Design for Reliability – Applied to development of subsea process systems

Trondheim, June 14th, 2010
MASTER THESIS
2010
for
stud. techn. Ingrid Almås Berg

DESIGN FOR RELIABILITY - APPLIED TO DEVELOPMENT OF SUBSEA PROCESS SYSTEMS
(Pålitelig design – anvendt på undervanns prosess-systemer)

The subsea power and process department at Aker Solutions is working to create innovative processing solutions within the subsea oil and gas industry. Reliability is one of the single most important factors in the operation of subsea systems. It is therefore vital to address product performance throughout the whole lifecycle of the equipment, from front-end design through installation and operation.

The main objective of this master thesis is to consider relevant methodologies and practices for reliable product design; discuss the application of these in the industry in general and for the subsea process industry in particular. The thesis shall describe the methods for reliable design throughout the lifecycle of a product/system and develop an appropriate methodology for a subsea process system. The identified methodology shall then be applied to the development of a specific process sub-system.

The main objective is further divided into the following more specific sub-targets or objectives:

1. Perform a literature study on the application of different methods for design for reliability. The literature study should cover, and discuss, methods normally applied across relevant industries.

2. Familiarise with systems and main equipment used within subsea process industry.

3. Based on learning from the literature study discuss and summarise the main factors that contribute to unreliability. Describe challenges for the subsea process industry in particular.
4. Suggest and develop a methodology for reliability performance and specification throughout five defined stages of a Product Life Cycle (Front-end, Design, Development, Production and Post-Production) of a typical Subsea Process System. Special attention should be paid to the first three phases.

5. Perform a case study to evaluate the applicability of the suggested methodology for a chosen stage of the life cycle. The case study should be applied to a chosen sub-system within a typical subsea process system.

Following agreement with the supervisor and the responsible professor, the various tasks may be given different weights.

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

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

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

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

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

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

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

Deadline: June 14th 2010.

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

Responsible professor/Supervisor at NTNU: Professor Marvin Rausand
Telephone: 73 59 25 42
Mobile phone: 456 66 265
E-mail: marvin.rausand@ntnu.no

Supervisor at Aker Solutions: Guro Rausand
Senior Subsea Engineer
Power, Processing & Boosting
Telephone: 67 52 74 17
Mobile phone: 472 34 442
E-mail: guro.rausand@akersolutions.com

DEPARTMENT OF PRODUCTION AND QUALITY ENGINEERING

Per Schjølberg
Associate Professor/Head of Department

[Signature]

Marvin Rausand
Responsible Professor
Preface

This master thesis is written at the Department of Production and Quality Engineering, NTNU, during the spring of 2010. The thesis is a part of the 5th year of the master program in Product Design and Manufacturing.

The title of the thesis is “Design for Reliability – Applied to development of subsea process systems” and it is carried out in cooperation with the Subsea Power and Process department at Aker Solutions. It is assumed that the reader has some prior knowledge of reliability analysis and probability, preferably through the course TPK4120 – Safety and Reliability Analysis. If a glossary is needed, it is suggested that the reader uses “System Reliability Theory” (Rausand and Høyland 2004). The report should be read according to the structure described in chapter 1.3, especially where appendices are concerned.

I would like to thank my supervisor Prof. Marvin Rausand and my co-supervisor Prof. Mary Ann Lundteigen at NTNU, and my supervisor at Aker Solutions, Guro Rausand, for guidance, contributions and advices throughout the semester. I also wish to thank the employees at the Subsea Power and Process department for their contributions and support during my stay at Aker Solutions.

Trondheim, June 11th 2010.

Ingrid Almås Berg
Abstract

New products arrive on the market every day. Whether it is a computer, a cellular phone or a car, the consumers are attacked by commercials enticing them to try “the newest invention”. Getting a customer to buy a product may be a challenge, but trying to keep him or her satisfied can be far more difficult. The regular western consumer is often well aware of what he or she demands of a product. Depending on the product, a safe failure can be accepted with a swift repair. What is not accepted is for a cellular phone to fail three times in seven months. Every product has an expected reliability. If the product cannot answer to this reliability, the manufacturer will be forced to repair products, answer to warranty claims and possibly suffer a large economic loss.

Some industries demand very high reliability of the systems they use, especially as the systems are expensive and failures could cause extreme harm. A country’s authorities have regulations for most industries and especially strict regulations for “high risk” industries. An example of a “high risk” industry is the petroleum industry. A normal requirement for new subsea process systems in this industry is an availability of 97%. To achieve such a high number, the reliability must be high as well. When a new Subsea Compression System (SCS) is built for Norwegian oil and gas production, the laws and regulations of the Norwegian authorities must be followed. These concern the maintainability and reliability of the system, as well as the safety of the system, the environment and the employees of the operator.

Reliability is an increasingly popular subject to consider for manufacturers and authorities around the world. A problem is that there are many different thoughts on how reliability can be achieved. To ensure a common understanding between authorities, manufacturer and client, several standards concerning reliability have been developed. These are often specific to an industry and one example is ISO 14224; Petroleum and natural gas industries – Collection and exchange of reliability and maintenance data for equipment.

With a large number of specified reliability standards, one should think that considering the product reliability throughout the product life cycle was normal. This is not necessarily the case. In the early parts of the product life cycle, before the physical development commences, many still believe that reliability activities are a waste of time, resources and money. What they do not consider is the fact that alterations are easier to perform before a product is manufactured than after.

A product life cycle is usually split into phases. For reliability activities in the product life cycle, Murthy et al. (2008) suggests eight phases. The first three occur during the pre-development, the two following take place during production, while the last three are part of the post-development. The events taking place in these phases and the main tasks of a reliability engineer are well described, and it is thus a good option for Design for Reliability.

Reliability engineering has existed as an engineering discipline for several decades now. Especially the nuclear and the aerospace industries have studied and developed methods for reliability. The methods can help detect and evaluate possible hazards and failure modes experienced by the system or product during its operational life. Some of the methods study how and why the hazards may occur, while other studies how a failure affects the overall system. Through probability estimates, the reliability of a system is found. Examples of such methods are HAZID, FMEA and FTA.
Even though we have methods for reliability straight in front of our nose, many are unaware of why they should be used. A system will never be 100% reliable, because of all the factors contributing to a reduced reliability. In all eight life cycle phases such factors can be found. Whether the manufacturer is in the car industry or the petroleum industry, many of the factors will be the same. One important issue is uncertainty, especially of the epistemic type. This is the uncertainty which we cannot know is there. It is hard to say whether the communication is good enough or if the inputs to the reliability methods are acceptable. Another factor is the human being who is unpredictable and thus unreliable. He or she partakes in every step of the product development and is thus probable to contribute to the decreased reliability. However, we cannot let the fear for such factors leading to less reliable products keep us from developing something new. By being aware of them, we can use the factors to employ reliability methods and thus increase the possibility that the methods are used correctly.

In using several methods to study the same product or system, we are more likely to get a full picture of the hazards, failures and overall product reliability. One type of analysis including several methods is the RAM analysis. This studies availability and maintainability together with reliability. The three disciplines are highly connected and equally important for the product performance. Although the RAM analysis is a very efficient tool, it cannot stand alone. It is necessary to use other methods prior to it to obtain the input, as well as some methods afterwards which can make use of the outputs.

Placing a reliability method at a random time during the design and development phases is not considered good utilization of the method. It must be used when the necessary information is available and the output can be of use. To combine and place the methods correctly, a methodology has been developed. This is described at a level meant for entirely new products, whether they are standard products or one-of-a-kind. The methodology is very general, but for industries where the reliability is very important, they should be specified. The specification can be according to the industry, but it would be even better according to organisation. A specified example has been prepared for a subsea organisation. The purpose of both the general and the specified methodology is to use them as a basis in the development of reliability programmes.

Reliability programmes are established specifically for one product development project, often for one phase at the time. It states why a method is chosen, when it should be used and the responsibilities where the product reliability is concerned. It should be based on the project risk, the project tasks and the available time and resources. Using a reliability methodology to choose the methods and their combination will simplify the programme development and ensure its quality.

For manufacturers who do not understand why reliability should be included in the design process, or how this can be done, a website is useful. The internet is highly accessible, easy to use and not time consuming. If a website for Design for Reliability first is developed, it can be used as an educational tool by and for reliability engineers. It can also help in the development of more specific methodologies and reliability programmes.

Reliability methods, methodologies and programmes will train a manufacturing organisation in thinking differently when they develop new systems and products. The outcome of the development will be products which are reliable, safe and functioning as they are supposed to. This will again lead to more satisfied customers. No customer will accept that reliability activities were left out of the product development when they stand with a failed product in their hands.
List of contents

Preface ................................................................. i
Abstract .............................................................. ii
List of contents ......................................................... iv
List of tables ........................................................... vi
List of figures ........................................................... vi

1. Introduction ................................................................. 1
   1.1. Objective ......................................................... 2
   1.2. Scope and limitations ............................................. 2
   1.3. Structure .......................................................... 3

2. Reliability ................................................................. 4
   2.1. RAMS ............................................................. 5
   2.2. Probability and reliability ...................................... 7
   2.3. Discussion ......................................................... 11

3. Subsea industry requirements ........................................ 12
   3.1. Petroleum Safety Authority .................................... 12
   3.2. Standards .......................................................... 14
   3.3. Further comments ............................................... 19

4. Product life cycle ......................................................... 21
   4.1. Phases in a general perspective ............................. 21
   4.2. 8 Phases for reliability ......................................... 23
   4.3. Discussion ......................................................... 26

5. Methods for reliability ............................................... 27
   5.1. PHA and HAZID ............................................... 29
   5.2. SWIFT ............................................................. 30
   5.3. FMEA ............................................................... 31
   5.4. FTA ................................................................. 33
   5.5. RBD ................................................................. 34
   5.6. HAZOP ............................................................ 36
   5.7. Reliability Growth ............................................... 38
   5.8. Accelerated testing .............................................. 40
   5.9. FRACAS .......................................................... 42
   5.10. Discussion ......................................................... 43

6. RAM analysis ............................................................. 44
   6.1. Method ............................................................. 44
   6.2. MIRIAM Regina .................................................. 45
   6.3. Use of outputs ..................................................... 46

7. Unreliability ............................................................... 48
   Phase 1 ................................................................. 49
   Phase 2 ................................................................. 51
   Phase 3 ................................................................. 53
   Phase 4 ................................................................. 54
   Phase 5 ................................................................. 56
List of tables
Table 1: Standards used in phases ................................................................. 20
Table 2: Project risk categorisation (ISO 20815 2008) ................................. 80

List of figures
Figure 1: The bathtub curve ........................................................................... 8
Figure 2: The repetition in a frequentist approach experiment ....................... 9
Figure 3: Experiment with previous knowledge in the Bayesian approach ....... 10
Figure 4: The data collecting process (ISO 14224 2006) ................................. 16
Figure 5: Design review process (IEC 61160 2006) ......................................... 18
Figure 6: Design review and response process (IEC 61160 2006) ................. 18
Figure 7: Phases, Levels and Stages (Murthy et al. 2008) .............................. 24
Figure 8: Connection between life cycle phases (Murthy et al. 2008) ............ 25
Figure 9: SADT model (Rausand & Høyland 2004) ....................................... 28
Figure 10: SADT PHA/HAZID ........................................................................ 30
Figure 11: SADT SWIFT .................................................................................. 31
Figure 12: SADT FMEA .................................................................................... 32
Figure 13: Fault Tree Process (NASA (A) 1999) ............................................. 33
Figure 14: SADT FTA ....................................................................................... 34
Figure 15: RBD ................................................................................................. 35
Figure 16: SADT RBD ...................................................................................... 36
Figure 17: HAZOP process (IEC 61882) ......................................................... 37
Figure 18: SADT HAZOP ................................................................................ 38
Figure 19: Reliability Growth process ............................................................ 39
Figure 20: SADT Reliability Growth ............................................................... 40
Figure 21: SADT Accelerated testing ............................................................... 41
Figure 22: SADT FRACAS .............................................................................. 42
Figure 23: Unreliability - reliability ............................................................... 48
Figure 24: The whispering game .................................................................... 50
Figure 25: Baseball ......................................................................................... 61
Figure 26: Reliability methodology phase 1 ................................................... 63
Figure 27: Reliability methodology phase 2 ................................................... 65
Figure 28: Reliability methodology phase 3 ................................................... 67
Figure 29: Reliability methodology phase 4 ................................................... 69
Figure 30: Reliability methodology phase 5 ................................................... 71
Figure 31: Reliability methodology phase 6 ................................................... 73
Figure 32: Reliability methodology phase 7 ................................................... 75
Figure 33: Reliability methodology phase 8 ................................................... 76
Figure 34: Front page of website for Design for reliability (http://folk.ntnu.no/ingribe) ...... 83
Figure 35: Life cycle (http://folk.ntnu.no/ingribe/productlifecycle.jsp) .......... 84
Figure 36: Phase 7 as opened from figure 35. ................................................ 85
Figure 37: Failure-reliability diagram ............................................................ 87
1. Introduction

On April 20th this year, a blowout occurred while the Deepwater Horizon oil rig was drilling in the Maconado Prospect oil field in the Gulf of Mexico. This led to an explosion which sank the rig into the sea, killed several crew members and gave way to an oil leak which has yet to be stopped six weeks later (Cleveland 2010). The accident has spurred heavy criticism against the petroleum industry, particularly as the accident is only one out of many. Today, the world’s population does not know how to live without oil and gas. Until new technology provides acceptable amounts of energy, or the oil and gas is spent, the petroleum industry will survive. We can only demand that the systems and technology used are as safe and reliable as possible.

Failures occur in every industry and it seems we cannot avoid them. A customer wants the product to perform as expected, being both reliable and safe. Minor failures are acceptable, but many and dangerous failures are insupportable. Manufacturers lose money, clients and credibility if their products fail prematurely. One solution is Design for Reliability, a discipline in which reliability activities are performed concurrently with the design. It is believed that shortcomings in the design affect the whole product (O'Connor 2002). The feedback from reliability analyses are thus expected to help the designers develop the most reliable system possible.

Design is a creative process, reliability analyses are not. Reliability activities are dependent on timing and strict rules. Some believe that reliability activities in the design phase are a waste of money. Testing of the materials and prototypes should be enough. However, this is likely to be a more expensive approach if the design needs alterations. To alter the design after the physical development is likely to cost more, both in time and money, than during the design process.

An example of a manufacturer who employs Design for Reliability in the product development is Aker Solutions. This company is one of several suppliers to the petroleum industry. Currently their Subsea Power and Process department is preparing a Subsea Compressions System (SCS) project for the Midgard field on the Norwegian continental shelf. The pressure in wells decreases as oil and gas flow out. To keep the flow rate above a critical minimum and maximise reservoir recovery, the SCS is a solution. Both Norwegian authorities and the client demand high reliability from subsea process systems. A failure in an SCS will not lead to a blowout, but possibly a loss in production or a minor leakage. The former will affect the income of the operator. The latter is likely to cause environmental damage. To prove to the client that Aker Solutions can fulfil the requirements, they need a reliability programme for the design and development. Similar reliability programmes are now also demanded in other industries such as the nuclear, the aerospace and the military industry.

Many methods for reliability have been developed throughout the years. They demand different inputs and provide the analyst with several types of outputs. If used correctly, they will give valuable input to the development and use of the products. To choose the best combination and timing of the methods, it is necessary to know the factors contributing to unreliability and how the methods can prevent them. It is of interest to establish a methodology based on the methods and the product life cycle. Can a general reliability methodology be a basis for specified reliability programmes? If a methodology simplifies the establishment of reliability programmes, can this be used to convince those who do not use reliability activities during the design phase? Can an internet site on the subject be of help and can it become a tool for reliability engineers in different industries?
1.1. **Objective**

The main objective of this master thesis is to study reliability methods and the factors contributing to unreliability, and use this to develop a methodology for Design for Reliability. Further, the methodology shall be used to develop a reliability programme applied for a specific phase of the product life cycle of a Subsea Compression System developed by the Subsea Power and Process department at Aker Solutions.

The objective is further divided into five main tasks:

1. How are the different methods used in Design for Reliability applied across the industries?
2. Prepare a system description of a system used within the subsea process industry.
3. Discuss and summarise the main factors that contribute to unreliability, specifically challenges for the subsea process industry.
4. Develop and describe a methodology for reliability performance and specification throughout the five defined stages of a Product Life Cycle of a typical subsea process system.
5. Perform a case study to evaluate the applicability of the suggested methodology for a chosen stage of the life cycle, applied to a chosen sub-system within a subsea process system.

1.2. **Scope and limitations**

The thesis assignment was given by the Subsea Power and Process department at Aker Solutions, who specialises on the subsea process industry. It was demanded that reliability in product design was applied to the industry in general and further for the subsea process industry in particular. The thesis is thus written with all industries in mind, while using the subsea process industry to exemplify the further use of the reliability methodology, unreliability issues and in the case study.

The thesis was carried out during a project development of a Subsea Compression System for the Midgard field. This field lies on the Norwegian continental shelf and is operated by Statoil. Any standards and regulations used as a basis for reliability methods in this thesis are thus restricted to those required by Statoil and followed by the Aker Solutions Subsea Power and Process department for this specific project. This implies that only Norwegian laws and regulations are described.

The study of systems and equipment used within the subsea process industry has mainly been limited to the items of interest to the Subsea Compression System. The more common types of equipment such as X-mas trees, well-heads etc. have thus not been in the focus of this thesis.

The product life cycle is normally studied through phases, but the number of phases varies. Task 4 in the assignment states that five phases; Front-End, Design, Development, Production and Post-Production are to be followed. Murthy et al. (2008) looks specifically into the subject of reliability in the product phases and suggests that a framework with eight phases is more suitable. This gives smaller gaps between the start and end of each phase and specifies whether the system is studied on a component, product or business level. It is thus easier to evaluate the answers needed for reliability purposes in each phase. After an agreement with the supervisors, it was decided that these eight phases should be the basis of the methodology.

As stated in the preface to this thesis, the reader is assumed to have some prior knowledge of the subjects reliability, statistics and probability. This limits the basic explanation of ordinary probability distributions and how each reliability method is performed. The assumption also helps limit the time spent before the main subjects of the report are addressed.
1.3. Structure

The first chapters study background issues for the methodology, beginning with an introduction to reliability and related concepts in chapter 2. Chapter 3 looks at the subsea process industry requirements concerned with reliability on the Norwegian continental shelf, and chapter 4 describes the life cycle phases of relevance to the report.

The subsequent chapters are generally following the sub-objectives described in 1.1. Chapter 5 looks into several methods created and used for reliability purposes. The methods are considered through the use of the Structured Analysis and Design Technique (SADT), which is also presented in this chapter.

Chapter 6 describes the Reliability, Availability and Maintainability analysis (RAM analysis), which is a collection of reliability methods and simulation tools. This type of analysis is often used for development projects across industries and gives a good overview of a product’s availability and reliability.

Factors contributing to unreliability are discussed in chapter 7. These are assumed to reduce the possible reliability of the product and may arise in all phases of the life cycle. The subsea process industry has been studied as an example in relation to the factors. The eight phases suggested by Murthy et al. (2008) are used as the background for the discussions.

A general methodology for Design for Reliability is described for each of the eight phases in chapter 8. Methodology here refers to a simple set of methods related to other development activities. No time frame is set, nor is any product specified. One figure for each phase is discussed and the main reliability tasks summarised. The general idea is that these tasks are managed by one or more reliability engineers, participating in the development together with other team members responsible for design, economy etc. A methodology has been developed for Aker Solutions to show how a more specific methodology for an organisation or industry can be prepared. This is based on the general methodology and Aker Solutions’ Technical Qualification model. The Technical Qualification can be found in appendix B and the Aker Solutions methodology in appendix C. These are placed in the appendices for confidentiality reasons, but should be studied together with chapter 8.

Chapter 9 describes the case study, an Equipment Reliability Management Programme (ERMP) developed for the Engineering, Procurement and Construction (EPC) phase of the Midgard SCS project. The ERMP is based on ISO 20815 and the Aker Solutions project execution model (PEM), found in appendix D. Appendix E contains the ERMP as it is presented to Statoil.

A website has been made in connection with this thesis, as a suggestion for how Design for Reliability and reliability methodologies can be presented on new arenas. The website can be found on http://folk.ntnu.no/ingribe and it is presented in chapter 10. A discussion on how it may be further developed into a tool for reliability engineers is also made.

The main questions for this thesis were how Design for Reliability can be used in the product life cycle through a methodology, and how a methodology can be specifically applied to several different projects. The results of the thesis are discussed, together with other concluding remarks, in chapter 11.

Appendix A contains a system description of the Midgard SCS which can be used in order to understand how the design has been developed prior to the start-up of the EPC phase. This is also a part of the answer to sub-target 2 described in chapter 1.1.
2. Reliability

The English word “reliability” is believed coined by the English author Samuel Taylor Coleridge in 1816. As quoted by Selah and Marais (2006), this phrase is the eldest recorded use of the word:

“He inflicts none of those small pains and discomforts which irregular men scatter about them and which in the aggregate so often become formidable obstacles both to happiness and utility; while on the contrary he bestows all the pleasures, and inspires all that ease of mind on those around him or connected with him, with perfect consistency, and (if such a word might be framed) absolute reliability.”

Today, reliability is used to describe persons and objects, although the latter might be the more popular. Most people have an understanding of what the term means and how to use it. A normal customer expects a TV to function longer than five years in a normal living room. The same customer would also understand that the TV cannot be expected to work for long outside in -50°C and rain. If the TV fails in the first case, the customer would complain about its reliability. A failure in the second case would normally not lead to a complaint. Technical reliability is defined as (IEC 60050-191 1990):

*The ability of an item to perform a required function under given conditions for a given time interval.*

A customer is likely to base his or her possibility for complaining about the failure of the TV on this. What the customer might not understand is how high product reliability is achieved. When new technology is developed, it is its ability to function as required which is the point of departure. If it is unlikely that the technology can perform as desired, there is little reason to consider under which conditions and what amount of time it must function. Reliability is an engineering discipline, using specifically developed standards and tools. Its objective is to help the design engineers and maintenance organisations achieve and sustain reliable and safe systems. IEEE describes the discipline in the following manner (IEEE 2009):

*Reliability is a design engineering discipline which applies scientific knowledge to assure a product will perform its intended function for the required duration within a given environment. This includes designing in the ability to maintain, test, and support the product throughout its total life cycle. Reliability is best described as product performance over time. This is accomplished concurrently with other design disciplines by contributing to the selection of the system architecture, materials, processes, and components -- both software and hardware; followed by verifying the selections made by thorough analysis and test.*

As IEC 60050-191 (1990) suggests, reliability is mainly concerned with a required function. An mp3-player which plays music is supposedly answering the definition. If the same mp3-player is unable to switch songs according to its owner’s wishes, is it still reliable? This depends on how the required function is defined. A required function is (IEC 60050-191):

*A function or a combination of functions of an item which is considered necessary to provide a given service.*

If the required function of the mp3-player includes the ability to “switch a track according to its owner’s wishes”, alongside “the ability to play music”, it must do so. An important step in the development of a reliable product is thus to make a thorough definition of the required function.
As explained by IEEE, reliability engineering also includes a consideration of maintenance. This hints towards an umbrella discipline called Reliability, Availability, Maintainability and Safety (RAMS). It suggests that these four disciplines are connected and affect one another. A product with high reliability, based on a well defined required function will not only satisfy its user on a level of functionality, it will also be safe and able to operate whenever demanded. All provided that the operational conditions are acceptable.

