NTNU – Trondheim
Norwegian University of
Science and Technology

Provision and Updating of Estimates of Reliability Parameters for Use in Reliability Analyses of Safety-Instrumented Systems

Magnus Woll Bjartnes

Master of Science in Product Design and Manufacturing
Submission date: June 2012
Supervisor: Marvin Rausand, IPK

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

NTNU

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

Date
2012-01-12

Our reference
MAL/LMS

MASTER THESIS
2012
for
stud. techn. Magnus Woll Bjartnes

PROVISION AND UPDATING OF ESTIMATES OF RELIABILITY PARAMETERS FOR USE IN RELIABILITY ANALYSES OF SAFETY-INSTRUMENTED SYSTEMS

(Fremskaffelse og oppdatering av estimat for pålitelighetsparametere til bruk i analyse av instrumenterte sikkerhetssystemer)

This master thesis is related to reliability assessment of instrumented safety barriers (also called safety-instrumented systems) on a new floating production, storage, and offloading (FPSO) vessel. The reliability requirements for functions performed by the safety-instrumented systems are set according to IEC 61508 and OLF 070. In these standards, safety integrity level (SIL) is used as the main reliability measure. The operator of the FPSO is currently using a general system for monitoring the performance of technical barriers – a *barrier performance dashboard*, in which SIL requirements and SIL performance monitoring have not yet been implemented.

The basis for this master thesis is the operator's need to align the SIL follow-up with the more general follow-up of technical barriers in the barrier performance dashboard. The scope of this master thesis goes, however, beyond this specific needs and aim to investigate some of the more fundamental issues concerning SIL follow-up – and especially related to provision and updating of estimates of reliability parameters.

In more specific terms, this master thesis aims to give more insight and knowledge about the following issues:

- Assumptions have been made in the design phase about the reliability performance of the safety instrumented functions. What are the pros and cons of using manufacturer data instead of historical data, for example, from OREDA for this purpose? How can these data be combined in a meaningful way?
- Some equipment is tested regularly, in addition to being operated more or less regularly, for example, daily or once a month. How can data from operation and testing be combined with the historical/manufacturer data to provide updated estimates of reliability parameters?
- There is a close link between test intervals and the reliability of a safety instrumented function. What types of analyses and input data are required for decision-making regarding test intervals?

- Reliability data is often collected for identical or similar components. However, the population within a single component type may be low on single FPSO. How can the confidence in reliability estimates be determined, taking into account the uncertainty about the results?

The blowdown system installed on the FPSO is used as a case study to demonstrate the application of the approach to be suggested.

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 11th 2012.

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

Responsible supervisor at NTNU: Professor Marvin Rausand
Phone: 73 59 25 42
E-mail: marvin.rausand@ntnu.no

Co-supervisors at NTNU: Professor Mary Ann Lundteigen
Phone: 73 59 71 01
Mobile phone: 930 59 365
E-mail: mary.a.lundteigen@ntnu.no

Supervisor in Teekay Petrojarl: Morten Søndrol, Senior Technical Safety Engineer
Mobile phone: 928 50 630
E-mail: morten.sondrol@teekay.com

**DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING**

Per Schjølberg
Associate Professor/Head of Department

Marvin Rausand
Responsible Supervisor

Preface

This is a Master's thesis in RAMS at NTNU, on the Department of Production and Quality Engineering. The thesis is carried out in cooperation with Teekay Petrojarl, during the spring semester of 2012. The idea to the topic was launched by Teekay, as there was certain issues related to the topic they wanted investigated and discussed.

Trondheim, 2012-06-10

Magnus Woll Bjartnes

Acknowledgment

I would like to thank Teekay Petrojarl for their positive attitude when I made contact regarding a possible collaboration, and for excellent follow-up during the semester. I would especially thank my supervisor at Teekay, Morten Søndrol, for his quick responses and useful inputs.

Next, I would like to thank my supervisor at Department of Production and Quality Engineering, Marvin Rausand. With his excellent guidance during the semester, the work with the thesis has turned out to be interesting, enjoyable, and very instructive. I will not hesitate on recommending him as supervisor for future students.

M. W .B.

Summary and Conclusions

Safety-instrumented systems are implemented in the industry to prevent accidents to occur and escalate. The blowdown system on a oil production ship is one example of such system. If a fire breaks out on the ship, the blowdown system's role is to remove the flammable gases from the current production lines on the ship. This is done by opening of the blowdown valves, that are installed on the different production lines. In this thesis, the blowdown system on a new Teekay ship, and espesically the valves, are applied as case. Since such systems are imporant to maintain the safety on the installation, they are subject to strict reliability performance requirements.

Before the SIS is put into operation, it is required to state a certain reliability target for the system. At present, Teekay estimates the reliability based on generic reliability data, or reliability data provided from the manufacturer of the equipment. There are uncertainties related to both of these sources. Generic reliability data are collected from different installations where the equipment are operating under different conditions and environment. The reliability is affected by its surroundings, and the generic data then reflects the average reliability in the entire industry. This implies that this data may not be accurate for equipment on a new ship with brand new equipment.

The manufacturer data, on the other hand are tested under controlled conditions, typically in a laboratory. This implies that the reliability reflects how the equipment performs when it is applied just as intended by the manufacturer. In industry, the equipment will most likely be handled more thoughly, and failures can be introduced during for example, maintenance.

This thesis suggests a new way of predicting the reliability. The estimated reliability is based on the mentioned sources, in addition to reliability data collected from the other ships in the Teekay fleet. By using expert opinions (e.g., opinions from operators and engineers), these sources are weighted to create a best possible estimate of the reliability. From these estimates, a probability distribution is constructed. This distribution states how likely the different values of the reliability are, where the thesis suggests to choose a rather conservative value even if it is not the most likely one.

After the system is put into operation, failure data becomes available from operation and testing. This data constitutes a reliability estimate based on operational data alone. Since safety

systems are designed to be highly reliable, few failures occur and this estimate is uncertain. Because of this, the thesis provides a method on how the operational data can be included in the probability distribution constructed in the design phase. As more operational data become available, the less is the contribution from the design phase assumptions.

If it comes to a point where the operational data proves that the reliability of the system differs significantly from what was assumed, it can be assessed whether the regular testing of the system can or should be changed. This thesis suggests that only operational data should be applied to decide such a change. A point which indicates that a sufficient amount of operational data is collected to trust this estimate solely, is provided.

Teekay performs annual testing on the entire blowdown system where the results are recorded and applied in further reliability calculations. In addition to these test, they perform monthly manual testing on the blowdown valves. This is because the valves fail more often than the other parts, and the operators on the ship want to be sure that they are functioning. It is shown how these tests influence on the average availability of the valves, and it is discussed how these tests can be applied as a means to increase the length between the more comprehensive annual tests.

The last part of the thesis investigates the uncertainty aspects related to the provided methods, models, and other relevant aspects in the process of collecting and applying reliability data. It is shown that there is a high degree of uncertainty related to all the aspects. Application of generic reliability data is a high contributor to uncertainty. The thesis provides a method on how the generic data can be compared to the data collected in Teekay. This comparison aims at providing a factor which reflects how the specific conditions on Teekay ships influences the reliability, compared to the average reliability found in generic data sources.

Sammendrag og konklusjon (Norsk)

Instrumenterte sikkerhetssystemer (SIS) er implementert i industrien for å forebygge og forhindre at ulykker oppstår og eskalerer. Et utblåsningssystem på et skip som foredler olje, er et eksempel på et slikt system. Hvis en brann bryter ut på et slikt skip, er utblåsningssystemets rolle å fjerne de brennbare gassene fra de aktuelle produksjonsrørene på skipet. Dette gjøres ved å åpne utblåsningsventilene som er installert på de respektive produksjonsrørene. I denne rapporten er et utblåsningssystem på et nytt Teekay-skip, og da spesielt utblåsningsventilene, brukt som studieobjekt. Ettersom slike systemer er viktige for å opprettholde sikkerheten på installasjonen, er de underlagt strenge pålitelighetskrav.

Før en SIS er satt i drift, skal det settes et visst pålitelighetskrav på systemet. Per dags dato estimerer Teekay påliteligheten basert på generisk pålitelighetsdata, eller pålitelighetsdata fra leverandøren av utstyret. Det er usikkerhet knyttet til begge disse kildene. Generisk pålitelighetsdata er samlet fra forskjellige installasjoner hvor utstyret opererer under ulike forhold og miljø. Påliteligheten på utstyr påvirkes av sine omgivelser, og den generiske dataen gjenspeiler derfor den gjennomsnittlige påliteligheten i hele industrien. Dette innebærer at denne dataen ikke nødvendigvis er nøyaktig for utstyr på et nytt skip som har helt nytt utstyr.

Leverandørdataen er basert på testing av utstyret under kontrollerte forhold, typisk i et laboratorium. Dette innebærer at påliteligheten reflekterer hvordan utstyret oppfører seg når det er brukt akkurat slik det er tiltenkt fra leverandøren. I industrien vil utstyret mest sannsynlig bli behandlet tøffere enn tiltenkt, og feil kan bli introdusert, for eksempel under vedlikehold.

Denne rapporten foreslår en ny måte å vurdere påliteligheten. Den anslåtte påliteligheten er basert på nevnte kilder, i tillegg til pålitelighetsdata samlet fra andre skip i Teekays flåte. Ved å bruke ekspertvurderinger (for eksempel meninger fra operatører og ingeniører) kan de forskjellige kildene vektes for å bestemme et best mulig estimat av påliteligheten. Fra disse estimatene lager man en sannsynlighetsfordeling. Denne fordelingen angir hvor sannsynlig de forskjellige verdiene av påliteligheten er, hvor denne rapporten foreslår å velge en relativt konservativ verdi, selv om denne ikke er mest sannsynlig.

Etter at systemet er satt i drift, blir feildata tilgjengelig fra drift og testing. Denne dataen utgjør et pålitelighetsestimat utelukkende basert på operasjonell data. Ettersom sikkerhetssyste-

mer er designet for å være pålitelige, vil få feil oppstå og dette estimatet er usikkert. På grunn av dette, tilbyr denne rapporten en metode på hvordan operasjonell data kan inkluderes i pålitelighetsfordelingen etablert i designfasen. Ettersom mer operasjonell data blir tilgjengelig, blir det mindre bidrag fra designfase-antagelsene.

Dersom det kommer til et punkt hvor den operasjonelle dataen beviser at påliteligheten av systemet er betydelig annerledes enn hva som var antatt, kan det vurderes om tiden mellom de regelmessige testene av systemet, kan eller bør endres. Denne rapporten anbefaler at bare operasjonell data skal brukes for å bestemme en slik forandring. Et punkt som indikerer at tilstrekkelig mye operasjonell data er samlet, til at dette estimatet kan brukes, er foreslått. Teekay utfører årlig testing på hele utblåsningssystemet hvor resulatene er registrert og brukt i videre pålitelighetskalkulasjoner. I tillegg til disse testene, utfører de månedlig manuell testing på utblåsningsventilene. Dette fordi ventilene feiler oftere en andre deler, og opereratørene på skipet vil være sikre på at de fungerer. Det er vist hvordan disse testene påvirker på den gjennomsnittelige tilgjengeligheten til ventilene, og det er diskutert hvordan disse testene kan brukes som et påskudd for å øke lengden mellom de mer omfattende årlige testene.

Den siste delen av rapporten identifiserer og diskuterer usikkerhetsaspektene relatert til metodene, modellene og andre relevante aspekter i samling og bruk av pålitelighetsdata. Det er vist at det er en høy grad av usikkerhet relatert til alle aspektene. Bruk av generisk pålitelighetsdata er en stor bidragsyter til usikkerhet. Rapporten tilbyr en metode på hvordan generisk data kan sammenlignes med dataene samlet i Teekay. Denne sammenligningen har som mål å finne en faktor som reflekterer hvordan de spesifikke forholdene på Teekay-skip påvirker påliteligheten sammenlignet med den gjennomsnittlige påliteligheten funnet i generiske datakilder.

Contents

Chapter 1

Introduction

1.1 Background

Safety-instrumented systems (SIS) are used to detect hazardous events and mitigate their consequences in a wide range of applications. The term *instrumented* implies that the system consists of one or more electrical, electronic and/or programmable electronic components. Since SIS are safety-critical barriers where critical failures in emergancy situations can lead to fatal accidents, there are strict requirements to their reliability performance. IEC 61508 (2010) is at present the key standard dealing with reliability requirements of SIS. The standard is performance-based and generic, and has made the basis for more application specific standards. IEC 61511 (2003) is one example, which is highly relevant on the Norwegian shelf since it deals with SIS in the process industry. Especially IEC 61508 has been critized for being comprehensive and complicated to interpret and apply. Due to this, the Norwegian Oil Industry Association (OLF) has developed OLF 070 (2004) which is a guideline on the application of the mentioned standards in the Norwegian petroleum industry.

