</b>	<b>N = 2</b>	<b>N = 3</b>	<b>N = 4</b>	<b>N = 5</b>	<b>N = 6</b>
<b>M = 1</b>	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.30$	$C_{1oo4} = 0.15$	$C_{1oo5} = 0.08$	$C_{1oo6} = 0.04$
<b>M = 2</b>	-	$C_{2oo3} = 2.4$	$C_{2oo4} = 0.75$	$C_{2oo5} = 0.45$	$C_{2oo6} = 0.26$
<b>M = 3</b>	-	-	$C_{3oo4} = 4.0$	$C_{3oo5} = 1.2$	$C_{3oo6} = 0.8$
<b>M = 4</b>	-	-	-	$C_{4oo5} = 6.0$	$C_{4oo6} = 1.6$
<b>M = 5</b>	-	-	-	-	$C_{5oo6} = 8.1$

Figure 5.1:  $C_{moon}$  factors

The difference between the methods can be illustrated by applying the  $C_{MooN}$ -factor approach to the example presented above. For the 1oo5 system, the  $C_{1oo5} = 0,08$ , and the corrected  $\beta_{1oo5} = 0,08 \cdot \beta$

$$PFD_{1oo5} \approx \frac{((1 - \beta_{1oo5})\lambda_{DU}\tau)^5}{6} + \frac{\beta_{1oo5}\lambda_{DU}\tau}{2} \quad (5.14)$$

The result can be seen in the second term, corresponding to the contribution from CCF failures on the system PFD. The high redundancy in the 1oo5 voting has marginalized the  $\beta_{MooN}$ , which in turn results in a reduced contribution from CCF failures on the system PFD.

Due to this powerful characteristic, the CCF modeling from the PDS method has been chosen as the preferred CCF modeling approach for the reliability assessment.

## Determining $\beta$

There are three main sources of  $\beta$  factors to common cause component groups

- Checklists
- Reliability databases
- Expert judgement

The IEC 61508 (2010) standard encourage the use of enclosed checklists to establish  $\beta$  factors based on the specific condition of the installation. The OLF070 (2004) guideline recommends the use of a generic  $\beta$  factor based on operational experience documented in reliability databases, and refer to  $\beta$  factors from the PDS method (Hauge et al., 2009b).

For initial calculations, applicable tabulated  $\beta$  factors from the PDS method (Hauge et al., 2009b) can be used. In Figure 5.3, the  $\beta$  factors are presented in connection with the proposed reliability data.

If efforts are made to reduce the influence of CCFs on a later stage, the result of the efforts can be quantified into the  $\beta$  factor, by using the *Active protection application specific  $\beta$*  approach developed for the PDS method (Hauge et al., 2009b). The idea behind the approach is to multiply the generic  $\beta$  with a parameter  $k_\beta$ , which can be chosen based on an assessment of the systems protection against CCFs. The numerical values for  $k_\beta$  can be extracted from Figure 5.2, adopted from the PDS handbook (Hauge et al., 2009b).

$k_\beta$	Protection	Comments
0.1	Very high protection	Separation/segregation and diversity/redundancy fully implemented
0.5	Extended protection	Some additional protection implemented and documented
1	Normal protection	Average level of protection – current practice
5	Reduced protection	Less protection than typically implemented

Figure 5.2:  $k_\beta$  parameters

### 5.1.4 Reliability Data

For a reliability assessment focusing on the PFD of various SIFs, the rate of *dangerous undetected* failures,  $\lambda_{DU}$ , and the *functional test interval*,  $\tau$ , are the most important parameters, governing the prediction of how often a safety function is likely to fail on demand. The following data is needed for each component:

- The rate of Dangerous Undetected failures,  $\lambda_{DU}$

- The functional test interval,  $\tau$
- $\beta$ -factors for common cause component groups

Other data relevant for the assessment:

- The failure rate of components in continuous operation,  $\lambda$ .
- The MTTR (mean time to repair) of components in continuous operation

Reliability data can be obtained from a variety of sources, such as generic databases, company-specific databases or joint databases from several companies within the same industry. While some databases provide failure rates for each relevant failure mode, other databases only provide total failure rates.

It is important that the data is applicable and conservative, and the [IEC 61508 \(2010\)](#) standard requires that any failure rate data used for verification purposes should have a statistical confidence level of at least 70% ([OLF070, 2004](#)). This means that company-specific databases must have a lot of data before they can be used for verification purposes.

Through the PDS project ([Hauge et al., 2009b](#)), a range of reliability data is analyzed and structured into a PDS Data Handbook ([Hauge et al., 2009a](#)), updated at regular intervals. The data is primarily obtained from the OREDA data handbooks, and the data provides best average estimates of equipment failure rates based on experience gathered mainly from the petroleum industry. The [OLF070 \(2004\)](#) guideline use PDS data as the primary source of reliability data.

The OREDA reliability data is based on maintenance reports from single item failures, and as such contain all failures both independent and CCFs. The status related to the contribution from CCFs on the data is not fully known ([Lundteigen and Rausand, 2007](#)). Through the RABL project ([Østby et al., 1987](#)), a list of reliability data for ballast systems is presented. The data consist mainly of old OREDA data, and is presented in appendix Figure [B.2](#).

As an expert judgement opinion on what data that should be applied, the PDS data from the example calculations in the [OLF070 \(2004\)](#) guideline is used and updated with data from the latest PDS Data Handbook, ([Hauge et al., 2009a](#)).

In Figure [5.3](#) a shortlist of the proposed reliability data is presented, along with applicable  $\beta$  factors. For a full review of the reliability data see appendix Figure [B.7](#) and [B.8](#).

Ballast tank configuration, pumps and valves	Type	$\lambda$ DU (per $10^6$ h)	$\beta$ -factor	Comment
Ballast tank valve	Valve + solenoid/pilot	3	3 %	DU failure rate is fail to open
Pump room valve	Valve + solenoid/pilot	3	3 %	DU failure rate is fail to open
Seachest valve	Valve + solenoid/pilot	3	3 %	DU failure rate is fail to open
Discharge valve	Valve + solenoid/pilot	3	3 %	DU failure rate is fail to open
Ballast pump	Centrifugal complete	Not available. Fail to start on demand = 9,4 per $10^4$ h	5 %	Failure rate includes only "fail to start"
Ballast control system	Type	$\lambda$ DU (per $10^6$ h)	$\beta$ -factor	Comment
Ballast control logic + I/O	Programmable safety system - single system	1	5 %	
Electrical components	Type	$\lambda$ DU (per $10^6$ h)	$\beta$ -factor	Comment
Manual pushbutton	Pushbutton	0,4	3 %	
Safety relay	Relay	0,2	3 %	
Isolation relay	Relay	0,2	3 %	
MCC shutdown relay	Relay	0,2	3 %	
Contactar	Relay	0,2	3 %	
Valve	Valve including actuator (ex. Pilot/solenoid)	2,1	3 %	
Solenoid/Pilot	Solenoid	0,9	2%/10%.	

Figure 5.3: Shortlist of applicable reliability data

## 5.2 Stepwise Procedure

The reliability assessment approach is based on the following stepwise procedure:

**Step 1:** Ballast system familiarization

**Step 2:** Identification of common cause component groups

**Step 3:** RBD construction

**Step 4:** Determination of reliability data

**Step 5:** PFD calculations

**Step 6:** Comparison with reliability performance targets

In the following section the different steps will be presented.

### 5.2.1 Step 1: Ballast System Familiarization

The first part of the reliability assessment is a thorough review of the ship specific ballast system. This is an important part of the procedure, as the subsequent steps and final results are highly dependent on the findings of the familiarization. The outcome of the review should include:

- A description of the differences between the ship specific ballast system and the base case ballast system, and associated implications on the system functions
- A list of the different SIFs, associated functional block diagrams and their criteria for successful execution
- Which components that are operated to achieve the SIFs, and how these components may fail

Relevant sources of information are: P&ID diagrams, flow diagrams, loop drawings for hydraulic and electrical systems, cause and effect diagrams, operation manuals etc. Design engineers or personnel familiar with the specific system should be involved in the familiarization process.

### 5.2.2 Step 2: Identification of Common Cause Component Groups

Based on the system familiarization, components that are dependent and may share the same failure cause shall be included in the same common cause component group. This ensures a basis for including CCFs in the subsequent calculations. The process is as follows:

- Identify components that are dependent
- Identify if any of these components may share the same common failure cause.
- Include these components in the same common cause component group

### 5.2.3 Step 3: RBD Construction

The next step is to model the RBDs of the SIFs based on the system familiarization and identified common cause component groups. For an introduction to RBD modeling, see [Rausand and Høyland \(2004\)](#). The process is as follows:

- Model the elementary utilities electric and hydraulic power first, and include these utilities as separate reliability blocks in the RBDs of the SIFs.



- Model the RBDs of the SIFs one by one, taking into account the voting configuration of redundant components.
- If common cause component groups have been identified, and these components are part of a redundant configuration in a SIF, the potential CCF among these components shall be modeled as a separate block in the RBD.

An important part of the utility modeling, is to include the possibility of loss of main power. If the switch to backup systems involve any human interaction, the possible non-fulfilment of this interaction should also be modeled.

A simplification can be made with regards to SIF1, SIF2 and SIF3. These SIFs perform two different operations, ballasting and deballasting, and should be modeled with two RBDs each. A simplification of the RBD modeling can be made by including both operations in the same RBD, since both operations are assumed to be carried out with the same amount of valves of almost the same type.

#### 5.2.4 Step 4: Determination of Reliability Data

The identified components of the ballast system should be coupled with the best available reliability data. Ship-specific data should be used if the data is available, well documented and has a statistical confidence level of at least 70%. This can be a real challenge, and if ship-specific data is not available, the data presented in Section 5.1.4 can be used. If expert judgements and other assumptions are made, these assumptions should be documented.

#### 5.2.5 Step 5: PFD Calculations

Important assumptions must be verified before the PFD of the various SIFs can be calculated. In Section 5.1.2 these assumptions are listed, and should be verified with design engineers or operators. The most important assumptions that should be clarified, are:

- a) If full functional tests are carried out at regular intervals, and to what extent these tests are capable of revealing *all* DU failures.
- b) If the operation of the ballast system is stopped once a DU failure is revealed, and whether or not the failure will be repaired immediately.

In the reliability assessment approach, it is assumed that the assumptions in Section 5.1.2 are valid. When the assumptions have been verified, the PFD of the various SIFs can then be calculated by successively calculating the PFD of the RBDs, using the formulae from section 5.1.2,

and reliability data from Section 5.2.4. The calculations can be done by hand, without the use of specialized software.

### **5.2.6 Step 6: Comparison with Reliability Performance Targets**

The final step is to present the results of the PFD calculations, and compare the results with the associated reliability performance targets. Deviations from the reliability targets should be discussed, and the different contributions from the different component groups or failure types may be extracted, including the contribution from CCFs on the reliability performance.

## 5.3 Defense Approach Against CCF in Ballast Systems

CCFs may be introduced during design of ballast systems as well as in the operational phase. In the following section, issues related to CCFs during ballast system design will be presented briefly, followed by a defense approach against CCFs to be used in the operational phase.

**Design Phase:** In the design phase, designers have the possibility to reduce the level of systematic failures to a minimum, reducing the systems potential for CCF. As presented in Section 3.2.1, systematic failures are dependent failures that can lead to CCFs, and special care should be made when choosing software systems, hardware components and installation procedures for the final design. Examples of potential sources for CCF introduced in the design phase may be:

- Design related: Pumps installed in the same location with the same external environmental exposure. Ballast valves not specified for operation in cold environments. Pump room valves with identical design, installed in the same environment. Ballast control station vulnerable to water ingress.
- Software related: Ballast control logic programming error, resulting in latent errors.
- Installation related: Valves installed in the wrong direction. Pollution in the hydraulic supply lines after pipe cutting and installation.