### 2.1. RAMS

Reliability, availability, maintainability and safety are interrelated disciplines; they may all be improved if one of them is improved. If focus is set on all four disciplines during design and development, the reputation of the manufacturer is unlikely to be damaged by the product. Requirements to the product can be given with RAMS as a basis. Such requirements can be split into four categories (Lundteigen et al. 2009):

- Functional safety and safety integrity requirements.
- Product safety requirements.
- Operational availability requirements.
- Maintainability and maintenance support requirements.

To understand these types of requirements, reliability, availability, maintainability and safety must be understood. Reliability was introduced in the previous section and will here only be discussed through the other three subjects in the RAMS discipline.

**Availability**

IEC 60050-191 (IEC 60050-191) defines availability as:

> The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

This definition focuses on repairable systems in the operational phase, stating that they are available when they function or are able to operate. Any downtime due to failure, maintenance or repair will contribute to a lower availability. Availability is the probability that the product will be in operation at a given time (Rausand and Høyland 2004). Mathematically, average availability is defined as the ratio between the uptime and the total time the product is meant to be in operation.

\[
A_{\text{avg}} = \frac{\text{uptime}}{\text{time in operation}}
\]

If reliability is described as “Mean time to failure” (MTTF), availability is MTTF divided by the sum of MTTF and the “Mean time to repair” (MTTR). MTTF and MTTR are defined mathematically in Rausand and Høyland (2004).

\[
A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}
\]
This formula indicates that the availability of a product increases proportionally with the reliability. A customer is interested in having the highest availability possible. If the downtime after a failure is very long, the equation shows that the reliability needs to be high for the availability to stay high. This does not mean that a product with low downtime can be produced without a thought to reliability, although this might give an acceptable availability. A very low reliability would mean frequent failures, which might even be more frustrating to the customer than the long downtime. Whether the availability is high due to high reliability alone or in combination with a low downtime, it is evident that the reliability is the key factor. It should therefore be in every manufacturer’s best interest to design for reliability.

**Maintainability**

Maintainability is the ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources (IEC 60050-191 1990).

Maintainability combined with reliability determines the product availability. The maintainability is a design feature that describes how easily a product or system can be maintained or repaired (IEC 60300 2003). For example, a subsea installation is placed on the seabed and it is only accessible through the use of specific intervention vessels equipped with tools such as Remotely Operated Vehicle (ROV). When a subsea process system fails, the simplicity of the repair operation depends on:

- Simple interfaces to the system
- Easily retrievable modules
- Available spare parts

If the reliability of a product has been considered from the early life cycle phases, it is known how it might fail. This information has probably also been used to establish an appropriate spare part philosophy based on which subsystems generally need the most maintenance. The interfaces are the keys to an easy system repair. The easier it is to reach the system, the easier it is to repair. The ability to retrieve a module which cannot be repaired sub sea or must be replaced is also important for the time to repair. Finally, the available spare parts decide how fast a repair may begin. If the part is considered very important for the availability, it is possible that a spare part is placed on the seabed for a lower repair time.

Good maintainability increases the availability and decreases the chances of leaving systems in a failed condition for a long time. An unrepaired failure may not only lead to a long system downtime, but it can also lead to problems with the safety of the system.

**Safety**

IEC 61508 (2005) defines safety as:

*Freedom from unacceptable risk.*

When a reliability analysis is performed, it considers the probability of the occurrence of a hazardous event leading to a function failure. The safety analysis will include this step and can therefore be performed as a continuation of the reliability analysis. A reliability analysis evaluates the possibility of failure and how to keep it from occurring. The safety analysis looks into the effects of a failure and
how to mitigate them. Together the two will give a full picture of how the initiation, development and consequence of a failure can be avoided.

The reliability, availability, maintainability and safety of an undeveloped product can only be considered through estimates. Based on previous knowledge, the probability that an event takes place can be discovered and used in the design process.

2.2. Probability and reliability

During a lecture held in 1929, Bertrand Russell said (Der Kiureghian and Ditlevsen 2009):

“Probability is the most important concept in modern science, especially as nobody has the slightest notion of what it means.”

Even today, 80 years after Russell’s lecture, there is no agreement on how to interpret probability. What there is an agreement on is that probability is helpful in the description of the future. The future is unknown and uncertain, but it is possible to predict upcoming events based on past experiences. Historical events are certain, and an example is the knowledge about how a condemned car performed its tasks. A new car can be expected to drive through the same areas, under the same conditions as the old car. The historical performance data of the condemned car can thus be used to find data for the new car. The events of the future are not known, but the information about what has happened may give a pointer to what is to come. Reliability is based on the probability of future events and estimated through the probability of how a system is expected to behave when experiencing them.

Data used for reliability estimates can be found through field experience, expert judgments and testing (Rausand 2005). Field experience data are collected and stored in data bases, such as the Offshore Reliability Database (OREDA). Expert judgements are derived by experts on the field who study previous information, the system, environmental conditions etc to find answers. Testing is done under specified and stable conditions. The three methods may also be considered together, but it is important to remember that they all have uncertainties connected with their answers. Uncertainty will always be found in relation to probability, especially as probability does not give any specific answer. For this reason, one cannot be uncritical in the use of probability estimates (Berg 2009).

The OREDA project is used in the Norwegian petroleum industry and gathers failure rate information from several companies. The database is used to make predictions and model the failure probabilities for different types of equipment under development. A normal model for failure rates is the bathtub curve.
This curve consists of three failure rate distributions, representing the three main phases of the operational life; infant mortality, normal life and wear-out. In the first phase, the unknown defects may become visible. During the normal life, the failure rate stays almost constant, while in the wear-out phase the product’s age makes it more likely to fail. For a reliability engineer, this is an easy way to show how the reliability of a function is connected with the item’s age. The probability distributions thought to be the most representative of the product’s behaviour through its life are chosen. When a curve is developed for the product life cycle, it can be used to explain why one failure rate is given for the whole operational life of a component.

The failure rates in OREDA are found through assumptions about how the data from different fields fit together. They are also considered constant through the assumption that infant mortality is removed through testing, while the wear-out phase is avoided by replacement. For this, the bathtub curve is an excellent explanatory model.

### 2.2.1. Probability approaches

As there is no agreement on what probability means or how the concept should be interpreted, many theories can be found. The main difference between the theories is the discussion of whether probability is a property of the object studied or something outside it seen only by the person studying it. From the most dominating theories, the Frequentist and the subjective interpretations, two main approaches are developed to find probability parameters. These are the Frequentist and the Bayesian approaches. The two are thought to be incompatible and some would even claim that a true scientist only accepts one of the approaches (Vallverdú 2003).

**Frequentist approach**

This approach is tightly knit to the theory that the probability is a property of the object. Among the theories related to this are the Classical probability theory, the Finite frequency theory, the Relative frequency theory and the A priori theories (Berg 2009). The values of interest are found through several trials performed under the same conditions over a long period of time. Probability is then the long-term fraction of times that an event occurs, in a large number of trials (NUREG/CR-6823 2003).
A very important aspect of the Frequentist approach is that all personal believes must be put aside. There is a real value $\lambda$ for the object studied and the objective is to infer it. The probability of the real value $\lambda$ is hence not up for discussion, only for the estimated value (Hallinan 2009).

When a new hypothesis has been developed, the goal of the frequentist approach is to see if it can be rejected. This is the normal approach often used in physics to decide whether a hypothesis is actually a law. The question is (Hallinan 2009); “Is the data probable given the null hypothesis?” The null hypothesis is then the alternative hypothesis which one uses to prove that the original hypothesis is wrong. If nothing goes against the hypothesis, it can be accepted.

Repeateable experiments are used to find the true value. However, the frequentists accept that to continue experiments for all eternity is unpractical. They therefore say that after a large amount of trials, the value is close enough to the real value to be plausible. This value can be used to represent the object studied in other studies.

Bayesian approach
The Bayesian or subjective approach desires to modify uncertainty through logic, believing that probability is a quantification of a person’s degree of belief. The probability is thus turned from a personal opinion into something rational through logic (NUREG/CR-6823 2003). The approach is based on theories such as the Subjective/Bayesian theory and the Impersonal theory.

While the Frequentist approach only considers information found through homogenous testing, the Bayesian approach accepts all known information. It is acceptable to have a prior belief about what one observes. This belief is then used to find the posterior value. As more information is obtained about the object studied, the estimate is updated further. While the Frequentists whish to prove that a hypothesis is correct by rejecting other hypotheses, the Bayesians prove correctness through the data supporting it (Hallinan 2009).

The goal is to update the prior belief through Bayes’ theorem:

$$P(B_r|A) = \frac{P(B_r \cap A)}{\sum_{i=1}^{k} P(B_i \cap A)} = \frac{P(A|B_r)P(B_r)}{\sum_{i=1}^{k} P(A|B_i)P(B_i)} \text{ for } r = 1, 2, \ldots, k$$
Bayes’ theorem here shows \( P(B_r | A) \) as the probability that event \( Br \) occurs given that event \( A \) has occurred. \( P(B_r \cap A) \) is the probability that \( Br \) and \( A \) occurs. \( Bi \) is all the possible events \( B \) and \( P(B_r) \) is the probability that \( Br \) occurs.

**Figure 3: Experiment with previous knowledge in the Bayesian approach**

**Choose a side?**

As the Frequency and the Bayesian approaches are based on such different foundations, which is the better and should one take a side? What is best for reliability purposes?

The frequentist approach has a point in that it stays as objective as possible. It would be nice if the values used to estimate reliability only were based on unbiased, proven findings. Sadly, this is almost impossible. Reliability data are usually experience data collected from several similar systems and products. These rarely operate under the exact same conditions. If experience data cannot be found, expert judgement is used. This is hardly unbiased. The only possibility to obtain data suitable for the frequentist approach is testing.

Although the Bayesian approach seems the obvious choice, it is not necessarily the best. The calculations used to find a value are more extensive than for the Frequentist approach. Simplicity is said to be the best value for scientific activity (Vallverdú 2003). The fact that Bayesian estimations often are biased is a definite downside to this approach. However, this downside is also what raises it above the Frequentist approach. We cannot estimate every little value through homogenous experiments or sampling. Nor is our main observational skill, seeing, unbiased. An experiment is based on observations. When we observe with our eyes, our brain uses memories to classify what we see. The classification then helps us understand what we just experienced. The same is done when we smell or hear something.

To decide which approach is the better is not easy. They both have their advantages and disadvantages. The question should maybe rather be which one is the best for the specific purpose of the probability estimation? Medicine often needs to be exact, especially when the research tries to confirm the bacteria leading to a certain disease. The Frequentist approach is then both suitable and
objective. For reliability we need more than we can get from the values suiting the Frequentist approach. The best might be to choose the approach best befitting the value one is estimating.

2.3. Discussion

Reliability is a subject of high importance in any industry. If a product is unreliable, high repair and warranty costs, dropping sales and a bad reputation can be the results. As reliability only is calculated through measures of probability, the results will be uncertain. The better knowledge one has of the system, probability approaches and reliability calculations, the easier it is to get an impression of the system’s reliability. Any estimation must be performed through careful consideration of how one should approach the probability and find a parameter. Both the Frequentist and the Bayesian approach can be used. In choosing an approach, it should be based on the type of information one has and how it may best be utilised.

Design for Reliability could be considered useless and time consuming. What any critics claiming this forget, is the fact that reliability does make a person look at the design through different eyes. Reliability demands an optimal design to avoid failures. To design for reliability does not mean that the reliability alone should be calculated and increased, but that the whole system should be reviewed for solutions which will keep it functioning as long as possible. Given that the use of reliability in the design process also leads to good maintainability and increased availability and safety, its importance during the product development should be obvious.
3. Subsea industry requirements

When a manufacturer is involved in a new project, the first step is to define the requirements and specifications relevant for that particular project. The requirements will typically be specified in the laws and regulations of the countries involved, the standards stipulated in the customer requirements, and internal standards and requirements within the organisation. All industries have some standards to follow on the subject of reliability, whether they are specific or very general and stated by organisations such as the International Organisation for Standardization (ISO) or the International Electrotechnical Commission (IEC).

As an example of how regulations and standards within an industry may affect a manufacturer on the subject of reliability, some of the requirements to the Norwegian subsea process industry are studied. Even for this particular industry there are too many standards and regulations for all to be discussed. A selection of requirements from Norwegian authorities, ISO and IEC have been made. The regulations of the authorities in a country must always be the highest priority and followed closely. Standards from organisations such as the ISO and IEC are often voluntary, but can be included in the client demands or mandatory within the manufacturing organisation.

3.1. Petroleum Safety Authority

The Petroleum Safety Authority (PSA) is a subordinate organisation of the Norwegian Ministry of Labour (PSA 2010). It is the regulator for technical and operational safety, including emergency preparedness for the Norwegian petroleum activity. This includes the preparation and presentation of regulations, as well as decisions on permits, orders, prohibitions and dispensations. For Aker Solutions this means that the Midgard SCS must be manufactured in accordance with these regulations. The installation and operation of the system must also be non-conflicting and although these phases are the responsibility of Statoil, the Subsea Power and Process department at Aker Solutions is responsible for making it possible.

The PSA has five regulations concerning operation on the Norwegian continental shelf (PSA 2010):

- The Framework Regulations
- The Management Regulations
- The Information Duty Regulations (Not of relevance to this thesis.)
- The Facilities Regulations
- The Activities Regulations

All of these must be followed by the operators and are meant to ensure that the operations are safe. This “safe” includes the employees, the environment and the production system.

The Framework Regulations

The Framework Regulations are concerned with health, safety and environment in connection with operations offshore (NPD (C) 2001). This includes the subsea part of operations and although no direct connection with RAMS activities is made, the regulations affects the systems developed at Aker Solutions. Based on demands for safe operations, the operators will set their requirements for the system safety. With highly reliable systems, they are likely to have fewer accidents.
The Management Regulations

In risk reduction, the party responsible shall choose technical, operational and organisational solutions which reduce the probability that failures and situations of hazard and accident will occur. (...) The solutions and the barriers that have the greatest risk reducing effect shall be chosen based on an individual as well as an overall evaluation. Collective protective measures shall be preferred over protective measures aimed at individuals.

This is stated in the first section of the Management Regulations (NPD (D) 2001), and means that Statoil in ordering an SCS from Aker Solutions must ensure that this is the best solution. This can be done by ensuring that the system requirements follow the regulations, and that they are answered by the system solution. It is thus evident that although Aker Solutions is not forced to follow the regulations, they are more probable to sell their products if they use them in their planning. As a reliability programme will be directly linked with the reduction of risk, the Management Regulations may be called a good reason to develop one.

The Facilities Regulations

The Facilities Regulations is fully named “Regulations relating to design and outfitting of facilities etc. in the petroleum activities” (NPD (B) 2001). This regulation has direct influence on the systems developed for petroleum purposes on the Norwegian continental shelf. It may thus be the most important and direct input to Aker Solutions. Any equipment designed by the Subsea Power and Process department has to comply with these regulations. Several requirements are given which concerns the demanded reliability of the system, especially for safety and failures. Section 4, design of facilities states the following (NPD (B) 2001):

“Facilities shall be based on robust and the simplest possible solutions and shall be designed so that
b) the major accident risk becomes as low as practically possible,
c) failure of a component, a system or one single mistake does not lead to unacceptable consequences,
d) the main safety functions, as mentioned in Section 6 on main safety functions, are maintained,
e) transport and handling of materials can take place efficiently and safely, cf. Section 12 on handling of materials and transport routes, access and evacuation routes,
i) provision is made for the lowest possible risk of pollution,
j) provision is made for fully satisfactory maintenance.”

The choice of reliability activities used in the development of new systems must fulfil these and other demands in the Facilities Regulations in addition to other requirements presented by the customer.

The Activities Regulations

The Activities Regulations states that the maintenance programme for an offshore installation shall be based on a thorough identification of failures and their causes and mechanisms (NPD(A) 2001) The probability of failure shall be the basis for a choice and classification of maintenance tasks. This applies to the manufacturer through the agreement of which information is to be passed on at handover. The necessary information fulfilling this regulation is found in the reliability analyses. The reliability analyses are thus not only performed to show that the equipment can function as demanded, but also to make a basis for the maintenance tasks. A RAM analysis can be very useful as it includes a consideration of the system’s maintainability. This is further discussed in chapter 6.
The PSA regulations are often referring to standards prepared especially for the Norwegian petroleum industry. These were previously published by NORSOK, but are now the responsibility of Standard Norge (PSA 2010). Among some of the standards relevant to reliability are:

- Z-008, criticality analysis for maintenance purposes
- Z-013, risk and emergency preparedness analysis

These standards are usually presented together with Z-016, which has now been turned into ISO 20815, Production assurance and reliability management.

3.2. Standards

Several other standards than those listed here are of interest, but these were considered the most useful at Aker Solutions Subsea Power and Process. Through the use of standards and by referring to them in documents, it is possible for all parties in a project to find and understand what is meant by a specific term or description.

Standards ensure desirable characteristics of products and services such as quality, environmental friendliness, safety, reliability, efficiency and interchangeability – and at an economical cost (ISO 2010).

3.2.1. NORSOK

Z-008 – Criticality analysis for maintenance purposes

Z-008 recommends that any preparations for a maintenance programme are started in the design phase (NORSOK Z-008 2001). This means that the system still will be in the hands of the Subsea Power and Process department, rather than with the future operator. The standard demands a consequence classification of the potential failures which is then connected with the different functions. With a proper RAM analysis included somewhere in the development process, it should be easy for the client to develop a maintenance programme before the system is put to use.

Z-013 – Risk and preparedness analysis

This standard links a risk analysis and the preparation and establishment of an action plan for emergencies. It is demanded that a risk acceptance criteria is set, the hazards identified and studied and that steps are taken in order secure the system according to the criteria (NORSOK Z-013 2008). Based on the information retrieved and the solutions suggested for the risks, the emergency preparedness programme will be established. Normally this standard is meant as an input throughout the life cycle, including after the system is in operation. For the development of a new system, the Subsea Power and Process department will do an extensive search for hazards as a response to the ordinary demands of a client. Although the emergency preparedness is the responsibility of the client and operator, the risk and reliability studies performed by Aker Solutions will be the main input when a new system is handed over. Z-013 and Z-008 may not be compulsory for the engineers at Aker Solutions, but they must be followed by their clients, and thus complied with.
3.2.2. ISO standards

The ISO standards are prepared by the International Organization for Standardization, which is a network of standard institutes in 161 countries (ISO 2010). Some of the standards are specified for the petroleum and natural gas industries and may therefore be looked upon as even more relevant than other standards. ISO is a non-governmental organisation without any authority to enforce the standards. To follow them is therefore a choice, unless otherwise is stated by the authorities in a country. This is also applicable to the specified standards which the Subsea Power and Process department may find itself subject to.

**ISO 20815 - Production assurance and reliability management**

This standard gives an outline of a programme for production assurance and reliability management. It states that the programme could be concerned with one phase alone, or the entire product life cycle. The main objective is that risk and reliability should be included as parts of the development process from an earlier stage than what has been the habit. ISO 20815 (2008) observes that, in traditional design processes technical safety and reliability aspects have generally not been considered until the equipment or component verification. This is too late if one desires an optimal design.

A production assurance programme outline is given in Appendix A of ISO 20815 (2008). Among the main objectives of such a programme are:

- A statement of the performance objectives and measurements for the subject in development.
- A description of the project risk explaining the extent to which activities are chosen for the programme.
- A description and distribution of the responsibilities and action management system for the reliability.
- An activity schedule including an overview of the activities to perform, when during the life cycle they should be performed and how they are connected with each other.

Statoil specifically asks for a reliability management programme based on ISO 20815 in the Midgard SCS development. This is further discussed in chapter 9.

Even without client demands for this standard to be followed, it may be very useful for a manufacturer. Any early reliability analyses must be performed by the party responsible for the development process. ISO 20815 (2008) indicates how different methods can be chosen and followed up throughout the process, in early as well as late phases. It may simplify the discussion of the allocation of time resources to different reliability tasks based on the project risk and the newness of the technology.

**ISO 13628, Design and Operation of Subsea Production Systems**

This standard is not specifically concerned with reliability, but does affect the design of the systems produced by the Subsea Power and Process department. It states requirements, recommendations and guidance for the areas which require consideration when a subsea production system is developed (ISO 13628 2005). Functional requirements do affect the reliability demands and it can therefore be useful for a reliability engineer to know this standard. ISO 13628 (2005) covers all phases of the product life cycle and several types of production systems in distinct parts.
ISO 14224 - Petroleum and natural gas industries – Collection and exchange of reliability and maintenance data for equipment

It is stated in this standard that its primary users are the owners and/or operators, who should find the data to be collected, available in the operating facilities (ISO 14224 2006). Designers and manufacturers are mentioned for the use of the reliability data, in connections such as lessons learned and reliability estimation inputs. The standard can be quite useful for the understanding of what a data collection truly is, its data and their uncertainties.

ISO 14224 emphasises that the following categories of data are to be collected (ISO 14224 2006):

- Equipment data: taxonomy, attributes etc.
- Failure data: cause, consequence etc.
- Maintenance data: action, resources, consequence, down time.

If these data are collected with all the available information of interest, all RAMS disciplines may easily be covered in analyses. All types of equipment and systems are of interest, whether permanently or temporarily installed. The data collecting process is described in figure 4:

![Data collecting process diagram](image)

**Figure 4: The data collecting process (ISO 14224 2006)**

High quality data is defined as the following (ISO 14224 2006):

- Complete in relation to specification
- Complying with definitions
- Accurate
- Properly stored
- Sufficient in population
- Relevant to the need of the user.