A SIS comprises three different subsystems. Input elements (e.g., pressure transmitters, detectors), logic solver (e.g., programmable logic solver) and final elements (e.g., valves). A SIS performs one or more safety-instrumented functions (SIF). For each SIF, a certain safety integrity level (SIL) is specified stating its reliability in terms of the average *Probability of Failure on Demand* (PFD). PFD is the reliability measure for low demand systems that according to IEC 61508, are demanded less then once per year. SIS that experiences demands more often than this, are referred to as high demand systems. The reliability measure of high demand systems are *Probability of Failure per Hour* (PFH). There are four different SIL levels where SIL4 is most reliable, and SIL1 is less reliable. Each SIL corresponds to a certain PFD or PFH interval. The blowdown system is a typical low demand system, and PFD is the relevant measure.

A SIS goes through different life-cycle phases, starting with the design/concept phase, before it is implemented and applied in normal operation. The predicted SIL is the SIL assumed in the design phase, while the achieved SIL is determined from testing in the operational phase. The predicted SIL can be based on a variety of sources, where generic reliability data or manufacturer specific reliability data probably are the most common to apply. There are several issues related to the accuracy of both of these sources. This can imply that use of the data can lead to unrealistic reliability estimates that does not reflect the reality.

A SIS is constructed to be a highly reliable system. This implies that sparse failure data are collected through the operational phase and little confidence in the empricial data from the operational phase can be obtained. This thesis applies the blowdown system on a Teekay FPSO which now is under construction, as case when reliability aspects related to these issues are investigated. Teekay performs annual proof testing of the blowdown system. In addition, they perform monthly manual testing of the blowdown valves which affects and complicates the average reliability aspects.

1.2 Objectives

With the issues from previous section in mind, the objectives of this thesis are:

1. Identify and discuss the problems related to the use of manufacturer data and historical data in the design phase of a SIS.

2. Provide a method and discussion on how failure data from operation and testing can be combined with prior reliability information applied in the design phase of the SIS.

3. Investigate and discuss how the manual tests, together with the proof tests, affect the reliability of the blowdown valves.

4. Investigate and discuss necessary aspects of considiration before the proof test interval can be changed.

5. Discuss the uncertainty related to the methods and the underlying factors provided in the thesis. Provide a method on how to decrease the degree of uncertainty in the estimates determined from the methods in this thesis.

These five objectives realizes the tasks given in the assignment text.

1.3 Limitations

The main topic of this thesis is reliability of SIS. Because of this there might be some inaccuracies when it comes to technical descriptions, or other descriptions that does not directly have anything to do with reliability aspects.

When discussing histrorical data sources, the focus is on OREDA. This is because Teekay apply OREDA as it main source to historical reliability data.

1.4 Structure of the Report

Chapter 2 introduces and discusses the fundamental Bayesian theory necessary to understand the rest of the thesis. Chapter 3 describes the blowdown system applied as case in the thesis. It describes how testing is executed on the system. Chapter 4 presents previous work related to the topic of the thesis. Chapter 5 investigates and discusses the reliability aspects of the blowdown system, and especially the valves. Chapter 6 investigates and discusses relevant sources to the prior distribution. The chapter discusses the issues related to historical data sources, and reliability data provided by the manufacturer. Chapter 7 suggests and discusses a new method on how to develop the prior distribution. Chapter 8 investigates and discusses fundamental factors that must be the basis if the proof test interval is assessed. Chapter 9 investigates and discusses relevant contributors to uncertainty in the different aspects of the thesis.

Chapter 2

Bayesian Theory

In this thesis the Bayesian concept and way of thinking are used to update generic reliability estimates applied in the concept and design phases of the SIS, to a more specific number as we gain data and knowledge from testing and potential activation of the SIS in the SIS follow-up phase. This chapter introduce and discuss the relevant concepts that are applied later in the thesis.

2.1 The Bayesian Idea and Approach

According to frequentist statistics, probability of an event is determined when the same action is repeated unlimited, or at least very many times. In our case, the number of failures on blowdown valves (BDVs) divided by the sum of operating hours. A SIS is designed to be highly reliable due to its role as a vital safety barrier, and few failures therefore occur even in a relative long time period. Obtaining an accurate estimate based on operational data from the SIS follow-up phase alone, therefore requires test data from a high number of the same components within the same environement collected over years of operation. This can be realized for some components within a SIS such as fire detectors which are installed in great numbers at many industrial installations. For other components of a lot less number (e.g., BDVs), an adequate accurate estimate will most likely never be achieved before decommisioning of the entire system. In Bayesian statistics, the uncertainties in the value of the parameter are expressed by probability distributions. This differs from the frequentist philosophy where no uncertainty about the parameter is included. As stated in Siu and Kelly (1998), the frequentists mean that the parameter has a true, albeit unknown value. In other words, the BDVs have a inherent failure rate which can be seen as a property of the BDVs. Since much data is needed to converge to this true value, the frequentist philosophy is not well suited for such cases where emperical data is sparse.

Obviously, it is of importance to have as accurate reliability estimates as possible through the life-cycle of the SIS. Only in that way it can be verified that the SIS performs within the intended SIL interval. What makes the Bayesian approach well suited for this purpose is that it allows us to update the reliability data continously as new information from testing becomes available. In other words, we use generic reliablity data, expert judgement, experience with related systems, or a combination of these as basis while new data are used to update the initial assumption of the reliability used in the concept and design phase. Based on this more or less subjective knowledge, we construct a *prior distribution* which expresses the initial assessment of the failure rate. Bayes formula expresses the conditional probability of an event A occuring, given that B has occured. The formula combines prior knowledge with current data to create a *posterior distribution*. In this thesis, the approach to the problem is to express the probability density of the failure rate given our knowledge in terms of accumulated test data, which mathematically is given in equation 2.1, which is Bayes formula in terms of the probability density function. $p(D|\lambda)$ is the probability density function for the observed data D given the unknown parameter λ. $\pi(\lambda)$ is the *prior distribution* for λ. $\pi(\lambda|D)$ is the *posterior distribution* for λ given that the data D has been observed. As we see from the equation, $p(D)$ in the denominator can be further expanded by *the law of total probability*.

$$\pi(\lambda|D) = \frac{p(D|\lambda)\cdot\pi(\lambda)}{p(D)} = \frac{p(D|\lambda)\cdot\pi(\lambda)}{\int p(D|\lambda)\cdot\pi(\lambda)\mathrm{d}\lambda} \tag{2.1}$$

2.2 Gamma Distribution

Both the *prior distribution* and the *posterior distribution* express how likely various values of the failure rate, are. The starting assessment given in the *prior* is revised as new data becomes available and we derive the *posterior*. Siu and Kelly (1998) states that arbitary combinations of likelihood functions and prior distributions, equation 2.1 must be evaluated numerically. Certain combinations will analytically result in posterior distributions which are of the same form as the prior distribution. This is refered to as *conjugate pairs*. Poisson likelihood - gamma prior pair is one example of such pair frequently applied in reliability problems. As Hamada et al. (2008) states, conjugate prior distributions can make posterior analysis easy because they eliminate the need to numerically determine normalizing constants. In this thesis, the focus will lay upon valves in the blowdown system of a FPSO. According to Rausand and Hoyland (2004), valve failures are assumed to occur according to a homogeneous Poisson process. The number of valve failures, $N(t)$, during an accumulated time t in service thus has the Poisson distribution in equation 2.2, where λ represents a realization of a random variable Λ. This equation is refered to as the *likelihood function*.

$$p(N(t) = n|\Lambda = \lambda) = \frac{(\lambda t)^n}{n!} e^{-\lambda t} \tag{2.2}$$

Equation 2.2 is used as input to equation 2.1 when constructing a probability density function. The Gamma distribution is used to describe the uncertainty in λ. The gamma prior density takes the form

$$f_\Lambda(\lambda) = \frac{\beta}{\Gamma(\alpha)} (\beta\lambda)^{\alpha-1} e^{-\beta\lambda} \tag{2.3}$$

The shape of the density of Λ can be determined by a sensible choice of the parameters α and β. *Parameterization* is a process to determine proper parameters to construct a realistic distribution. β corresponds to a *rate parameter*, which is the inverse of the *scale parameter*. The larger the *scale parameter*, the more the distribution spread out. For the gamma distribution, the mean and the variance are given by

$$\mathrm{E}(\Lambda) = \frac{\alpha}{\beta} \tag{2.4}$$

$$\mathrm{Var}(\Lambda) = \frac{\alpha}{\beta^2} \tag{2.5}$$

The mean value and the variance are known values in our case. Our goal is to determine the α and β so the distribution can be constructed. By combinding equation 2.4 and 2.5 we find that $\beta = \frac{\mathrm{E}(\Lambda)}{\mathrm{Var}(\Lambda)}$ and $\alpha = \beta \cdot \mathrm{E}(\Lambda)$. As we can see, both α and β can be determined by values of the mean and variance.

A property of conjugated priors is that the posterior distribution will have the same form as the prior distribution. We know that the prior distribution is determined by α and β. It can be shown(e.g. see Rausand and Hoyland (2004)), that the posterior distribution simply can be determined by substituting α and β with $\alpha + n$ and $\beta + t$ to receive the posterior distribution from the prior distribution given in equation 2.3. Thus the posterior will have the mathematical form as in equation 2.6.

$$f_\Lambda(\lambda|(n,t)) = \frac{\beta'}{\Gamma(\alpha')}(\beta'\lambda)^{\alpha'-1}e^{-\beta'\lambda} \tag{2.6}$$

where $\alpha' = \alpha + n$ and $\beta' = \beta + t$. By combining equation 2.3 and 2.2, with Bayes theorem given in equation 2.1, we obtain a more specific posterior distribution tailored for our specific application given in equation 2.7. Equation 2.7 shows how the different equations fits into Bayes's theorem.

$$f_\Lambda(\lambda|(n,t)) = \frac{\left[\frac{(\lambda t)^n}{n!}e^{-\lambda t}\right]\cdot\left[\frac{\beta}{\Gamma(\alpha)}(\beta\lambda)^{\alpha-1}e^{-\beta\lambda}\right]}{\int_0^\infty \left[\frac{(\lambda t)^n}{n!}e^{-\lambda t}\right]\cdot\left[\frac{\beta}{\Gamma(\alpha)}(\beta\lambda)^{\alpha-1}e^{-\beta\lambda}\right]\mathrm{d}\lambda} \tag{2.7}$$

2.3 Credibility Interval

Credibility interval is the Bayesian analogue to a confidence interval (Rausand and Hoyland, 2004). Confidence interval is applied in frequentist statistics. As earlier discussed, frequentists consider the parameter to be a fixed , but unknown value. This implies that a confidence interval is calculated only on the basis of this value. A Bayesian credibility interval on the other hand, incorporates information from from the prior distribution into the estimate. E.g., if the posterior distribution of the failure rate λ is determined, and the probability that $a \le \lambda \le b$ is 90 % then $[a,b]$ is the 90 % credibility interval for λ. To state this, it must be noted that a and b must be given as stochastic variables. A 95 % one-sided credibility interval for λ can then be expressed mathematically as in equation 2.8. λ_{95} is the 95th percentile in the distribution of λ. The 5th percentile, λ_{05}, can be found the same way. λ_{05} and λ_{95} then constitute a 90 % credibility interval for λ.

$$0.95 = \int_0^{\lambda_{95}} \frac{\beta'}{\Gamma(\alpha')}(\beta'\lambda)^{\alpha'-1}e^{-\beta'\lambda}\mathrm{d}\lambda \tag{2.8}$$

Evalutating the integral in equation 2.8 numerically is not easy. It can be shown (e.g. by Siu and Kelly (1998)) that the percentiles can be found using equations 2.9 and 2.10 where χ^2 corresponds to the certain quantile in the chi-distribution which value easily can be found in statistics tables. Note that $(2\alpha + 2n)$ states the degrees of freedom.

$$\lambda_{95} = \frac{\chi^2_{95}(2\alpha + 2n)}{2(\beta + t)} \tag{2.9}$$

$$\lambda_{05} = \frac{\chi^2_{05}(2\alpha + 2n)}{2(\beta + t)} \tag{2.10}$$

2.4 The Effect of Increasing Data

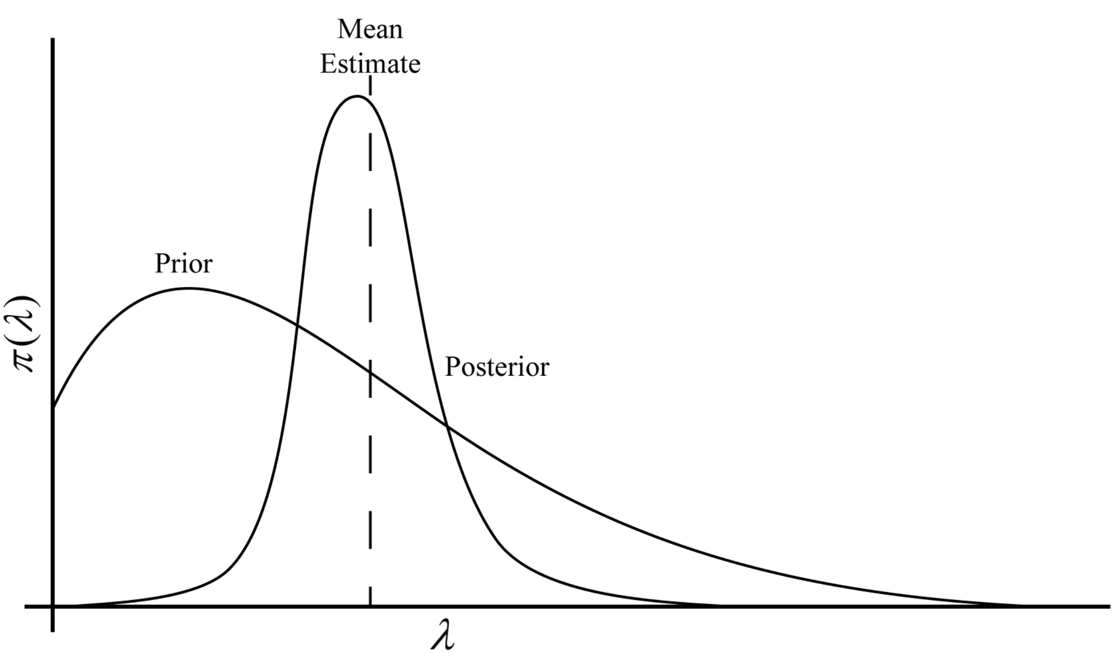

Figure 2.1: Effect of increasing data on posterior distribution

Figure 2.1 illustrates how the posterior distribution converges againts the "true" reliability of a device, e.g. a BDV, as n and t increase. As seen, the posterior distribution will be peaked about the *mode*, which is the value that occur most frequently in the posterior distribution. The mean failure rate estimate ($E(\Lambda)$) which states the most likely value of the failure rate, is found a little to the right of the vertex (mode) of the curve. This because of the "tale" of high possible values of λ, which basically is just a property of the gamma distribution. The higher values of n and t collected, the more narrow and peaked about the empirical mean value, the posterior distribution will be.