**Operational Phase:** In the operational phase the main source of CCF are failures introduced during functional testing, inspection and improper use of the system. The systematic failures described as excessive stress- and operational failures in Section 3.2.1, are introduced in this phase, and may lead to CCFs.

### 5.3.1 Defence Approach

As CCFs introduced in the operational phase will have a great impact on the reliability performance of the ballast system, a defense approach is presented, that can improve the operators ability to detect CCFs and avoid introducing new CCFs in the operational phase. These experiences can later be used in the design of new ballast systems. The defence approach is valuable as a tool to monitor the level of CCF on a systems, and can provide input into calculation methods developed to monitor the SIL level of SIFs in the operational phase.

The proposed CCF defense approach is based on an approach presented in [Lundteigen and Rausand \(2007\)](#), adapted to suit ballast systems. The CCF defense approach may be integrated with current practices for function testing, inspection and follow up of other safety critical equip-

ment on the FPSO. The approach is built around a general function test and inspection procedure presented through the activity blocks in Figure 5.4, adopted from Lundteigen and Rausand (2007). The tasks in the defence approach are:

**Task 1:** Proper planning of function tests and inspection

**Task 2:** Avoid introducing CCFs during function tests and inspection

**Task 3:** Improve the quality of failure reporting

**Task 4:** Identify CCFs through failure analysis

**Task 5:** Implement defense measures

**Task 6:** Validation and continuous improvement

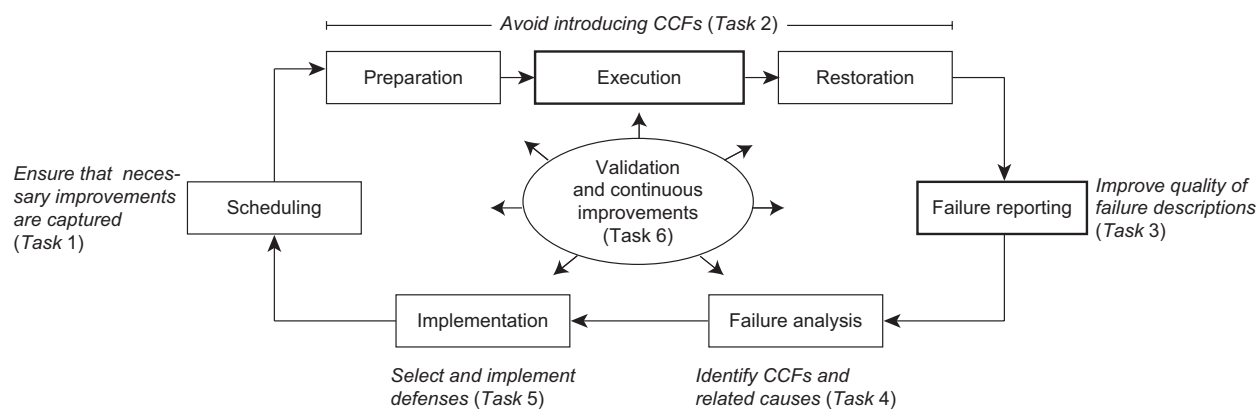


Figure 5.4: Main concepts of the CCF defense approach

**Task 1:** Proper planning of function tests and inspection

The defense approach will iteratively provide corrections to the function test and inspection procedure. Ensure that the latest improvements are updated in the maintenance management system before the next test.

**Task 2:** Avoid introducing CCFs during function tests and inspection

Function tests and inspections should be carried out with high awareness to CCF causes, as human errors, erroneous procedures and deficient work processes are potential sources of CCFs. Lundteigen and Rausand (2007) recommends the use of checklists to improve the defense against CCFs in these activities, and suggest the use of different checklists for preparation, execution and restoration. Deviations may then be discussed and compensated with the responsible technician. The slightly modified checklists are presented in Table 5.2, based on Lundteigen and Rausand (2007):

Checklist for preparation	Yes/No
(1) Have potential human errors during execution and restoration been identified and discussed?	Y/N
(2) Have human error incidents been experienced during previous execution?	Y/N
(3) Have compensating measures been identified and implemented to avoid human errors?	Y/N
(4) Are the personnel executing the test familiar with the test procedure?	Y/N
(5) Does the procedure have known deficiencies?	Y/N
(6) Does the procedure describe the necessary steps to safely restore the system/component?	Y/N
Checklist for execution	Yes/No
(1) Are the components operated within the specified environmental and operating conditions?	Y/N
(2) Are the components protected against damage from nearby work activities?	Y/N
(3) Are all the ballast system components labeled?	Y/N
Checklist for restoration	Yes/No
(1) Has the physical restoration of the components been verified?	Y/N
(2) Are any remaining inhibits, overrides or bypasses logged, and compensating measures identified and implemented?	Y/N
(3) Has the safety function been verified before start-up?	Y/N

Table 5.2: Checklists for preparation, execution and restoration during function tests and inspections

### Task 3: Improve the quality of failure reporting

Operators should report failures related to the ballast system components the same way as they would for other safety critical equipment.

Failure reporting should involve free text descriptions of failure causes, effects and detection methods, which can be used to verify the initial failure classification, and provide necessary information to decide whether a CCF has occurred. The following set of checklist questions based on [Lundteigen and Rausand \(2007\)](#) may be used during free text failure reporting.

Questions for free text description
(1) How was the failure discovered?
(2) What is believed to be the cause(s) of failure?
(3) What was the effect of failure on the ballast system function?
(4) Was the component tested or inspected differently than in the procedure? If yes, why?
(5) Has the component been overexposed to operational or environmental stress? If yes, what is the cause?
(6) Have similar failures been experienced previously?

Table 5.3: Questions for free text description during failure reporting

**Task 4:** Identify CCFs through failure analysis

Based on failure reports from the maintenance management system, the next step is to analyse and identify CCFs for the purpose of selecting appropriate defenses. [Lundteigen and Rausand \(2007\)](#) suggests a stepwise procedure

- **Step1:** Review the failure description and verify/correct the initial failure classification
- **Step2:** Perform an initial screening that captures failures that
  - a) have similar design or physical location
  - b) share failure causes
  - c) have been discovered within the same test or inspection interval
  - d) are not random failures as defined in section [3.2.1](#).
- **Step3:** Perform a *root cause and coupling factor analysis* of each identified CCF.
  - The analysis is a critical part of the defense approach, as it provides insight into the causes of CCF, and basis for identifying effective defenses.
  - If the root cause of a failure is difficult to identify, defenses against the coupling factor may be enough to stop reoccurrence of the CCF
  - The analysis should be carried out by a group of personnel.
  - A root cause and coupling factor analysis diagram can be used, as presented in [Lundteigen and Rausand \(2007\)](#).
- **Step4:** List the root cause and coupling factors in a cause-defense matrix, as presented in figure [5.5](#)

CCF	Root cause	Coupling factor	Defense alternatives	R	C	Impact (H/M/L)	Cost (H/M/L)
Failure in ballast valves	Solenoid stuck due to pollution in hydraulic supply	Identical design	Replace solenoids with more robust design		X	M	M
		Same hydraulic supply	Install filters in hydraulic supply	X		M	L
Failure in ballast pumps	Electric motor failure due to water ingress	Identical design	Replace pumps with more robust design		X	M	M
		Same location	Segregate the pumps Reduce the possibility of flooding	X	X	M H	M L

Figure 5.5: Cause defense matrix

**Task 5:** Implement defense measures.

Appropriate defenses against root causes and coupling factors may be found by considering a list of generic defense options, as in Figure 5.6, adopted from [Lundteigen and Rausand \(2007\)](#) which take into account possible design, procedural and physical improvements. The generic defense options should be considered a starting point for more specific defenses.

Generic defense options	
Administrative control	Improved preparation Improved coordination Improved responsibilities Improved feedback of experience Improved safety culture Improved training Improved quality control
Documentation	Improved drawings Improved functional description
Procedures	New procedure Improved procedure text (clarification, added scope or information) Improved quality control of restoration Improved test tools and calibration
Monitoring and surveillance	New alarm or alert. Implementation must follow IEC 61508 (1998)/61511 (2003) New condition or logic sequence
Physical barriers	Improved physical support or fastening Improved physical protection
Hardware or software modifications of SIS	Modifications requiring design changes. Redesign following IEC 61508 (1998)/61511 (2003)

Figure 5.6: Generic defense options against CCF

Selected defences should be listed in the cause-defense matrix, with indication of whether the root cause or the coupling factor is affected. Evaluations on impact and cost may also be added, where impact is understood as the ability of the defense measure to protect against future occurrences.

#### **Task 6:** Validation and continuous improvement

The activities related to function testing and inspection, as well as the approach taken to minimize the potential for CCFs during these activities, should be subject to regular validation and improvements. Maintenance personnel and technician should continuously improve the testing and inspection procedures, and evaluate the defenses implemented against CCFs. As an aid the validation of the activities in the operational phase, the checklist for validation in Table 5.4 can be used. The checklist is adopted from [Lundteigen and Rausand \(2007\)](#).



Checklist for validation	Yes/No
(1) Are the requirements for the safety function covered by the function test or inspection procedure(s)?	Y/N
(2) Are all personnel involved in ballast system testing, inspection, maintenance and follow up familiar with the CCF concept?	Y/N
(3) Are dangerous undetected failure modes known and catered for in the function test and inspection procedures?	Y/N
(4) Are the test limitations known?	Y/N
(5) Are all redundant channels of the safety functions covered by the function test or inspection procedure?	Y/N
(6) Are failures introduced during function testing and inspection captured, analyzed and used to improve the associated procedures?	Y/N
(7) Are failure detected during real demands analyzed to verify that they would have been detected during a function test or inspection?	Y/N
(8) Are changes in operating or environmental conditions captured and analyzed for necessary modifications to the ballast system or related procedures?	Y/N
(9) Are the calibration and test tools suitable and maintained according to the vendor recommendations?	Y/N
(10) Are personnel using the calibration and test tools familiar with their application?	Y/N
(11) Are procedure deficiencies followed up?	Y/N
(13) Are CCF systematically identified and analyzed, and defenses implemented to prevent their reoccurrence?	Y/N

Table 5.4: Checklists for preparation, execution and restoration during functional tests and inspections

# Chapter 6

## Case example: Petrojarl Foinaven FPSO

In this chapter a case example of the reliability assessment approach is presented. The reliability assessment approach is conducted on a ship shaped FPSO owned and operated by Teekay Petrojarl, one of the worlds leading FPSO operators.

### 6.0.2 Presentation of the Foinaven FPSO

The Petrojarl Foinaven, is a purpose built FPSO designed for oil production in the ultra harsh environments of the North Sea. The FPSO was delivered by Astano of Spain in 1996, and is currently operating on the Foinaven Field in the UK sector of the North Sea. The ship complies with the British continental shelf regulations, and is classified with DNV.

The ship´s production facilities comprise two parallel two stage separation trains for separation of crude oil, gas and produced water. The crude oil is temporarily stored in cargo tanks onboard, for subsequent offloading to shuttle tankers. The produced gas is used for generation of electricity, fuel to boilers, gas lift and is also exported to a nearby field for increased recovery purposes ([Petrojarl, 2011b](#)). The Petrojarl Foinaven FPSO in numbers:

Length overall	250.2 m
Breadth	34.0 m
Draught	12.8 m
Deadweight	43.2769 tonnes
Oil storage capacity	260000 bbls
Total ballast tank capacity	33580 m <sup>3</sup>
Crude oil production capacity	140000 bopd
Riser/umbilicals connected	12

Table 6.1: Petrojarl Foinaven FPSO in numbers



Figure 6.1: Teekay Petrojarl Foinaven

Ensuring proper stability of the ship is a high priority concern on the Foinaven FPSO. Due to a combination of a typically heavy topside design and a suboptimal cargo tank design, the vessel is highly dependent on a properly functioning ballast system to ensure acceptable inclination and draft of the vessel.