The standard also states how the data are verified and the limitations normally connected with data collections. If this information is used properly by the reliability engineer, or any other user, it should be easy to separate the useful data from those of low quality. It would also be possible to understand whether the data verification is acceptable. Unacceptable data verification means care must be taken when data are used.
ISO 17776 - Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment

ISO 17776 is a useful standard for information about the principal tools and techniques commonly used for the identification and assessment of hazards in the petroleum industry (ISO 17776 2000). It explains how the tools and techniques can be employed in the development of strategies for prevention, control and mitigation of possible hazardous events.

ISO 17776 (2000) defines the three main steps in hazard and risk assessment as:

1) Identification of hazard
2) Assessment of the risk
3) Elimination or reduction of the risk

The standard describes how the methods for hazard identification and risk assessment are to be chosen, the role of experience and judgment, and how checklists, codes and standards can be used. For a risk and reliability engineer the standard helps ensure a good risk management process. It can also ensure the understanding of why a method has been chosen over another and why certain decisions are labelled more important than other. ISO 17776 (2000) is highly descriptive and easy to read and follow. The annexes explain several tools and what information they can obtain.

3.2.3. IEC

The international electrotechnical commission prepares and publishes standards for the electrical, electronic and related industries (IEC 2010). Like the ISO it is a non-governmental organisation with member organisations in several countries around the world. There is no enforcement of the standards, but they are recommended as useful tools ensuring the standard of products.

For the subsea process industry these standards may give an input to how an activity shall be performed and followed up. As electrical systems are becoming more common sub sea, these standards are increasingly useful.

IEC 60300 - Dependability management

Dependability is a collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance (IEC 60300 2003).

IEC 60300 (2003) explains how a dependability management system may be organised and implemented in an organisation. It consists of several parts which explain the necessary steps, methods and procedures needed to establish a dependability programme. Part 1 explains the fundamentals of dependability management and provides the principals for organisations involved in the establishment and use of such programmes (IEC 60300 2003). The second part provides the guidelines for a dependability management programme, while part 3 introduces the suitable analysis techniques for dependability.

For a reliability engineer in an organisation where reliability and dependability have been overlooked and considered too expensive to use on a larger scale, the standard might be serviceable. It explains why dependability management is important and how it can be implemented according to organisation and product. It can be followed easily and employed without too many alterations or delays in normal production processes.
**IEC 61160 - Design review**

A design review is a planned, documented independent review of an existing or proposed design (IEC 61160 2006).

Reviews of the design at predefined stages in the product development process can be useful to ensure that product requirements are met with. IEC 61160 (2006) refers to design review as a repeatable, confirmatory and refining procedure. This is shown in figure 5:

![Design review process](image)

**Figure 5: Design review process (IEC 61160 2006)**

A design review is not a task specifically meant for the reliability engineer, but is thought to help his or her work in ensuring the product performance. The process requires planning, organising and reporting (IEC 61160 2006). Although a review is a good measure of control for the design, it is important that it stays exactly that. It is not meant to be a creative process or in any way lead to new designs for the product. The only design alterations based on the review that are acceptable must be due to unacceptable problems.

When the review process has been performed, it is up to the designers and other members of the development team to follow up on it. Figure 6 shows how the design review process can be performed and responded to.

![Design review and response process](image)

**Figure 6: Design review and response process (IEC 61160 2006)**
IEC 61508 - Functional safety of electrical/ electronic/ programmable electronic safety-related systems

The functional safety of a system depends on the inherent safety of the system and any extra protective systems. Together these must answer to the safety requirements set by the manufacturer, clients and authorities. IEC 61508 (2005) provides a method for the establishment of a safety requirements specification, through an approach for the application of safety activities during the life cycle. Product safety requirements concern the safety performance of products and are made both for intended use and foreseeable misuse (Lundteigen et al. 2009). This ensures that the activities are dealt with systematically.

IEC 61508 (2005) consists of seven parts which considers the general requirements, requirements for E/E/PE safety-related systems, software requirements, definitions and abbreviations, examples of methods for the determination of SIL, guidelines on application and an overview of techniques and measures. The first four parts are basic safety publications, while the last three are help to the implementation of the standard (IEC 61508 2005).

This standard is tightly connected with IEC 61511 and the two can therefore used together with advantage to the functional safety. Alone, this standard can give input to the reliability process through its allocation of safety requirements.

IEC 61511 - Functional safety – safety instrumented systems for the process industry sector

IEC 61511 (2003) is the process sector version of IEC 61508, but directed at system level designers, integrators and end users rather than vendors developing new devices (Lundteigen 2009). The standard follows the requirements given in IEC 61508, but they are modified to suit the practical situation, concepts and terms in the process industry.

IEC 61511 (2003) consists of three parts focusing on framework, definitions, system, hardware and software requirements, guidelines on application and determination of SIL. This confirms the similarity to IEC 61508 and the two are often treated simultaneously. The Norwegian Oil Association is one out of many who has created a guideline for the application of the two standards; the OLF 70 (Lundteigen 2009). This follows the Norwegian regulations and thus simplifies the approach for a reliability engineer in the petroleum industry.

3.3. Further comments

The standards mentioned here is only a selection of those which can be of use for a reliability engineer working within the subsea process industry. The ISO standards described might not be of specific interest. However, they all have useful inputs to reliability engineering. Depending on the system developed and the industry in question, the suitable standards should be studied and used according to the phases in which they belong. These standards can be used in the different phases according to table 1. X means the standard is used directly, O means it can be used, and “In use” means that the results of the standard having been used are applied.
Table 1: Standards used in phases

<table>
<thead>
<tr>
<th>Standard</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Z-008</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>X</td>
<td>In use</td>
<td>In use</td>
<td></td>
</tr>
<tr>
<td>Z-013</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>In use</td>
<td>In use</td>
<td></td>
</tr>
<tr>
<td>ISO 20815</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ISO 13628</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 14224</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>ISO 17776</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC 60300</td>
<td>X/</td>
<td>O/</td>
<td>O/</td>
<td>O/</td>
<td>O/</td>
<td>O/</td>
<td>O/</td>
<td>O/</td>
</tr>
<tr>
<td>IEC 61160</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC 61508</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC 61511</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Standards as those described here are not the only documents which can be relevant to follow. Several organisations developing new technology have defined levels for how far in the development process a technology is. These are often called Technology Readiness Levels (TRLs). In many industries the TRL documents are developed by specific organisations. Although each company may still have their own TRL documents, a document for the whole industry in a country makes it easier for conformity between the companies. In Norway, DNV has developed a document called “Qualification Procedures for New technology”, DNV-RP-A203, specifically for the petroleum industry.

The American Petroleum Institute has developed a structured approach to manage uncertainty throughout the product lifecycle, API-RP-17N, which is compatible with ISO 20815 (API-RP-17N 2009). This, as the DNV-RP-A203, is not a compulsory document, but highly recommended for the reliability to be properly implemented. This recommended practice goes through all the phases, and describes the most convenient reliability methods and tests.

Other interesting documents are those prepared by the Norwegian Oil Industry Organisation, OLF (OLF 2010). These explain how other standards may be utilized and implemented to the best interest of the petroleum industry.

The best way to identify useful standards is to follow the development in organisations such as IEC and ISO, and the laws and regulations in a country. Which of these are needed in a project can be found through the client demands, the concept and the requirements. In every organisation, it is up to the responsible for reliability to follow the development and make sure the most recent regulations and standards are known in a project.
4. Product life cycle

A product is usually only of interest to a consumer from the moment he or she considers buying it or is provided with it, until it is thrown away. Environmentalists might concern themselves with how the product is produced and later disposed of, as well as how it affects the environment while it is in use. For the manufacturer, a product is born the day the need for it develops and it lives on until it has been properly disposed of.

The lifespan of a product depends on what type of product it is. A normal toothbrush is only meant to be in use for a few months and its total length of life as a physical product may be less than a year. Equipments made for the subsea process industry are usually supposed to be operating for several years. Ships and boats may even be in use for decades. While the lifespan of different products differ, their life cycle is usually evaluated in the same way. A life cycle includes several phases concerned with the concept development, design, production, sale, use, maintenance and disposal. How many phases there are in a life cycle depends on the person looking at the product and his or her reason for separating it into phases.

There are several existing models showing the phases of a product life cycle. In some cases the life cycle is a closed loop where the disposal includes recycling and reuse. In other cases it is thought that the product ends its life at the dumpsite. In general a product life cycle model depends on the intended use of the model, whether it is developed for marketing, designers, or reliability engineers.

4.1. Phases in a general perspective

The main approach to how phases are defined is based on what the product goes through from it is first thought of, to its disposal. The IEC has defined six life cycle phases (IEC 60300 2003):

- Concept and definition
- Design and development
- Manufacturing
- Installation
- Operation and maintenance
- Disposal

The first phase focuses on the development from an idea to a product outline. Research is made to see if there is an opening for a new product on the market and what this opening demands from the product. Different concepts are considered and the product requirements specified. Based on the chosen concept, a detailed design process commences. This will establish the system architecture, hardware and software. During manufacturing, the product components are produced or collected from suppliers for assembly. The installation phase can be performed by the manufacturer, the operator or both together. During operation and maintenance, the product is in use and maintained as far as possible. When the maintenance costs go higher than the returns from the product while it is in use, it is time to dispose of it. The disposal phase includes the removal, dismantling and destruction or recycling of the product (IEC 60300 2003).

This life cycle model is suitable for most industries and companies, but the IEC 60300 (2003) does not describe each phase with much depth. All organisations can choose which separation of phases they prefer. An example is the very common five-phased model. This is employed by many organisations and is separated into the following phases:
The five phases are used in connection with several project models and can be extended or divided depending on the type of project. An example of an organisation supporting this product life cycle is Aker Solutions. As the projects the Subsea Power and Process department currently work on concern systems handed over to a client after manufacturing, the last two phases are of less interest than the previous. They may have a say in how a system should be operated and disposed of, but it is not the responsibility of the Subsea Power and Process department. The wish for the future is that the Subsea Power and Process department can produce more standard products, in which case the phases might be slightly altered.

A quick comparison to the six phases in IEC 60300 (2003), shows that these five phases are mainly concerned with design and development. The post-production phase will last longer and possibly include more tasks than any of the other phases, but it seems to be far less interesting. For a manufacturer without responsibility after handover this makes sense.

**Front-End**

In the front-end phase an opportunity or a need for a new product has emerged. New technology may give way for improved or new products that were impossible to produce earlier on. The need for a new product idea can also be developed as a response to customers’ complaints or through competition (Murthy et al. 2008).

When the new opportunities have been recognised, a filtering of ideas should be performed to find the best suitable options for a new product. This filtering should answer the following questions (Murthy et al. 2008):

1. Does the idea fit within the business market or technology focus area?
2. Are the business opportunities attractive (potential market size, growth etc.)?
3. Is it technically feasible to develop and produce the product?
4. Are there any potential hindrances that may stop the project (Intellectual property, legislative and/or environmental issues)?

When a product idea has been chosen for further use, the product and business objectives must be defined and customer requirements identified. A product concept is then developed. It defines the main functions and sub-functions, as well as the relationships between the main components. The development of a new product may be considered as a project. A project plan should therefore be prepared, including a schedule, an allocation of responsibilities and resources, performance measures and risk management plans.

**Design**

Based on the product concept and requirements found in the front-end phase, the internal arrangements and interactions of the product can be determined. This concerns the sub-systems, assemblies, sub-assemblies and the components. A definition of the functional decomposition and relationships between these is vital to the establishment of the product architecture.
As soon as a definition is ready, a more detailed design of the product can be prepared. Component properties will now be set, detailed drawings made and a bill of materials written. According to Sim and Duffy (2003), design activities can be classified as:

- Design definition activities
- Design evaluation activities
- Design management activities

These activities should be performed concurrently to ensure an optimal design fitting the purpose and concept of the product. Finally a review of the design should be carried out to verify the product architecture (Murthy et al. 2008).

**Development**

The development phase is where the prototype is made and tested. This is meant to verify that the product can be manufactured according to the planned design. When a product is custom-built, the performance agreed upon between customer and manufacturer should be verified. The actual performance must also be proven to be higher or equal to the desired performance. Through the tests performed in this phase, problems can be discovered, understood and resolved (Murthy et al. 2008).

**Production**

The main challenge of the production phase is to uphold the designed-in performance throughout the manufacturing process (Murthy et al. 2008). This is due to the inability of a production system to produce exactly similar outputs. Variations in the production process, the materials used, and the surrounding environment mean that special strategies must be used to keep up the quality of the end product. Process control, inspection and product testing are methods used to ensure a high quality of the end product.

**Post-Production**

When the product is ready for use, it is turned over to a customer. The customer is either found in a large market, or the specific buyer of a custom-built product. In both cases the transportation and product support are important parts of the post-production. When the customer is ignorant of the product’s existence, the producer needs to include promotion, pricing and distribution channels in the phase as well (Murthy et al. 2008). The product support is perhaps the most important part of the post-production, as its focus is on keeping the customer content. Normal activities could include installation, maintenance, warranties, repair and disposal.

Neither the six phases described in IEC 60300, nor the five phases used by Aker Solutions are especially concerned with, or developed for, reliability purposes. A model comprising eight phases in which reliability is the first objective is suggested by Murthy et al. (2008).

### 4.2 8 Phases for reliability

The eight phase model has three different systems: stages, levels and phases. The three stages are concerned with the physical development of the product, whether it is under planning, production or released to a market. For the linking between business objectives, attributes and characteristics of the product and its components, three levels are described. Finally the stages and levels are combined as showed in figure 7, while the development of the product travels through the combinations in 8 different phases.
### Stages I-III
- **Pre-Development**
  - Non-physical conceptualisation of the product with increasing level of detail.
- **Development**
  - Physical embodiment of the product through research, development and prototyping.
- **Post-Development**
  - The remainder of the product life cycle (production, sale, use, etc.).

### Levels I-III
- **Business level**
  - Linking the business objectives for a new product to desired product attributes.
- **System, i.e., product level**
  - Linking product attributes to product characteristics – the product is treated as a black-box.
- **Component level**
  - Linking product characteristics to lower level product characteristics, at an increasing level of detail.

### Phases 1-8
**Phase 1**: The need for a new product is identified and the decisions related to the product attributes are made from an overall strategic management level of business. Data are collected and analysed in order to see whether a new product is of interest to the consumers. Based on this, generation and screening of ideas is done and a feasible option chosen. Finally the product concept and the performance requirements are formed and evaluated.

**Phase 2**: Based on the requirements from phase 1 the desired performance is found. Overall product reliability is derived and compared with the product requirements and the desired performance. This is especially important as an evaluation if the product is custom-built. The comparison of the predicted and desired performance decides whether or not the process may proceed to phase 3.

**Phase 3**: In this phase the detailed design is carried out through a functional analysis. The system is decomposed into several sub-systems, down to the component level. It is important that the previously set requirements are answered throughout the system. The functional analysis helps assign...
requirements and functions to each component. From this, the predicted reliability of each component can be calculated for the overall product, and compared with the desired reliability. If the comparison shows an acceptable reliability, phase 4 may begin.

**Phase 4:** When this phase has been reached a physical development of the system begins. Starting on the component level, tests are performed to ensure an appropriate production and that the desired reliability is achieved. Testing continues up to the highest possible level and leads to a testing of the overall product reliability if feasible. Any problems discovered through the tests must be corrected, either through changes in design or choice of material. The testing is limited by the costs and available time. If the product is custom-built, the testing is more important and operational tests should be included.

**Phase 5:** In this phase it is suggested that a prototype is released to a limited number of customers who can evaluate its features and test it in normal user circumstances. During the tests, logs must be kept for later analysis of failures and success. If the results are positive phase, 6 may be initiated.

**Phase 6:** The first step in this phase is to design a production process for serial production. In order to ensure the quality of the product and the production process, control limits are set and a quality control plan prepared. This helps the follow-up of process variations. Such variations are unavoidable, but may, with proper attention, be kept within acceptable limits. Tests should be performed during the production to eliminate assembly errors, defects and early component failures. Before release of a batch of products, a final sample testing could be done to ensure the reliability performance of the finished product.

**Phase 7:** When the product is released to the market and is in use, it is interesting to look at the field performance. Data collected through warranties, repairs and other feed-backs should be collected continuously. Analyses could then be used to identify the actual product performance and reliability. The analyses must take into account the variability in usage intensity, operating environment, and the customer perspective. A comparison of actual and desired performance can be made and in case of a mismatch, a cause and solution should be found for further production or new development projects.

**Phase 8:** Here the performance of the product released for sale is evaluated from an overall business perspective. An analysis of all available data is performed and compared with the desired performance from the first phase. If the actual and desired performances do not match, a backwards iteration towards phase 1 must be done in order to find and implement the necessary actions. The results can be used to evaluate the success of the product and as lessons learned in later development projects.

Figure 8 shows how the phases are connected through the three stages and can be compared with the basic 5-phase product life cycle.

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Phase 5</th>
<th>Phase 6</th>
<th>Phase 7</th>
<th>Phase 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-development</td>
<td>Development</td>
<td>Post-development</td>
<td>Front-end</td>
<td>Design</td>
<td>Development</td>
<td>Production</td>
<td>Post-production</td>
</tr>
</tbody>
</table>

*Figure 8: Connection between life cycle phases (Murthy et al. 2008)*
4.3. Discussion

The life cycle models presented here are only a few out of many. Both the five-phase and the eight-phase models are mainly concerned with the events before the release and installation of the product. To split the route from idea to finished product in many steps will possibly give more focus on the task at hand and shorter time to a milestone is reached. For this reason, the eight-phase model is good. However, it is also important that the increased number of phases does not lead to a decreased overview of the process. For reliability purposes it can be argued that the eight-phase model is more suitable. This model makes it easier to see which information has been found as the tasks of each phase are more distinct. The model has been created with reliability performance in mind, while the five-phase model is directed towards the production process. In the case that the five-phase model is preferred, it may be possible to use the comparison in figure 8 to implement reliability at the correct moment.

For later chapters in this thesis, the eight phases of Murthy et al. (2008) has been chosen as a basis for both the discussion of how unreliability may occur, and to suggest a new methodology for design for reliability. In general it can be said that everyone in need of separating the product life cycle into phases must evaluate the purpose of the separation and the specific case. A decision should be based on what simplifies the utilisation of the product life cycle the most.
5. Methods for reliability

In every industry the RAMS disciplines are viewed through different eyes. This has especially affected the development of different methods used to analyse reliability and safety. The methods are not necessarily very industry specific, but they have been developed from the specific need the industry sees. In large parts, the industries can be separated in two; those who considers the aftermath of a failure and those reviewing the events leading up to failure. The former is more likely to have been responsible for the development and use of methods for safety, while the latter mostly is interested in methods for reliability. A characteristic of the latter is that if a failure occurs, there is little which can prevent the final catastrophic consequence to take place. Examples of such industries are the nuclear, the aerospace and the military industries. If something goes wrong with a nuclear reactor, it is quite possible that the consequence will involve far more than the destruction of the nuclear plant. A failure during a space mission is highly likely to not enable the crew to return safely to the earth. Finally, if a missile is detonated while it is still attached to a boat or an airplane, little can be done to prevent it from destroying its host.

Among the industries where the aftermath of a failure has been given the most focus is the offshore industry. This industry has existed for more than sixty years, successfully transporting oil from below the seabed to onshore installations (Offshore 2009). Throughout most of this period, the main focus of reliability and safety engineers has been on the aftermath of an accidental or hazardous event. Equipment reliability has been considered through the use of separate analyses and these have not always been performed early on in the product life cycle. Although the reliability of a product has been considered important, the offshore industry has few standards for reliability methods and programmes. One reason might be the actual possibility of preventing a failure from developing into a catastrophe.

In a presentation on reliability strategy for the subsea process industry given in 2003, BP stated that reliability analyses should be integrated to the design phase. They also found that no specific guidance existed for the setting and allocation of reliability requirements in the subsea process industry. A goal was set to allocate reliability down to the component level and educate more personnel on reliability issues. (Williams 2003).

The methods used at a certain point of the life cycle will depend on how the product is manufactured, its intended use and how far into the development it is. In the earliest development phases, preliminary studies of the reliability can be performed, while in phases where the product is materialised, physical tests become possible. For a product produced in large numbers, for instance an mp3-player, tests leading to destruction may be used. Prototypes can be developed at little expense and depending on the product’s size the tests may be performed by employees bringing the product home. When the product is of such a scale or cost that it can only be made once, destructive testing is harder to apply. Non-destructive testing is in use, but these rather prove the ability to perform than the failures. One such test is factory acceptance test (FAT), whose main goal is to confirm that all parts of the system functions as intended. Alterations may be done after this test in case of unacceptable results.

The subsea process industry is a very good example of how specific conditions might demand more of the system reliability for custom made products than standard product. In this industry it is likely that the products are of a very large scale, expensive and made to order. The environment of the product when it is in use is less accessible to human beings and more demanding than in most industries. Depending on the oil or gas field’s calculated lifetime, a product can be required to operate for many
Due to new developments increasing the field’s lifetime, a product can be demanded to last even longer than originally planned. All these factors increase the importance of reliable designs. The little accessible environment is a difficulty shared with the aerospace industry, while the extension of planned time in use is a trait shared with the nuclear industry. An example is France where they currently are extending the life of nuclear plants with ten years more, from the previous expected twenty years. This can be both dangerous and press the systems towards their wear-out phases. Thorough and precise methods for reliability are thus needed to confirm that the extended life is acceptable.

Reliability methods and SADT
The more commonly applied methods for the analysis of reliability are not made to suit all phases of a product life cycle. Nor can they include every aspect of interest to an analyst. All methods need certain inputs and produce specific outputs. The outputs of one method may be the input of another. Some of the methods are more overlapping, but necessary together for the output they give. Other can stand alone at a specific point in the life cycle, but will not give the most useful outputs without the help of a later method analysing them. The methods are not necessarily stuck to one single phase, but can be updated throughout the life cycle. A good example is the failure mode and effects analysis (FMEA) which exists in several formats, and can be useful in many phases.

Each method will be presented through the structured analysis and design technique (SADT).

As shown in this figure, there are four main elements in the SADT model. A function is the method which is to be performed. The inputs are the energy, materials and information needed to perform the reliability method. Mechanisms are the people, facilities and equipment needed to perform the function. Controlling elements for a reliability method are standards, requirements, demands and budgets. Finally, the outputs are the results after the method has been used (Rausand & Høyland 2004).