2.5 Introducing Loss Function

A loss function expresses how events lead to associated consequences. In this thesis, a loss function is not introduced mathematically, therefore the concept is only discussed. A loss function can either be symmetrical (or quadratic) or non-symmetrical. In the context of the reliability of SIS, this can be described as follows. We know that the purpose of a SIS is to reduce the risk related to a certain activity in different applications. To implement and operate a SIS, costs money. In the long run it is expected that this investment will pay off since it reduces the risk of loss of lifes and big economical loss in case of an accident. The performance of a SIS is measured in terms of its reliability. Obviously, it costs more money to implement and maintain a SIS of a very high reliability than a SIS with low reliability. The question now arises about how reliable the SIS must be to optimally balance the costs related to the implementation and operation of a SIS, and its contribution to save lifes and save economical loss in case of an accident. The ALARP principle (see e.g., Rausand (2011)) states that the risk of e.g. an process installation should be reduced to what is practically and economically reasonable. To spend disproportionate much money on increasing the reliability of a SIS from a high level to an extremely high level will not contribute very much to the overall risk level of the installation, and will thus not be reasonable. Anyway it will be favourable, and in some cases mandatory, to state high reliability requirements on SISs since they deal with safety of humans. The point is that the effect of increasing reliability flattens out above a certain point, while the cost related to it, will increase. We now understand that the loss function related to this is non-symmetrical.

Chapter 3

The Blowdown System

In this thesis, the blowdown system on a Teekay FPSO is used as case when different aspects related to provision and updating of reliability parameters are investigated. This chapter introduces and describes the system, and provides a description on how testing is performed on the entire system and on the blowdown valves alone. The descriptions in the chapter will be used as basis when reliability aspects are discussed in Chapter 5.

3.1 Description of the System

Figure 3.1 shows a blowdown system installed on a pipeline from a separator applied in oil and gas production. Oil, gas, and waste are during normal operation, flowing into the separator through the pipeline equipped with a emergency shutdown valve (indicated as ESV 1 in the figure). Further, the the oil and gas are separated from the non-recoverable waste and continue further through the production line. The separator described above is typically a 1st stage separator which implies that it is the first separator reached after the oil has been extracted from the seabed. The oil goes through several separators before it gets the desired purity.

It is a well-known fact that especially gas is a highly combustible material, and that gas exposed to pressure can lead to explosive fire in case of ignition. The main ingredient in the pipelines is oil which produces gases in case of high temperatures. This implies that if a fire breaks out on a FPSO or similar production facility, and the pipelines are exposed to the fire and heat, the pressure in the pipelines will increase and the risk related to rupture and a ex-

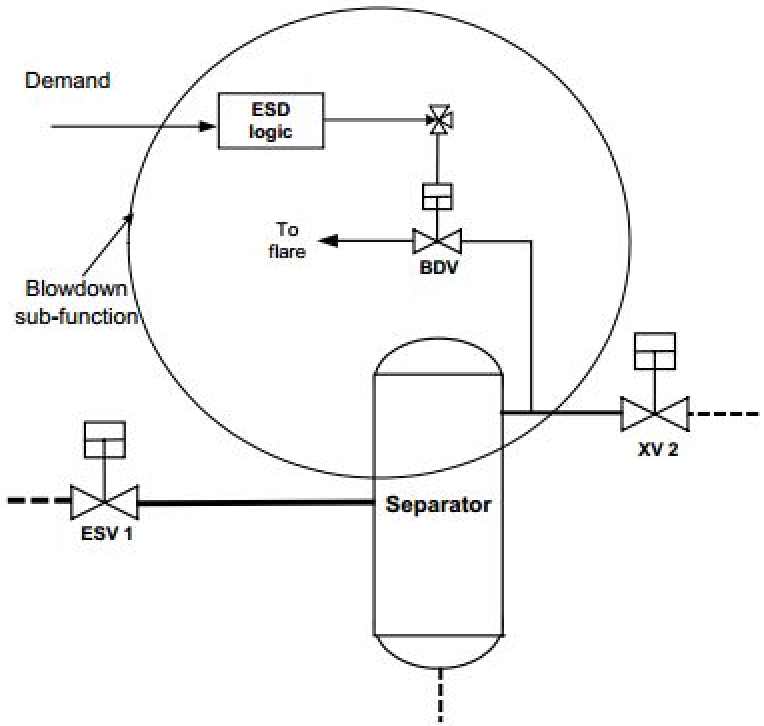

Figure 3.1: Definition of the blowdown system from OLF 070 (2004)

plosive fire of catastrophic dimentions, is high. It is in such scenarios the blowdown system can contribute to reduce the risk. As indicated in figure 3.1, the outgoing production pipeline is equipped with a pipeline leading into a BDV. In case of an emergency situation, e.g. the scenario described above, the BDV is opened sending the contents in the pipeline and separator to flare. In this way, the pressure is reduced and the risk of rupture, fire, and escalation is reduced. To give insight in the full purpose of the blowdown system, S-001 (1999) lists the following purposes of the blowdown system during an accidential event or emergency situation:

- in the event of a fire to reduce the pressure in process segments to reduce the risk of rupture and escalation
- reduce the leak rate and the duration of the leakage and thereby ignition probability (in case of leakage on the pipeline)
- in some cases avoid leakage at process upsets
- route gases from atmospheric vent lines to safe location

3.2 Activation of the Blowdown Valve

The BDVs applied on the Teekay FPSOs are solely ball valves. According to Wikipedia, a ball valve is a valve with a spherical disc, the part of the valve which controls the flow through it. The sphere has a hole, or port, through the middle so that when the port is in line with both ends of the valve, flow will occur. When the valve is closed, the hole is perpendicular to the ends of the valve, and flow is blocked. During normal production, the BDV is kept closed by a actuator which compress a spring in the valve. Air pressure is the utility medium that creates the force that compresses this spring. The solenoid valve that supply the actuator with air, is kept open by electric power from the emergency shutdown (ESD) logic. The ESD logic is supplied with electric power from UPS (Uninterruptible Power Supply). The UPS is a unit which maintain a continous delivery of electrical power even when the external power supply fails. Logically, the UPS is dependent on energy storage. If the external power is absent so long that the stored energy is depleted, the ESD logic loses its power supply which makes the solenoid valve switch position so the air pressure on the actuator bleeds of. The spring in the BDV is then released and the BDV opens. This implies that the BDVs are fail safe open. The BDVs are only activated through the control room via the ESD logic, rather than direct activation by overpressure in the equipment.

3.3 Execution of Tests

A proof test is, according to IEC 61508, a test that is performed to reveal all dangerous SIS failures, and as stated in Rausand and Lundteigen (2008) it often requires human interaction during preparation, execution, and restoration. Teekay performs proof testing of the blowdown system once every 12 months. The blowdown system is pressurized and the valves are opened via signals from the ESD logic which is operated from the control room. Further the travel time, the time until the BDV is fully opended, are automatically registered. In addition to this annual proof test, Teekay perform monthly tests on the BDVs. These tests are less comprehensive and the results from the tests are not registered for use in reliability work in the future. These tests are only performed so the operators "are sure" about functioning BDVs on the FPSO. In these monthly tests, the BDVs are not opened via the ESD logic, they are only manully operated. Also in these tests, the system is pressurized. If failures on one or more BDVs are revealed during these monthly tests, the BDVs are immediately repaired. The most common example of failures revealed in these tests are BDVs stuck in closed position due to physical obstackle, for example corrosion related. If such failure occur, the BDV are simply operated and maneuvered until the valve successfully goes from closed to open position. Reliability aspects related to this manual testing are discussed in Chapter 5

Chapter 4

Literature Survey

This chapter presents previous work related to the topics in this thesis. Since the main objective of the thesis is related to updating of reliability parameters for use in reliability analyses of SIS, this has been the focus of the literature survey.

4.1 Presentation of Relevant Papers

Hauge and Lundteigen (2008a) is a report carried out by SINTEF Techology and Society in Trondheim. The report is a part of the PDS method which is a method used to quantify the safety unavailability and loss of production for SIS. More specifically the report is a part of the research project *Management and follow-up of SIS integrity*, and is a guideline on how reliability issues can be threated in the operating phase of the SIS. The report is mainly written by the professors Stein Hauge and Mary Ann Lundteigen, and these authors have in retrospect of this report prepared research papers on SIS follow-up. These papers will be presented afterwards. The current PDS report is comprehensive and covers the most important aspects to consider in SIS operation phases. This includes SIS documentation and premises, planning and execution of activities, verification of SIL requirements, and updating of failure rate and test intervals based on operational experience. Since this thesis deals with the last point, only the work in that part of the report is presented.

The purpose of the PDS report is to describe a method on how to update the failure rate assumed in the design phase, with operational specific failure data. Based on this failure rate updating, a method on how to update the proof test interval of the specific components are further provided. The process for updating the failure rate is based on Bayesian updating, where the failure rate from design are updated with opereration experience. This implies that the updated failure rate estimate is based on both sources until sufficient operational experience is collected, and the failure rate is fully empirically calculated. The method suggest a certain cutoff point that expresses what is sufficient operational experience, based on statistical information in the OREDA handbooks. When the failure rate is updated, and the results claims that the equipment is significantly more or less reliable than assumed in the design phase, the test interval can be assessed. Based on an estimated 90 % confidence interval for the updated failure rate, the method propose conservative rules on when and how much the proof test interval can be changed. This approach is restricted to either halve or double of the test interval. The report also provide a more flexible approach where a more limited change of the test interval is considered. Here, the new test interval is calculated by multiplying the original test interval with the ratio old failure rate over updated failure rate.

Hauge and Lundteigen (2008b) is based on the experience from the PDS research project. The paper discusses challenges related to SIS performance monitoring after requirements from IEC 61508 became relevant in the industry, it discusses application of performance indicators and performance targets, and provides a method on how to use plant specific data to monitor the SIS performance. The results from the monitoring are applied to evaluate the proof test interval. This paper does not provide a method on how the failure rate can be updated with operational experience, which was the case in Hauge and Lundteigen (2008a). Instead the mean number of failures for the identical components during a certain time period (typically the proof test interval) are calculated based on the generic failure rate applied in the design phase. Further a counts control chart are applied, where the number of failures experienced in the following observation periods are plotted in the chart where the range of number of failures vary around the calculated mean value. An upper and lower limit of the range are specified to define the acceptable variation of the number of failures. The evalution of the proof test intervals must be based on the empricial failure rate calculated by the accumulated data from the relevant observation period, further this method of updating test intervals is identical to the method presented in Hauge and Lundteigen (2008a).

OLF 070 (2004) includes a method for updating interval for proof tests of SIS. The method in OLF 070 is a simplified approach of the methology presented in Vatn (2006), which was criticised for being too complicated to apply in the industry, and therefore a less comprehensive approach was included in OLF 070. Vatn (2006) provides a methology on how failure rate can be updated using a Bayesian approach. The updated failure rate is used to evaluate the proof test interval, which also was the case on the previously presented work (which in fact was carried out after this paper). The prior gamma distribution based on design phase estimates are constructed by so called uncertainty parameters, which in fact corresponds to the scale and rate parameter which was discussed in Chapter 2. These parameters are calculated by assuming a best possible estimate of the failure rate and a conservative estimate of the failure rate. The prior distribution is updated with operational data, and the posterior distribution is derived. An updated estimate of the failure rate can now be found. This method on updating failure is adopted in Hauge and Lundteigen (2008a), which was presented earlier in this chapter. Vatn suggests applying failure cause analysis to correct the best and conservative failure based on how the prospective situation, with respect to this failure cause, will be.