## 6.1 Reliability Assessment of the Foinaven FPSO Ballast System

The main body of the Foinaven FPSO consist of a double bottom and a double hull divided into ballast tanks on port and starbord side of the ship. Three main ballast pumps are located in the aft ballast pump room.

In addition to the main ballast tanks, one ballast tank is located at each side of the turret, and ballast tanks are also arranged in the forward and aft sections of the vessel. These tanks are operated by two ballast trim pumps located in the aft engine room, and two ballast trim pumps in the forward engine room. These additional ballast tank systems will not be included in the assessment. In the following sections, the stepwise procedure of the reliability assessment approach is conducted.

### 6.1.1 Step 1: Ballast System Familiarization

#### Main deviations from the base case ballast system

The ballast system on the Foinaven FPSO is similar to the base case ballast system in Section 3.1.1, but some important deviations exist. The system familiarization is based on a detailed study of the Foinaven ballast system presented in appendix Figures B.9 and B.10, an interviews with personnel familiar with the specific system. The main deviations and the related implications on the system functions is presented:

#### *Ballast Tank Configuration, Pumps and Valves:*

- The ballast tank valves are of fail-to-set design.
  - Implication: Upon loss of electric power, hydraulic power or control of the ballast operation, the ballast valves will not fail to a safe position, and water migration is possible in and out of the open ballast tank.
- Three pumphroom valves are hydraulically operated throttle valves.
  - Implication: Not accounted for. Assumed identical to butterfly valves.

#### *Electric Power System*

- Upon loss of main electric power, all hydraulically operated valves are unavailable for operation. In order to regain control of the valves, the emergency backup system must be functioning, and three hydraulic cabinets for operation of hydraulic valves must be reset by physically locating and resetting the hydraulic cabinets Petrojarl (2011a). The cabinets are located in three different sections of the ship.
  - Implication: Critical barrier function unavailability upon main electric power loss. Multiple human error possibilities during resetting operation.

#### *Hydraulic Power System*

- Assumed identical to base case hydraulic system

#### *Ballast Control System*

- The emergency stop function only stops the ballast pumps.
  - Implication: Critically reduced emergency stop barrier function. Emergency stop barrier function ineffective during gravity based ballasting operations to sea, or during pumpless ballasting operation between starbord and portside ballast tanks.

- The ballast system can be fully controlled from the bridge or from a designated NCC control room.
  - Implication: Enhanced redundancy in the control system. The redundancy has not been accounted for due to the extensive assessment needed to fully verify the actual level of redundancy in the control system. Assumed identical to base case ballast control system.

### **Description of the SIFs and Associated Components**

The Foinaven FPSO ballast system is capable of performing SIF1, SIF2 and SIF3 as described in Section 3.1.5. The emergency stop function on Foinaven does not fulfill the requirements of SIF4. In order to fulfill the requirements of SIF4, the emergency stop function must meet all the prerequisites of a successful operation, not only stop ballast pumps upon demand.

- **SIF 1:** To ballast/deballast starbord ballast tank system in response to operator command
  - The SIF is successful when: (1) One of the starbord ballast tanks is ballasted/deballasted to sea in response to operator command, by using ballast pump 2 or 3. (2) The ballasting operation stops upon operator command.
- **SIF 2:** To ballast/deballast portside ballast tank system in response to operator command
  - The SIF is successful when: (1) One of the portside ballast tanks is ballasted/deballasted to sea in response to operator command, by using ballast pump 1 or 2. (2) The ballasting operation stops upon operator command.
- **SIF 3:** To ballast/deballast between starbord and portside ballast tank system in response to operator command
  - The SIF is successful when: (1) One of the portside ballast tanks is ballasted/deballasted with one of the starbord ballast tanks in response to operator command, by using ballast pump 1, 2 or 3. (2) The ballasting operation stops upon operator command.
- **SIF 4:** Emergency stop of ballast system operation in response to operator command
  - Not accounted for.

### **6.1.2 Step 2: Identification of Common Cause Component Groups**

The main common cause component groups are:

Common cause component group	
Ballast valves	Identical design Same internal and external environmental exposure Same hydraulic supply Same potential failure causes
Pumps	Identical design Same internal and external environmental exposure Same electric supply Same potential failure causes
Pump room valves	Identical design Same internal and external environmental exposure Same hydraulic supply Same potential failure causes

Table 6.2: List of identified common cause component groups

A major source of potential for CCFs may be found if the ballast control system is subject to a full system breakdown and analysis. The operator controls, the control logic, and all associated electrical components located in the same area may be susceptible to CCF, with reference to the Ocean Ranger accident. In the case study, the ballast control system is assumed identical to the simplified single unit control system in the base case system.

The potential for common cause failure amongst the components in the electric and hydraulic power systems have not been accounted for.

### 6.1.3 Step 2: RBD Construction

#### RBD Modeling of Elementary Utilities

##### *RBD Electric Power System*

The RBD of the electric power system is modeled as a redundant system, with two separate channels.

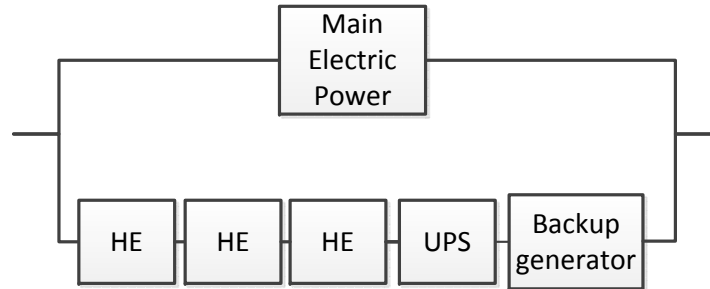


Figure 6.2: RBDel

In case of loss of main electric power, the RBD represents the necessary blocks needed to fulfill the function. The UPS reliability block represent the UPSs necessary to support the ballast control system and operator screens. The emergency backup generator is represented by an individual block. The possible non-fulfillment of the human interactions needed to regain control of the ballast system upon loss of main electric power is represented by three Human Error reliability blocks. The three blocks represent the three human interactions needed at three separate locations.

#### *RBD Hydraulic Power System*

The RBD of the hydraulic power system is modeled as a redundant system, with two separate channels, to highlight the accumulator function in case of loss of main hydraulic power.

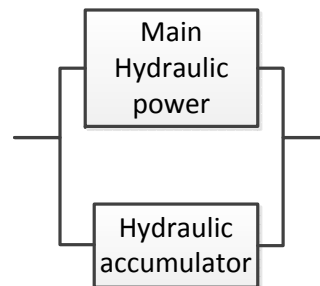


Figure 6.3: RBDhyd

#### **RBD Modeling of Individual SIFs**

The SIFs are modeled by evaluating the components needed to execute the different functions according to the success criteria of the different SIFs. The RBDs of the SIFs are modeled based on the system familiarization in step 1. As the operator can choose any of the ballast tanks on each side of the vessel to carry out SIF1, SIF2 and SIF3, this option is modeled as a redundant configuration with a *1oo5* voting. Pump functions are modeled with the respective voting of the pumps. Potential CCFs in redundant configurations are modeled as separate blocks in the RBDs.

*RBD1. SIF 1: To ballast/deballast starboard ballast tank system in response to operator command*

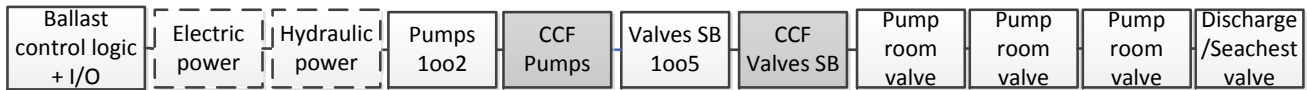


Figure 6.4: RBD1

*RBD2. SIF 2: To ballast/deballast portside ballast tank system in response to operator command*



Figure 6.5: RBD2

*RBD3. SIF 3: To ballast/deballast between starboard and portside ballast tank system in response to operator command*



Figure 6.6: RBD3

*RBD4. SIF 4: Emergency stop of ballast system operation in response to operator command*

Not accounted for.

#### 6.1.4 Step 4: Determine Relevant Reliability Data

Ship-specific data is not available for the assessment. Reliability data is collected from section 5.1.4, and presented in Figure 6.7.



Component type	Failure rate $\lambda$ DU (per 10 <sup>6</sup> h)	Test interval $\tau$ (h)	$\beta$ -factor	PFD single item	Comment
Ballast valve	3	2190	3 %	3,29E-03	Includes valve + solenoid/pilot
Pump room valve	3	2190	3 %	3,29E-03	Includes valve + solenoid/pilot
Seachest/Discharge valve	3	2190	3 %	3,29E-03	Includes valve + solenoid/pilot
Ballast pump	-	-	5 %	9,40E-04	Includes only fail to start
Ballast control logic + I/O	1	8760		4,38E-03	
Emergency backup generator	-	-		9,40E-04	Assumed identical to ballast pump fail to start
Component type (Continuous operation)	Failure rate $\lambda$	MTTR	$\beta$ -factor	Average unavailability of the item	Comment
Main electric power system	1,14E-04	10		1,14E-03	Ref. assumption 3
UPS	1,14E-04	10		1,14E-03	Ref. assumption 3
Main hydraulic power generator	3,00E-06	10		3,00E-05	Ref. assumption 3
Hydraulic accumulator	1,14E-04	10		1,14E-03	Ref. assumption 3

Figure 6.7: Reliability data used in the case example

No.	Description of assumptions related to reliability data
1	Ballast valves, pump room valves and discharge/seachest valves are assumed to be function tested every 3 months (2190 hours)
2	The ballast control logic is assumed to be function tested once per year (8760 hours)
3	The estimated failure rates and MTTR of the components in continuous operation: Main electric power generators: $\lambda = 1/8760$ (Once per year), MTTR= 10h. UPS: $\lambda = 1/8760$ (Once per year), MTTR= 10h. Main hydraulic power generator: $\lambda = 3 \cdot 10^{-6}$ (RABL), MTTR= 10h. Hydraulic accumulator: $\lambda = 1/8760$ (Once per year), MTTR= 10h.
4	The PFD of a ballast pump includes only "fail to start". The valve failure rates only include the DU failure mode "fail to open".
5	The human interventions are assumed equal to "Operator response to alarms" in table 5.1. $PFD_{HE} = 0,1$

Table 6.3: Description of assumptions

### 6.1.5 Step 5: PFD Calculations

For the PFD calculations, it is assumed that all assumptions in 5.1.2 are valid. The elementary utilities are calculated first, followed by calculations of the various SIFs. For all calculations, the formulaes from section 5.1.2 are used together with reliability data from figure 6.7.