The basic method will be presented first, then the required input, the mechanism, the control and lastly the output.
5.1. **PHA and HAZID**

In the beginning of the product life cycle little information is available, unless the product is a new generation of another product. The reliability analyses performed at this stage cannot demand too much input. Their output, on the other hand, ought to give information which increases the knowledge about the product features. An analysis which can be performed early is preliminary hazard analysis (PHA). This method is a semi-quantitative analysis which helps identify potential hazards and accidental events, ranks the events according to severity and considers hazard controls and follow-up actions (Rausand 2005). PHA was developed by the US army and has later spread through to other industries. Another slightly different type of PHA, with the same objectives and need for inputs, is HAZID (hazard identification).

The PHA procedure consists of four steps; PHA prerequisites, hazard identification, consequence and frequency estimation, and risk ranking and follow-up actions (Rausand 2005). All parts of a system or product must at first be considered in a search for hazards. This includes failure modes, known maintenance operations, safety systems and potential human errors. The frequencies and severities of each hazard should be considered and classified in classes ranging from “improbable” to “frequent” and from “negligible” to “catastrophic” (MIL-STD-882D 2000).

**Inputs**

Any information about the system; design plans, concept definitions etc. is useful input. Checklists can be followed to remember all elements which are to be studied and what is to be studied about them. Other inputs such as risk information and block diagrams may come from similar existing systems (Stapelberg 2009).

**Mechanisms**

The mechanisms of this analysis are based on team work. The members should complement each other with different backgrounds and knowledge, enabling a more complete review of the whole system. If little information can be obtained, useful techniques for the retrieval of inputs can be what-if techniques and brainstorming (Rausand 2005). These techniques are based on imaginative thinking and are generally thought efficient for team work.

**Control**

In some industries there are standards describing how the PHA is to be performed and which outputs the final report should include. The main part of demands to the analysis will be given by the organisation it is performed for. This will depend on the limitations of time and costs given to perform the analysis. All product requirements which have been established can be considered, both as input to the analysis, and as controlling the main focus of the analysis. Both PHA and HAZID are described in ISO 17776 (2000), which is a standard especially prepared for the petroleum and natural gas industries. This can thus be used as a means of control for the Subsea Power and Process department at Aker Solutions.

**Outputs**

A PHA will produce a list of all hazards considered, including where they may originate from and a ranking of how grave the event’s occurrence can be. The latter will be very useful for later reliability analyses, if some hazards need to be prioritised above others (MIL-STD-882D 2000). To present the outcome of the PHA, a worksheet is made. This worksheet is standardised in several industries and will give a clear perspective of the different hazards connected to the system studied. There are few, or
sometimes no differences between the worksheets of the HAZID and the PHA. The worksheets will mostly depend on the systems and the organisations that employ the analyses (Ødegaard 2003).

![Diagram](Image)

**Figure 10: SADT PHA/HAZID**

### 5.2. SWIFT

The structured what-if technique (SWIFT) is a brainstorming technique where a team search for hazards through questions like “What if...?” and “How could...?” (Kritzinger 2007). It was originally developed for the chemical process industry and is today also used in other industries, for instance the aircraft industry. SWIFT mainly considers systems at higher levels, either the complete system as a whole, or a sub-system. The technique is an alternative to HAZOP as it is less time consuming and costly. These two methods do not operate on the same level of detail. It is thus possible to use them as complementary studies (MoD 2010). SWIFT is easy to use through all phases and for many purposes, for example as a study of a manufacturing process.

There is no specific standard for the SWIFT technique, but it is mentioned in the ISO/IEC 31010 (2009). The normal procedure includes a definition of the activity and problems of interest, a generation of what-if questions and responses, and a report on the findings. If the method is performed after a PHA or HAZID, many hazards will already be known. The SWIFT could then go further into the question of how the hazard would affect the system, and whether the rankings made were correct. A negative side of the SWIFT is that a problem is likely to stay unnoticed if the team fails to ask the correct questions. Another problem is its inability to produce quantitative results which can answer the more complex risk-related questions (Tech 482/535 2005).

**Inputs**

To perform a SWIFT analysis, it is necessary to have a basic system description, a definition of the activity, and some problems of interest. These inputs, along with a checklist for which elements one should study, would give all the information needed.

**Mechanisms**

The mechanisms of this method are the chosen team. It is very important for the success of the analysis that the team members have sufficient experience with the system and the technique. They must also be able to understand the output of other analyses performed before the SWIFT. The technique itself is a mechanism through the questioning.
Control

Controlling factors are few for the SWIFT. It does not demand much time or cost to perform it, nor has it been standardised. The main controlling factors would thus be the resources and whether any political issues affect the questions asked. The latter may happen in most reliability analyses and is troubling if it leads to the exclusion of failure considerations with dangerous effects. This method is described in the ISO/IEC 31010 (2009) standard which also shows it against other techniques.

Outputs

Outputs from the SWIFT are hazards, their causes and possible effects. Together with other hazard identification tools it can provide a good overview of the problems possibly faced by the system. This can be used as inputs to FMEAs, FTAs and other reliability analysis methods.

5.3. FMEA

Failure modes and effects analysis (FMEA) is a systematic technique for the study of failures. It was developed in the 1950s by reliability engineers for the study of military system failures (Høyland & Rausand 2004). FMEA is meant to be an input to the design process, enabling alterations of problems before the design is too settled (MIL-STD-1629A). In order for this to be possible it is suggested that the FMEA is performed as early as possible in the development process. As the development progresses, it is possible to keep filling in the failure information. This can be useful for other reasons than reliability, for instance safety and maintenance. The FMEA can be extended to include a criticality ranking of the different failures. In this case the criticality ranking is a combination of a severity measure set for the failure mode and its frequency of occurrence (IEC 60812 2006). When the FMEA is extended, it is called a Failure mode, effects and criticality analysis, FMECA.

The FMEA is usually a bottom-up analysis, where as many components, assemblies and subsystems as possible are included. To begin the analysis, a study of how each part may fail is done (Rausand & Høyland 2004). This should be followed by the study of why they occur, what their possible effects are, and how they can be detected. It could also be studied how the failures might be compensated for and whether they are dangerous or not.

Inputs

To perform the Failure modes and effects analysis, it is necessary to have an overview of the system. The main inputs to the FMEA are system design drawings, functional breakdowns, and a list of the possible hazards and failure modes found in previous analyses. If criticality is added, information about the failure frequency should be obtained as well.
Mechanisms

The FMEA demands an understanding of the development and consequence of a failure. Worksheets are used to keep the results of the analysis in a logic and comprehensible format. These can be adapted to each FMEA, but will normally include the columns in table 5. Although the analysis can be performed by one person alone, it is believed that team work is the most suitable. This is due to the magnitude of possibilities in the design which may lead to failure (IEC 60812 2006).

<table>
<thead>
<tr>
<th>Function</th>
<th>Operational mode</th>
<th>Failure mode</th>
<th>Failure cause or mechanism</th>
<th>Failure detection</th>
<th>Effect of failure</th>
<th>Failure frequency</th>
<th>Severity ranking</th>
<th>Criticality</th>
<th>Risk reducing measures</th>
</tr>
</thead>
</table>

Control

The FMEA has spread to almost all industries and has been developed for several other purposes than product reliability, for example project management. Among the standards and handbooks explaining the method and its application are MIL-STD-1629 (1980) and IEC60812 (2006). Based on the industry and the relevant standard, it is possible for an organisation to develop its own guidelines. Another possible means of control is to evaluate the impact the analysis has on the design. If the analysis is performed untimely, its effect may be hard to notice, but some useful outputs can still come of it (MIL-STD-1629 1980).

Outputs

The FMEA gives a good overview of the different issues to watch out for in the design and during the system’s operational phase. It can function as an input to several analyses, for example Fault Tree Analysis and Reliability Block Diagram. The listing of the criticality of the failure modes may be used to decide necessary alterations in the design and maintenance tasks during the operational life. With a thorough analysis, the worksheets will give a clear overview of the system, its failure modes and their effects. This will be useful throughout the product life cycle and in future projects.

Although the FMEA is well incorporated in most industries, including the subsea process industry, there are criticisms against it. The method itself is time consuming, especially if absolutely all component failures are examined to the same level of detail (Rausand & Høyland, 2004). Another problem is that the method only focuses on one failure mode at the time, leaving it unsuitable for the study of dependent failures. It is thus a possibility that systems with a fair degree of redundancy are insufficiently analysed.
5.4. FTA

"A Fault Tree is a graphic depiction or model of the rationally conceivable sequences of events within a complex system that could lead ultimately to the observed failure or potential failure." (NASA (A) 1999)

The Fault tree analysis (FTA) is a deductive method where the analyst starts with the final hazardous event and traces it back to the original failure (NUREG-0492 1981). It was first introduced for the safety evaluation of the launching system for the Minuteman I missile in 1962 (Høyland & Rausand 2004). Later improvement has lead to a very extensive use in most industries where risk and reliability studies are performed. One reason may be the method’s ability to give an overview of an entire system based on a few problems (NUREG-0492 1981).

For reliability purposes, it is important to start the FTA development as early in the product life cycle as possible and update it concurrently with the design development (IEC 61025 2006). As the original hazard is traced back through the possible contributing failure events which lead to it, the contributors are put into boxes and connected. The connections are based on whether a failure can occur alone or not in order to induce the next event. Underneath the failure, an and- or an or-gate is placed to describe the connection between the contributors. The final level in the Fault Tree is normally at the component level, but this is optional. Figure 13 shows how the procedure is performed and what the end product looks like.

As the bottom-level is entered into the tree, the contributor’s failure rates or probability of occurrence can be included. If all the necessary estimates for this level are obtained, it is possible to estimate the failure rate or probability of the occurrence of the top event. This will be done by following the gates from the bottom and up to the top. The method can be found in Rausand & Høyland (2004). FTA is helpful when a system is complex with many potential failures leading to a larger problem (NASA (A) 1999). It is easy to read, while systematic in its approach.

**Inputs**

The top event will be chosen from the previous hazard identification analyses, while the system design is needed to trace the contributors. As the design becomes more detailed, more contributors may be
discovered. To calculate failure rates and probabilities for the top event, estimates for the basic events are required (IEC 61025 2006).

**Mechanisms**
The FTA can be performed by one analyst alone, but a very thorough knowledge of the system is needed. In cases where the systems are too complex for one person, it is recommended that a team is used (IEC 61025 2006). As the fault trees may become too large to be drawn up manually, it can be very useful to work with computer tools, for example CARA Fault Tree (Rausand & Høyland 2004). These tools are often also able to calculate the failure probabilities and failure rates for the top event, and discover the minimal cut sets.

**Control**
There are several standards and guidelines existing for the FTA, for example IEC 61025 (2006) and ISO 17776 (2000). Again the procedure should depend on what the organisation demands of it. How far down it goes will therefore be decided by the organisation’s need. A reasonable manner in which it is possible to see whether the fault tree is reasonable, is through comparison with system breakdown structures.

**Output**
The output from the FTA can be used to improve the design, evaluate the possible preventive measures against failures and give input to reliability block diagrams (RBD). As the fault trees show the effect one undesirable event has on the system as a whole, it is possible to evaluate whether preventive measures, or design alterations are the best. The failure rates and probabilities calculated in the FTA can become useful for the estimation of MTTFs.

**5.5. RBD**
A reliability block diagram (RBD) presents the connection between the different components fulfilling a particular system function. The purpose is to show how the system can function or fail depending on the specific components. Where a fault tree has been made, a transformation to an RBD may be possible, and vice versa (Høyland & Rausand 2004).
To create an RBD, three types of system information must be studied (NASA (C) 1999):

- Functional systems architecture data
- Component reliability data
- Mission times/Operating times

When an analyst has these data, he or she can determine the relationships between the components as either serial or parallel. The components placed in a k-out-of-n (k-o-o-n) relationship, where the system functions even when some components fail, will also be noted. An RBD is easy to understand through its graphical representation. When a diagram of this type is presented, it can prove why parallel structures generally are considered stronger than series structures. In the former, the system's ability to function depends on its strongest link, while in the latter it will depend on the weakest.

The creation of the block diagram can only start after the difference between success and failure has been established (IEC 61078 2006). As there are possibilities for a system function to be in a state less than 100%, but higher than 0%, one could say that success is above 80%. When this is done, the system can be divided into blocks that are linked according to how the information passes through the system. By applying reliability information to each block, pivotal decomposition may be used to calculate the system reliability. This is also useful for the analysis of component importance through methods such as Birnbaum’s measure. Pivotal decomposition and component importance is described in Rausand and Høyland (2004) and will thus not be further discussed here.

![Figure 15: RBD](image)

**Inputs**
The inputs to the Reliability Block Diagram are system design, failure definitions, k-o-o-n relationships and redundancy information. A fault tree can be turned into an RBD and the other way around, but the RBD is the easiest to read with respect to the connections of components, assemblies and subsystems (Rausand & Høyland 2004).

**Mechanisms**
In order to perform the RBD, knowledge about the system is needed, both concerning its composition and how the elements work together. If the system is very complex, including k-o-o-n structures, switches and parallel structures, it is useful to perform the analysis in a team. RBDs can become very large and complex, and it is thus helpful to employ computer programs. Such a program will keep the information separate and facilitate calculations such as component importance and overall system reliability.

**Control**
What controls the method is the interest of the organisation ordering it and the design progress. The decision of what a success is will be decided by the system requirements. Creating the RBD, the
design is the basis and it is thus also the main element which may show that the RBD is put together as it should be. Any changes in the design should be a reason to update the RBD. The RBD is described together with Boolean methods in IEC 61078, which may be used for control of the performed RBD.

**Outputs**

One useful type of output from the RBD is minimal cut sets showing the smallest number of failed components leading to the loss of a system function. This can help the understanding of the weakest links within a system. If the RBD is used to find the system reliability and component importance, it could be entered into other analyses, or used to compare with previous studies. The downside with the RBD is that it cannot be used for repairable systems (Rausand & Høyland 2004). These should be analysed through Markov diagrams, which are described in Rausand and Høyland (2004).

**5.6. HAZOP**

The hazard and operability study (HAZOP) was first published in the late 1960s for ICI Mond Division and further developed and published for the ICI Petrochemicals Division in 1974 (Swann & Preston 1995). It is a structured and systematic method, performed as a team work with members specialised in different areas necessary to understand the defined system (IEC 61882 2001).

The objective is to identify the potential hazards in the system and the possible operability problems, for instance causes for operational disturbances and deviations (IEC 61882 2001). An attempt is made to find all possible deviations from the intended design of the system. The search is performed through the use of a number of guide words triggering the imagination of the team members. An example is the word “More” which is supposed to bring the thought to a problem where the deviation is an increase compared with the intended design. If it is used for a component controlling the amount of pressure, “more” could mean that a valve accepts a higher pressure than intended. Figure 17 shows how the analysis may be performed.
Figure 17: HAZOP process (IEC 61882)

Inputs
The input to the HAZOP is the system design and the operational information for the system. If similar systems exist, hints may be acquired for the guide words. A HAZOP study can be done in several life cycle phases, but is recommended performed just before the design is fixed. The design should then be detailed enough to contain the information needed to answer the guide words (IEC 61882 2001).
Mechanisms
In order to perform the HAZOP, team work is necessary. Together, the members should agree on the guide words and how the system is to be studied. Little is needed to perform the HAZOP and depending on the extent of the study, the analysis may be performed within a small time frame.

Control
To control the analysis, the IEC 61882 (2001) is a good instrument. Any specific demands for the output of the analysis will also be of interest. The design drawings can be utilised as a proof of whether the identified problems are realistic or not.

Outputs
When the HAZOP has been performed, the outputs are used for improvements in the design, and to alter routines in the operation. HAZOP can be performed for several purposes, and is very useful for the discovery of problems to watch out for in the manufacturing phases.

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>System design</td>
<td>Industry standards e.g. IEC 61882</td>
</tr>
<tr>
<td>Process information</td>
<td>Organisation demands</td>
</tr>
<tr>
<td>Previous knowledge similar systems</td>
<td>Time/ Cost / Resources</td>
</tr>
<tr>
<td>Operational/ Environmental conditions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mechanisms</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>System knowledge</td>
<td>List of hazards</td>
</tr>
<tr>
<td>Team work</td>
<td>Hazard information</td>
</tr>
<tr>
<td></td>
<td>Process and system alteration ideas</td>
</tr>
</tbody>
</table>

![Figure 18: SADT HAZOP](image)

5.7. Reliability Growth
Reliability growth is a physical test method. The intention is to improve the reliability through a test-analyse-and-fix technique. A component will be tested under increasing amounts of stress until failure. The test results are then analysed and if they do not satisfy the requirements, improvements will be made. This process continues until the reliability requirements are met with (Murthy et al. 2008).

For products that are very expensive and built as one-of-a-kind, it can be hard to perform reliability growth tests. Reliability growth is meant to lead to a failure, which cannot be accepted for the overall product in this case. Sub-systems and components which are not expensive and time consuming to develop can, on the other hand, be subject to the tests.

What a reliability engineer must be aware of is that the amount of “runs” which are performed in the reliability growth process has an effect on the outcome. For every run, the component or system is pushed further towards failure. This must be considered in the analysis as the previous load can mean that the system fails in run three, although it can handle more stress than what it was subjected to.
As reliability growth tests usually are performed as early as possible during the product’s physical life, little knowledge is available. The results of the tests must therefore be studied carefully by analysts with good understanding of the necessary physical and mathematical analyses, and an ability to make sound judgments (Blischke & Murthy 2000). In the subsea process industry and other industries where the products are the prototypes, reliability growth tests are restricted. The tests must then be performed on components that can be tested to failure and are not too expensive for this purpose. What the analysts have to remember in this case is that the results from component tests may not give all the answers. When the component becomes a part of the complete system, the possibility of new failures might occur that were not found through previous testing (Weibull.com (B) 2010).

**Inputs**
To perform the reliability growth test, prototypes of the components and the results of analyses performed implying necessary testing will be needed. Other information will be the outer limits a type of material can handle under stress, and how the tests are performed.

**Mechanisms**
To perform the tests, qualified personnel is needed. Proper equipment and laboratories with good environmental conditions for the tests are also necessary mechanisms of this method. Some of the more important factors for a successful reliability growth test are good management, tests that give comprehensible answers, the ability to identify the root cause of failures, effective corrective actions and valid reliability assessments (Weibull.com (B) 2010). The reliability found in this type of analysis is based on how the system responded to the testing and corrections. It is therefore vital that the measures taken are thought-through and sensible.

**Control**
Control of the reliability growth tests will depend on resources, time and money. The number of runs will vary with time and resources. The organisation developing the system may also have some demands concerning which tests the system should undergo and the conditions they should be performed in, for instance specific temperatures. IEC 61014 (2003) suggests programmes for reliability growth and may be followed both as a mechanism and as control.

**Outputs**
The main outputs will be how the tested elements handle the stresses they are subjected to and whether alterations must be done to the production of the system. If the reliability growth tests are used on
materials in a very early phase, the output might be used as inputs to the design phase when the materials are chosen.

5.8. Accelerated testing

Accelerated life testing is a method where an object is forced to fail. Failures are induced by submitting the product to stresses it will experience during its operational life, but at a larger scale. A reliability engineer is interested in failure data for the operational life, for example failure rates. The main problem with such data is the time it takes before a failure. Databases can be useful to obtain failure data, but they rarely consider the differences between the operational conditions of the items that have failed (Weibull.com (A) (2010)). Accelerated life testing can therefore be a solution both to the environmental differences and the time it takes to obtain the data.

The tests for this method can generally be split into two categories; qualitative and quantitative tests. The former is useful for the detection of failure modes and failures, while the latter gives input to life predictions and failure data, for example MTTF (www.weibull.com). Qualitative tests are primarily made to pressure the product to failure and provide results fast. Examples of such tests are the elephant test, the torture test, HALT and shake and bake tests. These do not necessarily employ time as a measure and it can thus be hard to say something about the life time of the product. Quantitative tests can be divided in two; accelerated usage rate tests and overstress acceleration tests (www.weibull.com). The first is convenient when the products are not in continuous use, such as dishwashers and coffee machines. Possible testing methods would then include using the products with an elevated frequency.

As with reliability growth, custom-built products might not suit this type of testing. The components and sub-systems which are easy to produce and inexpensive can be tested instead. A very important aspect of this method is that the reliability engineer must be aware of what type of product he or she handles. A product which is in continuous use should not be subjected to accelerated usage tests. For a product which is turned on and off, it might be interesting to use both accelerated usage tests and overstress acceleration tests. For qualitative tests, it must be evaluated whether it is likely that the product will be subject to increasing pressure over time.
Inputs
Accelerated life tests cannot be performed without knowledge about the materials in the system, the operational and environmental conditions and the possible system failures. Based on this information, it can be possible to deduce which tests are the most appropriate.

Mechanisms
As this method is physical, it is very important to have the appropriate resources. For the test operators, it is necessary with knowledge about the materials used in the product and its mechanical construction. Otherwise the test may be performed incorrectly or the results misinterpreted. The analysts will also need this knowledge, in order to subtract the correct results.

Control
The main constraints and controls for this type of analysis are time, money, legislations and the product type. Time issues affect the tests available, especially when they demand much time for preparation and execution. Depending on the tests chosen and the materials used in the product, it may be very expensive to perform tests. If the materials are expensive to obtain, it is not desirable to use it for destruction alone. Legislations can affect the tests through the time an operator is allowed to work or the emissions they might lead to. When products only are produced once or in very few numbers, the accelerated life testing can be difficult to employ. Among the standards suitable for the control of this method are IEC 62059 (2008) and IEC 60068 (1995).

Outputs
The outputs from the accelerated life tests may be used to confirm previously predicted reliability estimates. They can also help improve the manufacturing process and the design. If the tests are performed after the design is frozen, alterations will be difficult. A possible use of the outputs could be for maintenance and check-ups on specific modules and sub-systems which seems more probable to fail. If it is desirable to test before the design is frozen, it is possible to do testing on items which already exists. When the results are analysed and given as failure data for a longer life, they can be stored for later development projects.

Figure 21: SADT Accelerated testing
5.9. FRACAS

Failure reporting analysis and corrective action system (FRACAS) is a closed-loop method where the supplier and customer work together to study the product reliability. The main purpose is to have all failures in both hardware and software systems reported, analysed and understood. All information concerning a failure will be recorded, identifying the failed items, symptoms, operating times and time of failure (MIL-HDBK-2155 1995). The verification of the failure and the successful corrective actions are important to prevent the failure from recurring (MIL-HDBK-2155 1995).