Hauge and Lundteigen (2009) builds on Hauge and Lundteigen (2008b) and Vatn (2006). The paper introduces a new approach of four steps which basically are made up by the methods provided in the mentioned papers. It applies the number of DU failures as performance indicator which is measured agains the integrity target value which indicates the maximum value of failures before the actual PFD exceeds the predicted PFD. When it comes to updating of failure rate, it provides one method based on empirical data alone, similar to the method in Hauge and Lundteigen (2008b), and a bayesian method identical to the one in Vatn (2006). The extention of Vatn's work, is some guidelines on how to select the conservative estimate of the failure rate. The evaluation of the proof test interval is similar to the flexible approach in Hauge and Lundteigen (2008a).

Hauge and Lundteigen (2010) is the last paper in this serie carried out by Lundteigen and Hauge. The methology in this paper is identical to Hauge and Lundteigen (2009).

Chapter 5

Reliability Aspects

As described in Section 3.3, Teekay performs monthly testing of the blowdown valves in addition to the annual proof test of the entire blowdown system. This chapter discusses the issues related to this monthly testing, and to what extent they influence on the reliability of the system.

5.1 Proof Testing

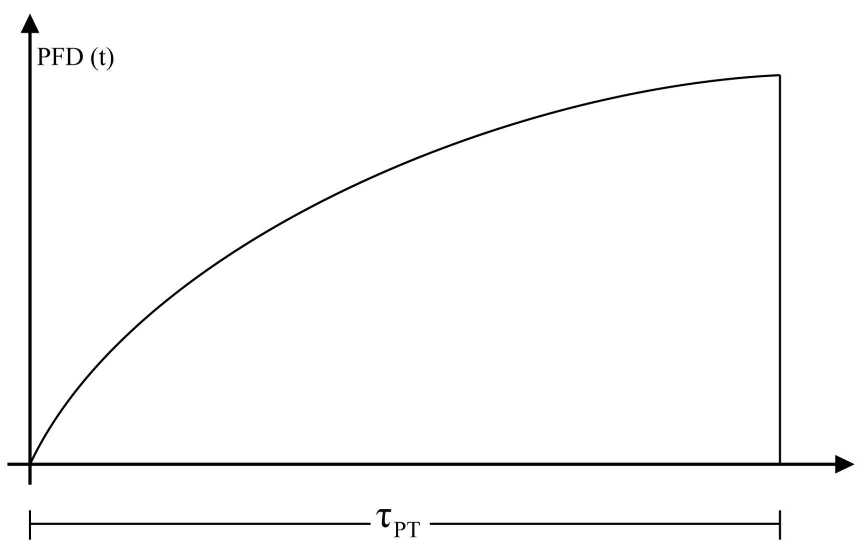

Figure 5.1: PFD of a periodically tested BDV

Figure 5.1 illustrates how the reliability, in terms of the *Probability of Failure on Demand* (PFD), increases as the time elapses (e.g., see Rausand and Hoyland (2004)) before the proof test is executed with an interval $\tau = 12$months. The proof test is assumed to be a *perfect test* (see e.g. Rausand and Lundteigen (2008)) which means that we assume that the tested item is as good as new immidiatly after the test and that the test reveals all *dangerous undetected* (DU) failures. The test coverage of the proof test can then be expressed as in equation 5.1 where λ_{DU} is the total DU failure rate, and $\lambda_{\mathrm{DU,PT}}$ is the rate of DU failures revealed by the proof test.

$$\theta_{\mathrm{PT}} = \frac{\lambda_{\mathrm{DU,PT}}}{\lambda_{\mathrm{DU}}} = 1 \tag{5.1}$$

The graph in figure 5.1 illustrates the reliability development when the only testing performed on the BDVs, is the annual proof test. Following section will discuss how the reliability of the BDVs are affected by the additional manual testing.

5.2 Manual Testing

Rausand and Lundteigen (2008) discusses reliability aspects related to *partial stroke testing* (PST) (see also e.g., Summers (2000)), which is a way of testing process shutdown valves by operate the valve just enough to reveal certain failure modes related to the valve leaving its open position. Note that the function of a shutdown valve is to close, in contrast to a blowdown valve which must open on demand. PST is less comprehensive than traditional proof test and can either be:

- implemented as a supplement to the proof test to improve the reliability
- implemented as a means to extend the functional test interval

For the manual tests it is the exact same case. At present, Teekay performs these tests to improve the average reliability of the BDVs. Or as the operators on the FPSOs say: "We do the manual tests to make sure that the BDVs are functioning". One of the questions Teekay wanted to investigate through this thesis, is whether these manual tests could be used to argue that the proof test interval can be extended, which corresponds to the second bullet point above. Before this question can be answered, a discussion assessing the manual test coverage and how they affect the reliability, must be carried through.

5.2.1 Assessing the MT Coverage

As we know from section 5.1, full test coverage is assumed when performing a proof test. Teekay claims that also the manual tests has a test coverage of 100 %. From OREDA (2009) we find the following failure modes for BDVs:

1. FTO (Fail to Open) - The BDV fails to open on demand
2. DOP (Delayed Operation) - The travel time of the BDV is too long, or the BDV does not fully open. This failure could be either *critical* or *degraded* (see Chapter 6) depending on wheter the BDV opens sufficiently (fast) to fullfil specified performance requirements.
3. ELU (External Leakage - Utility Medium) - Leakage of the medium that compresses the spring. In this case, air pressure. This could lead to full or partial opening of the BDV.

FTO is obviously a dangerous failure mode. DOP will also be a dangerous failure if the failure is categorized as *critical* in OREDA. It can be argued that also *degraded* failures should be included as dangerous failures since there is uncertainty related to the competence of the staff reporting these failures. This is further discussed in Chapter 6. The last failure mode, ELU, is not categorized as a dangerous failure since such a leakage leads to a open valve which could interupt the production, but not cause a dangerous situation in case of over-pressure. Since Teekay operates the BDVs to a full stroke when they execute the manual tests, both failures related to FTO and DOP are fully revealed. This implies that a full test coverage on the manual tests is realistic and logic. Anyway, there are good reasons for investigating cases where we assume the test coverage to be less than 100 %. The methodology presented in thesis can, with some adjustments, be applied to other SIS elements with similar test strategies. An example of such SIS, is the *Emergency Shutdown* (ESD) system where ESD valves (ESDVs) constitute the output devices. ESDVs shall stop the liquid/gas flow to the processing equipment and have therefore the opposite function compared to BDVs. Another argument, is that the manual tests not test the entire function, only the valves. This implies that the risk contribution from the ESD logic is only tested in the proof tests. The test coverage of the entire function is thus not 100 %.

As mentioned in section 5.2, PST can be performed between the function tests on ESDVs. The reliability aspects of PST on ESDVs are close to what is presented about the manual tests on the BDVs, but for PST on ESD the test coverage is not 100 %. This can be examplified by the dangerous failure mode LCP (Leakage through Closed Position) (OREDA, 2009) which is a failure mode that is impossible to test through PST. The reliability models for both full test coverage, and not full test coverage, are described and investigated in following sections.

5.2.2 Reliability Model. 100 % Coverage

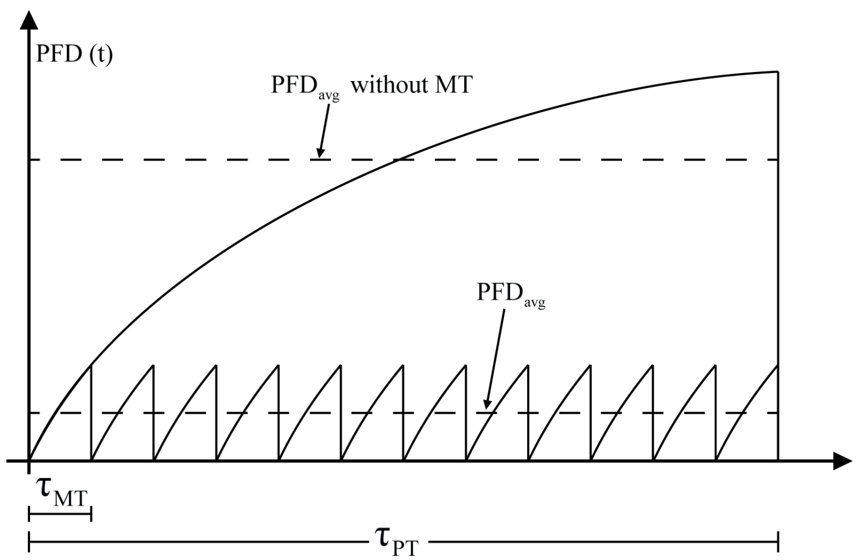

Figure 5.2: PFD of a manual and functional tested BDV

Figure 5.2 illustrates the development of the PFD of a BDV that are proof tested every $\tau_{\text{PT}} = 12$ months and manually tested every $\tau_{\text{MT}} = 1$ month. In this section, we assume the test coverage of the manual tests to be 100 %. This was discussed in section 5.2.1 and is in accordance to what Teekay claims and relevant data in OREDA. The test coverage for the manual tests is then given mathematically as in equation 5.2, exactly as the case for the function tests given in equation 5.1 in Section 5.1.

$$\theta_{\text{MT}} = \frac{\lambda_{\text{DU,MT}}}{\lambda_{\text{DU}}} = 1 \tag{5.2}$$

As we can see from figure 5.2, the manual monthly tests have the same impact on the reliability on the BDVs as the proof tests, which is quite obvious since they have the same test coverage $\theta_{\text{FT}} = \theta_{\text{MT}} = 1$. We know from reliability theory (see e.g., Rausand and Hoyland (2004)) that the average PFD of a proof tested BDV is given as in equation 5.3.

$$\text{PFD} \approx \text{PFD}_{\text{PT}} \approx \frac{\lambda_{DU}\tau_{FT}}{2} \tag{5.3}$$

When Teekay performs reliability calculations, they calculate the average PFD based on the proof test interval $\tau_{\text{PT}} = 1$ year. This will be a very conservative estimate when the manual tests are assumed to have 100 % test coverage. As seen on figure 5.2, the test interval is in practice only from last executed manual test to the time of the proof test, which in this case is 1 month. Since we know that $\tau_{\text{PT}} = 12 \cdot \tau_{\text{MT}}$, it implies that the average PFD will be 12 times lower than what is determined using the original proof test interval.

5.2.3 Reliability Model. < 100 % Coverage

When the manual tests are assumed to have a test coverage $\theta_{\text{MT}} < 1$, the reliability aspects will be more complex. $\theta_{\text{MT}} < 1$ implies that the manual test only reveal a part of the failures that are revealed in the proof test where $\theta_{\text{PT}} = 1$. See respectively equation 5.2 and 5.2 for the mathematical expression. Figure 5.3 illustrates the development of the PFD of a BDV proof tested every

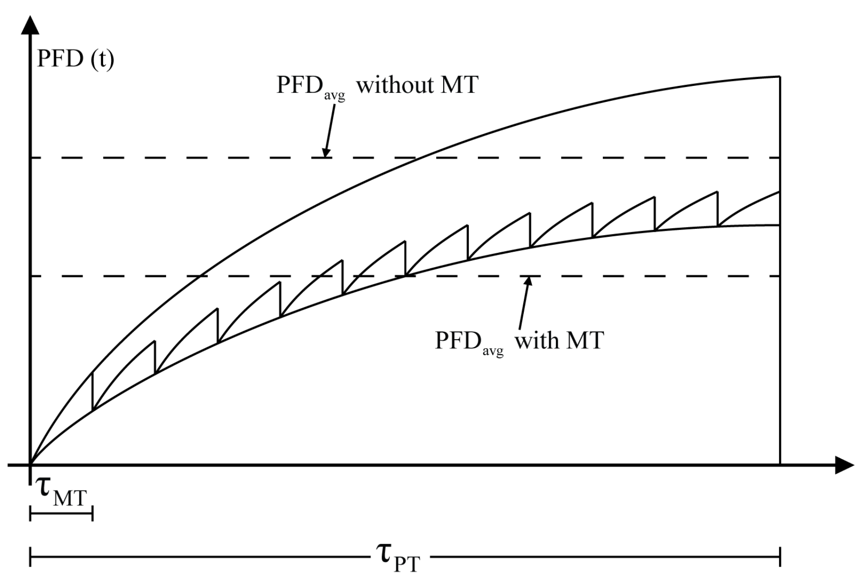

Figure 5.3: PFD of a funtional and manually tested BDV

$\tau_{\text{PT}} = 12$ months and manually every $\tau_{\text{MT}} = 1$ month. In contrast to the situation illustrated in figure 5.2, the BDV will not be as good as new (PFD = 0) after every manual test executed. This implies that the PFD will be continously increasing as time elapses until the functional test is executed. As earlier discussed, the manual tests detect a fraction of the DU failures, depending on the exent of the test coverage θ_{MT}. The average PFD can therefore be expressed as in equation 5.4.

$$PFD \approx PFD_{\mathrm{PT}} + PFD_{\mathrm{MT}} \approx (1-\theta_{\mathrm{MT}}) \cdot \frac{\lambda_{\mathrm{DU}}\tau_{\mathrm{PT}}}{2} + \theta_{\mathrm{MT}} \cdot \frac{\lambda_{\mathrm{DU}}\tau_{\mathrm{MT}}}{2} \tag{5.4}$$

The ratio $(1-\theta_{\mathrm{MT}})$ indicates the fraction of DU failures that are not revealed by manual testing, only by proof testing. Since the manual test revealed a fraction of θ_{MT} DU failures, the average PFD is be the sum of PFD_{PT} and PFD_{MT}. As stated in Rausand and Lundteigen (2008), the estimated PFD is improved when the manual testing (PST in the article) is introduced, since a portion of the DU failures are detected and corrected within a shorter time interval after their appearence, then by function testing.