#### PFD Elementary Utilities

##### *PFD Electric Power System*

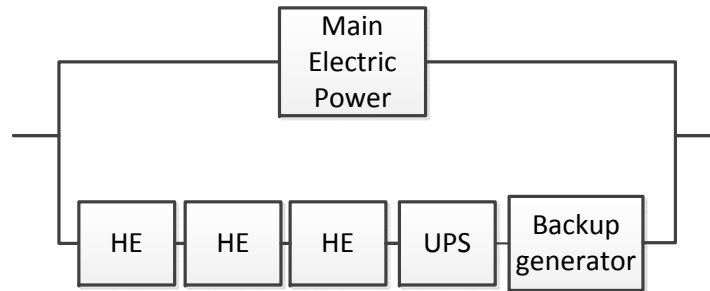


Figure 6.8: RBDelec

The RBD consist of a complex *1oo2*-configuration comprising different types of components. Calculating  $PFD_{elec}$  is done by utilizing the non-conservative approximation from 5.4 coupled with the correction factor from 5.5. The PFD of the human interventions are assumed equal to "Operator response to alarms" in Table 5.1.

$$PFD_{channel1} = PFD_{Mainelec} \approx A_{avstrek} \approx \lambda \cdot MTTR = \frac{1}{8760} \cdot 10 = 1,14 \cdot 10^{-3}$$

$$PFD_{channel2} = PFD_{HE} + PFD_{HE} + PFD_{HE} + PFD_{UPS} + PFD_{backupgen}$$

$$PFD_{HE} = 0,1$$

$$PFD_{UPS} \approx A_{avstrek} \approx \lambda \cdot MTTR = \frac{1}{8760} \cdot 10 = 1,14 \cdot 10^{-3}$$

$$PFD_{backupgen} = 9,4 \cdot 10^{-4}$$

$$PFD_{channel2} = 0,1 + 0,1 + 0,1 + 1,14 \cdot 10^{-3} + 9,4 \cdot 10^{-4} = 3,02 \cdot 10^{-1}$$

$$PFD_{elec} = PFD_{channel1} \cdot PFD_{channel2} \cdot CF_{1oo2} = (1,14 \cdot 10^{-3})_{channel1} \cdot (3,02 \cdot 10^{-1})_{channel2} \cdot 4/3 = \underline{4,6 \cdot 10^{-4}}$$

##### *PFD Hydraulic Power System*

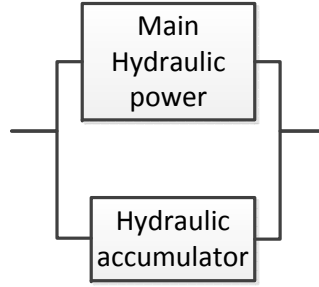


Figure 6.9: RBDhyd

The RBD consist of two non-identical items configured as *1oo2*-configuration. Calculating PFD-hydr is done by utilizing the non-conservative approximation from 5.4 coupled with the correction factor from 5.5. The

$$PFD_{channel1} = PFD_{Mainhyd} \approx A_{avstrek} \approx \lambda \cdot MTTR = 3 \cdot 10^{-6} \cdot 10 = 3 \cdot 10^{-5}$$

$$PFD_{channel2} = PFD_{Acc} \approx A_{avstrek} \approx \lambda \cdot MTTR = \frac{1}{8760} \cdot 10 = 1,14 \cdot 10^{-3}$$

$$PFD_{hydr} = PFD_{channel1} \cdot PFD_{channel2} \cdot CF_{1oo2} = (3 \cdot 10^{-5})_{channel1} \cdot (1,14 \cdot 10^{-3})_{channel2} \cdot 4/3 = \underline{4,6 \cdot 10^{-8}}$$

### PFD of Ballast Pumps

Since the reliability data identified for the ballast pumps only include the "fail to start" on demand failure mode, the PFD of redundant ballast pump configurations should be calculated with some care, especially when including CCFs. For a *1oo2* pump configuration, the  $PFD_{1oo2pumps}$  can be calculated by utilizing the non-conservative approximation from 5.4 coupled with the correction factor from 5.5:

$$PFD_{1oo2pumps} = PFD_{pump} \cdot PFD_{pump} \cdot CF_{1oo2} = (9,4 \cdot 10^{-4})_{pump} \cdot (9,4 \cdot 10^{-4})_{pump} \cdot (4/3) = \underline{1,2 \cdot 10^{-6}}$$

For a *1oo2* pump configuration modeled with CCF:

$$\begin{aligned}
 PFD_{1oo2pumps}^{ind} + PFD_{1oo2pumps}^{CCF} &= \\
 \frac{((1 - \beta_{1oo2})\lambda_{DU\tau})^2}{3} + \frac{\beta_{1oo2}\lambda_{DU\tau}}{2} &= ((1 - \beta_{1oo2})^2 \cdot PFD_{1oo2pumps})_{1oo2pumps}^{ind} + (\beta_{1oo2} \cdot PFD_{pump})_{1oo2pumps}^{CCF} \\
 &= \underline{\underline{((1 - \beta_{1oo2})^2 \cdot 1,2 \cdot 10^{-6})_{1oo2pumps}^{ind} + (\beta_{1oo2} \cdot 9,4 \cdot 10^{-4})_{1oo2pumps}^{CCF}}}
 \end{aligned}$$

For a 1003 pump configuration modeled with CCF:

$$PFD_{1003pumps} = PFD_{pump} \cdot PFD_{pump} \cdot PFD_{pump} \cdot CF_{1003} = 9,4 \cdot 10^{-4} \cdot 9,4 \cdot 10^{-4} \cdot 9,4 \cdot 10^{-4} \cdot (2) = \underline{2 \cdot 10^{-9}}$$

$$\begin{aligned} PFD_{1003pumps}^{ind} + PFD_{1003pumps}^{CCF} = \\ \frac{((1 - \beta_{1003})\lambda_{DU\tau})^3}{4} + \frac{\beta_{1003}\lambda_{DU\tau}}{2} = ((1 - \beta_{1003})^3 \cdot PFD_{1003pumps})_{1003pumps}^{ind} + (\beta_{1003} \cdot PFD_{pump})_{1003pumps}^{CCF} \\ \underline{\underline{((1 - \beta_{1003})^3 \cdot 2,0 \cdot 10^{-9})_{1003pumps}^{ind} + (\beta_{1003} \cdot 9,4 \cdot 10^{-4})_{1003pumps}^{CCF}}} \end{aligned}$$

### PFD of SIFs

#### PFD SIF1: To ballast/deballast starbord ballast tank system in response to operator command



Figure 6.10: RBD1

The RBD of SIF1 consist of a series structure of non-identical items. The two elementary utility functions, electric power and hydraulic power, are identical to the corresponding RBDs in Section 6.1.5. Ballast control logic is modeled as a single item. The redundant ballast pump function is modeled as a single item with a 1002 configuration, with  $\beta_{1002} = C_{1002} \cdot \beta = 1,0 \cdot 0,05 = 0,05$ . The contribution from CCF of the pumps is modeled as a separate item in the RBD. The redundant valve configuration is modeled as a single item with a 1005 configuration, with  $\beta_{1005} = C_{1005} \cdot \beta = 0,21 \cdot 0,03 = 0,0063$ . The contribution from CCF of the valves is modeled as a separate item in the RBD. Finally, the pumproom valves and the discharge/seachest valve are modeled as single items.

$$\begin{aligned} PFD_{SIF1} = PFD_{logic} + PFD_{elec} + PFD_{hydr} + PFD_{1002pumps}^{(ind)} + PFD_{1002pumps}^{(CCF)} \\ + PFD_{1005valvesSB}^{(ind)} + PFD_{1005valvesSB}^{(CCF)} + PFD_{prv} + PFD_{prv} + PFD_{prv} + PFD_{dsv} \\ \mathbf{Pumps:} PFD_{1002pumps}^{(ind)} + PFD_{1002pumps}^{(CCF)} = \\ = ((1 - 0,05)^2 \cdot 1,2 \cdot 10^{-6})_{1002pumps}^{ind} + (0,05 \cdot 9,4 \cdot 10^{-4})_{1002pumps}^{CCF} = (1,2 \cdot 10^{-6})_{1002pumps}^{ind} + (4,7 \cdot 10^{-5})_{1002pumps}^{CCF} \end{aligned}$$

$$\text{Ballast valves: } PFD_{1005valvesSB}^{(ind)} + PFD_{1005valvesSB}^{(CCF)} = \frac{((1 - \beta_{1005})\lambda_{DU,V} \cdot \tau)^5}{6} + \frac{\beta_{1005}\lambda_{DU,V} \cdot \tau}{2} =$$

$$\frac{((1 - 0,0063) \cdot 3 \cdot 10^{-6} \cdot 2190)^5}{6} + \frac{0,0063 \cdot 3 \cdot 10^{-6} \cdot 2190}{2} = (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF}$$

$$PFD_{SIF1} = \left(\frac{1 \cdot 10^{-6} \cdot 8760}{2}\right)_{logic} + (4,6 \cdot 10^{-4})_{elec} + (4,6 \cdot 10^{-8})_{hydr} + (1,2 \cdot 10^{-6})_{1002pumps}^{ind} + (4,7 \cdot 10^{-5})_{1002pumps}^{CCF}$$

$$+ (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF} + 3 \cdot \left(\frac{3 \cdot 10^{-6} \cdot 2190}{2}\right)_{prv} + \left(\frac{3 \cdot 10^{-6} \cdot 2190}{2}\right)_{dsv}$$

$$PFD_{SIF1} = (4,4 \cdot 10^{-3})_{logic} + (4,6 \cdot 10^{-4})_{elec} + (4,6 \cdot 10^{-8})_{hydr} + (1,2 \cdot 10^{-6})_{1002pumps}^{ind} + (4,7 \cdot 10^{-5})_{1002pumps}^{CCF}$$

$$+ (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF} + 3 \cdot (3,3 \cdot 10^{-3})_{prv} + (3,3 \cdot 10^{-3})_{dsv}$$

$$PFD_{SIF1} = \underline{\underline{1,8 \cdot 10^{-2}}}$$

### PFD SIF2: To ballast/deballast portside ballast tank system in response to operator command



Figure 6.11: RBD2

The RBD of SIF2 consist of a series structure of non-identical items. The two elementary utility functions, electric power and hydraulic power, are identical to the corresponding RBDs in section 6.1.5. Ballast control logic is modeled as a single item. The redundant ballast pump function is modeled as a single item with a *1002* configuration, with  $\beta_{1002} = C_{1002} \cdot \beta = 1,0 \cdot 0,05 = 0,05$ . The contribution from CCF of the pumps is modeled as separate item in the RBD. The redundant valve configuration is modeled as a single item with a *1005* configuration, with  $\beta_{1005} = C_{1005} \cdot \beta = 0,21 \cdot 0,03 = 0,0063$ . The contribution from CCF of the valves is modeled as a separate item in the RBD. Finally, the pumproom valve and the discharge/seachest valve are modeled as single items.

For the Foinaven FPSO, SIF1 and SIF1 have identical RBD setups. The reliability blocks refer to

other components, but since they are the same type of components, the outcome of the calculation will be the same if the same data is used and the same assumptions hold.