Inputs

For reliability purposes, FRACAS is best used together with other analyses. The intention of this method is to use it as a tool while the product or system is in use. Other methods suited for earlier phases should be used as inputs. An example of how a combination of FRACAS and another method can be favourable is the coupling of FRACAS with FMEA/FMECA (MIL-HDBK-2155 1995). FMEA/FMECA can give input to FRACAS by descriptions of failure modes which are encountered. A failure reported through FRACAS can be brought back to complete the FMEA/FMECA.

Mechanisms

FRACAS is dependent on accurate input data, well prioritised goals, and time and resources (Hallquist & Schick 2004). A reporting system should be agreed on between the manufacturer and the client, and used as a mechanism for the reporting. The people reporting and analysing the failures needs thorough knowledge of the system and the nature of the failures affecting it.

Control

In FRACAS, the extent of the failure is a control parameter. A failure leading to a destructive consequence takes time and money to investigate. If the destructions are extreme, it might not even be possible to find any answers. Another control issue is the agreement between the manufacturer and the client. This will regulate how the reporting is done and what information the parties are sharing. FRACAS is shortly described in IEC 60300 (2003) and SEMATECH (Villacourt and Goviul 1994) which may be used to follow up the planning and use of the method.

Outputs

Outputs of the FRACAS method are of use to later development projects. All lessons learned will lead to less repetition of failures and history might therefore not repeat itself.

![Figure 22: SADT FRACAS](image)
5.10. Discussion

The methods described in this chapter are some of the more well-known tools used by reliability engineers. All of them are applied across most industries, depending on product type. Which method one ends up with should depend on the life cycle phase, the desired outputs, the product and the available resources. A methodology for Design for Reliability must contain a selection of different reliability methods based on their ability to complete each other.

Early in the life cycle, the method choice will be constrained by the existing information about the product. Many parts may not be specified and changes will probably occur later on. During later phases, the input to the analyses can be found from other similar products, methods performed in the previous phases and tests. Depending on the cost, size and utilisation of an item, certain methods may not be applicable at all.

Using SADT as a tool to evaluate the applicability of a method can be preferable when there is a need to act in accordance with specific constraints and demands for the desired outputs. If a reliability programme is desired, the SADT can show which methods may follow one another to complete each other and the reliability picture. It is for example evident in this chapter that FMECA and FTA are useful together in order to show both simple and dependent failures.

Some of the methods are already used together in specific types of analyses, in order to develop a specific overview of a product. One such method is the reliability, availability and maintainability (RAM) analysis. This uses FTA and RBD among other methods.
6. RAM analysis

A RAM analysis considers the reliability, availability and maintainability of a system. As mentioned in chapter 2, reliability and availability are tightly connected through their definitions. Maintainability is an important parameter as it describes the downtime in case of a failure; if the maintainability is poor the availability will decrease. Reliability and maintainability defines, in large parts, the availability of a system.

The RAM analysis should be used in early design phases in order to contribute to the optimisation of the design of a system. The RAM analysis can give valuable information with regard to recommended sparing and repair philosophies, as well as advice in connection with the optimal redundancy introduced into a design. In later phases of a project the RAM analysis is used mainly as a verification activity to show compliance with requirements.

6.1. Method

RAM analyses use information about expected time to failure of components, downtime in case of a failure, spare part philosophies, and planned maintenance in order to study the overall availability of a system. Due to the amount of information handled, it is not uncommon to use computer tools. These will then use the input information, relate it according to the system design and operation, and simulate the events of the operational life to obtain an overall availability.

In order to build a model of a system in a RAM analysis computer tool, the following inputs are required:

- Definition of system boundaries, assumptions and limitations
- Identification of main failure modes and corresponding effects
- Definition of reliability input data on component/module level
- Definition of repair requirements

After the study boundaries for the system have been identified, FMECA can be a useful input. The FMECA provides possible failures for each system component, the cause and criticality of each failure, and detection and repair methods. If possible to determine, the detection time of a failure may also be useful.

To establish detailed reliability data for each component or sub-system it is often useful to prepare RBDs or FTAs. These methods allow for detailed assessments of each component in order to establish failure rates and MTTF estimates.

The downtime caused by a failure includes the period from detection of a failure until the repair has been carried out and the system is in operation. This is an important subject which can be studied by RAM analyses. For some systems the downtime will be more extensive than others. While a radio antenna which cannot receive signals only needs to be changed for the radio to work, a subsea process system requires far more specific equipment for repair.

If a module in a subsea process system needs to be changed, a replacement must be brought from storage to the specific location of the system. When the sub-systems and modules weigh several tons, it is evident that diving is not an option for installation, sub sea repair and retrieval. Vessels capable of carrying the load and lowering them into the sea and place them correctly are needed, as well as technology such as ROVs (Remotely Operated Vehicles). The ROVs can connect the different
modules and operate manual valves on the system. Information about which vessels are required along with the mobilization time of these vessels is required as an input to a RAM analysis of a subsea process system whose downtime must be found.

For the intervention vessels, the period defined as the mobilization time includes the period from detection of failure until the vessel is located and properly operational at the repair site, including:

- Diagnostics of failure and recommendation of repair activity.
- Preparation and approval of work order issued to Service Company.
- Spare part and tool handling, as well as possible transportation
- Identification and organization of appropriate intervention resources, clarification of responsibilities, crew familiarizing with the failure/problem.
- Preparation and approval of mission procedures
- Manpower/resource transportation to field, preparation for intervention (including vessel demobilisation from other work, transit to shore, mobilisation of dedicated equipment for intervention on the site and transit to field).

The active repair time, mean time to repair (MTTR), is the time from the intervention vessel has arrived at the Midgard field, to the time when the fault has been rectified (by repair or replacement of equipment).

A reduced downtime can be obtained through an effective sparing philosophy. If a failure occurs in a component, the downtime will depend upon whether the component has to be repaired, or whether replacement by a spare is sufficient. If no spares are available the mean time to repair will increase substantially. When a spare is available the expected active repair time will be reduced to a couple of days (retrieve and replace on site). If no spare is available the active repair time may vary from a couple of months to a year.

Capital spares should be available for the most critical items in a system; this will significantly improve the availability of a system. The location of the spare parts and the time required to load them onto a vessel will also be important factors with regard to the maintainability of a system.

When all the necessary input parameters have been determined, the computer model of the system can be built. The input parameters are logged for each item, including failure rates, repair times, mobilization times of vessel, spare parts required, and amount of production lost upon a failure etc. Factors such as weather conditions will also be included in the analysis.

All possible combinations of events, and repair operations will be randomly simulated in the computer program and the overall availability calculated from it.

### 6.2. MIRIAM Regina

MIRIAM Regina is a commercial software package for reliability and availability analysis. It was developed in close cooperation with Norwegian oil companies and has been used for several field development studies. In the Subsea Power and Process department it is used to evaluate the operational performance of subsea process systems, considering the availability, production capability and maintenance resource requirements (Rausand 2005). The results are based on stochastic simulations of the inputs sent through a model describing the system.
The model is defined through boundary points, process stages and storage points. Boundary points are where the inputs enter and the outputs exit the system. Process stages are components or functional units as they are in real life, often broken down to sub-component stages. The storage points are the buffers of the system which can be used to contain or release flow depending on restrictions in the system (Rausand 2005). The entry point, functional units and exit point are linked together through connections, describing the shape and flow paths in the model.

Before MIRIAM Regina is used, the following is done:

- Definition of study objective, approach and metrics
- Definition of study boundary, assumptions and limitations
- Identification of main failure modes and corresponding effects (often through previous FMECA)
- Definition of reliability input data on component/module level (failure rates and MTTF, can be found through detailed assessments of each component through FMECA, FTA and RBD - see descriptions below)
- Definition of repair requirements, repair time and intervention vessel mobilization time

When all inputs and necessary data are entered into the program, simulations including sensitivities for different concepts can be run. MIRIAM Regina uses the Monte Carlo simulation technique which generates random values for the uncertain variables, based on the probability distributions describing the inputs (Berg 2009). A number of simulation runs are made in order to obtain a full picture of all events which may occur, and how they affect the system’s availability. The Monte Carlo simulation technique is also referred to as Monte Carlo next-event simulations and can be studied further in Berg (2009), Rausand (2005), and Rausand and Høyland (2004). The results of the simulation runs are transported to excel sheets where they can be further studied. These results include production availability and deliverability, subsystem criticalities, resource and spare part usage etc. (Rausand 2005). The outputs of most interest to Aker Solutions and their clients are the availability and the productiveness, which together describes the production regularity.

Regularity is a term used to describe the capability of a production system of meeting demands for deliveries and performance (Rausand & Høyland 2004).

6.3. Use of outputs

The outputs from MIRIAM Regina and RAM analyses can be used as foundation for decisions concerning necessary design alterations, maintenance programmes and operation of systems. Among the outputs there should be a critical components list. The critical component list can be used as input to suggest design changes, such as increased redundancy, that will improve the reliability of the most critical components, or to suggest an optimal maintenance and sparing philosophy.

The availability of a system is in a large part affected by spare part and intervention philosophies. The outcome of the RAM analysis can show where capital spares are required, the number of spare parts required for each item, and it can also give input to the appropriate storage of these spare parts.

The mobilisation time for spares should be as short as possible. If it is shown that some spare parts need far more time to be obtained and transported than is desirable, it can be decided that one spare part should be installed on the seabed or moved to an easier location.
The RAM analysis gives an overview of the number of interventions required per year for the system. An overview of the intervention frequency can be used for operational expenditure (OPEX) calculations with regard to vessel costs etc. and to outline an effective maintenance philosophy.

As with outputs from any methods where probability is used, there are uncertainties. MIRIAM Regina is no exception, and basically there are two types of uncertainties which an analyst must be aware of; parameter uncertainty and model uncertainty. The input parameters may have errors in them, either the chosen distributions are wrong or the inputs are incomplete or erroneous in themselves. This is parameter uncertainty. Model uncertainty is directly connected with any models chosen or made for the simulation. These may have errors in them or not be extensive enough to explain the real system. Other types of uncertainty exist and can be found in the RAM analysis, but these are of less importance.

Rausand (2005) described a problem with MIRIAM Regina concerning the lacking ability to model any other probability failure distributions than for the time to failure. There are no possibilities for implementation of probability distributions on other reliability parameters such as failure rates. Uncertainty for reliability parameters is almost impossible to implement and the thought of their quantification was not even a concern when MIRIAM Regina was developed. In the Norwegian petroleum industry, the main inputs often come from ORED. The opening chapters of the ORED handbook mention the assumptions made and that there are uncertainties in the data (OREDA 2002). This, along with the fact that new systems rarely have much experience behind them, should make it evident that more considerations of uncertainty could be desirable in MIRIAM Regina. Problems and limitations are further discussed by Rausand (2005).

Although there are uncertainties associated with the tools for RAM analyses, the outputs can be of great importance. To obtain an exact calculation of the availability is not the most important application of the RAM analysis tool. It is rather more interesting to identify the most critical components in a system, and to use the tool as an input for optimisation of design, sparing and intervention
7. Unreliability

A search for synonyms for the word “unreliability” returns inaccuracy, instability, credibility gap and insecureness among other answers (Thesaurus.com 2010). These are all good substitutions although they might be considered too specific when they are used to describe an item. Unreliability is defined as “not reliable” or “not dependable”. This would mean that it is the exact opposite of reliability, but the origin of unreliability might as well be the same as for reliability.

Before starting a discussion of factors which may contribute to unreliability, it is useful to understand what is meant by the term “unreliability”. Reliability is considered in terms of probability, thus it is always between zero percent and 100 percent. One can think of unreliability as 0 percent on the scale, being the opposite of reliability. But, another option is to think of 0 percent as “no reliability expected”. This would render the word “unreliability” useless. If a product is 100 percent reliable, one knows that it cannot fail to perform its intended function. When the product is believed to have no reliability at all, one does not expect the product to perform the function one considers using it for. This implies that the product is outside of the perspective of reliability as reliability depends on an intended function. Unreliability can be the opposite of reliability, but when we are considering a given product, we have expectancy of its “ability to function”. Keeping unreliability as a term for when the product is expected to function, but fails to do so, we can look at unreliability as something which decreases the reliability. Factors contributing to either reliability or unreliability could determine whether a product moves up or down the probability scale for its ability to function. Factors contributing to unreliability are negative, while factors contributing to reliability are positive.

The calculations and predictions of a system’s reliability are based on assumptions, reliability methods and previous experiences. If any of these are unreliable, unsuitable or uncertain, the actual reliability will be different from the predicted reliability. If the inputs to the reliability analysis are unreliable or unsuitable themselves, and known to be so, they can easily be excluded. The problem is if this is not known. In that case, unreliable or unsuitable factors are basically the same as uncertain factors. Uncertainty is a problem where the lack of knowledge leads to the wrong inclusion or exclusion of information.

Uncertainty usually arises from a lack of knowledge or randomness in samples (Paté-Cornell 1996), where the former is referred to as epistemic uncertainty and the latter as aleatory uncertainty. Unreliability arising from uncertainty can be affected by both of these categories and if the category is known, there may be a possibility of reduction as well. Aleatory uncertainty is unpredictable and is accepted through the assumption that a phenomenon has an intrinsic randomness (Kiureghian &
More knowledge about the phenomenon is not believed to alter this type of uncertainty, but it is thought possible to study the randomness through uncertainty probability distributions. These are used to show the outcome of the randomness and give an indication on how the uncertainty of the input parameters is distributed in the output. Epistemic uncertainty is reducible through increased knowledge. It can be split into either model, parameter or data uncertainty and be studied according to what type of uncertainty it is (Drouin, Parry et al. 2009). The concept of uncertainty and how it can be specifically studied and understood is further discussed in Berg (2009).

The reliability of a product can also be altered by the events and thoughts which where not brought to the table during its design and development. Whether such events are positive or negative to the reliability cannot be known in advance, but due to the possibility of a negative outcome, care should be taken to avoid it throughout the process. The basic factors may be discussed and defined by their origins, but to understand how they develop and affect a system, it is perhaps more useful to look at them through the phase they arise in. The eight phases presented by Murthy et al. (2008) are used here. In each phase the factors will be discussed in a general and a subsea perspective.

**Phase 1**

During this phase a customer presents a request proposal to possible manufacturers who reply with bid proposals (Murthy et al. 2008). The request proposal will include information on what functions the product must be capable of performing, performance requirements and general information about environment etc. A bid proposal will indicate how the product can perform the desired functions and be realised. It should also indicate the performance levels and the costs. After one or more rounds where the possible manufacturers are narrowed down to one, a contract is signed and the main control of the project handed over from the customer. This phase ends when a decision is made whether to proceed with a development project or not.

There are four main factors which can have an undesirable effect on the reliability in this phase. These are:

- Bad communication
- Lack of knowledge
- Lack of information/data
- Misunderstanding/misinterpretation

Communication is the main activity during the first phase and if it is not executed properly, it will be hard to know what the desires and requirements truly represent. All the information is given through communication channels of some kind and it is how these channels are handled that is of importance. A well known children’s game is the “whispering game”, where one child starts out whispering one phrase to another child. The second child whispers it to a third child who continues the chain. This ends when the last child in the group has been given the phrase and speaks it out loud. A very normal effect of the whispering chain is that the end result turns out quite differently from what the first child whispered. This is an example of how communication with many segments and different understandings can be unfortunate.
Another problem occurring with communication is when the basic definitions and knowledge used by the communicators is different. This can be exemplified through the use of technology readiness levels (TRLs) in the industry. While a client has one standard they follow, the manufacturer might use another. Normally this would be investigated and the best solution chosen, but in the case that it is not discovered, a product might be approved on the wrong grounds in a later phase. A possibility is that those using the documents are of different nationalities, with different mother tongues. Their understanding of documents, such as TRLs, might then lead to problems which are not discovered. Communication cannot be avoided in this phase or any other phase, but it can be improved through an elimination of the number of elements in the communication line. Language difficulties will always be present, but this should be a good reason to ask more questions in order to ensure that the understanding is the same.

Lack of knowledge and lack of information are here separated and given different meaning. The first is meant as a lack of knowledge and education of the users of the information, while the latter indicates that all the available information has not been obtained. Lacking knowledge can lead to misuse and misinterpretation of analysis methods and their results. In the first phase this means that any studies done for the establishment of a concept can give a wrong belief of what is a feasible product. The problem will exist throughout all phases of the life cycle as new analyses are done and new possible failures and hazards discovered. The lacking knowledge will also affect the communication if one party does not have the ability to understand the other.

Lack of information is an epistemic uncertainty. It can be improved through a search for more information and data, but if it is not known that something is missing, it will be hard to see the reason to do more research. Any epistemic uncertainty leads to shortcomings in the inputs to reliability analyses and will in the first phase render possible decisions on the wrong grounds. If Statoil does not have appropriate information about the pressure in a well, the functional design specification for an SCS will be wrong and in the end the system may fail to work as intended.

Misunderstandings and misinterpretations of data can happen at any time. In the first phase it will have the same effect as lack of knowledge and information. It is an epistemic type of uncertainty, were the information is available and easily altered for the correct use. It should hence be obvious that a second evaluation of any interpretation of data must be done. Lacking information takes time to retrieve and may be overcome if other information can indicate the correct answer. Misinterpretation, on the other hand, is easily done and easily corrected.
Many problems may arise in the first phase and any factors known to contribute to uncertainty must be studied thoroughly. If an error arises in this phase and is allowed to live on, it will continue to affect the system throughout the other phases. While reliability analyses can overlap each other and remove problems in later phases, no analysis can alter the problems and errors in the requirements set in the first phase. These must be correct to begin with.

**Subsea Process Industry**

During this first phase, the Subsea Power and Process department will do research, including reliability estimates, to find out whether the project is feasible and worth doing. Normally little has been done of reliability studies this early, but in order to win the project, it is often important to show that a certain reliability or availability can be met with. This will be done through estimations based on previous projects and the OREDA handbooks.

The OREDA handbooks are based on data collected from the offshore installations of operators in Norway. All data collections will have associated uncertainties. The uncertainties are due to the data being collected in different locations with different operational conditions (OREDA 2002). The failure rate data are assumed constant, as explained for the bathtub curve in chapter 2. Any assumptions and misunderstandings connected with the appropriate use of these data can lead to the impression that a reliability requirement can be reached more easily than in reality. The effect of this will mainly be that more work has to be done later in order to achieve the desired reliability. Mitigation can be possible through thorough knowledge of ISO 14224 (ISO 14224 2006)

**Phase 2**

When the focus of the product life cycle turns to technical specification at product level, one enters into phase 2. First, the desired product reliability will be derived from the requirements set in phase 1. The specifications and customer requirements can include variables, such as availability, which can be used to obtain this. During phase 2, alternative system architectures for the product are reviewed and the best response to the desired performance is chosen. An important feature of phase 2 is how the engineering of the product is included in the product development. Before this stage, the product is more of an idea, than on the paper with realistic measurements and technologies supporting it. As the system architecture is decided, models can be used to find the overall predicted reliability and product performance. FTA, RBD and FMECA may be used and the two first ones can be particularly useful to find the best architecture. Any results will be measured against the desired reliability and performance. Only when these are reached can phase 2 be completed.

The main factors which may lead to a decrease in the actual reliability during this phase are:

- Wrong assumptions and interpretations
- Miscalculations
- Parameter uncertainties
- Wrong time and cost limits

The first two are epistemic uncertainties, while the latter can be both epistemic and aleatory uncertainty. Parameter uncertainty can both be a wrong choice of parameter, and randomness connected with the chosen parameter.

If the desired product reliability is interpreted wrong, or the assumptions concerning the system architecture is badly thought through, the reliability may be allocated erroneously. While allocating the reliability, calculations will be made which can go wrong. Nothing should be accepted too lightly at
this stage. A wrong allocation can lead to too low reliability being demanded from one or more parts of a system. Another possibility is that a part which actually can have lower reliability is set higher than one which needs high reliability. Both possibilities will lead to a wrong understanding of the system throughout the project. If the desired product reliability is wrong, either in itself or for the components and sub-systems, a manufacturer might release a system which should not have been accepted for release.

Even if the allocation is correct, the system architecture can be wrong. Poorly chosen system architecture can lead to more specific product characteristics being left out. This will also decrease the chance of reaching the highest reliability possible.

When methods for reliability are used, it is important that the analysts have expert knowledge of the method, and a good understanding of the inputs to get relevant outputs. When the architecture of a system or sub-system is based on the results from an FTA, the mistakes made during the analysis will have an impact. Possible factors contributing to unreliability may therefore be wrong use of the method, the inputs or the outputs of an analysis. Wrong use is epistemic uncertainty, as is a wrong interpretation of the outputs. If the input parameters have some randomness in them, aleatory uncertainty will propagate through the fault tree into the output. As said at the Subsea Power and Process department: “Shit in equals shit out.”

This phase, as most other phases, will be constrained by limitations of time and costs. With a project management unable to understand the content of a phase, the limits can be wrong or poorly exploited. If it is discovered that a technology is unacceptable while an FTA or FMECA is performed, it will take time to find more information or other alternatives. If there is no time available, the results will be meek, showing only that the system is not good enough. The same can be the result if there are no resources available to perform further analyses. This might lead to the closure of a perfectly feasible project. Such problems can occur and should be accounted for when the phase is planned.

The main factors which contribute to reduced reliability in this phase are related to uncertainty about the preferred characteristics/configurations for a product. Uncertainty about the allocation of the reliability requirements to these configurations will also be important to follow. The main problem is to make the correct choices, both for specifications and design. A bad choice will persist and possibly accumulate throughout the whole product life cycle if no changes are made. The specific challenge of phase 2 is to have the correct understanding of the design and notice how the reliability of one item truly affects the whole system.

**Subsea process industry**

When a subsea process system development reaches this point, the system architecture will be developed by a team of engineers with different backgrounds. If anyone among them assumes that a decision is good enough without knowing how it affects the system reliability, weaknesses in the system design may be the result. It is therefore important to involve a reliability engineer in the design process to give input to, for example, choice of a parallel structure over a series configuration.