Chapter 6

Sources to Prior Distribution

This chapter discusses sources that can be used to construct the prior distribution in the design phase of the SIS. At present Teekay applies either reliability data from the manufacturer or historical reliability data from generic sources when they specify the predicted failure rate in the design phase of the equipment. This chapter discusses issues related to both of these two sources.

6.1 Informative Prior Distributions

Bayesian theory distinguishes between *informative prior distributions* and *noninformative prior distributions*. A *noninformative prior distribution* is appropriate when we have no prior knowledge of the true value of the failure rate. Rausand and Hoyland (2004) states that a noninformative prior distribution is characterized by giving no preference to any possible parameter value. They are intended to be objective, letting the data provide most of the information content. The noninformative priors are usually mathematically derived (Smith et al., 2009). An *informative prior distribution* on the other hand, is appropriate when we have knowledge about the parameter value before we collect data. The blowdown system case in this thesis is a typical reliability problem where relevant prior information is available. For such cases, Hamada et al. (2008) lists the following six sources of information for constructing informative prior distributions:

1. physical/chemical theory

2. computational analysis
3. previous engineering and qualification test results from a process development program
4. industrywide generic reliability data
5. past experience with similar devices
6. expert judgement

As Smith et al. (2009) states, a difficult part of the analysis is the process of translating prior information into the probablistic format necessary to apply Bayes Theorem. According to the Bayesian approach, the prior is a probability distribution of different scenarios of the reliability of the components, or in other words, our degree of knowledge about the possible outcomes. The prior must capture the state of our knowledge independent of information from the data collection. Yet it is important to note that according to the Bayesian approach, the failure rate of the modeled component does not have the probability distribution as its inherent property.

Ideally we want to make use of and combine all insight that are available to construct an as accurate prior as possible based on our knowledge. As Siu and Kelly (1998) discuss, the development of an informative prior distribution can be a challenging process, because it requires the analyst to convert his own qualitative notions of probability into quantitative measures. At present, Teekay does not apply this Bayesian approach which implies including different sources to knowledge in a prior distribution. Instead they specify the failure rate estimate as either the estimate provided from the manufacturer or an estimate from generic reliability data sources. The following sections highlight the most important issues related to the use of data from these sources in reliability calculations, starting with generic historical data sources. An alternative method, where the Bayesian idea and approach is applied when estimating and updating the failure rate, is described in Chapter 7.

6.2 Historical Data Sources

Teekay has access to two historical data sources in their calculations. The first source is the *Offshore Reliability Data* (OREDA) which comprises five handbooks presenting historical data on failure frequency of equipment in the process industry. Each book contains data collected in different time periods since the early 80s. OREDA is a joint venture of different companies which implies that the data presented in the handbooks are average values made up of failure reports from the participating companies. In addition to the handbooks, there exists a detailed, computerized database which is only available for the participating companies (which Teekay is not). In this database, specific information related to the failures can be found. Each participating company can find specific information related to their own data, and anonymous information related to failures from other companies.

The other source to historical reliability data applied by Teekay, is the PDS Data Handbook (Hauge et al., 2010). PDS is a method used to quantify the safety unavailability and loss of production of SIS. The main source to the data presented in the PDS handbook is the OREDA database and handbooks. In contrast to OREDA, PDS presents the data specifically so they fit into the concepts provided in IEC 61508. Since PDS is mainly based on OREDA data, so the following discussion will mainly be based on issues related to the data collection and data provision in the OREDA handbooks.

As allready introduced, OREDA comprises of several companies that report reliability data based on internal maintenance reports in each company. The data is collected over a wide range of different offshore oil and gas installations. Each installation is different in terms of operating environment, treatment and conditions of the equipment. Due to the fact that the data in the OREDA handbooks is not traceable, it is unknown to the OREDA handbook user what was the underlying factors of each failure, and the operating conditions of the equipment where the failures were collected. The number of failures for some types of equipment is relatively few. This implies that the OREDA data of a specific equipment can be too optimistic/pessimistic because of the difference in operating environment, etc. Whether it is too optimistic or too pessimistic remains unknown since we do not know the details of the failures in OREDA.

OREDA classifies failure modes in three groups, here presented as in OREDA (2009) :

1. *Critical:* A failure that causes immediate and complete loss of a system's capability of providing its output.

2. *Degraded:* A failure that is not critical, but that prevents the system form providing its

output within specifications. Such a failure would usually, but not necessarily, be gradual or partial, and may develop into a critical failure in time.

3. *Incipient:* A failure that does not immediately cause loss of a system's capability of providing its output, but which, if not attended to, could result in a critical or degraded failure in the near future.

In a safety perspective, which is relevant for SISs, failures that prevent the SIS from performing its SIFs are of interest. A *performance requirement* is stated for each SIF. In practice, it is adequate to state performance requirements for vital components within the SIS, e.g., the BDVs in a blowdown system where the requirement could be to fully open within e.g. 20 seconds. If the valve fails to open, it is a critical failure, but if the valve opens but not within the stated time limit, it is a degraded failure. To be categorized as a degraded failure, the function needs to be in place. The problem with this categorization is that it requires a competent staff to put the failures into the right category. It is reasonable to assume that a substantial part of the operators within the different reporting companies are not competent to evaluate what failures that belongs to each category.

Technology in all applications are continously improved. Cars, mobile telephones and other equipement that we make use of in our everyday life, are of much higher quality today than what it was 5-10 years ago. It seems senseless comparing mobile telephone technology of today with the techology of the past. Even if using mobile telephones as example is rather extreme, it illustrates an issue which is relevant for the discussion of OREDA data quality. It seems reasonalble that using reliability data collected from old and used equipment on brand new equipment, leads to conservative estimates. OREDA assume constant failure rate in the useful life period (see *bathtube curve* in e.g., Rausand and Hoyland (2004)) of the equipment, which is a common assumption in reliability calculations. However, according to OREDA (2009), no statistical tests have been performed to verify the assumption of a constant failure rate. In a practical manner, it is likely to assume that the failure rate will increase as the equipment is used and exposed to, at least for some equipment, harsh environmental conditions. According to Hauge et al. (2010) *systematic failures* are failures that can be related to a particular cause other than natural degradation and forseen stessors. Typically they occur due to errors made during specifications, design, operation and maintenance phases of the lifecycle of the SIS. OREDA does not separate between systematic failures and other failures, so possible systematic failures introduced in the useful life period of the equipment, are included in the handbooks. This support that it can be argued that the assumed constant failure rate is inaccurate.

6.3 Manufacturer Data

Manufacturer reliability data is provided by the producer of the equipment. There are primary two types of such data:

1. Self-testing of the equipment
2. Collected field data from installed equipment

The first point implies that the manufacturer tests the equipment in their own sites (e.g. a laboratory). Such testing is typically *accelerated* which implies that stress is added for the purpose of accelerating the failure process. For example, increased temperature can be used as stressor to reveal possible failure mechanisms e.g. corrosion. The idea of this type of testing is to experience more failures on a reduced time. An important issue related to such self-testing is that the equipment are allways placed under controlled conditions.

Data in OREDA includes systematical failures and failures potentially caused by misuse of the operators. Non of these are included in failure data provided by the manufacturer. Only primary failures related to inherent failure mechanisms triggered by foreseen stressors are revealed.

EXIDA is an example of a company that, among other things, provides functional safety certification according to the requirements and concepts in IEC 61508. EXIDA completes a technical analysis of the equipment including software testing in addition to *Failure Modes, Effects and Diagnostics Analysis* (FMEDA). The software testing, FMEDA and expert judgement are used to determine a failure rate so the equipment can be certified to a specific SIL interval. Reliability data from EXIDA and similar companies can be a proper alternative to the manufacturer data, since involving a third party may give a more objective view. EXIDA also publish reliability data in handbooks. See for example, EXIDA (2007a), EXIDA (2007b), and EXIDA (2007c).

The second point above implies that the manufacturer receives failure reports related to their equipment applied on the installations. Such failure reporting is often related to a warranty deal between the manufacturer and the operating company, which also is one of the problems related to manufacturer data. Failure reporting occur during the period of the guarantee, but when the period has passed, the operating companies experience no direct value of reporting failures and thus the part of failures reported to the manufacturer decreases. This implies that the reliability data provided by the manufacturer is thrustworthy only during the warranty time. And even during the warranty time, EXIDA estimates that only 70 % of failures are reported to the manufacturer. Another problem of the manufacturer data is that operational time of the equipment is unknown. We only know that the equipment has experienced a failure, not the operational time of the equipment. Ultimately this can imply that a estimate where the failure data is based on failures reported, and numbers of devices sold, without even knowing if the sold equipment is applied. This leads to very optimistic reliability data.

Chapter 7

Updating of Failure Rate

Chapter 2 gave an introduction to how Bayesian methods and concepts can be applied to update the failure rate assumed in the design phase of a SIS with empricial failure data experienced in the operational phase. According to Siu and Kelly (1998), Bayesian parameter estimation consists of 4 steps. The first step is the identification of the parameter to be estimated. The second step is the development of a prior distribution that appropriately quantifies the analyst's state of knowledge about the unknown parameter. The third step is the collection of of evidence and construction an appropriate likelihood function. The fourth and final is derivation of the posterior distribution. These four steps create the basis for the method and discussions provided in this chapter. The chapter aims at creating a guideline on how the Bayesian updating process can be performed including discussions on how to include different sources in the prior distribution.

7.1 Development of Prior Distribution

As mentioned in Chapter 6, the most challenging part of a Bayesian updating procedure is to develop a meaningful prior distribution which reflects our sources to knowledge in the best possible way. In practice there is no need to overestimate the importance of a prior of extraordinary degree of accuracy. We know from Chapter 2 that the effect of the prior distrubution decreases as new data becomes available. No matter how inaccurate the prior distribution reflects the "true" reliability of a component, the posterior distribution converges to the "true" reliability (based on empirical data) in the long run. However, for the BDVs on a single FPSO investigated in this thesis, there is nothing such as the long run. Few failures will occur on a relative long time period, and an appropriate prior can therefore compensate for sparse empirical data. There can potentially be many sources to knowledge about the parameter to be estimated (see Chapter 6). Since Teekay has a fleet of FPSOs where failure data for each FPSO has been recorded, this is a key source when developing the prior distribution. This data is be more trustworthy than data from generic historical data provided in for example, OREDA. In contrast to the OREDA data, that is collected from stationary installations, the Teekay FPSO data is FPSO specific. This implies that the underlying causes to the failures that can be related to FPSO-specific incidents or conditions, are included in the total failure rate. In OREDA, the data is collected from different companies, which implies that the failure causes can not be traced, which obviously can be done internally in Teekay. The failures collected in OREDA also include potential systematic failures that typically can have been introduced during maintenance of the system. In other words, OREDA reflects the average of how well the companies avoid systematic failures. Teekay does not know exactly how well they avoid systematic failures compared to other companies, and the Teekay data are therefore more accurate related to this. It seems clear that more emphasis should be put on the Teekay FPSO data than the generic data from OREDA. Anyway, OREDA data is not useless in the process of developing the prior distribtion. The Teekay data can be compared to the OREDA data and it can be determined whether the Teekay data seems too optimistic or pessimistic, and potential different failure modes can be investigated and compared.