For this case example, it assumed that the same assumptions hold for the components in SIF1 and SIF2. The PFD of SIF2 will then be same as the PFD of SIF1.

$$PFD_{SIF2} = PFD_{SIF1} = \underline{\underline{1,8 \cdot 10^{-2}}}$$

### PFD SIF3: To ballast/deballast between starbord and portside ballast tank system in response to operator command

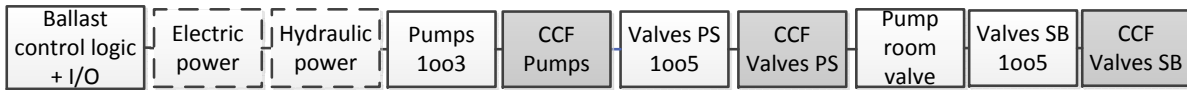


Figure 6.12: RBD3

The RBD of SIF3 consist of a series structure of non-identical items. The two elementary utility functions, electric power and hydraulic power, are identical to the corresponding RBDs in Section 6.1.5. Ballast control logic is modeled as a single item. The redundant ballast pump function is modeled as a single item with a *1oo3* configuration. The contribution from CCF of the pumps is modeled as separate item in the RBD, with  $\beta_{1oo3} = C_{1oo3} \cdot \beta = 0,30 \cdot 0,05 = 0,015$ . The redundant valve configurations are modeled as single items with *1oo5* configurations, with  $\beta_{1oo5} = C_{1oo5} \cdot \beta = 0,21 \cdot 0,03 = 0,0063$ . The contribution from CCF of the valves is modeled as separate items in the RBD. Finally, the pumproom valve is included as a single item.

$$PFD_{SIF3} = PFD_{logic} + PFD_{elec} + PFD_{hydr} + PFD_{1oo3pumps}^{(ind)} + PFD_{1oo3pumps}^{(CCF)} + PFD_{1oo5valvesPS}^{(ind)} + PFD_{1oo5valvesPS}^{(CCF)} + PFD_{prv} + PFD_{1oo5valvesSB}^{(ind)} + PFD_{1oo5valvesSB}^{(CCF)}$$

$$\begin{aligned} \textbf{Pumps: } PFD_{1oo3pumps}^{(ind)} + PFD_{1oo3pumps}^{(CCF)} &= \\ ((1 - 0,015)^3 \cdot 2,0 \cdot 10^{-9})_{1oo3pumps}^{ind} + (0,015 \cdot 9,4 \cdot 10^{-4})_{1oo3pumps}^{CCF} &= \\ (2 \cdot 10^{-9})_{1oo3pumps}^{ind} + (1,41 \cdot 10^{-5})_{1oo3pumps}^{CCF} &= \end{aligned}$$

$$\textbf{Ballast valves PS: } PFD_{1oo5valvesPS}^{(ind)} + PFD_{1oo5valvesPS}^{(CCF)} = \frac{((1 - \beta_{1oo5}) \lambda_{DU,V} \cdot \tau)^5}{6} + \frac{\beta_{1oo5} \lambda_{DU,V} \cdot \tau}{2} =$$

$$\frac{((1 - 0,0063) \cdot 3 \cdot 10^{-6} \cdot 2190)^5}{6} + \frac{0,0063 \cdot 3 \cdot 10^{-6} \cdot 2190}{2} = (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF}$$

$$\text{Ballast valves SB: } PFD_{1005valvesPS}^{(ind)} + PFD_{1005valvesPS}^{(CCF)} = \frac{((1 - \beta_{1005}) \lambda_{DU,V} \cdot \tau)^5}{6} + \frac{\beta_{1005} \lambda_{DU,V} \cdot \tau}{2} =$$

$$\frac{((1 - 0,0063) \cdot 3 \cdot 10^{-6} \cdot 2190)^5}{6} + \frac{0,0063 \cdot 3 \cdot 10^{-6} \cdot 2190}{2} = (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF}$$

$$PFD_{SIF3} = (4,4 \cdot 10^{-3})_{logic} + (4,6 \cdot 10^{-4})_{elec} + (4,6 \cdot 10^{-8})_{hydr} + (2 \cdot 10^{-9})_{1003pumps}^{ind} + (1,41 \cdot 10^{-5})_{1003pumps}^{CCF}$$

$$+ (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF} + (3,3 \cdot 10^{-3})_{prv} + (2 \cdot 10^{-12})_{1005valves}^{ind} + (2,1 \cdot 10^{-5})_{1005valves}^{CCF}$$

$$PFD_{SIF3} = \underline{\underline{8,22 \cdot 10^{-3}}}$$

### 6.1.6 Step 6: Comparison with Reliability Performance Targets

In Table 6.4, the calculated PFD values are compared to the minimum SIL performance requirements presented in Table 3.2.

	Reliability target	Target achieved	PFD <sub>SIF</sub>
Foinaven SIF1	SIL1	Yes	$1,8 \cdot 10^{-2}$
Foinaven SIF2	SIL1	Yes	$1,8 \cdot 10^{-2}$
Foinaven SIF3	SIL1	Yes	$8,22 \cdot 10^{-3}$
Foinaven SIF4	SIL2	N/A	N/A

Table 6.4: Comparison with reliability performance targets

The results of the calculations show that the ballast system on the Foinaven FPSO is fully capable of reaching the proposed minimum reliability performance requirements for ballast systems, as long as all the assumptions from Table 6.3 hold, including the various functional test intervals. It should be emphasized that most of the reliability data used is not ship specific, but based on applicable data gathered from the offshore industry. In order to reduced the CCF potential in the operational phase to a minimum, the CCF defense approach from Section 5.3 may be applied. In addition to the quantitative results, the reliability assessment identified several critical deviations from the base case ballast system leading to reduced safety barrier functionality. These deviations and their implication on the system functions are presented in Section 6.1.1.

# Chapter 7

## Summary and Recommendations for Further Work

### 7.1 Summary and Conclusions

The main objective of the master thesis has been to suggest a reliability assessment approach for ballast systems, and include recommendations to how reliability requirements should be set for this type of system. As a part of fulfilling the main objectives, a series of tasks have been performed.

The literature survey is presented in three parts. The first part document previous work in the field of ballast system reliability in Section 1.2, the second part present the regulations governing ballast systems on the NCS in Section 2, and the third part document the reported safety and reliability challenges, incidents and accidents related to ballast systems in Chapter 4.

As a basis for the reliability assessment approach, a typical ballast on a ship shaped vessel is presented in Chapter 3, and the interface between the system and the electric and hydraulic power systems on the ship is described. The system and the main components are presented at a level of detail that provides a foundation for reliability assessments of different ballast system designs. The safety critical functions of the system are identified and the ballast system is defined as a *safety barrier against unacceptable inclination and draft of the vessel*.

The ballast system is then classified as a SIS, and the safety critical functions of the ballast system are classified as SIFs installed to protect against hazards that may lead to loss of stability and draft of the vessel. The concept of safe state of the FPSO is discussed in Section 3.1.5, and the desired behaviour upon fault conditions for the ballast system components is described.



A HAZID and hazard-barrier matrix is used to analyze the adequacy of the ballast system as a barrier, and in Section 3.2 a failure analysis is conducted to identify failure causes and failure modes that may influence the reliability performance of ballast systems, including the possibility of having CCFs among the components. A FMECA is conducted and documented in worksheet B.3, B.4 and B.5.

Relevant methods for defining reliability performance requirements for ballast systems are presented and discussed in Section 3.3. The risk based approach of the IEC 61508 (2010) standard is compared to the *minimum SIL requirement* approach from the OLF070 (2004) guideline. The minimum SIL requirement approach is chosen as the state-of-the-art approach for defining SIL requirements to ballast system SIFs, and a set of proposed minimum SIL requirements are presented.

A reliability assessment approach for ballast systems is presented in Chapter 5. The reliability assessment approach is based on a RBD technique, and can be used to calculate the PFD of the SIFs in the ballast system. The potential for CCFs among the components can be included in the calculations, and the assessment is developed to give conservative estimates for reliability performance. In Chapter 6 the reliability assessment approach is applied to the ballast system of the Petrojarl Foinaven FPSO, as a case example of the approach.

A defense approach against CCFs in ballast systems is presented in Section 5.3. The defence approach can be implemented in the operational phase, to reduce the influence and reoccurrence of CCF during maintenance and testing of the ballast system components.

## 7.2 Discussion

Despite the importance of well functioning ballast systems on ships and floating facilities, and a series of incidents and accidents where the unreliability of ballast systems have been a contributing factor, not a lot of research has been carried out within the field of ballast system reliability. The requirements to these systems are still based on prescriptive maritime regulations, although initiatives have been taken to include ballast systems under the performance based regulations of the offshore industry. This has been done under the regulatory regime on the NCS since 2004, as described in Section 2.

The typical ballast system presented in Chapter 3 is the result of simplifications making the model applicable to a range of designs without losing the most important details. During actual verifications, the simplification should be verified and the level of detail should be as high as possible.

The proposed reliability performance requirements of the ballast system functions are based on the minimum SIL requirement approach of the [OLF070 \(2004\)](#) guideline. The requirements are not especially strict. As part of a continuous improvement effort, the requirements should be higher, but in line with the idea of the guideline, these requirements should be seen as minimum requirements.

The strength of the proposed reliability assessment approach is the practical stepwise procedure, and the flexible RBD modeling combined with conservative approximation formulae for reliability performance calculations. The reliability assessment can be performed without using specialized software, and the contributions from CCFs can be included in the diagrams and calculations. A limitation of the approach is that the RBDs can be quite large if a lot of details are included in the assessment. If complex modeling is needed to assess a subsystem of a ballast system, e.g. the control system, FTA can be used to model and quantify the PFD of the subsystem, and subsequently include the results into the RBD.

The case example of the reliability assessment approach show that the proposed reliability performance requirements can be achieved by performing functional tests at regular intervals, and that the stepwise procedure may also identify important improvement potentials for ballast systems. A limitation of the case example is the lack of ship specific failure data that would have increased the relevance of the results.

### **7.3 Recommendations for Further Work**

In the suggested reliability assessment approach, the various SIFs are assessed individually, and the effect of CCF is limited to the specific SIF being analysed. The first proposal for further work is to investigate the dependency between the various SIFs, and the effect of CCF among different SIFs.

The second proposal is to develop a detailed reliability assessment approach for ballast control systems that can assess the true redundancy in the control system, and evaluate the spurious trip and dangerous failure potential.

The third proposal is to develop a risk analysis methodology based on the possible outcomes of ballast system fault states. The analysis can be based on extensive scenario modeling and ETA techniques.

# Bibliography

- Askedal, S., Heia, O., Hanson, B., o. Hundseid, Kjeldstad, K., Kristensen, V., Kvitrud, A., Lauridsen, Ø., Solheim, R., Tharaldsen, J., and og I. Årstad, H. Ø. (2011). Deepwater Horizon-ulykken - Vurderinger og anbefalinger for norsk petroleumsvirksomhet.
- Baunan, T. (1996). FPSO's Fulfilling Shelf Requirements by the Maritime Approach. *Offshore Technology Conference (OTC), Houston*.
- Chen, H. and Moan, T. (2003). Probabilistic modeling and evaluation of collision between shuttle tanker and FPSO in tandem offloading. *Reliability Engineering and System Safety* 84.
- Chen, H., Moan, T., and Verhoeven, H. (2007). Safety of dynamic positioning operations on mobile offshore drilling units. *Reliability Engineering and System Safety* 93.
- Hansen, K. B. (2007). Risikoanalyse for ballast systemet paa flyterigger. *Universitetet i Stavanger, Masteroppgave*.
- Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. (2009a). *Reliability Data for Safety Instrumented Systems. PDS Data Handbook, 2010 Edition*. SINTEF Technology and Society: Safety Research.
- Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. (2009b). *Reliability Prediction Metod for Safety Instrumented Systems. PDS Method Handbook, 2010 Edition*. SINTEF Technology and Society: Safety Research.
- Hauge, S. and Onshus, T. (2009). Reliability data for safety instrumented systems, pds data handbook, 2010 edition. Technical report, SINTEF Technology and Society: Safety Research.
- IEC 60812 (2006). *Analysis Techniques for system reliability. Procedure for failure mode and effects analysis (FMEA)*. International Electrotechnical Commission.
- IEC 61508 (2010). *Functional safety*. International Electrotechnical Commission.
- IEC 61511 (2004). *Functional safety - Safety instrumented systems for the process industry sector*. International Electrotechnical Commission.