A subsea project faces all the challenges discussed for this phase. Phase 2 will contain estimates which, unlike phase 1, have a direct impact on the choices made for the system design. No assumptions can be made without good reasoning and the OREDA database uncertainties must be understood to the fullest. The parameters from OREDA will contain aleatory uncertainties and must thus be treated as such. Any miscalculations can make a large impact on the results. As the technology is advanced, often complex and maybe even new, the time and cost frames for the design phases must
be decided with care. A rushed design will not benefit the reliability of the product. During these early phases, reliability issues can be discussed freely and problems be eliminated without physical interventions, and at low cost.

**Phase 3**
This is the phase where the detailed design takes place. Based on the decisions made in phases 1 and 2, the engineers must decompose the system into sub-systems and all the way down to the component level. From the component level, the engineers should go upwards and find the total predicted reliability based on the new information, and decide whether it is acceptable or not. The reliability predictions are based on existing knowledge about other similar components. A design should be accepted if proven to have an acceptable reliability. Through the reliability allocated in phase 2, the proof can be found faster than if no allocation has been done. Methods for estimation of reliability that have been applied in the previous phase should be updated as more information becomes available.

When the engineers and designers work in this phase, it is very important that their choices are thoroughly considered and that all previous decisions are included. The product should not waver from the product requirements, or from the decisions made in phase 2. By this point, all the basic information about the operational conditions and the system functionalities should be known. The factors discussed in phase 2 are also applicable to this phase:

- Wrong assumptions and interpretations
- Miscalculations
- Parameter uncertainties
- Wrong time and cost limits

A problematic factor could be the wrong interpretation of how an error in one component affects the rest of the sub-system, or how the other sub-systems react to it. This might even be forgotten in the process of predicting the reliability. Possible effects between sub-systems can be discovered through the application of reliability block diagrams and similar models, but even these methods are incomplete. This will be due to a lacking understanding of the system, or wrong assumption about how it works.

As a part of phase 3, the methods for reliability evaluation and prediction are applied at a detailed level. The amount of necessary inputs will be high and it is up to the analyst to know what they are and how to use them. The attributes which are to be examined must be chosen, as well as the depth of examination and the analytical approach (NASA (B) 1999). The completeness and suitability of the analysis will thus only depend on the assumptions and choices of the analyst. If some of the basic assumptions are unreliable, the final answer will be less reliable than imagined.

Miscalculations, parameter uncertainties and the wrong choice of time and cost limitations may arise as in phase 2. The main difference from phase 2, where unreliability problems are concerned, is that after phase 3 the design is frozen. This means that unreliability issues in the assumptions and calculations which have not been discovered at the end of phase 3 will not be implemented in the design.
**Subsea process industry**

This subsea process industry is to a large extent affected by all the factors discussed for general products in phase 3. Estimations of the product reliability will be done, the final elements in the system will be decided and the design is frozen. No assumptions can be made lightly and all choices must be studied thoroughly before they are made.

The OREDA handbook will now be used a final time. This is also a phase where difficulties concerning documents such as technology readiness levels (TRLs) can become important. These documents are often internal to the companies, but contain the same terms and types of information. They can therefore have different interpretations of the same elements. A TRL document describes the maturity a technology, whether it is an idea, a proven concept, has been tested or used for a decade. As the design is frozen, the system ought to have reached a level described as “proven concept” which is demonstrated by the analyses performed.

Aker Solutions have eight technology readiness levels (ref [76]). This number is quite normal, but what a level means may change within an industry. In order to ensure a common understanding between the companies, it is necessary to decide which document to follow. The main problem with assumptions concerning how far the development has come is the belief that a project goes by faster or slower than it does. This could mean a more relaxed or stressed environment in the project organisation. Other documents differing between a manufacturer and a client can lead to similar problems according to the type of document.

**Phase 4**

When the reliability of the design has been predicted, the physical product must be manufactured in line with the production. During phase 4, the development starts with the components and continues on higher levels. A good technique in this phase is the TAAF, Test, Analyse and Fix, where a new component may be developed and tested several times until it has reached the required abilities. Among the tests performed are stress tests and accelerated tests. If the test results are acceptable, the component is accepted. This can be done to all components and sub-systems, and if the final system is a prototype not intended for later use, this can be tested as well. For some manufacturers it may be hard to perform many destructive tests, especially if the prototype can is the same as the final deliverance.

Physical testing shall be performed to prove that a product has been manufactured as specified during phases 1 to 3. Shortcomings or errors made during the previous phases can be revealed through testing and mitigating actions may be implemented.

Among the problems which can affect the reliability negatively are:

- Lacking knowledge of production/manufacturing facilities
- Lacking resources
- Misinterpretations
- Time/cost issues
- Construction system problems

An important part of this phase is the planning of the manufacturing and assembly of the components, sub-systems and system. If the planning team does not have the required competence to understand how the facilities enable the production, it might leave steps out of their plans. The production must be properly prepared and performed. Otherwise the different parts of the system will have errors in them,
or be assembled in a manner which is not desirable. Another reason why lacking knowledge on this point is difficult is the testing possibilities. If the potential for the use of the facilities for testing is not seen, tests which ought to have been performed might be ruled out. Although it is reasonable to believe that there is enough knowledge about the facilities, it is the combination of this and the understanding of which tests are needed that can be the greatest problem of the phase. If a necessary test is left out, an unacceptable item might be put to use, creating unreliability in the system.

Another reason why a test can be left out is a lack of resources able to perform it. In some cases the personnel who know the materials and the tests can be unable to oversee the procedure. The correct personnel are vital for the tests to be performed correctly. They will be able to help the analysis through their knowledge of how the test results should be interpreted. Misinterpretations can lead to an unacceptable component being accepted or an acceptable item being left out. The first will be problematic to the reliability while the latter will affect the time and costs available for other tests. Time and costs are the constraints of the tests in phase 4. These factors may limit the number of tests performed, the time to analyse the results and the extent to which a test may be performed.

The sub-contractors could also be a factor if diseases, strikes or production problems lead to components being less reliable than they otherwise would have been. If the problems are not discovered early enough and the parts considered acceptable without testing by the manufacturer, they could contribute to a lower actual reliability than predicted. This affects the time and cost of the project, and is a management issue.

The final factor of importance in this phase is problems with the construction systems. If the technology for the construction is in a bad shape, the parts produced will be affected. Dimensional problems are likely to be discovered, but internal cracks and alterations in metals and other materials can stay unnoticed. This can severely reduce the reliability of the final product.

If the manufacturer’s product is custom-built and the prototype is handed over to the customer, phase 4 is the last phase. If the tests are accepted and verify the predicted performance and reliability of the system, handover will be the next step. In this case phase 5 is of little or no interest. It is thus imperative that any problems which lead to a decreased reliability in this phase are studied, understood and an endeavour is made to avoid it. Problems with the manufacturing process are discussed under phase 6.

**Subsea process industry**

This phase is as important for the subsea process industry as for any other industry. The physical development of a system is expensive and must be planned very well. In some cases, all destructive testing is undesirable for a product and it is then even more important that the planning has considered all errors which may occur. However, factory acceptance tests showing whether the different system functions as supposed to or not, will be performed. A subsea process system is unlikely to be tested as heavily as a car, but some checks should be done to see that the materials are not damaged or weakens the overall system.
Phase 5

When the products are meant to be produced on such a scale that the costs of prototypes are small compared to the production costs for final products, it can be useful to let consumers test them before a release to the market. Such tests will need good follow-up and good information to the consumers about how they shall document their usage. This phase will return information on the reliability of the prototypes, but the utilization will differ from one consumer to another. The analysts must therefore consider the differences carefully in order to reach a proper conclusion from the experiment.

Problematic factors in the phase are related to the information given out and gathered about the product:

- Lacking information to test consumers
- Erroneous reporting

A possible factor is the information given about the test. If it is badly explained or given in such a way that the consumers try to find ways to break the prototype rather than using it normally, the outcome of the test may be invalid. This testing is the last to be performed before the large scale production and release to the market. It is therefore even more important that the prototype testing is comparable with the actual use during the operational life.

Erroneous reporting from the consumers can be a direct effect of lacking information given before the experiment started. If the reporting is inadequate or incorrect, the analysis of the reports will be based on the wrong grounds as well. This can lead to changes in the production process that are for the worse rather than the better. Bad reporting could also lead to measures not being taken to improve the product.

Subsea process industry

This phase is not of specific interest to the subsea process industry. What may be said is that if any end-of-development-tests are performed here, the same factors as discussed in phase 4 can be considered.

Phase 6

Phase 6 is mainly concerned with production and is only relevant in cases where more than one product is manufactured. If the product is custom-built and delivered after phase four, then this phase is of little relevance. Nevertheless, the factors of decreased reliability may be relevant during the production of custom-built products as well. The main factors are:

- Deviations in the production process
- Human interaction/handling

No process can be exactly the same every time and this is especially true when a large number of the same product is manufactured. For this reason the production process must be followed carefully to avoid deviations outside any acceptable limits, for example 2-3 mm diameter for a pipe. An undiscovered deviation can lead to reduced or altered inherent reliability. When the deviations are created by mechanical equipment, it is possible to make adjustments or repairs that erase the problem. Even though most parts of a manufacturing process may be done mechanically, there are still humans involved. The human being is considered to be very unpredictable and human errors are easily made. If a bolt is supposed to be tightened by a person during the production process, he or she might tighten
it too hard or loose without knowing it. This can affect the reliability of the product. To adjust such a problem is not the same as with a machine, especially as it can be harder to discover.

Any handling which has not been considered in an analysis can alter the reliability negatively. To foresee human handling, an analyst must know how the process will be designed and how the operation is performed. The tightening of a bolt is a rather small part of an operation and to consider all errors that can take place will be difficult. Human handling is generally a large factor which cannot be overseen. It is the most unpredictable, but it may also be the easiest to instruct. Through the use of methods such as HAZOP or SWIFT, it can be possible to study the operational hazards in the production process. If all the human handling has been thoroughly gone trough beforehand, both during the production process design and when the workers are instructed, the risk of mistakes can be reduced.

**Subsea process industry**

Human handling in the product development and assembly is an important issue for the subsea process industry. A bolt which is not tight enough can mean that a system is unable to handle the pressure from its inside or the water on the seabed. A bolt which is too tight can create cracks in the construction. The “little things” that might not be a problem above water can create extreme problems sub sea. Small deviations, erroneously tightened bolts and nuts etc. are nearly impossible to correct as soon as a system has been installed sub sea.

The best manner in which problems inflicted by human handling can be corrected is through repeated learning and clear instructions. Human beings cannot be taken out of the process, but they can be given the task of learning how the errors arise, their effect and how they can be avoided.

Aker Solutions do have some series production and is currently looking into the possibility of developing more standard shelf ware for subsea petroleum purposes. With this in mind, the Subsea Power and Process department should look carefully into the mass production and review all the difficulties which may arise in this phase. One thing is to evaluate the production of one item, another thing is series production. Any of the problems discussed for this phase will then be even more relevant, and more care must be taken to study the deviations in the production process.

**Phase 7**

Phases 7 and 8 are post-sale and the product is therefore no longer in the hands of the developers. A system can be operated by the same company that manufactured it, but it will now be in use and only maintenance can have an impact on the actual reliability. Phase 7 is placed on the product level and therefore concerns the reliability performance of the product alone. For a standard product produced for many customers, the reasons for a decreased reliability will be different for each item. The conditions they are used in and how they are handled will depend on the consumers, as the products are left entirely to them. The goal of the manufacturer in this phase is to collect the information about how soon and why a product fails. For standard products this means that the complaints and the repair information during the warranty period are the only sources of information.

The factors which can be affected by the manufacturer in this phase are associated with the transport, installation and basic user information:

- Unconsidered transport environment
- Stresses during transport and installation
- Lacking information to customer
- Misinterpretation of failure

In handing over a product to a client or a market salesman, transport is the main step taken. During transportation the product can be exposed to environmental conditions that it was not built to handle. Unexpected stresses and vibrations may occur if it is not handled carefully. At installation, the procedure would normally be well prepared in advance, but one cannot always get perfect conditions during the operation. If the weather is an important factor for the installation to run smoothly, sudden changes can give way for stresses to occur.

While a product is in use it may be exposed to mishandling which can affect its ability to perform an intended function. A wooden box is usually meant to be a dry place to store things. Normally one would say that for this purpose it would be rather reliable. If the box was used as a stool to get a glass down from a highly placed shelf, its reliability could be altered. A box which has been used as a stool may get cracks in it. The cracks can open the box to air and water leading to the content not being kept in its desired state. Altered or decreased reliability from unintended use is hard to consider for an analyst, as the discovery might depend more on imagination than knowledge. In order to avoid misuse or complaints about how a product functions after such mishandling, the information given to the customer must be well thought through. It is a known case that many customers avoid reading manuals, but this does not mean that they are unnecessary. The manufacturer has a duty to inform the customers. Any problems which occur due to a lack of information can reflect poorly on the manufacturer and lead to warranty claims.

If a product has failed and repair is demanded, a maintenance programme is normally prepared some time in advance. It should therefore not be a problem to return the product to normal operational state fast. However, neither a maintenance programme, nor prepared repair actions can help the avoidance of misinterpreted failures. This will lead to a wrong choice of maintenance activities and possibly ruin the product. If the product is returned with a fault, it can be dangerous for the customer to use.

The main objective of this phase, for a reliability engineer, is to obtain information on how the product performs while in use. Information about the failure in standard products will normally be found through warranty cases and repair information. For the custom-built product it can be easier to keep in touch with the customer, but it might be more difficult to obtain the repair information unless the manufacturer performs the repair. The root cause of a failure is much needed information for the manufacturer, if the overall reliability performance is to be evaluated. This does not affect the reliability of the product, but may indirectly affect the reliability of a future product. However, it is hard to do anything to prevent the lack of returned information. The only option is for the manufacturer to go actively into the task of getting updates from the buyers.

**Subsea process industry**

When Statoil approaches Aker Solutions, they ask for custom-built products. Such products will meet with the same factors decreasing their reliability as the standard ones. The main differences are that the operational conditions are well accounted for, and there is thus less chance of mishandling during operation. However, mishandling cannot be left out entirely as long as human beings are involved. The systems are normally made on demand and the information concerning its use is well communicated between the producer and the user.

We cannot look away from the possibility of bolts being tightened too hard or too loose, nor can we think that transport in the subsea process industry is safe. Although systems have been transported to subsea locations for several decades, the transportation is not perfect. A system transported from...
manufacturing at Tranby outside Oslo to testing at Nyhamna in Møre and Romsdal will be subject to several stresses. Some parts of the transportation will go by land, other parts by sea. Loading a system from a stable position onto a means of transportation can subject it to rotations and forces which have not been accounted for. The systems are usually quite heavy and will be pulled quite heavily in order to be moved. During transportation, there will be movements forcing the system backwards, forwards and sideways in its container. If it is not well secured, it can crash with walls and other elements. The opposite problem may occur if another element is badly secured and crashes into the system. All of these possibilities can affect the system in a negative way, rendering it less reliable.

Systems developed by the Subsea Power and Process department are meant to be installed sub sea. This means that the installation is especially difficult and that the operations must be performed by machines. The crew during the installation will usually be placed on a boat while an ROV performs the tasks sub sea. If the weather and the sea suddenly became very challenging, the operations would have to stop. Due to uncertain weather conditions, stresses changing the actual reliability can occur during installation.

During operation, the FRACAS system can be used for reporting of failures, maintenance etc. If the agreement is badly written between Aker Solutions and the client, Aker Solutions risks bad reporting. Although the returned information will be easy to handle and confirm, any lacking information can affect later projects. This is especially important to be aware of if the Subsea Power and Process department wishes to develop “shelfware” products.

**Phase 8**

Phase 8, as 7, demands input from the users and operators of the products and systems. This phase also needs input about the performance on the market based on price, market share and competition. The main difficulty is the gathering of enough information and then the proper application of this information. A reliability engineer might not see this phase as very useful, especially as it is used to analyse the business success of the product. However, the analyst needs to use the information found here to see which reliability tasks should be performed in later development projects. It can also be studied how important the reliability is to the customer. Just because a product did well, it should not be thought that the reliability programme was unnecessary. It should rather be analysed what contribution it made.

The factors which can be a problem here are:

- The missing information about product performance
- Wrong analysis methods
- Relaxed relationship to the usefulness of the output for reliability

As in phase 7, the information gathered for analyses of the product performance will depend on the information returned to the manufacturer by the customers. As the overall performance is desired, sales can be included in the analyses. The product’s success, if it is a standard product, can be found from information returned by the salesmen and the manufacturer’s sales department. However, there might still be some clients who do not return the product in case of failure. The satisfaction of the customer is also hard to be informed about without questionnaires or the information salesmen might have obtained. The estimated product performance depends on so many inputs being obtained that it can be a highly uncertain estimate. For a custom-built product, this estimate should be easier to get correct.
The methods used to analyse the returned information can be highly speculative as they will depend on an interpretation of a person’s opinion. Some could claim that “OK” means good performance, while other would call it “barely satisfactory”. Alone or together with a too relaxed relationship to the usefulness of the product performance analysis for reliability purposes, the information could be rendered useless for future products.

**Subsea process industry**

This phase is where the manufacturer must go through the total performance of the product. A subsea process system will have only one client and performance data should be easily retrieved. FRACAS can again be a very useful tool. It is now even more important that misinterpretations of the satisfaction of the client are expressed in a manner which is understood by the reliability engineer. The main influence on reliability will mainly be noticed if the analyses are used as lessons learned in later projects. If the client is misinterpreted, the future project can be built on a system which is not satisfactory after all. Finally, the stored results must be easily accessible in the future.

### 7.1. Discussion

Most of these factors may not be possible to consider through estimates and normal analysis methods. They depend on some sort of interaction, either between people or directly with the system. If the specifications in phase 1 are not properly thought through, or have errors or holes in them, the whole design and development process may go wrong. In phase 2, the allocation of functions and reliability will decide the outline of the system. If this is not performed correctly, the outcome can be a system which does not function optimally, or has a lower overall reliability than it is believed to have. Phase 3 is concerned with the very detailed level, before the design is fixed. Accepting an unacceptable design is a possibility and although the root cause can be found in phase 1 or 2, it is not impossible that a poorly done research job in phase 3 is the reason for the acceptance. From phase 4 and through to the transportation in phase 7, direct human interaction with the system becomes an issue. The human being is called both uncertain and unreliable. How a person performs a task is rarely possible to foresee. The effects can be minor or major, but to discover the cause is hard. Finally, in phase 7 and 8, the reliability of the system lies in the hand of its user. The manufacturer is responsible for the information brought to the customer, but he or she cannot supervise how the product or system is handled. In these last phases, the reliability engineer will be concerned with the gathering and analysis of information about the system’s performance. These tasks can be highly important for later projects and should not be taken lightly. Any errors can lead to the wrong inputs being passed on to later development projects.

What can be done to diminish the occurrence or effect of the factors contributing to unreliability, is to think through the process from the product is designed, through its production, transportation and installation, to the operation in the field. Each phase ought to be gone through by the team working in the specific phases. The team members must consider the tasks performed in each phase and what the product must endure while in development and use. In this way they will be aware of the pitfalls they must avoid and work more consciously throughout the phase.

A what-if analysis may easily detect problems such as those discussed in this chapter. Whether they are discovered or not will then depend on which processes one involves in the analysis and how the questions are asked. If the main factors have been thought through in advance, it is more likely that they can be avoided. A simple checklist for each phase should be easy to prepare and equally simple to use. What one must be aware of is that the uncertainties and possible factors discussed here will not always give a negative output. It is hence important to consider whether one is negative or positive to
the uncertainty brought into the project, possibly accepting one uncertainty and avoiding another. As long as the possibility of negative factors does not become a reason to fear that all new developments will be a failure, being aware of them can be of help.

“Never let the fear of striking out keep you from playing the game” (A Cinderella Story).

Figure 25: Baseball
8. Methodology for reliability in the product life cycle

The factors contributing to unreliability are basically the same for all production industries, whether they specialise in custom-built products or shelfware. Some of them are directly tied up to errors made during analyses which are meant to improve the reliability. Others arise with the manufacturing, transportation and physical use.

All of the methods for reliability discussed in chapter 5 and 6 are available to all industries, only limited by the product type. Although there are reasons to doubt the effectiveness of these methods, it is more likely that problems are discovered with them than without them. If they are put together according to the project phases and tasks, the overall output could prove to be quite useful. With this in mind, it should be possible to make a general methodology for reliability, independent of industry, product or organisation. If the methodology is properly implemented, and thoughts are made in each phase about the possible factors reducing the reliability, it should be easier to mitigate some of the problems. It should also be more likely that the estimated reliability for the final product is correct.

If we want a product with high reliability, it is necessary to prioritise reliability during the design and development, as well as during later phases. With a proper methodology, it should be easier to analyse and evaluate the reliability on a regular basis. A general methodology can be implemented in all industries, but it should never be done without precaution. The methodology must rather be considered as a starting point for each industry or organisation to develop their own, more specific, methodologies.

8.1. Methodology in phases

In this chapter, one general methodology will be suggested. This has then been applied to the Aker Solutions project execution model for technical qualification (Appendix B), for the development of a more specific methodology for the Subsea Power and Process department, which is described in appendix C. The purpose of this is to show how a general methodology can be implemented by any industry or organization. Both methodologies are described through flow-diagrams for each of the phases. As the three final phases are not in the technical qualification, the three last phases in the Aker Solutions’ methodology are only described through text.

The methodologies are based on the following two questions:

- What has to be done in this phase?
- Which methods can be employed?