Figure 7.1 illustrates the sources that are suitable as inputs to analyst that shall construct the prior distribution. As seen, expert judgment is included as one of these sources in addition to the data sources discussed ealier in this chapter and Chapter 6. According to Rausand (2011), the use of expert judgment becomes necessary when data from real applications are scarse or nonexisting. Expert judgment elicitation is a process for obtaining data directly from experts in respons to a specific problem. Application of expert judgment can be very useful when the prior distribution is determined. It is important to note that expert judgment and the application of it, is a very large academical field which is just superficially treated in this thesis. We recognize from Chapter 2 that parameterization is the process to determine proper parameters to construct a realistic distribution. For the gamma distribution, these parameters are the scale

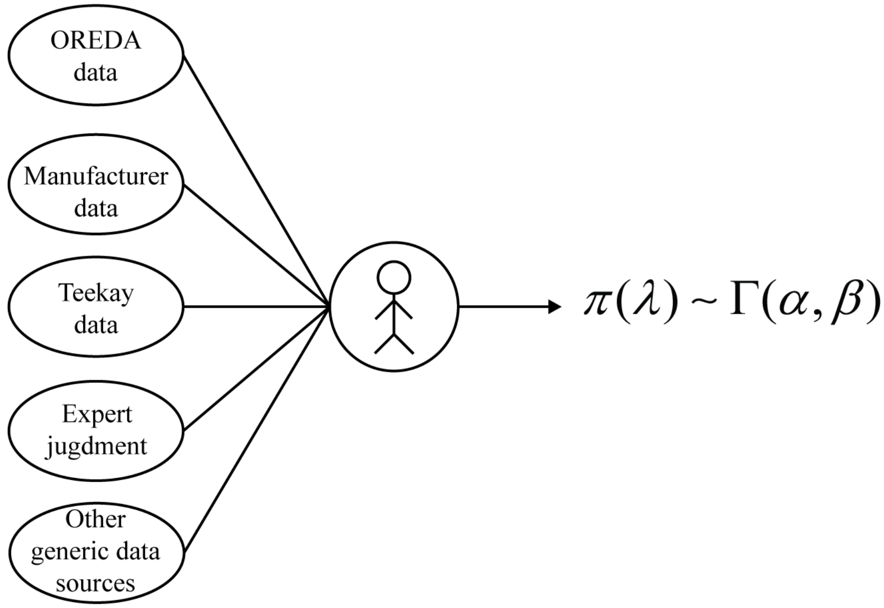

Figure 7.1: Definition of the blowdown system from OLF 070 (2004)

and rate parameters, α and β. Parameterization is basically what development of a prior distribution is all about, but as earlier discussed, the issue is to weight all relevant sources into the parameters leading to an accurate prior distribution. Equations 2.4 and 2.5 in Chapter 2 show how the mean value and variance are given in terms of β and α. Since this is two equations with two unknowns, β and α can be found by known mean and variance. According to Teekay, if comparing the different reliability performance on the different FPSOs, we find big differences. As was the case for generic data collected from different installations, the failure rate is affected by different mutual factors such as differences in design of the blowdown system, how often and well service on the system is performed, age of the FPSO, different environmental conditions, and varying quality of the maintenance procedures on the different FPSOs. If we calculate the empirical value of the mean, based on the total number of failures (n) and total operating hours (t) of all FPSOs, we end up with a mean value that does not tell us much about what reliability performance we can expect on a brand new FPSO. As discussed in Chapter 6, new equipment is expected to be more reliable than old and used equipment. These arguments support that use of expert judgement with the idea of "filtrate" the collected data and do an evalution about what is relevant and what is not. An expert can in this case for example, be a FPSO operator with a good reputation, years of experience and a thorough knowledge about the blowdown system. If we ask her about her opinion about the mean value of the failure rate, she can probably be able to give a fair estimate. Note that she can give her answer in terms of for example, number of failures per year instead of a direct estimate of the failure rate, which is less intuitive. If we ask her about an estimate of the variance, she probably does not have a clue. We recognize equations 2.9 and 2.10 from Chapter 2, that are used to calculate percentiles in the prior or posterior distribution. By asking the expert to estimate a worst-case scenario in terms of number of failures, she will probably be able to give an estimate which is better than what we can find from any data source. Through her experience, she can recall a period (e.g., 12 months) where an abnormally high number of failures on the BDVs occured. The calculated failure rate for this period can be assumed to be e.g. the 90th percentile in the distribution. The same can also be done on the other end of the distribution by finding a best-case estimate of the failure rate. Combining these two equations will then lead to the parameters β and α.

The author of the thesis concludes that the best way of calculating the parameters β and α is to combine

- the equation for the mean value (equation 2.4), where the mean value ($E(\Lambda)$) is mainly based on the Teekay FPSO data and expert judgement

- the equation for certain percentile in the distribution (equation 2.9 or 2.10), where e.g. the conservative percentile is mainly based on the Teekay FPSO data and expert judgement

It must be noted that a formalistic method on how to combine emprical Teekay FPSO data with expert opinions is not provided in this thesis. Further reading on this topic can, for example be found in Houmb et al. (2000). The reason why it is favourable to combine these two equations instead of e.g. the 10 % percentile and 90 % percentile, is that the mean estimate is probably what we with best certainty can assess. The problem with the percentiles is that we need to decide the failure rate and what percentile it belongs to. Another problem related to use of equation 2.9 and 2.10 is that α is included as the determination of degrees of freedom, and can thus lead to problems in the matematical derivation. Still, it can easily be solved by an equation-solving spreedsheat which is easy to construct.

An alternative to these equations is to apply the approximation of the variance as shown in equation 7.1. This method is first applied in Vatn (2006). $\lambda_{\text{DU-CE}}$ corresponds to a conservative estimate of the failure rate. This conservative estimate must be less pessimistic than in the preferred method since the difference between the conservative estimate and the mean estimate is an approximation of the standard deviation.

$$\beta = \frac{\mathrm{E}(\Lambda)}{\mathrm{Var}(\Lambda)} = \frac{\mathrm{E}(\Lambda)}{(\lambda_{\text{DU-CE}} - \mathrm{E}(\Lambda))^2} \tag{7.1}$$

A summarization of how to develop the prior distribution step is provided:

1. Determine the parameters β and α as described above

2. The parameters are used to construct the gamma distributed prior as given in equation 2.3

The prior distribution is now constructed and an important question arrises. What specific percentile in the distribution shall be applied to verify that the blowdown system perform within the specified SIL level and other further reliability calculations?

It can be tempting to believe that a very conservative percentile should be applied due to the blowdown system's role as a safety barrier, but as discussed in Section 2.5, choosing a too conservative estimate can lead to higher costs and work effort, compared to the effect on the safety level. As stated in Hamada et al. (2008): *Beware of conservatism. Realism is the desired ideal, not conservatism.*

On the other hand, the development of a prior distribution is associated with a high degree of uncertainty, and when human safety is directly affected by the reliability performance of the blowdown system, a quite conservative percentile should be considered. This is also stated in IEC 61508, which requires that any failure data used shall have a statistical confidence level of at least 70 %. Based on the knowledge of the author, and the discussions provided in this thesis, it is found no arguments for choosing a more conservative value than what is stated in IEC 61508.

7.2 Updating to Posterior Distribution

After the prior distribution is developed based on all our knowledge about the system, the prior distribution is updated to a posterior distribution as emprical data become available. This type of updating is in literature refered to as *Two-stage Bayes method* (see e.g., Siu and Kelly (1998)). The first stage is to create a prior distribution for λ based on our knowledge (which is done in previous section), and in the second stage, update this prior distribution using plant-specific data. The updating to a posterior distribution is a lot simpler than the development of the prior, since we now only need to deal with empirical data which is perfectly objective. The updating process is just a straight-forward application of Bayes' theorem. Since the relevant equations and theory are provided and presented in Chapter 2 we only summerize how the updating is performed stepwise.

1. Update the parameters so $\alpha' = \alpha + n$ and $\beta' = \beta + t$ where n is number of failures and t is the total operation time

2. The updated parameters are used to construct the gamma distributed prior as given in equations 2.6 or 2.7

Chapter 8

Changing the Test Interval

Chapter 5 discusses how the average reliability on the BDVs are affected by the proof tests and the manual tests. Chapter 7 discusses how historical data and expert judgement can be used to develop a prior distribution of the failure rate, and how this estimate can be updated as new data become available for the new FPSO. If it during the operation phase of the BDVs can be proved that their reliability performance differs significantly from what was expected, it can be assessed whether the proof test interval can be increased or decreased. This chapter discusses how the manual testing and the updated failure rate estimate can be applied as a pretext to a potential proof test interval extention.

8.1 Fundamental Factors

When an updated failure rate is calculated, it can be of interest to consider the length of the proof test interval. According to IEC 61508, a certain SIL level can be specified for every safety instrumented function (SIF) on a SIS. Anyway, it is normal practice that the equipment manufacturer claims a certain SIL level for different components. As discussed in Chapter 6, the quality of the reliability data provided from the manufacturer can be questioned, and probably a better way of estimating the failure rate (which in addition to the test interval corresponds to a certain SIL level) to apply in the design phase, is provided in Chapter 7. To ensure that the reliability performance of the BDVs is below the risk acceptance criteria (see e.g. Rausand (2011)) after the system is put into operation, proof testing is performed and the results are recorded.

As stated in Hauge and Lundteigen (2008a), change of test interval is generally most relevant for components with a significant amount of operational experience, either based on a high number of installed components and/or several years of operation. The number of BDVs installed on an FPSO are relatively low, and the blowdown system experiences few real demands between the proof tests. Since the proof tests are executed annually we now understand that many years of operational experience will be required before an assessment on changing the test interval can be a realistic topic. We know from Chapter 5, and equation 5.3 that PFD, which is the measure of the reliability of SISs, is a function of the failure rate and the proof test interval. The proof test interval is decided before the SIS is put into operation and is, at least theoretically, chosen in accordance with the estimated failure rate to keep the average reliability below an accepted or desired level. As already introduced, the operational experience must therefore prove that the failure rate on the BDVs is significantly better or worse before the test interval can be changed. Now the interesting question arises. What is sufficient operational experience?

8.2 Sufficient Operational Experience

As discussed in Chapter 7, the FPSO specific conditions have strong influence on the reliability of the SIS installed on the specific FPSO. The prior distribution development is, in the suggested method in this thesis, mainly based on historical data from other Teekay FPSOs and expert opinions and judgement. Even if the prior distribution is developed as accurately as possible, there is obviously a high degree of uncertainty related to this distribution and the actual estimate applied in the reliability calculations. Because of this, Hauge and Lundteigen (2008a) recommends to only rely on operational experience when the proof test interval shall be assessed. This makes sense since changing the test interval, and at least if increasing it, is a major decision which directly influences the safety on the FPSO, and a high degree of certainty on our estimates must be achieved before taking such a decision.

To specify a cut off point which states that enough confidence in the empricial data is achieved so contribution from the prior can be removed, is no obvious task. It can be argued that it makes no sense to specify such a point since this transition occur so gradually. Anyway, this current issue is relevant when the proof test interval shall be evaluated. If it comes to the point that change of the proof test interval can be relevant, it makes no sense to include contribution from the prior, since the applied estimate with high certainty was wrong. A specified cut off point can at least be used as guidence on when an change of the interval can be assessed. Hauge and Lundteigen (2008a) suggest following cut off point:

- *When the statistical confidence in $\hat{\lambda}_{DU}$ is comparable to the confidence in the design failure rate λ_{DU} then it is justifiable to apply only operational experience.*

Where $\hat{\lambda}_{\mathrm{DU}}$ is the failure rate estimate based solely on operational data. From this claim, OREDA data have been investigated to identify when this typically will occur and it is found that the upper 95 % percentile in the confidence interval for the critical failure mode will be in order of 2-3 times the mean value. Based on this, it is stated that $\hat{\lambda}_{\mathrm{DU}}$ can be applied solely if the upper 95 % percentile is approximately 3 times the mean value or lower.

If we transfer this cut off point suggestion to the Bayesian method in this thesis, it implies that the α and β are calculated by the emprical mean value and its variance (Equations 2.4 and 2.5). If the 95 % percentile in this distribution is less then 3 times the empirical mean value, it is an indication on enough operational data to remove the contribution from the prior.

An objection against this method, is that it is implied that the design failure rate estimate is based on OREDA data. In the method in Chapter 7 in this thesis, OREDA data is just one out of several sources to knowledge about the prior failure rate distribution. Since such a high effort has been put down in the determination of this prior distribution, it should be put more trust to than more or less uncritical use of OREDA data when estimating the failure rate in design phase of the equipment. Based on this, it can be argued that the distribution should be narrower than what is suggested in Hauge and Lundteigen (2008a), before contribution from the prior is removed and operational experience are solely applied.

8.3 Updating the Test Interval

Given the fact that it seems clair, both quantitatively and qualitatively, that operational experience can solely be trustet and applied, the next step is to assess how much the test interval can be increased or must be degreased. From Chapter 7, the 70 % percentile in the prior distribution is suggested as the specific design failure rate, given as λ_{70}. The 70 % percentile must also be applied in the distribution determined by the operational data, given as $\ddot{\lambda}_{70}$. The original proof test interval is given as τ_{PT}, then the maximum allowed new test interval if the actual PFD shall not be lower than the predicted PFD from design phase, is:

$$\ddot{\tau}_{\text{PT}} = \frac{\lambda_{70}}{\ddot{\lambda}_{70}} \cdot \tau_{\text{PT}} \tag{8.1}$$

The result from equation 8.1 provides the theoretical limit of how much the proof test can be changed while the reliability remains unchanged. Obviously, there is no point in changing the test interval unless there exists good reasons for doing it, or if the the operational experience demostrates that the reliability performance is below required or desired level, and the test interval must be decreased to fulfil the requirement. An increase of the proof test interval should be considered in the context of a cost-benefit function, and in accordance to the suggestions in Vatn (2006), the increase of the length of the test interval (in one updating) should never exceed 50 % or 0.5 year.