- Leonhardsen, R. L., Ersdal, G., and Kvitrud, A. (2001). Experience and Risk Assessment of FPSOs in Use on the Norwegian Continental Shelf: Description of Events. *International Offshore and Polar Engineering Conference, Stavanger*.
- Lundteigen, M. A. and Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*.
- Lundteigen, M. A. and Rausand, M. (2009). Reliability Assessment of Safety Instrumented Systems in the Oil and Gas Industry: A Practical Approach and a Case Study.
- MacDonald, A., Cain, M., Aggarwal, A. K., Vivalda, C., and Lie, O. E. (1999). Collision Risks Associated with FPSOs in Deep Water Gulf of Mexico. *Offshore Technology Conference (OTC), Houston*.
- Nesje, J. D., Aggarwal, R. K., Petrauskas, C., Vinnem, J. E., Keolanui, G. L., Hoffman, J., and McDonnell, R. (1999). Risk Assessment Technology and its Application to Tanker Based Floating Production Storage and Offloading (FPSO) Systems. *Offshore Technology Conference (OTC), Houston*.
- OGP (2006). Guideline for managing marine risks associated with FPSOs. *The International Association of Oil & Gas Producers (OGP)*.
- OLF070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*.
- Østby, E., Berg, M., and Festøy, B. (1987). *Ballast System Failures And Other Faulty Weight Conditions*. RABL Risk Assessment Of Buoyancy Loss and Other Faulty Weight Conditions. PPS3: Ballast System.
- Overfield, R. E. and Collins, J. F. (2000). Quantitative Risk Assessment as a Design Tool – Recent FPSO experience. *Society of Petroleum Engineers (SPE) Conference, Stavanger*.
- Petrobras (2002). Final Report Inquiry Commission P-34 Listing.
- Petrojarl, T. (2011a). Operation Manual, Stability and Ballast System.
- Petrojarl, T. (2011b). Petrojarl Foinaven Information Brochure.
- PSA (2011). Guidelines for application for Acknowledgement of Compliance (AOC) for mobile facilities intended for use in the petroleum activities on the Norwegian Continental Shelf.
- Rausand, M. (2011). *Risk Assessment Theory, Methods and Applications*. Wiley.

- Rausand, M. and Høyland, A. (2004). *System Reliability Theory - Models, Statistical Methods, and Applications - Second Edition*. Wiley.
- Rocha, G. C., do Amaral Vasconcellos, J. M., and Frutuoso e Melo, P. F. F. (2010). Functional Reliability Study of the Electrical Power System, Automation System and Ballast system to Maintain the Balance of a FPSO Platform. *Society of Petroleum Engineers (SPE) Conference, Rio de Janeiro, Brazil*.
- Sklet, S. (2006). Safety Barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*.
- Tinmannsvik, R., Albrechtsen, E., Bråtveit, M., Carlsen, I., Fylling, I., Hauge, S., Haugen, S., Hynne, H., Lundteigen, M., Moen, B., Okstad, E., Onshus, T., Sandvik, P., and /Oien, K. (2011). Deepwater Horizon-ulykken: Årsaker, lærepunkter og forbedringstiltak for norsk sokkel. *SINTEF Report*.
- Tronstad, L. (2009). The Use of Risk Analysis in Design: Safety Aspects Related to the Design and Operation of a FPSO. *Society of Petroleum Engineers (SPE) Conference, Stavanger*.
- U.S. Coast Guard (1983). Marine Casualty Report. Mobile Offshore Drilling Unit (MODU) Ocean Ranger.
- Vinnem, J. E. (2000). Offshore Technology Report. Operational safety of FPSOs: Initial Summary Report. *HSE Health & Safety Executive*.
- Vinnem, J. E., Hauge, S., Huglen, Ø., Kieran, O., Kirwan, B., Rettedal, W., Skåren, T., and Thomas, J. J. (2000). Systematic Analysis of Operational Safety of FPSOs Reveals Areas of Improvement. *Society of Petroleum Engineers (SPE) Conference, Stavanger*.
- Vinnem, J. E., Kvitrud, A., and Nilsen, L. R. (2006). Stabilitetssvikt av innretninger på norsk sokkel - Metodikk for risikoanalyse.
- Watson, I. A. and Smith, A. M. (1980). Common cause failures - a dilemma in perspective. *Reliability Engineering 1 (1980)*.

# Appendix A

## Acronyms

**AOC** Acknowledgement of Compliance

**BF** Barrier function

**CCF** Common cause failure

**D** Dangerous failure

**DNV** Det Norske Veritas

**DU** Dangerous undetected failure

**DD** Dangerous detected failure

**ETA** Event Tree Analysis

**EUC** Equipment under control

**FTA** Fault tree analysis

**FMEA** Failure mode and effect analysis

**FMECA** Failure mode, effect and criticality analysis

**FPSO** Floating Production, Storage and Offloading

**HAZID** Hazard identification

**HEP** Human error probability

**HRA** Human reliability analysis

**I/O** Input-output

**MTTF** Mean time to failure

**MTTR** Mean time to repair

**MooN** M-out-of-N voting

**NCS** Norwegian Continental Shelf

**NMA** Norwegian Maritime Authority

**OLF** The Norwegian Oil Industry Association

**PSA** Petroleum Safety Authority Norway

**PDF** Probability of failure on demand

**PFH** Probability of a dangerous failure per hour]

**P&ID** Process and instrumentation diagram

**QRA** Quantitative risk analysis

**LOPA** Layer of protection analysis

**RABL** Risk Assessment of Buoyancy Loss

**RAMS** Reliability, availability, maintainability and safety

**RPN** Risk priority number

**SIL** Safety integrity level

**SIS** Safety instrumented system

**SIF** Safety instrumented function

**S** Safe failure

**SU** Safe undetected failure

**SD** Safe detected failure

**UPS** Uninterruptible power sources

## **Appendix B**

### **Additional Information**



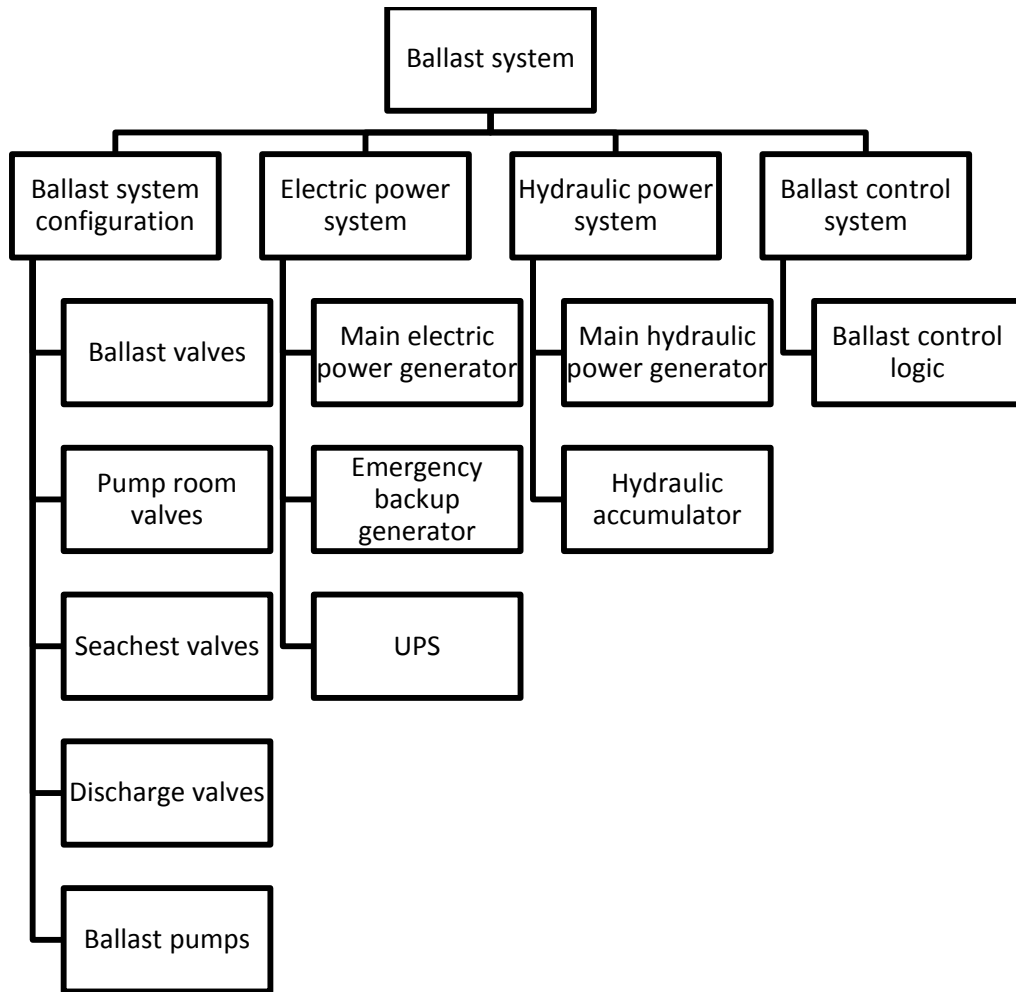


Figure B.1: Hierarchical breakdown of the ballast system

Item	Failure rate (per hour)	Data source
1. Ballast valves Hydr. operated, butterfly		
- Critical failure	$12 \cdot 10^{-6}$	OREDA
- Fail to close (per demand)	$2 \cdot 10^{-3}$	OREDA
- Blocked	$1.7 \cdot 10^{-6}$	OREDA
- Faulty indication	$15 \cdot 10^{-6}$	OREDA
- Internal leakages (sign.)	$3 \cdot 10^{-6}$	OREDA
2. Check valve (hydr.system)		
- All modes	$3 \cdot 10^{-6}$	IEEE
3. Hydr. pipes ( $\phi < 3''$ )		
- All modes (pr. km)	$0.5 \cdot 10^{-7}$	Magpie
- Rupture/plugged (per section)	$3 \cdot 10^{-11}$	WASH 1400
4. Hydr. power supply unit		
- Critical	$3 \cdot 10^{-6}$	OREDA
- Erratic control	$7 \cdot 10^{-6}$	OREDA
5. Electronic control unit (PLC, typical)		
- Critical failure	$30 \cdot 10^{-6}$	OREDA
6. Level indicator		
- Critical	$0.7 \cdot 10^{-6}$	OREDA/IEEE
- Erratic output	$0.4 \cdot 10^{-6}$	OREDA/IEEE
7. Pipe (ballast water)		
- Sign. external leak (pr. km)	$2 \cdot 10^{-9}$	ICI
8. Ballast water pump system		
- Fail while running	$3.2 \cdot 10^{-4}$	Study of ballast system oil tanker Veritec report 85-3410
- Fail to start (per demand)	$10^{-2}$	OREDA