As shown in figure 8, the five product life cycle stages (Front-end, Design, Development, Production and Post-Production) may be split in eight. As the Subsea Power and Process department at Aker Solutions mostly develop custom-built products, the Front-end, Design and Development phases are the most important. In the eight-phased model these three phases are phases 1 to 5. As shown in appendix C, the phases 6 to 8 do not have the same focus as the first 5. In the general methodology, all phases are equally important. Except for in phase 5 where the products are tested, there are few differences between standard and custom-built products. They all go through the same phases and are subject to many similar project activities. The methodology is thus made for a very general perspective, including all kinds of production industries.
Phase 1

<table>
<thead>
<tr>
<th>Project tasks</th>
<th>Project reliability tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opening for a new product</td>
<td>QFD</td>
</tr>
<tr>
<td>Customer requirements/ market desires</td>
<td>Reliability, availability and maintainability requirements</td>
</tr>
<tr>
<td>Product specifications</td>
<td>Desired reliability</td>
</tr>
<tr>
<td>Generating ideas</td>
<td>GAP analysis</td>
</tr>
<tr>
<td>Concept chosen and defined</td>
<td>HAZID, SWIFT, Early FMEA</td>
</tr>
<tr>
<td>Concept accepted?</td>
<td>Create reliability programme</td>
</tr>
<tr>
<td>Recommend concept definition?</td>
<td>Reliability report phase 1</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Terminate project</td>
<td>Client check-up for acceptance</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Client acceptance?</td>
<td>Phase 2</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Figure 26: Reliability methodology phase 1

Figure 26 shows the main development tasks during this phase of the project. The opening for a new product is either found through a gap which appears in the market, or through the proposal given to the manufacturer by a client. The main problems discussed for this phase in chapter 7 concerns communication, knowledge and available data. While a client will provide requirements, studies must be performed to derive all the desires and requests in a market. To understand what the client or a market analysis means, a QFD, quality functional deployment, can be useful. This is a method in which the customer expectations are identified and translated into technical characteristics (Yang 2007). A customer usually wants high reliability as this implies that the system is able to perform the desired function for a certain amount of time. What the QFD can do is to identify where this reliability
is demanded and from that the reliability targets could be set. QFD is not a tool specifically made for reliability engineering and was therefore not discussed in chapter 5. More information on the method can be found in Yang (2007). From the QFD, information can be exported back to the study of the customer requirements and onwards to derive more specific requirements. These can again be used in the product specifications.

Phase 1 is the time to ensure a proper specification. This should include a definition of failure in relation to the product function, a description of the environments the product will be exposed to and a statement of the reliability requirement where critical failures and effects have a low probability of occurrence (O’Connor 2002). When stating the reliability requirement, it should be verifiable and sensible according to the use of the product. Reliability requirements can be specified according to time, failures or a success ratio, as long as they seem achievable, logic and useful.

When the project team during phase 1 generates ideas which may fulfill the product specifications, they will decide to go further into those which they believe are feasible. A GAP study should be performed to see what the manufacturer already has and is able to do and how far it is to the goal. A GAP analysis is a technique where the questions “Where are we?” and “Where do we want to be?” are answered (IfM 2010). A team with multiple backgrounds should be able to look at what is demanded of the new product, compared with what the current technology may do. If entirely new technology must be developed, the GAP analysis becomes less interesting. The most important outcome of a GAP analysis is an overview of the technology needed. A reliability engineer could be present in the GAP analysis team and look into the reliability of current technology compared with the reliability required by a customer. When the GAP analysis is done, it will be easier to choose a concept based on the width of the technology gap. GAP analysis can be further studied on Federal Agencies (2010).

To aid the decision of whether this concept is acceptable, early analyses should be done to evaluate the possible reliability. Possible methods are HAZID, SWIFT and FMEA which do not need too much input information. Information of use is found in studies and lessons learned from previous projects of a similar type. If the reliability seems to be in the area of the desired reliability, it is reasonable to accept the concept.

When a concept has been accepted and a decision made to proceed with the project, it is recommended to create a reliability programme. A reliability programme is here a combination of methods which are connected with specific project tasks. The reason why a set of methods are chosen is given, and timing for the project specified. The reliability programme should be based on the requirements and targets for the reliability of the product (Yang 2007). Planning for reliability will increase the probability that the final product is reliable, and diminish the costs of sudden reliability checks and unexpected failures. An early investment in reliability activities will also decrease later costs due to lacking investigation of failures. For this reason the programme should stress that reliability tasks are performed concurrently with and throughout the development (MIL-STD-785B 1980).

When the concept is accepted and the programme prepared, the methodology suggests that the client is involved for a final acceptance. This is only relevant if a client is involved in the project. Together, the client and the development team should go through the information they have received from each other and the decisions made. While doing so, they shall evaluate whether the concept is based on a common understanding or not. If there are any unanswered questions or misunderstandings, the team should return to a previous part of the phase and trace the problem to find a solution. This final check-up can be helpful to diminish the problems described for this phase in chapter 7.
Summary
In phase 1 the following reliability activities should take place:

- A QFD translating what the customer wants and requirements for reliability.
- A GAP analysis to decide what the new product is missing to fulfil the requirements.
- Early reliability studies; HAZID, SWIFT and FMEA.
- Planning of a programme which establishes the reliability throughout the life cycle.
- Check-up with the customer.

Phase 2

<table>
<thead>
<tr>
<th>Phase 2</th>
<th>Project tasks</th>
<th>Project reliability tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input from reports phase 1, e.g. HAZID, SWIFT and FMEA results</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System break-down into sub-systems, assemblies and components</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Define system architecture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliability allocation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update FMEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FTA and/or RBD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RAM analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create overview of reliability predictions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compare predictions with desired reliability and requirements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System architecture acceptable?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Document reliability results etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phase 3</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 27: Reliability methodology phase 2](image-url)

Murthy et al. (2008) describes phase 2 as the phase where the system architecture is defined. This includes a break-down of the system in order to describe the sub-systems in more detail. What is not clarified is the detailed design of how the components are linked together and other specific details, this will be done during phase 3. Based on the requirements and specifications set in the first phase, it is now desirable to predict the overall product reliability. The hope is to find an architecture whose predicted reliability matches the desired reliability from phase 1.

To start the system break-down, the results from the previous phase are used. The concept will include information about how a function can be carried out and what the system must be able to do. Simultaneously with the system break-down, it is possible to allocate the reliability. The desired reliability is usually given as an overall requirement. To obtain this reliability, it is necessary for all the sub-systems and components to have a desired reliability as well. A reliability allocation means...
that a desired reliability is assigned to each part, depending on what is thought feasible and how this fulfils the overall reliability.

As the system is better described through sub-systems and components, it can be useful to update the FMEA. If no FMEA has been performed, this is the time to start one. As soon as the sub-systems and their functions have been defined, one could start questioning their possible failures, which are more specific than those of the system as a whole. The information could then be implemented in an FMEA and studied further. As far as possible, the FMEA should be developed into an FMECA. With criticality included, it can become a very useful input to a RAM analysis.

Phase 2 is the phase where the reliability truly can be built into the product (Yang 2007). As the product architecture comes together, it is time to develop RBDs and FTAs. These methods may point out the weak links in the system structure. When the components start falling into place, more information should be retrieved on failure rates and these methods can then provide the engineers with the overall system failure rates. If they are performed together with a RAM analysis, they may even lead to a prediction of the overall availability. The outcome of the analyses should be used in an overview of all the predictions of interest to the reliability.

The predicted overall reliability and availability should be compared with the requirements and used to decide whether phase 3 may commence. When a system architecture is chosen, it must be proved acceptable. If it is not suitable for the concept, a new evaluation of the system break-down must be performed.

Useful tools both in phase 2 and phase 3 are computer-aided engineering methods. These can show the different options for system architectures and the placement of components. Simulations may be made on how the system reacts to stresses and failure modes can be evaluated. How far one can go in phase 2 depends on which level one studies the system at and the computer program’s demands. The best options for simulations will be found in phase 3 when the detailed design takes place. A good choice if such tools are used is to start preparing the simulations in phase 2 and complete them in phase 3. Simulations for reliability purposes are mainly connected with RAM analyses, but may also be used to study the development of fault propagation through a system. The latter is of great interest to safety where barriers must be considered. No computer tool is able to include all aspects concerning a system and one must therefore be aware of the limitations not to be misled into trusting the accuracy and completeness of the software models (O’Connor 2002).

**Summary**

During this phase the following activities should be performed:

- Reliability allocation to all sub-systems and known components.
- Identification of hazards connected with the sub-systems and functions through an updated FMEA.
- Preparation FTA and RBD which can be used with a RAM analysis or alone.
- Prediction of an overall reliability and comparison with desired reliability.
Phase 3

Phase 3 is where the very detailed design is made and the final design is frozen before the physical development commences in phase 4. The main task of a reliability engineer in this phase is to ensure that the reliability predictions from phase 2 are made more accurate as the component specifications are fixed. This is the last phase in which it is possible to make alterations without a direct intervention into the physical realisation of the product.

Based on the architecture established in phase 2, a functional analysis of the system should be done. This will help assigning specific functions to each component, assembly and sub-system. Although some similar work might have been done in phase 2, this is the absolute definition of how the main function of the system is provided. Concurrently with the functional analysis, decomposition for reliability should be performed. The latter would be a continuation of the allocation from phase 2, but based more specifically on the functions being fixed.

As the design is about to be frozen, it is useful to perform an extensive HAZOP study. The design is now sufficiently detailed for the questioning mechanisms of the HAZOP to produce meaningful answers (IEC 61882 2001). The HAZOP can also be used as new input to methods which are already
used in the project. An FMECA should be completed with more details about the failures which may occur in a component. The FTA or RBD made in phase 2 should be completed with more specific failure rates and possible new connections of the functions. Where it is possible, criticality estimations performed as part of the RAM analysis in phase 2 should be updated. Through criticality classification of different components and sub-systems, planning for future maintenance and testing can be commenced. This will increase the possibility of maintaining the reliability and availability of the product while it is in use.

At the end of phase 3, it is important that all requirements are met with. The design can only be frozen when it is acceptable according to the specifications from phase 1. Upon entering phase 4, there should be no doubt that the product predicted reliability is the best it can be. Only issues connected to production, transport, installation and wear are now controlled for the reliability not to be altered. To omit such alterations, the problems evaluated for transport and installation ought to have been studied along with other hazards. Any difficulties with production may be tackled when the manufacturing is planned.

**Summary**

In phase 3 it is important to follow up the reliability requirements and specifications, as well as predictions made in previous phases. The main steps to take are:

- To follow the detailed design in settling the specifications which give the best reliability.
- To perform a HAZOP based on the new details and specifications.
- To update any reliability tools used in phase 2 based on new information.
- To study the criticality of each component and consider these for future maintenance actions and testing.
According to figure 7, we reach stage II, development, when phase 4 begins (Murthy et al., 2008). This stage lasts through phases 4 and 5 where production planning, testing and prototype development take place. Phase 4 suits both custom-built and standard products, although custom-built products tend to be the prototype whereas the prototype stays a prototype for the standard products.

All the specifications, requirements and design drawings will now be used to develop a plan for the production. Before this planning is done, a thought to whether some items may be procured or not should be given. If it is possible, a plan could be made for the enquiry, receipt and testing of the items. The testing might only be necessary where the subcontractors cannot provide acceptable information themselves. The reason for the testing is to see whether the procured items match the predicted reliability (Murthy et al. 2008). If they do not match, more research must be done in order to develop suitable components.

For new technology, plans must be made for the development. The planning of the manufacturing should not only include when and where an operation takes place, but also which parameters it must stay within. A reliability engineer may not have much knowledge of how the manufacturing process is best performed, but can look into previous problems occurring in this phase. The information retrieved should be used to see where the planners must take the operations under extra strict observation. Useful inputs to such plans are FMEA, SWIFTs and HAZIDs. As humans will be involved in the development process, human factors potentially affecting the process negatively should also be analysed.
When the production plan has been made, a plan for testing of materials and prototypes should be prepared. The reason for preparing the production plan before this test plan, is that the production plan will include information about the stresses and temperatures the materials will be subjected to. Among the factors contributing to unreliability discussed in chapter 7, are the misinterpretation and wrong use of tests. An important question to ask when failures occur in tests is “Will they occur in use?” To answer this it is necessary to investigate the actual physical or chemical cause of failure (O’Connor 2002). A test can easily be misleading if it is performed on the wrong grounds. By this stage it is evident that the product will be able to perform its intended function, the question now is what may stop it from doing that. A test should therefore not be performed to demonstrate the successful achievement, but the failure causes.

While the tests are planned and executed, the reliability engineer must prepare for reception of the results and how they are to be analysed. As the development should not take more time than intended, it is necessary that the analysis results are ready as fast as feasible. If possible, the analyst should give input to which tests are needed, for example accelerated life tests and reliability growth. The tests must be prepared with the component, sub-system or system in mind. Whether the reason for the test is to discover new failures or evaluate failure rates, it must be accordingly.

While the prototype is produced, there is little other for the reliability engineer to do than to follow up on any deviations in the production machinery. Such deviations should be analysed to see how they affect the product, but could also be used in the preparation of factory acceptance tests (FAT) and customer tests. A full-scale test where the system is evaluated to see if it functions as planned. FATs are used in several industries when the systems are ready for use. The tests can lead to new alterations if necessary, but the hope is that it only confirms that a system is ready for operation. Full-scale testing can be performed together with the client and should therefore be placed in phase 5, straight before handover.

Even with many tests performed, the true value of a life parameter will stay unknown. We cannot say when a failure will occur, but we may be able to find the distribution of an expected value (O’Connor 2002).

**Summary**

Among the steps to take for reliability in this phase are:

- Include reliability in the production planning.
- Compare the reliability performance of existing components with the predicted reliability from phases 2 and 3.
- Prepare for tests which demonstrate possible failures.
- Study the outcome of the tests and see if a part of the production must be repeated.
## Phase 5

<table>
<thead>
<tr>
<th>Project tasks</th>
<th>Project reliability tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAT</td>
<td>Analysis of results</td>
</tr>
<tr>
<td></td>
<td>Estimate overall reliability</td>
</tr>
<tr>
<td>Suggest alterations where reliability is unacceptable</td>
<td>For larger market/series production</td>
</tr>
<tr>
<td>Alterations</td>
<td>For dedicated client/custom built products</td>
</tr>
<tr>
<td></td>
<td>Prepare for customer testing</td>
</tr>
<tr>
<td>Release to testing customers</td>
<td>Prepare for customer testing</td>
</tr>
<tr>
<td>Gather customer test reports</td>
<td>Prepare for hand-over</td>
</tr>
<tr>
<td>Analyse reports</td>
<td>Hand-over</td>
</tr>
<tr>
<td>Suggest alterations where results are unacceptable</td>
<td>Analyse test results</td>
</tr>
<tr>
<td>Prepare for series production</td>
<td>Prepare phases 6, 7 and 8.</td>
</tr>
</tbody>
</table>

### Figure 30: Reliability methodology phase 5

The progression to a failed state is time-variant (O’Connor 2002). The main objective of phase 5 is to obtain information on field performance through operational testing (Murthy et al. 2008). Testing in the field will last longer than accelerated tests and give answers as to how the product will be used and how it operates under different conditions. The progression to failure and the failures will hence be more realistic.

Before the prototypes are handed over to a customer or a client, the FAT must be performed. This will check that the system functions as intended, in an environment similar to the actual operational environment. The results of such tests can be used to suggest alterations if necessary and for the estimation of an overall inherent reliability. As the latter might be hard, it could be considered through an updated FMEA or RAM analysis.
Phase 5 is split into two categories after the FAT; larger market/series production and dedicated client/custom-built products. If the system is handed over after the FAT, little more than preparing a FRACAS and all the reliability documents is necessary for the reliability engineer. The next phase is then number 7. For products intended produced on a larger scale, the customer testing will commence after the FAT. As suggested in chapter 7, there may be some issues with the tester’s understanding of what is to be reported and how it should be done. It is thus critical that the reliability engineer prepares easily understood documents containing this information.

The next step is to gather and analyse the reports. Any specific test results which are not positive should lead to alterations, or in the worst case that the project is terminated. Alterations which are feasible can be performed with the mass production in phase 6. Information from the analysis of the test reports can be used to update FMEAs, FTAs etc. for later use in other projects.

The main objectives for the reliability engineer in this phase are (Murthy et al. 2008):

- Verification of the reliability studies conducted during the project.
- Providing appropriate data for justifying operational procedures and policies
- Modifications with respect to reliability and maintainability.
- Providing appropriate data to be utilised in subsequent phases.

As phase 5 ends the reliability engineer should prepare for the following phases where the product is in operation and relying on its actual reliability and ability to perform. When the product is handed over to a customer there is little left for the manufacturer except repairs, warranty-claims and follow-up. The reliability analyst should now study the actual performance of the product. If preparations for this are made, it might be easier both to obtain the necessary information, and to analyse and use it for future projects.

**Summary**

In this phase the main reliability activities are:

- Follow-up of FAT and customer tests.
- If possible update existing reliability information.
- Plan alterations if found necessary after operational tests.
- Prepare for the following phases.
**Phase 6**

The last three phases in the model belong in stage III, which is post-development. Phase 6 is concerned with the production as the product is ready to be sent out on the market. For custom-built products of which there is only one of a kind, this phase is of little or no interest. Some parts concerning the production of components and the general production process are of interest, and should be implemented in phase 4. Custom-built products which there are more than one of, for example trains and ships, can be considered to go through this phase.

The main concerns discussed for this phase in chapter 7, are the deviations due to variations in the production process. Some human handling will also occur, mostly due to operations which cannot be performed by machines. Human handling here includes both mechanical operations and transportation.

In general the engineers who are not directly involved in the production may have little to do in this phase. The main concern of a reliability engineer in this phase would be to ensure that the items are within the acceptable limits for conforming items (Murthy et al. 2008). The production personnel can check the items for conformity, leaving the reliability and design engineers to decide the limits of acceptability. Any testing of the produced items will depend on what the items are tested for and how strict the reliability requirements are. If the product requires very high reliability or is very expensive to produce and repair, 100% testing is desirable.

The output of tests in this phase can be useful for reliability and design engineers in later projects. Any information acquired about the production process may be used to decide in which way a product should be produced. It can also be employed to decide how strict the testing must be to retain the desired design specifications. Finally, the information about the production process can say something...
about the expected costs of the erroneous items produced. A useful tool would be root cause analysis studying the reasons for any problems encountered during the production. Root cause analysis can be further studied in (NASA (E) 2010).

As the products are prepared for transport and release, the reliability engineer should perform analyses of the hazards which may affect the product. This is a very important part of the product life cycle, due to the possibility of destruction of very sensitive items. Even though the transport only includes plastic outdoor chairs, the possibility that something might break is present. Given that the transport will depend on the road, as well as how the product is tightened in a vehicle, the main reliability tools available are SWIFT, HAZID and HAZOP. These can cover a large number of possible hazards, while not being too specific about the functions that are damaged. Any problems should be resolved through suggestions of how they can be prevented.

**Summary**

In phase 6 the following could be considered reliability activities:

- Prepare for testing of produced items.
- Gather and analyse test results. Perform a root cause analysis.
- Report the problems and store information for later use.
- Study the hazards of transportation and suggest preventive measures.
### Phases 7 and 8

Phases 7 and 8 are both dependent on the customers for information for reliability purposes. Only when the manufacturer is the operator of the product, can all existing information about the actual product reliability and performance be gathered. Phase 7 is placed on level II which is the product level. This means that it is the reliability performance of the product in the field that is studied.

When the product is handed over from the manufacturer, nothing but the actual reliability is of interest. The regular consumer will not be impressed by the predicted reliability, but by what the product gives in return for the money spent. A good design, where reliability was taken into account during development, will have considered the possibility of various operational environments (Murthy et al. 2008). When failures occur, customers can choose to use the product warranty and ask for repair or a refund. If the product is custom-built, the reporting and repair depends on the contract between the manufacturer and the client. It is the choice of complaining about the product which will give information to the manufacturer on the performance of the product. Without such information it would be nearly impossible for a product to be analysed for actual reliability.

For both standard and custom-built products the information retrieved about failures in the field should be analysed for a root cause. This is where the FRACAS system is of great use. Based on the root cause analysis and the general information, the reliability engineer should try to estimate the actual performance and reliability of the product. Most of the information and feed-back will be negative and it is therefore hard to see whether the actual reliability truly is a good estimate. However, for the sake of future projects, it is useful to have some thought on the product performance. If positive data are wanted, questionnaires might be the easiest way to obtain them. As it is unlikely that all the information about a product or system in its operational life can be retrieved, the actual reliability will be shown as a distribution around the actual value.

---

**Figure 32: Reliability methodology phase 7**

<table>
<thead>
<tr>
<th>Project tasks</th>
<th>Project reliability tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warranties and repairs</td>
<td>Gathering of information</td>
</tr>
<tr>
<td>Customer/Client follow-up</td>
<td>Reception of FRACAS reports</td>
</tr>
<tr>
<td></td>
<td>Root Cause analysis of new failures</td>
</tr>
<tr>
<td></td>
<td>Analysis of performance and estimation of actual reliability</td>
</tr>
<tr>
<td></td>
<td>Document reliability results etc.</td>
</tr>
</tbody>
</table>

---
Summary
The tasks to be performed for reliability purposes in this phase are:

- Gathering of field performance, failures, complaints, positive feedback etc.
- Root cause analysis of failures and operational problems.
- Analysis of the actual reliability.
- Storing of information for later use.

Phase 8

<table>
<thead>
<tr>
<th>Project tasks</th>
<th>Project reliability tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales follow-up</td>
<td>Root Cause analysis of failures discovered from sales follow-up</td>
</tr>
<tr>
<td>Analysis of earnings</td>
<td>Analysis of overall performance</td>
</tr>
<tr>
<td>End project</td>
<td>Documentation and lessons learned from entire project</td>
</tr>
</tbody>
</table>

**Figure 33: Reliability methodology phase 8**

The questions that should be answered in this phase are the ones that truly show the market success of the product. This phase belongs on the business level and is from a reliability perspective concerned with how the product reliability affected the business objectives (Murthy et al. 2008). These objectives were defined as early as phase 1 where they described the desired performance of the product.

Phase 7 and 8 are very similar as the data must be collected from outside the manufacturer, analysed for root causes and reported for use in new processes, preferably in phase 1. The main difference is that the sale, market share and revenue must be included as well (Murthy et al. 2008). The popularity of the product will not only depend on the amount of consumers that buy it, but how the product corresponded to their wants and desires. For reliability reasons it is of interest to see whether the actual reliability of the product affected the sales, complaints and market shares. The manner in which the overall success of the product was affected may tell the manufacturer what reliability demands the customers have. For the custom-built products the main objective of this phase is to decide which improvements can be made for the execution of future jobs (Murthy et al. 2008).

For the project as a whole, it is important that this phase is used to gather information from the shops which sold the products, and the manufacturer’s sales department. This might not be a part of phase 7 and is therefore useful now. In some cases a system returns more than what it was worth, other times less. Often information of this type is more likely to be given to a vendor than the manufacturer. An analysis of the overall performance of the product and how it was affected by the reliability must be based on all available information, not just the failures.
For both standard and custom-built products, phase 8 closes when the product’s market performance has been analysed and nothing more can be gained for future developments. In all phases the documentation of the reliability is demanded. In this final phase, this should be used for the review of the project and then stored for later use. Lessons learned from the project can stop history from repeating itself and are thus highly important to avoid unnecessary difficulties in future project and create feasible reliability programmes.