8.4 Including Manual Tests

Chapter 5 discusses how the manual tests (described in Section 3.3) influences on the average reliability on the BDVs. Since the manual tests are performed monthly, while the proof tests are performed annually, it was found that the average PFD on the BDVs is in practice 12 times lower if 100 % test coverage was assumed. First, it must be stated that if the results from the manual tests can be used as a means to increase the proof test interval, they must according to IEC 61508, be threated systematically and be recorded just as the results from the proof tests. At present, this is not done on the Teekay FPSOs. The other issue with the manual tests, is that the entire blowdown function is not tested. According to IEC 61508, each SIF shall be tested. The manual tests are BDV specific. On the other hand, it is common practice in industry to weigh the risk contribution from the different subsystems and test them seperately. In the blowdown system case, the BDVs will be a significantly bigger contributor to risk than the ESD logic, so it is sensible that they are tested more often. There are several benefits related to future recording of the failure data from the manual tests:

1. Operational data on the BDVs will be collected 12 times faster, leading to a higher certainty in the reliability estimates
2. The data can be applied to prove a lower PFD (see equation 5.4 in section 5.2.3) and thus also lower risk on the FPSO.
3. The new PFD of the BDVs can be applied as a means to increase the proof test interval.

Chapter 9

Uncertainty Aspects

When the prior distribution of the failure rate was developed in Chapter 7, a high degree of uncertainty is related to the method and the underlying factors and procedures. Even the updating to the posterior distribution is associated with some aspects of uncertainty. This chapter discusses the different contributors to uncertainty, and provides a method on how the degree of uncertainty can be reduced in future reliability assessments.

9.1 Uncertainty Categories and Contributors

In literature, it is common to distinguish between two main categories of uncertainty, based on presentation in Rausand (2011):

- *Aleatory uncertainty*: Uncertainty caused by natural variation and randomness. Examples of aleatory uncertainty are variations in wind speed, wind direction, precipitation, product quality etc.

- *Epistemic uncertainty*: Uncertainty caused by lack of knowledge, which can, in principle, be eliminated if we can acquire sufficient knowledge about the study object.

Based on these definitions, we understand that epistemic uncertainty is the main, and probably only type of uncertainty relevant for the different aspects related to the case in this thesis. The main contributors to uncertainty are often classified into three main categories: *model uncer-*

tainty, parameter uncertainty, and *completeness uncertainty*. In the following sections, relevant contributors to uncertainty are discussed based on these three categories.

9.1.1 Model Uncertainty

Model uncertainty is related to the different models that are chosen to express actual real situations. Such models will allways be a simplification of the real situation, but is necessery so mathematics and statistics can be applied to evaluate different properties of the model quantitatively. Rausand (2011) indicates that model uncertainty can stem from whether

1. the model reflects the main properties of the study object
2. the analyst fully understand the model

In this thesis, the Gamma distribution is used to describe the uncertainty in the failure rate. The reason why the Gamma distribution is chosen is that the posterior distribution are of the same functional form as the prior distribution, and that the prior distribution is conjugated to the Poisson likelihood function (see Chapter 2), and thus make the posterior analysis easy. Another statistical distribution can be chosen, but leads to mathematical expressions which are hard to solve and analyze. This implies that the Gamma distribution not necessarily models the real situation perfectly, but are chosen due to practical reasons. It is therefore uncertainty related to how well the Gamma distribution reflects the real situation. Now it might be questioned if the choice of the Poisson likelihood function is a source to uncertainty. The answer to this is no, since an constant failure rate is assumed. This brings us over to the next uncertainty category.

9.1.2 Parameter Uncertainty

Parameter uncertainty is related to the inputs required to model a certain situation. In this case this is input data necessary to construct the prior distribution, and further the input data necessary for the updating to the posterior distribution. There are also parameters related to the testing that contributes to uncertainty. We know that the parameters α and β are necessary inputs to construct the prior distribution, and as discussed in Chapter 7, several sources create the basis when the parameters are determined. In the case study, these are mainly generic data sources, Teekay historical FPSO data and expert judgement. Determining α and β on these sources is probably the main source to uncertainty. Several questions arise: Is the generic data collected from a wide range of installations relevant for the current FPSO? What is the quality of the generic data and the Teekay FPSO data? Is constant failure rate a realistic assumption? Is historical data of old equipment relevant for brand new equipment? Can we trust the experts? Expert judgment is debated, is it applied optimally? These questions illustrates how uncertainty is induced into the failure rate. The posterior distribution is updated with specific failure data from the current FPSO. This is obviously a less controversial process than what was described above, and thus leads to less uncertainty. Anyway, there is uncertainty related to this as well. For example, there is uncertainty related to if total operating time of the equipment are correctly determined, and if the number of relevant failures are correct.

So far, parameters leading to uncertainty in the failure rate has been discussed. Calculating the average PFD of the BDVs, also requires relevant test parameters. The manual test interval and proof test interval are constant and easy measurable, and are thus not contributing to uncertainty. On the other hand, we do assumptions related to the test coverage. Have all relevant failure modes been identified? If 100 % coverage has been assumed on the manual tests, and it is wrong, it implies that the PFD is continously increasing until next proof test. Our assumption then gives an unrealistic picture of the reliability of the BDVs and thus also the risk and safety on the FPSO. Assuming full test coverage on the proof tests is normal, but the same issues as on the manual tests are relevant here.

9.1.3 Completeness Uncertainty

Completeness uncertainty is related to the quality and scope of a process. In this case, this process is related to how data is collected, evaluated and applied, and if all relevant issues are considered. An important contributor to the uncertainty is the competence, or more precise, the lack of competence of the employees involved in all parts of the process. It can be argued that all factors influencing the completeness uncertainty, can be traced back to lack of compentence or knowledge of the employees. Are all relevant failure modes of the BDVs identified? Does the operators, that have direct dealings with the failures, enough competence to classify and report the failures correctly? Does the reliability engineers apply the data correctly? For the blowdown system case and similar cases, it is impossible to conclude that all relevant factors are included in the process, and there will allways be uncertainty related to the scope of the problem to be addressed.

9.2 Increasing the Confidence of the Failure Rate Estimate

The fact that generic reliability data sources can lead to uncertainty when the data are applied in specific applications, is well-known and well-debated. The generic data source represents an average value generated from all included installations where each installation has its unique factors that affect the failure rates. This was discussed in Chapter 6. This section provides and discusses a method on how to investigate these specific factors so the confidence in prospective failure rate can be determined with higher confidence.

9.2.1 Influencing Factors

We know, according to Teekay, that the reliability performance on the BDVs on the different FPSOs differs a lot due to different risk influencing factors (RIFs). Table 9.1, adopted from Brissaud et al. (2010), is a list of RIFs. As seen, the list is comprehensive and the RIFs are quite specific. It must be noted that this list is generic, and some of the listed RIFs are not necessarily relevant in this particular case. We now assume that the different RIFs are measurable, and introduce equation 9.1 where the RIFs are represented as a vector $\mathbf{V} = (V_1, V_2, \cdots, V_n)$.

$$\lambda = \lambda(\mathbf{V}) \tag{9.1}$$

The value of λ cannot be determined without specifying the value of $\mathbf{V}$. Calculating $\mathbf{V}$ is obviously very complicated since the contributing RIFs are undefined and complex. An example that illustrates how complex it is: Assume that the reliability of BDVs are affected by the portion of sand in the oil in combination with the velocity the oil has through the valve. This does not mean that the reliability are affected by high portion of sand, or high velocity, it is just in combination they have a negative effect. This is just a single example. Evaluating this example together with all other RIFs numerically, obviously is a very complicated task. Another problem

Category		Influencing Factors
Design		System type
		Working principle
		Dimensions (size, length, volume, weight)
		Materials
		Component quality (quality requirements, controls)
		Special characteristics (supply)
Manufacture		Manufacturer
		Manufacture process (procedures, controls)
Installation		Location (access facilities)
		Assembly/Activation (procedures, controls)
Use	EUC	Equipment Under Control (EUC) type
		Special Characteristics
	Solicitation	Type of load (cycling, random)
		Frequency of use
		Loading charge/Activation threshold
		Electrical load (voltage, intensity)
	Environment	Mechanical constraints (vibration, friction, shocks)
		Temperature
		Corrosion/Humidity
		Pollution (dust, impurities)
		Other stresses (electromagnetism, climate)
	Requirements	Performance requirements
		Failure modes (recorded failures)
Maintenance		Frequencty of preventive maintenance
		Quality of preventive maintenance
		Quality of corrective maintenance

Table 9.1: Risk influencing factors

related to the RIFs, is that they are not necessarily measurable, and if the RIFs are measurable, it is hard to quantify how much effect differences in the measures, have. For example, we see from table 9.1 that climate can be a RIF. Climate is hard to quantify, and it is even harder to determine how change of climate effects the failure rate of the blowdown valves. Quantitative approaches have been tried, see e. g. Brissaud et al. (2010), but due to the high degree of uncertainty related to such approach, this thesis rather provide and recommends a (semi-) qualitative approach.

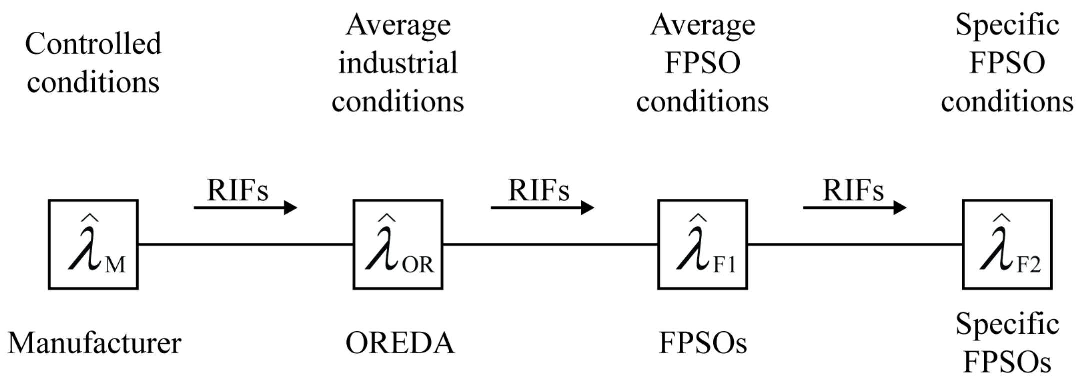

Figure 9.1: Influencing the Failure Rate

9.2.2 Investigating the Ratios

Figure 9.1 illustrates how the failure rate varies due to different unique RIFs that are relevant for the different applications as indicated in the figure. We know from Chapter 6 that one way the manufacturer determines the failure rate of a specific component, for example specific BDVs, is to test the components under controlled conditions. This estimate will normally be optimistic since no unintended use of the BDV is taken into account, and the failure rate therefore reflects how the BDVs perform when the use is within the manufacturer's intended limitations. When the BDVs are applied in the industry, they experience harsh use and environment, and systematic failures can be introduced, typically during maintenance. The data in OREDA takes this into account since the data are collected in real operation. The problem with OREDA data is that they reflects an average value which implies that the specific conditions for every installation cannot be traced. In the light of this we introduce equation 9.2 where λ_M is the manufacturer failure rate estimate, λ_{OR} is the OREDA failure rate estimate, and π_1 is the ratio between the two estimates. This ratio therefore the represents how the average industrial RIFs influence the "fundamental" failure rate.

$$\lambda_{OR} = \lambda_M \cdot \pi_1 \tag{9.2}$$

One of the key issues related to the application of OREDA data on reliability assessments on FPSOs, is that the OREDA data not necessarily reflects the FPSO specific conditions that will influence on the reliability of the equipment. Since reliability data from all Teekay FPSOs are available, and that all RIFs on each FPSO (theoretically) are identifiable, this collection of data can constitute an important source of knowledge about the reliability performance on Teekay FPSOs compared to data in OREDA. One option is to pool the data from all Teekay FPSO, and determine a factor π_1 as in equation 9.2. This factor express the FPSO specific influence on the failure rate compared to the genric data in OREDA. Now an interesting question arrises. What RIFs are unique for FPSOs compared to the fixed installations where most data in OREDA are collected from? This question is beyond the knowledge of the author of the thesis and should be assessed by competent personnel. Anyway, some logical suggestions are provided:

- Harsher environmental conditions (e.g. due to FPSO movements, and shorter distance to water that might increase the corrosion rate)
- Less people. Can imply that the access to competent personel during e.g. maintenance is more limited.

After these RIFs are identified, the factor π_1 can be calculated, and we get an idea of how the RIFs affect the reliability. For future application of OREDA data, we can in this way determine how the average FPSO specific conditions differ from the average conditions in the industry in terms of the factor π_1.

We know that the mutual reliability performance on the different Teekay FPSOs differs a lot. To increase the confidence and knowledge in future failure rate estimates, the unique RIFs on each FPSO should be identified and investigated. The listed RIFs specific for FPSOs are now not relevant since they are common for all and thus not make a difference. Typical unique RIFs between FPSOs was listed in Section 9.2.1. Investigating these RIFs numerically by e.g. the method described above where a ratio between the different FPSO failure rates are calculated, can be a possibility. Since the mutual RIFs on the different FPSOs are less general compared to FPSO versus fixed installation, and several FPSOs exist leading to multiple ratios, it is probably better to investigate the RIFs qualitatively by comparing different FPSOs and see whether there are similarities indicating significant change of the failure rate. This could typically be routines related to maintenance or that specific equipment brands indicates better/worse reliability. Although this method does not lead to a concrete number, it increases the knowledge about what influences the reliability, which can be usefull both when equipment on future FPSOs is to be chosen, and when prior reliability distributions is to be determined.