Figure B.2: RABL datasheet

Description of unit		Description of failure				Effect of failure			Risk		
Item	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the subsystem	On the system function	Failure mode classification IEC61508	Frequency class	Consequence class	RPN
<b>Ballast tank valves</b>											
	Open water flow	Closed	FTO Valve fail to open on command	Actuator failure	Hidden	Ballast tank closed	Tank cannot be ballasted/deballasted	DU	2	5	7
		Closed	ST Spurious trip valve opening	Solenoid failure	Evident	Ballast tank open	Tank may be unintentionally ballasted/deballasted	DD	2	4	6
		Closed	LCP Leakage in closed position	Valve seat erosion	Evident	Ballast tank leaking both directions	Tank may be unintentionally ballasted/deballasted	DD	2	3	5
	Close water flow	Open	FTC Valve fail to close on command	Solenoid failure	Hidden	Ballast tank open	Tank may be unintentionally ballasted/deballasted	DU	2	4	6
		Open	ST spurious trip valve closure	Solenoid failure	Evident	Ballast tank closed	Tank cannot be ballasted/deballasted	DD	1	5	6
<b>Pump room valves</b>											
	Open water flow	Closed	FTO Valve fail to open on command	Actuator failure	Hidden	Pipe section closed	Pipe section unavailable	DU	2	4	6
		Closed	ST Spurious trip valve opening	Solenoid failure	Evident	Pipe section open	Uncontrolled flow pattern	DD	2	3	5
		Closed	LCP Leakage in closed position	Valve seat erosion	Evident	Pipe section leaking both directions	Uncontrolled flow pattern	DD	2	3	5
	Close water flow	Open	FTC Valve fail to close on command	Solenoid failure	Hidden	Pipe section open	Uncontrolled flow pattern	DU	2	3	5
		Open	ST spurious trip valve closure	Solenoid failure	Evident	Pipe section closed	Pipe section unavailable	DD	2	4	6
<b>Seachest valves</b>											
	Open water flow	Closed	FTO Valve fail to open on command	Actuator failure	Hidden	Seachest closed	Seachest function unavailable	DU	2	5	7
		Closed	ST Spurious trip valve opening	Solenoid failure	Evident	Seachest open	Uncontrolled flow pattern	DD	2	4	6
		Closed	LCP Leakage in closed position	Valve seat erosion	Evident	Seachest leaking	Uncontrolled flow pattern	DD	2	4	6
	Close water flow	Open	FTC Valve fail to close on command	Solenoid failure	Hidden	Seachest open	Uncontrolled flow pattern	DU	2	5	7
		Open	ST spurious trip valve closure	Solenoid failure	Evident	Pipe section closed	Seachest function unavailable	DD	2	4	6
<b>Discharge valves</b>											
	Open water flow	Closed	FTO Valve fail to open on command	Actuator failure	Hidden	Discharge closed	Discharge function unavailable	DU	2	5	7
		Closed	ST Spurious trip valve opening	Solenoid failure	Evident	Discharge open	Uncontrolled flow pattern	DD	2	4	6
		Closed	LCP Leakage in closed position	Valve seat erosion	Evident	Discharge leaking	Uncontrolled flow pattern	DD	2	4	6
	Close water flow	Open	FTC Valve fail to close on command	Solenoid failure	Hidden	Discharge open	Uncontrolled flow pattern	DU	2	4	6
		Open	ST spurious trip valve closure	Solenoid failure	Evident	Discharge closed	Discharge function unavailable	DD	2	5	7

Figure B.3: FMECA of the ballast system valves

Item	Description of unit		Description of failure			Effect of failure		Failure mode classification IEC61508	Risk			
	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the subsystem	On the system function		Frequency class	Consequence class	RPN	
Ballast pump												
	Pump water	Off	Fail to start on demand	Pump motor failure	Hidden failure	Pump function unavailable	Reduced ballasting/deballasting function	DU	1	5	6	
		Off	Spurious trip pump start	Motor control failure	Evident failure	Pump function activated	Uncontrolled flow pattern	SD	1	3	4	
		On	Spurious trip stop	Motor control failure	Evident failure	Pump function unavailable	Reduced ballasting/deballasting function	DD	1	5	6	
		On	Failure during operation	No control signal	Evident failure	Pump function unavailable	Reduced ballasting/deballasting function	DD	1	5	6	
		On	Failure to stop on demand	Motor control failure	Evident failure	Pump function activated	Uncontrolled flow pattern	SD	1	3	4	
Ballast control logic	Provide electric control signals	Standby	Failure to signal valve on demand	Control logic failure	Hidden failure	Valve operation unavailable	Loss of valve control	DU	1	5	6	
			Failure to signal pump on demand	Control logic failure	Hidden failure	Pump function unavailable	Loss of pump control	DU	1	5	6	
			ST spurious trip signal valve	Control logic failure	Evident failure	Uncontrolled valve operation	Loss of valve control	DD	1	5	6	
			ST spurious trip signal pump	Control logic failure	Evident failure	Uncontrolled pump operation	Loss of pump control	DD	1	4	5	
		Active	Failure to stop valve signal on demand	Faulty feedback from valves	Hidden failure	Uncontrolled valve operation	Loss of valve control	DU	1	5	6	
			Failure to stop pump signal on demand	Faulty feedback from pumps	Hidden failure	Uncontrolled pump operation	Loss of pump control	DU	1	3	4	

Figure B.4: FMECA of the ballast system pumps and control system

Description of unit		Description of failure				Effect of failure			Risk			
Item	Function	Operational mode	Failure mode	Failure cause	Detection of failure	On the subsystem	On the system function	Failure mode classification IEC61508	Frequency class	Consequence class	RPN	
Main electric power generator	Provide electric power	On	Failure during operation	Generator failure	Evident failure	Main electric power unavailable	Loss of main electric power for ballasting operations	DD	1	5	6	
			Failure to stop on demand	Generator control failure	Evident failure	Main electric power active	Main electric power available for ballasting operations	SU	1	1	2	
			Spurious trip stop	Generator control failure	Evident failure	Main electric power unavailable	Loss of main electric power for ballasting operations	DD	1	1	5	6
			Fail to start on demand	Generator failure	Hidden failure	Main electric power unavailable	Loss of main electric power for ballasting operations	DU	1	1	5	6
			Spurious trip start	Generator control failure	Evident failure	Main electric power active	Main electric power available for ballasting operations	SD	1	1	1	2
Emergency backup generator	Provide electric power	Standby	Fail to start on demand	Generator failure	Hidden failure	Backup electric power unavailable	Loss of backup electric power for ballasting operations	DU	1	5	6	
			Spurious trip start	Generator control failure	Evident failure	Backup electric power available	Backup electric power available for ballasting operations	SD	1	1	1	2
			Spurious trip stop	Generator control failure	Evident failure	Backup electric power unavailable	Loss of backup electric power for ballasting operations	DD	1	1	5	6
			Failure during operation	Generator failure	Evident failure	Backup electric power unavailable	Loss of backup electric power for ballasting operations	DD	1	1	5	6
			Failure to stop on demand	Generator control failure	Evident failure	Backup electric power available	Backup electric power available for ballasting operations	SD	1	1	1	2
UPS	Provide electric power	Standby	FTS Accumulator fail to activate	UPS failure	Hidden failure	Backup UPS power unavailable	Loss of backup electric power for ballast control systems	DU	1	5	6	
			Accumulator failure during operation	UPS failure	Evident failure	Backup UPS power unavailable	Loss of backup electric power for ballast control systems	DD	1	1	5	6
			Failure during operation	Hydraulic pump failure	Evident failure	Main hydraulic power unavailable	Loss of main hydraulic power for ballasting operations	DD	1	1	5	6
Main hydraulic power generator	Provide hydraulic pressure	On	Failure to stop on demand	Control signal failure	Evident failure	Main hydraulic power available	Main hydraulic power available for ballasting operations	SD	1	1	2	
			Spurious trip stop	Control signal failure	Evident failure	Main hydraulic power unavailable	Loss of main hydraulic power for ballasting operations	DD	1	1	5	6
			Fail to start on demand	Hydraulic pump failure	Hidden failure	Main hydraulic power unavailable	Loss of main hydraulic power for ballasting operations	DU	1	1	5	6
			Spurious trip start	Control signal failure	Evident failure	Main hydraulic power available	Main hydraulic power available for ballasting operations	SD	1	1	1	2
			Failure during operation	Accumulator failure	Hidden failure	Backup hydraulic power unavailable	Loss of backup hydraulic power for ballasting operations	DU	1	1	5	6
Hydraulic accumulator	Provide hydraulic pressure	Standby	FTS Accumulator fail to activate	Accumulator failure	Hidden failure	Backup hydraulic power unavailable	Loss of backup hydraulic power for ballasting operations	DU	1	5	6	
			Accumulator failure during operation	Accumulator failure	Evident failure	Backup hydraulic power unavailable	Loss of backup hydraulic power for ballasting operations	DD	1	1	5	6
			Failure during operation	Accumulator failure	Evident failure	Backup hydraulic power unavailable	Loss of backup hydraulic power for ballasting operations	DD	1	1	5	6

Figure B.5: FMECA of the ballast system utilities

Component	Voting	Case 1		Case 2		Case 3		Case 4		Case 5	
		PFD per component	System PFD	PFD per component	System PFD	PFD per component	System PFD	PFD per component	System PFD	PFD per component	System PFD
Ballast control logic + I/O	1001	4,40E-03	4,40E-03	4,40E-03	4,40E-03	4,40E-03	4,40E-03	4,40E-03	4,40E-03	4,40E-03	4,40E-03
Tank valve + solenoid/pilot	1001	1,00E-02	1,00E-02	6,57E-03	6,57E-03	3,29E-03	3,29E-03	1,10E-03	1,10E-03	3,29E-03	3,29E-03
Pumps	1002	9,40E-04	5,00E-05	9,40E-04	5,00E-05	9,40E-04	5,00E-05	9,40E-04	5,00E-05	9,40E-04	5,00E-05
Ringmain/manifold valve + solenoid/pilot	1001	1,00E-02	1,00E-02	6,57E-03	6,57E-03	3,29E-03	3,29E-03	1,10E-03	1,10E-03	3,29E-03	3,29E-03
Discharge valve + solenoid/pilot	1001	1,00E-02	1,00E-02	6,57E-03	6,57E-03	3,29E-03	3,29E-03	1,10E-03	1,10E-03	3,29E-03	3,29E-03
Total function PFD	-	-	0,034	-	0,024	-	0,014	-	0,0077	-	0,014
Corresponding to SIL level:			SIL 1		SIL 1		SIL 1		SIL 2		SIL 1

Figure B.6: Calculation of minimum SIL requirements

Ballast tank configuration, pumps and valves	Component type	OLF070 component classification proposal	OLF070 comment	$\lambda$ DU (per 10 <sup>6</sup> h)	Datasource $\lambda$ DU	$\beta$ -factor	Datasource $\beta$ -factor
Ballast tank valve	Hydraulically operated valve	Deluge valve (Valve + solenoid/pilot)	DU is fail to open, control signal loop normally de-energized	3	PDS data handbook 2010. Table 5. "Deluge valve (complete)"	3 %	PDS data handbook 2010. Table 7. "Deluge valve"
Pump room valve	Hydraulically operated valve	Deluge valve (Valve + solenoid/pilot)	DU is fail to open, control signal loop normally de-energized	3	PDS data handbook 2010. Table 5. "Deluge valve (complete)"	3 %	PDS data handbook 2010. Table 7. "Deluge valve"
Seachest valve	Hydraulically operated valve	Deluge valve (Valve + solenoid/pilot)	DU is fail to open, control signal loop normally de-energized	3	PDS data handbook 2010. Table 5. "Deluge valve (complete)"	3 %	PDS data handbook 2010. Table 7. "Deluge valve"
Discharge valve	Hydraulically operated valve	Deluge valve (Valve + solenoid/pilot)	DU is fail to open, control signal loop normally de-energized	3	PDS data handbook 2010. Table 5. "Deluge valve (complete)"	3 %	PDS data handbook 2010. Table 7. "Deluge valve"
Ballast pump	Electric centrifugal pump	Fire water pump (Centrifugal)	DU is fail to start, not including fail while running. Includes power transmission, pump unit, control and monitoring, lubrication system and misc.	Not available. Fail to start on demand = 9,4 per 10 <sup>4</sup> h	OLF: OREDA 2002, 1.3.1.18 The failure rate includes only the critical failure mode "fail to start ("Fail while running" not included).	5 %	OLF070: PDS data
<b>Ballast control system</b>	<b>Component type</b>	<b>OLF070 component classification proposal</b>	<b>OLF070 comment</b>	<b><math>\lambda</math> DU (per 10<sup>6</sup>h)</b>	<b>Datasource <math>\lambda</math> DU</b>	<b><math>\beta</math>-factor</b>	<b>Datasource <math>\beta</math>-factor</b>
Ballast control logic + I/O	Programmable safety system	Programmable safety system - single system		1	OLF070 Table A1. PDS data handbook 2010. Data dossier 5.2.2.1	5 %	PDS data handbook 2010. Table 7. "Programmable safety system"

Figure B.7: Reliability data applicable to ballast systems

Electrical components	Component type	OLF070 component classification proposal	OLF070 comment	$\lambda$ DU (per $10^6$ h)	Datasource $\lambda$ DU	$\beta$ -factor	Datasource $\beta$ -factor
Manual pushbutton	Manual pushbutton	ESD pushbutton		0,4	PDS data handbook 2010. Table 5. "ESD push button"	3 %	PDS data handbook 2010. Table 7. "ESD push button"
Safety relay	Safety relay	Relay		0,2	PDS data handbook 2010. Table 5. "Relay"	3 %	PDS data handbook 2010. Table 7. "Relay"
Isolation relay	Isolation relay	Relay		0,2	PDS data handbook 2010. Table 5. "Relay"	3 %	PDS data handbook 2010. Table 7. "Relay"
MCC shutdown relay	MCC shutdown relay	Relay		0,2	PDS data handbook 2010. Table 5. "Relay"	3 %	PDS data handbook 2010. Table 7. "Relay"
Contactator	Contactator	Relay		0,2	PDS data handbook 2010. Table 5. "Relay"	3 %	PDS data handbook 2010. Table 7. "Relay"
Valve	Valve	ESV/XV incl. Actuator (ex. Pilot) (Emergency Shutdown Valve)		2,1	PDS data handbook 2010. Table 5. "ESV/XV (ex. Pilot)"	3 %	PDS data handbook 2010. Table 7. "ESV/XV (Main valve + actuator)"
Solenoid/Pilot	Solenoid/Pilot	Solenoid		0,9	OLF070 Table A.3.	2%/10%.	OLF 070. 10% for pilot valves on same valve, otherwise 2%.