Summary
The reliability tasks in this phase are:

- Gather data on the product performance not found in phase 7.
- Perform a root cause analysis of new data.
- Analyse the new data together with the output from phase 7.
- Separate the information which may be useful in the future and store it.
- Close the reliability part of the life cycle.

8.2. Comparisons and discussion
All development projects are special and whether it prepares a standard or custom-built product, the best choice of reliability tools and methods will change from time to time. Any choice should be based on which findings the reliability engineer needs and the existing knowledge about the product. Even when the outcome only intends for a new generation to be made, there is a need for fresh input. Just as the variation in the manufacturing process never will produce two exact matches, no phase will ever be repeated in the exact same way.

To develop new concepts and designs, a large amount of creativity is needed. Forcing creative work into frames with too many rules is not effective. The creative parts of the product life cycle are therefore best suited to be controlled in such a manner that the outcome is suitable for the project and kept within a certain time limit. As the creative parts of a product life cycle are mostly taking place at the same time as the desired and predicted reliabilities are estimated, there will be a conflict. A reliability programme demands discipline, control and the use of rules and guidelines (O’Connor 2002). The output of the creative processes must therefore be exact enough for use. The synergy of the designer and a reliability engineer demands time for that feedback between the two parties. This feedback will help the decision of whether the creative process is going in the right direction or not. To relax the activities connected with reliability estimations can lead to reduced reliability and it is therefore better to have a strict design process.

A reliability programme must correlate with the design and development programme and concurrent engineering is the only option. In this chapter the reliability activities suitable for each phase of the product life cycle have been discussed. They are considered an integrated part of the development programme and, as shown in the diagrams, the output from reliability methods should be used as input to the decision points where a phase is concluded. When the reliability tasks and responsibilities are given as mandatory in the procedure, the reliability will become a part of the design.

The main differences between the general methodology and the one for Aker Solutions, are dependent on the tasks performed in the phases. As the technology qualification does not follow the same phases as used for the general methodology, there are bound to be some methods which appear in different places. What is interesting is that the methodologies have more similarities than differences. This is assumed to be the effect of the general methodology being prepared for all types of products. As the
products pass through the same phases and are subject to many of the same project tasks, there is little reason while the general methodology would not be similar to the specified one.

An important aspect of these methodologies is that they are prepared for entirely new technology and therefore includes as many tasks as thought necessary. The case study will look into whether it is possible to adjust them for systems where the technology is known and the project risk is somewhat smaller than for new technology. It will also show how a methodology can become the basis of a stricter programme with limits, project risk categorisation and a specific goal.
9. Case study – ERMP

The objective of the case study was to prepare an ERMP (Equipment Reliability Management Programme) for the EPC phase of the Midgard Subsea Compression System (SCS) development. This should be based on the methodology suggested in chapter 8, and adapted for the Aker Solutions methodology in appendix C. One criterion to the ERMP was a demand that it should be in accordance with the ISO 20815 standard. It was also asked that the EPC phase followed the Project Execution Model (PEM appendix D) used for development projects in Aker Solutions. The ERMP report can be found in appendix E. A system description of the SCS is given in appendix A.

Among the differences from the general methodology and the one suggested for Aker Solutions are:

- The PEM does not follow the eight phases of Murthy et al. (2008)
- The technology qualification is not used as a basis
- The technology is not entirely new
- The system studied is specific for the ERMP

Although the EPC phase does not directly correspond with the eight phases, many of the steps follow in the same order as in phases 2 to 5. It is therefore considered that the tasks suggested for these phases in the methodology can be applicable in the EPC phase. The main reason for not using the technology qualification in the case study is connected with the newness of the technology. A similar system has already been designed and is currently in development. The Midgard SCS is thus not entirely new technology.

The ERMP is written for the Midgard SCS alone and thus based on work done in previous phases of the project. Some reliability activities have already been performed, however, as the design develops and the current technology is further studied, there may be alterations on the Midgard SCS and new reliability estimates will be needed. This is the main reason for the implementation of new reliability allocations and analyses in the EPC phase. The previous analyses are then updated and more thorough reliability studies of the sub-systems and assemblies performed.

Among the main constraints for the ERMP are time, other project activities and resources. The time limit for the EPC phase is four years and it should therefore not be problematic to perform the reliability activities. Nevertheless, time may be a constraint in connection with the other project activities and any delay in these will delay the information flow to the reliability activities. The reliability programme must be performed concurrently with the other development tasks. Finally, the resources necessary for a reliability activity will depend on its inputs and the mechanisms needed to perform them. Some activities may only need one person, while others give better results with a team, for instance HAZID and HAZOP.

9.1. ISO 20815, the methodology and the ERMP

Technical safety and reliability aspects are often not considered until a verification or testing point for equipment (ISO 20815 2008). This will usually be at a late stage of the development process, when the design is near to fixed or after manufacturing has started.
9.1.1. ISO 20815

Appendix A in ISO 20815 (2008) gives the outline for a Product Assurance Programme which has been used in the development of the ERMP. It lists the following as parts in the programme:

- Terms of reference
- Production-Assurance philosophy and performance objectives
- Project risk categorisation
- Organisation and responsibilities
- Activity schedule

In order to implement a reliability or product assurance programme in a project, a scope, philosophy, objective and justification must be given for it. A risk categorisation will help determine the activities chosen and to what extent a reliability programme is necessary. If the project is categorised as low risk, with well known technology, there is little reason to have a very costly reliability program. The organisation and responsibilities describe who will perform the reliability activities and the responsible for follow-up and acceptance. Finally, the activity schedule includes the reliability programme and a methods description.

The risk categorisation for projects is done according to three levels:

- Low
- Medium
- High

Table 3 shows how the project risk categorisation is suggested defined by ISO 20815 (2008):

<table>
<thead>
<tr>
<th>Technology</th>
<th>Operating envelope</th>
<th>Technical system scale and complexity</th>
<th>Organisational scale and complexity</th>
<th>Risk class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mature technology</td>
<td>Typical operating conditions</td>
<td>Small scale, low complexity, minimal change of system configuration</td>
<td>Small and consistent organisation, low complexity</td>
<td>Low</td>
<td>Low-budget, low-risk project using field-proven equipment in the same configuration and with the same team under operating condition similar to previous projects.</td>
</tr>
<tr>
<td>Mature technology</td>
<td>Typical operating conditions</td>
<td>Moderate scale and complexity</td>
<td>Small to medium organisation, moderate complexity</td>
<td>Low or medium</td>
<td>Low- to moderate-risk project using field-proven equipment in a operating envelope similar to previous projects but with some system and organisational complexity.</td>
</tr>
<tr>
<td>Novel or non-mature technology for a new or extended operating environment</td>
<td>New, extended or aggressive operating environment</td>
<td>Large scale, high complexity</td>
<td>Large organisation, high complexity</td>
<td>Medium or high</td>
<td>Moderate- to high-risk project using either novel or non-mature equipment or with new or extended operating conditions. Project involves large, complex systems and management organisations.</td>
</tr>
</tbody>
</table>
In the ERMP, it is considered acceptable to rate the risk between these levels as “low to medium” and “medium to high”. This has been done in order to avoid misunderstandings of how a level should be interpreted. “Low to medium” implies that although the risk is low, it is not to be ignored. “Medium to high” signifies that even though the risk is high, everything is not unknown and new.

9.1.2. The methodologies

The tasks in the ERMP are based on the risk categorisation and chosen from the general and the Aker Solutions methodology. As the EPC phase is not the first phase in the Midgard SCS project, several hazards have already been identified and reliability estimates calculated. These can now be used when the design is specified further. Even with previous information, changes in the design and new operational requirements will lead to a need for new hazard identification processes. In the ERMP it is considered that such processes will be performed in several formats throughout the EPC phase until the design is frozen. Some of the methods are suggested as updates while others may return for new purposes.

The suggested methodology in relation to chapter 8 is in general more thorough than the ERMP for the EPC phase activities. There are several reasons for this, among them the specific system and the other concurrent activities. It is also important to note that it is easier to suggest a large amount of activities than to perform them all. In a different project, a larger number of the methods, or different methods from the methodology may be chosen for a reliability programme.

In appendix C it has been suggested that the FMEA in particular should be updated as often as possible, even after the design is frozen. For the Midgard SCS project, the FMEA is last updated at before the system design basis is completed and the major interfaces frozen. This is logic as there is little possibility of altering the design any more, but as there is a possibility of new failure modes being revealed in testing it might have been better to keep an opening for updates. The FMEA is probably not used much in the next project phases, but it can be useful in future projects.

9.1.3. Combining ISO 20815 and the Aker Solutions methodology

The standard and the methodology do not go against each other, but rather work as supplements. To choose the correct methods and implement them at the right place is not evident from the combination. Although the methodology states where a method should be placed according to a project activity, there is nothing stating which methods are to be preferred. As ISO 20815 does not give much input on this point, the reliability engineer is left to figure it out according to the activities in the specific project. By comparing them with the methodology, this should be achievable. However, it might have been desirable to have an indication of which tasks are imperative for the different risk categorization levels.

What might be done is to prepare a document in relation to either the methodology or ISO 20815, stating which methods are the most basic and which are only needed for high risk projects. This would be based on the assumption that a low risk project only needs a few methods performed, while a high risk project needs as many as possible. Such an assumption is not necessarily the best, but it does follow the need a reliability engineer has for new information in projects. A low risk project, as shown in table 2, already has an extensive amount of input information. It is therefore not in need of many new analyses before the lacking information is obtained. For a high risk project, the opposite is the case. Although such information could be given with ISO 20815 and the Aker Solutions methodology, it would still be up to the reliability engineer to know which outputs, and thus which methods, he or she needs.
9.2. Discussion

Although the methodology suggested in chapter 8 is not perfectly applied to the ERMP in the case study, little suggests that the methodology is wrong. The ERMP is written for a specific system and actual project, while the methodology is theoretical. The Subsea Power and Process department has the PEM and the requirements of the client to follow. In addition, the existing manner in which reliability activities are performed is proven through other projects. Reality is rarely the same as theory, but it can confirm its relevance.

This ERMP rather confirms than demands an alteration in the methodology. What may be done is to remove some of the repetition of methods and testing activities, but this might again suit a different project perfectly. As long as the methodology is not intended to be applied directly, but as a basis for the creation of project specific reliability programmes, it can be accepted as it is. In such a case it is necessary that it is more thorough than required as the projects will ask for different inputs and amounts of reliability activities. If it is not thorough enough, demanding projects can be negatively affected through lacking methods having been suggested in advance.

What were not defined in this ERMP were the standards which are to be followed specifically for the project. However, as this is for one phase alone, the overall documents concerning the project can include this and it might therefore be considered unnecessary. If the ERMP was meant for the entire project, the standards should maybe have been further specified and implemented. To include the standards would not be likely to alter how the ERMP was used, but it could have an affect on the engineers while they are searching for the best manner in which the chosen methods are performed. Anything which increases the awareness of why reliability is important is positive for the product or system developed.
10. Design for reliability website

If a manufacturer has a difficult time understanding why reliability should be a part of the design process or how it should be implemented, a website can be of use. We often use the internet to obtain new information and it has become one of the main sources when we wish to study a new subject.

A website has been created to study how a tool for a reliability engineer can be developed. It could be used either to explain reliability to a business executive, or to obtain tips and useful information for daily work. The website is based on the findings described in this report. The first page is directed at those who are not familiar with design for reliability or why it is a useful tool. The text links the reader on to a basic page which describes the product life cycle and a page describing different methods for reliability.

![Figure 34: Front page of website for Design for reliability (http://folk.ntnu.no/ingribe)](http://folk.ntnu.no/ingribe)
The page describing the product life cycle is based on the model suggested by Murthy et al. (2008). From the table describing the process, similar to that of figure 3, links to each phase may be found. The phases all have one page each, including a description and the belonging methodology.

The stages and levels are further described here, while the phases are described separately. Each phase are described in general terms and shown together with a methodology for design for reliability specific for the phase. The methodology is a suggestion for the implementation of reliability methods according to the task in the development project.

Figure 35: Life cycle (http://folk.ntnu.no/ingribe/productlifecycle.jsp)
Phase 7 begins with the product being released to the market. It is now interesting to see how it performs in the field. For custom made products, the use of FRACAS may now pay off. The returned information form FRACAS can be implemented together with other information obtained about the product performance, availability and failures. For products produced in series, most of the information will be in the customer complaints, repair and occasional failure. For a reliability engineer it could be interesting to see what causes the failures and how they occur. It would also be interesting to see how often a failure occurs and which failure types are the most frequent. This information could then be used to analyse the actual reliability of the product. After having compared the actual and desired reliability, the results ought to be stored for later projects as “lessons learned”.

Figure 36: Phase 7 as opened from figure 35.

All the relevant methods suggested for a phase are linked to the description of the methods for reliability. As the RAM analysis consists of more than one method, this has been given its own page. For those who wish to skip some pages, a menu is found on the top of each webpage.

10.1 Further suggestions

Currently the website is a very basic description of how design for reliability may be used in the different phases. It suggests a methodology and it is up to the users to decide how this can be
implemented for their processes. Someone who is sceptic to reliability activities being mixed with the design process can study the purpose and how it should be done. Although this website is at an early stage, it can be developed into a better tool through the following suggestions:

- The methodology figures can be given links to the methods within themselves.
- Examples of how the methods are used could be included.
- A project could be used as an example in each of the phases.
- A form could be developed where the phase and design tasks are filled in, returning a reliability programme suggestion.

Many other suggestions could be given as well, but these are thought the most helpful to the users. Links within the figures can be easier to use, while examples of the utilisation of the methods and phases will improve the understanding. Especially the last point would be of interest if the page is to become an interactive tool. For someone who wishes to develop a reliability programme for their project, without much experience, this could be an easy solution. By plotting in the phase the programme is needed for and the planned project tasks, a corresponding set of reliability methods could be developed. This only requires a rather simple computer programme. If it is desirable to specify the project even more, a risk categorisation according to ISO 20815 can be implemented in the form as well. The main constraint of the tool would be the understanding of the user. A reliability programme suggested by the tool cannot be used without care. The user must therefore study the suggestion and choose whether the methods are suitable to the particular project or not.

The website is rather unspecific as all industries are meant to use it. For more specific use, a computer program could be developed. This would include the same information as the website, but could be more extensive in the explanations. The methods ought to be well explained, possibly with information on which standards they are described in. A possibility of uploading experience from previous projects should also be included. This information would provide the user with comments on how the method was performed and the results. As long as the information is used as input, not as an answer, this could work rather well.

An option for the company buying the program would be that their own specified methodology could be implemented. The reliability programmes returned by the tool would then be far more specific and possibly easier to use in the product development. Many further solutions could also be added, but this should depend on the interest of the potential buyers.
11. Concluding remarks

To perform reliability studies of an unfinished design can seem unreasonable for several reasons. It does cost money, demand extra resources and forces the designers to follow specific schedules which might limit their creativity. This can be said about every attempt to control the development process. Nevertheless, manufacturers do have to develop new products within time frames and according to performance demands. Reliability engineering is a case of being precautionary rather than “wise after the event”. It is at its best when the results are invisible and no failures occur. New products are introduced to the consumers all the time. In order to win a place in the market and keep the customers happy, the manufacturer must develop new products quickly without affecting the reliability negatively. Design for Reliability seems to be a good solution.

The first reliability methods were developed to study the possible failures in a system, but they were also responsible for making the design engineers more conscious about how they developed a new system. The reliability and safety became far more important than low costs and efficient production. Reliability analyses can provide the designers with hazardous scenarios met by the product in the future. This can either lead to new alterations or increased confidence in the existing design.

Chapter 7 is dedicated to factors contributing to unreliability. Although several more factors can be discussed, the selection in this chapter shows that there are reasons to wonder how good reliability it is possible to achieve. The vision is absolute reliability, where the systems never fail while in use. Absolute reliability cannot be called impossible, but it is impossible to know that it is absolute before the product reaches its end of life. We do not have the ability to foresee the future, but through the use of reliability methods, the product reliability can be increased. If the methods are used correctly, at the right time and with other overlapping methods, it might be possible to achieve absolute reliability without being conscious of it.

The goal of a manufacturer could be to reach the highest reliability possible, but this might not be the most beneficial in the long run. To perform many reliability methods will increase the costs of the product. This will again render the product expensive and possibly turn customers against investing in the competitors’ products. The reliability methodology includes a great amount of methods and so does the ERMP. It will be up to each manufacturer, after consultation with the reliability engineer, to consider the number of methods that shall be employed. Projects involving a custom-built product are likely to afford more reliability methods than projects for standard products. The clients of custom-built products are often more willing to pay for high reliability than a regular customer at a sports store. The optimal number of reliability methods is hard to find, but a diagram showing costs of failures and costs of reliability methods can be used. This is shown in figure 37.
Without any money spent on reliability methods, it is likely that the costs of failures will be high. With many reliability methods, the failures will be fewer. To set the costs of failures against those of reliability will, as shown in the diagram, give an optimum. This is a useful tool when the requirements to the reliability are not set in advance. Thus, standard products in particular can benefit from this diagram.

### 11.1 Methodology and use

The reliability methodology presented in this thesis is based on the assumption that reliability activities throughout the product life cycle will give increased reliability. It is further assumed that activities can overlap each other and together give a good overview of the product reliability. The intention is for the methodology to be a tool for the development of reliability programmes. Here the eight phases are defined through their main project tasks, but as shown with the Aker Solutions reliability methodology this can be specified according to organisation.

Standards such as ISO 20815 prove the possibility of developing reliability programmes based on the project risk. If this standard is used together with the methodology, as in the case study, it will take less time to define why the programme is necessary and which methods are to be used. If the methodology is used as a tool that any organisation could alter to suit its project execution model, it could easily be adapted to all new projects. The condition which then has to be fulfilled is that the organisation’s methodology is suitable for very high risk projects with entirely new technology. It is easier to leave out a reliability activity than including one more. This is the reason why Aker Solutions’ technical qualification was used for the development of the Aker Solutions methodology.

ISO 20815 and other standards for reliability are great input to organisations wishing to use Design for Reliability in their projects. Seeing how useful it was to have the methodology ready before the case study, it could be suggested that a standardised methodology should be developed as well. This methodology would have to be open for specification according to industry and organisation. Its objective must be to ensure that reliability methods are shown according to which phase they suit and how they ought to follow each other. This would increase the possibility of a correct implementation of the methods and hence increase the confidence in their outputs.

Chapter 10 described a website developed based on this thesis. It shows that there are possible ways in which Design for Reliability and a general methodology can be explained without too much cost. The chapter also suggests how a website can be turned into a tool used by those learning how to implement reliability in their design. As reliability becomes a more interesting topic to manufacturers in all industries, such a tool is of high interest.

### 11.2 Recommendations for further work

The time constraints of the project are such that the methodology has not been studied as intensively as could be desired. One suggestion is that it could be applied to several projects in different industries and with varying risk levels. In comparing how the methodology is applied and followed up by the different organisations, the adequacy of the methodology can be analysed. Alterations might be suggested for further development.

If it was thought reasonable to prepare a reliability methodology for a standard, either alone or as an addition to another standard, this should be studied. Although it is quite hard to make a tool like this suit every industry and organisation, it is not impossible. An enquiry into what the relevant organisations needs must be done. This enquiry should include questions about the project tasks...
performed during the product life cycle, the reliability demands the organisation must answer to and which reliability methods they already employ. In using this as a basis, a methodology could be developed.

Design for Reliability has become a household concept with many manufacturers around the world, but there are still those who doubt its usefulness. It would be interesting to perform two projects starting from the same concept but with only one using Design for Reliability. The outcome of tests performed by “customers” can show if there is a difference. If the products are fixed to achieve the same reliability, it becomes evident which were the less costly. The success of such an experiment will depend on the designers’ awareness of reliability issues and the tests performed during manufacturing. It is possible that the outcomes are so different that a comparison will be difficult.

Comparative studies could also be done for reliability programmes. In this case it is reasonable to suggest that the same project is performed a set of times but with small alterations in the programmes. The alterations would be the methods chosen and the number of methods. This could possibly prove the use of extensive reliability programmes in high risk projects and thinner programmes in low risk projects. Also here there can be difficulties proving the effect if the projects turn out very different from one another.
12. References


   [http://www.ieee.org/portal/site/relsoc/menuitem.e3d19081e6eb2578fb2275875bac26c8/index.jsp?&pName=relsoc_level1&path=relsoc/Reliability_Engineering&file=index.xml&xsl=generic.xsl] [viewed 9/02/2010]


25. ISO (2010) *About ISO* [http://www.iso.org/iso/about.htm] [viewed 04/05/2010]


44. NORSOK Z-008 (2001) *Criticality analysis for maintenance purposes*. Oslo, Norwegian Technology Centre


46. NPD(A), (2001), Regulations relating to conduct of activities in the petroleum activities (The Activities Regulations), [Online]. Available from: [http://www.ptil.no/activities/category399.html](http://www.ptil.no/activities/category399.html)

47. NPD(B). (2001) *Regulations relating to design and outfitting of facilities etc. in the petroleum activities(The Facilities Regulations).* [Online]. Available from: [http://www.ptil.no/facilities/category400.html](http://www.ptil.no/facilities/category400.html)


   http://www.iq.harvard.edu/blog/sss/archives/2006/02/bayesian_vs_freu.shtml [viewed
   27/05/2010]


    Department of Production and Quality Engineering, NTNU, Norway.


63. Selah, J.H. and Marais, K. (2006) Highlights from the early (and pre-) history of reliability
    engineering. Reliability Engineering and System Safety. 91, 249-256


    in Engineering Design. London, Springer

    Prevention in the Process Industries, 6, 349-353.

    Illinois University [Class notes presented by ASSE students] Available from:
    www.ceet.niu.edu/depts/tech/asse/tech482/what_if_analysis.doc

    thesaurus.com/browse/unreliability


    System. SEMATECH [Online] Available from:

    www.weibull.com/AccelTestWeb/acceltestweb.htm


76. Confidential references
Appendices

There are 6 appendices to this report numbered from A to F. Except for the preliminary report the appendices are confidential and therefore left out of the main report. The appendices are meant to be read together with the main report and a description of how this should be done is given in chapter 1.3.

The appendices are the following:

A) System description of the Midgard Subsea Compression System
B) Project execution model for Technical Qualification in Aker Solutions
C) Aker Solutions methodology for reliability
D) Project Execution Model (PEM) for Aker Solutions
E) Equipment Reliability Management Programme (ERMP) for the Midgard SCS
F) Preliminary report