9.2.3 Discussion on Quality of Methods

It is quite ironic that a method on how to reduce uncertainty in future reliability estimates is associated with so high degree of uncertainty. We know from Chapter 6 that the quality of OREDA data can be questioned, and the same issues are transferable to the Teekay FPSO data. It also requires a high amount of data before statistical methods with high certainty can support or reject certain hypotheses that can be found relevant. If we assume that the ratio between OREDA data and FPSO data allways have been constant, a possible way of increasing the amount of data is to pool data from all OREDA phases. The same must be done with FPSO data from corresponding phases. If we in addition to this, include data from other systems than the blowdown system, a fair indication on the difference between the applications should be expected. The inclusion of more than one type of equipment must of obvious reasons be done sensible.

Chapter 10

Summary and Recommendations for Further Work

10.1 Summary and Conclusions

This thesis investigates different reliability aspects related to provision and updating of estimates of reliability parameters. A blowdown system on a Teekay FPSO under construction is applied as case. The entire thesis is based on concepts, methods, and ideas from the Bayesian theory and approach. Chapter 2 introduces and discusses the Bayesian theory in the light of its application and usefulness when it comes to updating of reliability parameters. It is shown that the Bayesian approach is well suited for this purpose due to its capability to transform subjective knowledge into quantitative measures and in that way determine a prior distribution which further can be updated with empirical data, giving a posterior distribution.

It is assumed a constant failure rate such that the valve failures are assumed to occur according to a homogeneous Poisson process. The gamma distribution is conjugated to the Poisson process which makes the updating to a posterior distribution easy. Because of this, the gamma distribution is chosen to model the probability distribution of the failure rate.

Chapter 3 describes the blowdown system, its purposes, and its role as a safety-critical barrier. Further, it is described how the blowdown valve is activated on demand, how the blowdown system is annually proof tested, and how the blowdown valve is manually tested every month.

Chapter 4 presents relevant previous work related to updating of reliability estimates and test intervals of SIS. Each of the papers was considered relevant for the topic of this thesis, but the contents of some of the papers are quite similar.

Chapter 5 investigates and discusses the reliability aspects relevant on the blowdown valves. Proof testing is presented in accordance to theory, which implies that full test coverage is assumed. The manual tests performed on the valves are found to have quite similar reliability impact as partial stroke testing, which is debated and discussed in literature. The test coverage of the manual tests is assessed, and it is shown that full test coverage can be a realistic assumption based on findings in OREDA. When full test coverage is assumed, it is shown to have big positive impact on the reliability of the blowdown valves.

The chapter also investigates the case where the test coverage is not 100 %. The PFD is then continously growing before the next proof test, and the manual tests are shown not to have the radical impact (depending on the test coverage) on the average PFD, as was the case when full test coverage was assumed.

Chapter 6 discusses what is relevant sources to include in a Bayesian prior distribution. It is stated, based on findings in relevant literature, that the determination of a prior distribution is the most complicated part of a Bayesian updating process since qualitative knowledge must be transfered to quantitative measures. At present Teekay does not determine a prior distribution when failure rate estimates are assessed in the design phase of the equipment. Instead it is specified as either the estimate provided by the manufacturer of the equipment, or it is based on generic data sources. Further in this chapter, issues related to these two sources are presented and discussed. The data in the generic data sources are collected from a wide range of companies and installations, and thus presents data that reflects the average in the relevant industry in terms of operating conditions, environment, and other relevant factors. Each failure cannot be traced, which implies that it is unknown whether the specific failures are relevant for certain applications. The data is also questionable due to uncertainty about the competence of the staff that evaluates the failures, and that the reliability data for old equipment is not necessarily relevant for new equipment.

Manufacturer data is specific reliability data provided by the supplier of the equipment. This data is either based on self-testing of the equipment, or field data based on reports from the different companies, typically in connection with failures on equipment. The testing can lead to optimistic estimates since the testing is executed under controlled conditions, and thus only reveal primary failure modes and causes. When the equipment is applied in industry, it experiences thougher use and conditions which can increase the failure rate.

Failure estimates based on reported field experience to the manufacturer of the equipment, are inaccurate since the reporting almost exclusively is related to a warranty deal. When the warranty period is over, a very small part of the failures on the equipment are reported.

Chapter 7 provides and discusses a method on how the prior distribution of the failure rate can be determined in a best possible way. The method is based on inclusion of relevant sources that can increase the knowledge about the failure rate. This includes generic reliability data and manufacturer data which at present is applied by Teekay in the design phase, but it is suggested to rely more on previous reliability data from other FPSOs in the Teekay fleet, in addition to expert judgment. By applying expert judgment, it is possible to weigh the different sources and "filtrate" what is most relevant. The prior distribution is suggested constructed by determining proper estimates of the mean failure rate, and a conservative estimate of the failure rate of the distribution. When the prior distribution is constructed, it is suggested to apply the 70th percentile in the distribution when a certain number shall be further applied in reliability calculations. This is in accordance to IEC 61508.

The updating to a posterior distribution is further described. This is a straight-forward application of Bayes theorem which was introduced in Chapter 2. The number of failures, and the total sum of operating hours are simply added to the parameters in the prior, which was shown in Chapter 2.

Chapter 8 discusses what fundamental factors that need to be the basis before an eventual update of the proof test interval can be assessed. It is argued that only operational experience are applied to decide a change of the test interval. To make the operational experience credible, a certain amount of data must be collected. The thesis suggests that the distribution based on only operational data, should be so narrow that the 95th percentile in the distribution, is maximum 3 times the mean value, before operational experience are solely trusted. Given that this requirement is fulfilled, the test interval can be changed relatively to the new failure rate estimate, as long as it is good qualitative reasons to perform the change.

Chapter 9 discusses the different contributors to uncertainty relevant for the different aspects in the case in the thesis. It is shown that there is a high degree of uncertainty related to the relevant aspects. It is assumed that the main contributor to uncertainty, is related to the application of different data sources to determine the prior distribution. This is because of the uncertainty of the relevance of the different data. This is also understated by the discussions in Chapter 6.

Further, this chapter provides a method and discussion on how generic data, with higher certainty, can be applied in future reliability calculations. This is done by investigating the ratio between the failure rate estimate based on Teekay FPSO data, and the failure rate estimate based on OREDA. This ratio expresses how much the FPSO specific risk influencing factors affect the failure rate, compared to the industrial average reflected by the OREDA data. For future use of OREDA data, we now have an idea if OREDA provides conservative or optimistic data when they are used on FPSO equipment.

Together these chapters realize the targets stated in Section 1.2.

10.2 Discussion

As discussed in Chapter 9, there is a high degree of uncertainty related to the relevant aspects of the topic of the thesis. To predict the reliability of technical systems that are not put into operation, is obviously a task associated with high uncertainty. The point is therefore not to eliminate all uncertainty, that is in a practical manner, impossible. The focus is rather how to reduce the uncertainty in the different aspects. If comparing the provided method on how to determine the prior distribution of the failure rate, with the way that Teekay, at present, specify the failure rate in design, it is fair to state that the new method with higher probability, leads to a more accurate estimate on the design failure rate. This because of the inclusion of more sources that are weighted due to its relevance. Teekay specify the design failure rate as either the estimate provided in OREDA, or based on manufacturer data. This is not optimal, but in fact not the biggest problem. The problem is that the failure rate in operational phase, is either specified as the estimate from design, or the empirical estimate from operation. For a blowdown system, that experiences few failures, this is inadequate. The Bayesian method provided in this thesis, leads to a gradual transition between the failure rate from design, and the failure rate based on operational experience, which is well suited for SIS that experience few failures.

There is no doubt that the methods provided in the thesis, are comprehensive, and it requires effort to implement them in the daily work. Anyway, for experienced reliability engineers the concepts are rather easy to understand. The main contribution from the thesis is probably the concepts, methods, and discussions regarding the prior distribution development, and updating to a posterior distribution. If this is implemented, Teekay will perform state of the art with respect to updating of reliability parameter updating. The methods in the thesis, also indirectly, forces Teekay to be more familiar with its FPSOs, and its equipment. By investigating how different risk influencing factors affects the reliability of the equipment, the future estimates on new equipment will be more and more accurate as the knowledge increases.

10.3 Recommendations for Further Work

This section suggests possible extensions of the work in this thesis.

- When developing the prior distribution, how can expert judgment be applied in best possible way?
- Investigate and state the FPSO specific RIFs. If comparing the Teekay FPSO data with the industrial average reflected by OREDA data, can it be stated that the FPSO specific RIFs significantly affects the failure rate on certain components? How trustworthy is this method with respect to the different contributors of uncertainty?
- The Teekay FPSOs operates under different conditions and environment. Investigate how these differences influence on the failure rate of the equipment.

Bibliography

Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., and Bereguer, C. (2010). Failure rate evaluation with influencing factors. *Journal of Loss Prevention in the Process Industries*, 23:187–193.

EXIDA (2007a). *Safety Equipment Reliability Handbook. Volume 1: Sensors*. EXIDA.

EXIDA (2007b). *Safety Equipment Reliability Handbook. Volume 2: Logic Solvers & Interface Modules*. EXIDA.

EXIDA (2007c). *Safety Equipment Reliability Handbook. Volume 3: Final Elements*. EXIDA.

Hamada, M. S., Wilson, A. G., Reese, S., and Martz, H. F. (2008). *Bayesian Reliability*. Springer.

Hauge, S. and Lundteigen, M. A. (2008a). Guidelines for follow-up of safety instrumented systems(SIS) in the operating phase. Technical report, SINTEF.

Hauge, S. and Lundteigen, M. A. (2008b). A new approach for follow-up of safety instrumented systems in the oil and gas industry. *Safety, Reliability and Risk Analysis: Theory, Methods and Applications (ESREL 2008)*.

Hauge, S. and Lundteigen, M. A. (2009). Updating failure rates and test intervals in the operational phase: A practical implementation of IEC 61511 and IEC 61508. *Reliability, Risk and Safety - Theory and Applications (ESREL 2009)*.

Hauge, S. and Lundteigen, M. A. (2010). Management of safety integrity in the operational phase. *Inside Functional Safety*, Available at: http://www.insidefunctionalsafety.com/ Accessed: 9 June 2012.

Hauge, S., Lundteigen, M. A., and Haabrekke, S. (2010). *Reliability Prediction Method for Safety Instrumented Systems*. 07 Gruppen AS.

Houmb, S. H., Johnsen, O. A., and Stålhane, T. (2000). Combining disparate information sources when quantifying security risks. Available at: http://www.idi.ntnu.no/grupper/su/publ/siv/rmci04-houmb-johnsen-stalhane.pdf. Accessed: 14 May 2016.

IEC 61508 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. The International Electrotechnical Commision, Norsk elektroteknisk komite.

IEC 61511 (2003). *Functional safety - Safety instrumented systems for the process industry sector*. The International Electrotechnical Commision, Norsk elektroteknisk komite.

OLF 070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. Oljeindustriens landsforening.

OREDA (2009). *Offshore Reliability Data*. OREDA participiants, SINTEF.

Rausand, M. (2011). *Risk Assessment: Theory, Methods and Applications*. WILEY.

Rausand, M. and Hoyland, A. (2004). *System Reliability Theory. Models, Statistical Methods, and Applications*. WILEY.

Rausand, M. and Lundteigen, M. A. (2008). Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, 21:579–588.

S-001 (1999). *Technical Safety*. NORSOK.

Siu, O. N. and Kelly, D. L. (1998). Bayesian parameter estimation in probablistic risk assessment. *Reliability Engineering & System Safety*, 62:89–116.

Smith, C., Kelly, D., and Dezfuli, H. (2009). Probability-informed testing for reliability-assurance through bayesian hypothesis methods. *Reliability Engineering and System Safety*, 95:361–368.

Summers, A. E. (2000). Partial-stroke testing of block valves. *Instrument Engineers Handbook*, 4.

Vatn, J. (2006). Procedures for updating test intervals based on experience data. ESREDA seminar on Reliability of Safety-Critical Systems.

Wikipedia. http://en.wikipedia.org/wiki/Ball_valve. Accessed: 22 May 2012.

Curriculum Vitae

Name:	**Magnus Woll Bjartnes**
Gender:	Male
Date of birth:	2. August 1986
Address:	Stadsingeniør Dahls gate 21, N–7015 Trondheim
Nationality:	Norwegian
Email:	magnusbjartnes@gmail.com
Telephone:	+47 41932202

Language Skills

Norwegian as first language. Speaks and writes English fluidly. Basic skills in German.

Education

- Verdal Videregående Skole (Collage). 2002-2005
- Compulsory military service. CSS Batalion, Bardufoss, Norway. 2005-2006
- Mechanical Engineering. NTNU. Specialization in RAMS. 2006-2012

Experience

- Sarens AS. Summer job, 2009 and 2010
- Kværner AS. Summer job, 2011.
- First job after graduation: Aker Solutions, Trondheim. Starting August 2012

Hobbies and Other Activities

Training, Climbing, Guitar, Music, Reading