Figure B.8: Reliability data applicable to ballast systems



Table B.1: Stability incidents reported to the PSA

Date	Facility (Built)	Type	Description	Source
18.12.2000	Transocean Arctic (1986)	Semi sub.	Spurious trip of ballast pumps	1
12.02.1995	Transocean Arctic (1986)	Semi sub.	Spurious trip of ballast pump. Pump overheated.	1
14.06.1995	Transocean Arctic (1986)	Semi sub.	Spurious stop of ballast pump after 1 minute. Fail while running.	1
01.12.1995	Transocean Arctic (1986)	Semi sub.	Unreliable level indicators in ballast tanks. 400-600mt deviation between calculated and observed displacement.	1
18.04.1996	Transocean Wildcat	Semi sub.	Ballast pipe leakage close to seachest valve.	1
13.08.1998	Transocean Prospect	Semi sub.	Failure in automatic ballast tank level indicator	1
27.08.1998	Transocean Prospect	Semi sub.	Ballast control screen frozen image.	1

Table B.2: Stability incidents reported to the PSA

Date	Facility (Built)	Type	Description	Source
21.01.1999	Polar Pioneer	Semi sub.	Overfilling of ballast tanks. Ballast water migration through vent holes	1
09.08.1999	Transocean Wildcat	Semi sub.	Rig list due to forgotten ongoing gravity filling of ballast tank	1
18.02.2000	Transocean Arctic	Semi sub.	Three incident of spurious trip of same ballast pump within 48 hours	1
16.11.2000	Transocean Wildcat	Semi sub.	Water migration into open manhole during ballasting for operational draft	1
22.01.2001	Polar Pioneer	Semi sub.	Failure in ballast tank level indicators	1
23.02.2001	Transocean Wildcat	Semi sub.	Leaking through ballast tank valve in closed position during ballasting for operational draft.	1
10.05.2001	Polar Pioneer	Semi sub.	Valve in ballast system leaking i closed position	1
29.12.2001	Transocean Arctic	Semi sub.	Ballast valve failure during test. Damage to the ringmain line due to sudden water migration	1
05.05.2003	West Alpha	Semi sub.	Ballast tank valve leakage in closed position	1
02.08.2004	Bideford Dolphin	Semi sub.	Ballast tank valve leakage in closed position	1

Table B.3: Stability incidents reported to HSE (UK) 1980-2003

Date	Facility (Built)	Type	Description	Source
1986	N/A	Semi sub.	"A malfunction of the semi's ballast control system caused the rig to list 9 deg. before control was obtained and the uprighted after 90minutes. Five helicopters helicopters flew in in case of evacuation".	2
1990	N/A	Semi sub.	"Electrical failure of power supply to ballast control system. Ac output power inverter on ups tripped offline, battery backup to to systems feeds through the inverter and was not able to come in to keep system running. Three seperate operator stations were without power for approx. 8 min. until UPS was reset. No observable damage was done to UPS system, nor can fault be duplicated. Ballast control system went into failsafe condition preventing loss of trim or stability. System was restored to full operational capability."	2
1999	N/A	Floating production (details unknown)	Two gas alarms in production system."Possible software anomalies also caused GT shutdown and starting failures on emergency power generation. During the period of power loss deluge activation occurred in a number of fire zones due to loss of air pressure and a list of 5 degrees to Starboard developed due to the free flow of the ballast through open valves in the system. At no time was the vessel in stability at risk and would have stabilized at around 6-8 degrees once levels in the ballast tanks had settled."Actions:"Manual intervention by emergency teams to close ballast valves at local controls."	2
2000	N/A	Semi sub.	During exploratory drilling."Control of the starboard ballast desk was lost and all the remote operated valves went to open position."Series of valves closed by manual intervention. Rig trimmed to 6 degrees. Regained control. Emergency scrambling. Coastguard informed.	2
2000	N/A	Semi sub.	Rig started listing. "On checking ballast panel noticed all valves showing open & closed"A burst water line had short circuited the starboard emergency ballast control panel. Water intake stopped. Rig list 3 degrees. Starboard ballast system stabilized.Rig trimmed using port ballast system.	2

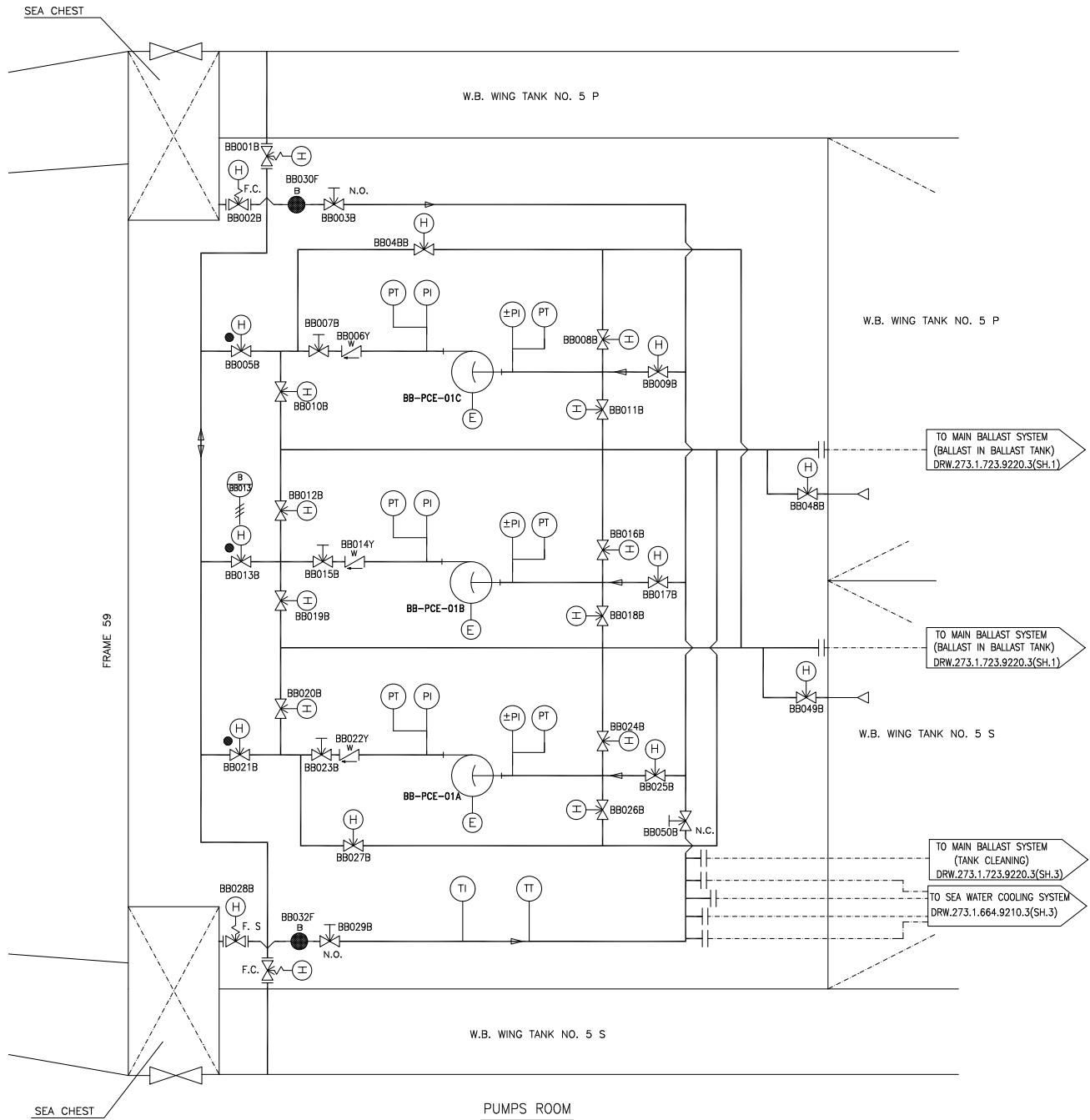


Figure B.9: Foinaven ballast system flow diagram 2

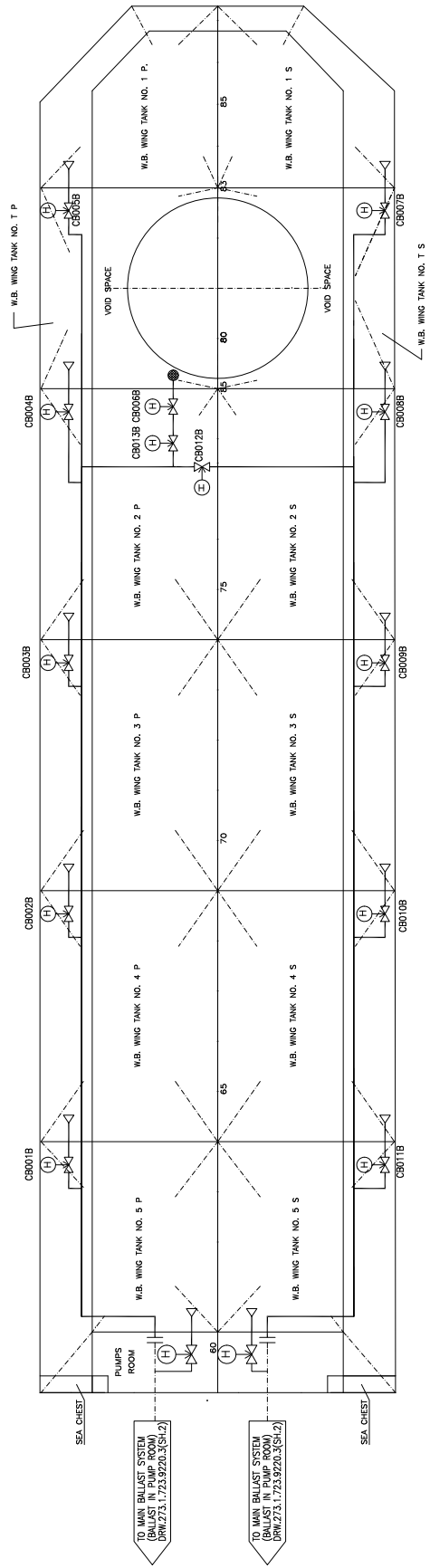


Figure B.10: Foinaven ballast system flow diagram 1