Well Safety

Risk Control in the Operational Phase of Offshore Wells

Doctoral Thesis

by

Kjell Corneliussen

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

Trondheim 2006

Synopsis

The essential function of an oil and gas producing well is to transport hydrocarbons from the reservoir to the processing equipment in a cost effective and safe manner.

The importance of well safety has been recognized and accepted for a long time, and significant improvements concerning both design and operating procedures have been made. In spite of these improvements, failures still occur and will probably continue to occur in the future. The industrial and technological development, the extended lifetime of wells, and recent regulations and standards imply that there is a need for a systematic approach towards well safety during the entire life cycle of a well.

For a well the main risk contributor is a blowout. The acceptable mean time between blowouts is very long compared with the lifetime of a well. In such situations Rasmussen (1994) states that the risk involved in operation has to be predicted analytically from the first beginning and the proper defenses have to be designed from this prediction. Use of predictive methods in the well risk assessment is not new. However, descriptions and guidelines on how to apply the analysis techniques in the well life cycle are fragmented.

The main objective of this thesis has been the development of procedures and methods for risk assessment of oil and gas wells. The work is limited to the well operational phase. The procedures and methods provide status of the well risk level during the life cycle from installation to abandonment of the well. The main focus is on the two main safety functions of the well:

a. To prevent uncontrolled leakage of well fluids from the well to the environment. This function is usually referred to as *well integrity* and is a *continuous* safety function that may fail at any instant of time.

b. To *shut in the well flow* in case of a dangerous incident on the downstream side of the x-mas tree. The shut-in function is an *on demand* function activated in a random critical situation.

In this context a systematic approach means to describe a procedure for risk assessment, with focus on quantitative/predictive analysis as a means to provide input to the assessment. The risk assessment is based on existing and new methods and knowledge gained during the PhD work. To arrive at such procedures and methods, it was necessary to:

1. Describe the state of the art related to analysis and control of the functions mentioned above.
2. Describe regulations, standards, and industry practice, giving requirements to well safety in the operational phase.
3. Identify commonly accepted analysis methods applied in risk assessment of wells, with focus on quantitative analysis techniques.
4. Identify input reliability data available for quantitative well safety analyses and discuss the quality of the data.
5. Assess the applicability of existing well safety analysis methods and, if necessary, suggest improvements.
6. Suggest improvement in application of reliability input data.
7. Develop a systematic approach for risk assessment of oil and gas wells in the operational phase. In this context a systematic approach means to assess well risk when a well component failure occurs in the operational phase. The basis for the risk assessment is the quantitative analysis techniques identified.

The use of risk assessment methods to assess well risk in the operational phase is not new. However, some of the steps in the risk assessment procedure are new. Also a set of well risk factors (WRF) for assessing well risk in the operational phase is new. More explicit the following contributions from the thesis are identified:

- A systematic approach for well risk assessment in the operational phase. A set of WRFs are identified that influence the total well risk. The procedure is aimed at risk assessment in the operational phase after a well component failure has occurred.
- A method for constructing barrier diagrams. A barrier diagram is a structured way of describing a well as a barrier system. In the thesis it is shown how to calculate failure probability directly from the barrier diagram. Alternatively, the barrier diagram construction rules allows for converting the barrier diagram to a fault tree.
- A framework for assessing well component failure causes, acceptable deviations in well component performance, and dependent failures.
- A method for calculating the safety unavailability of safety functions, and a method for calculating the safety unavailability for different configurations of surface controlled subsurface safety valves.

Preface

This thesis reports the work carried out during my PhD study at the Norwegian University of Science and Technology (NTNU), Department of Production and Quality Engineering. The research was initiated in 2000, and financed by a research scholarship from NTNU. The research was halted for a one year period in 2003 because of project work at my current employer ExproSoft AS.

The study builds on two parts. The first part constitutes of a series of courses with exams. The second part is the work reported in this thesis.

The main objective of this thesis has been the development of procedures and methods for risk assessment of oil and gas wells. The work is restricted to the well operational phase. The procedures and methods provide status of the well risk level during the life cycle from installation to abandonment of the well. The main focus is on the two main safety functions of the well:

a. To prevent uncontrolled leakage of well fluids from the well to the environment. This function is usually referred to as *well integrity* and is a *continuous* safety function that may fail at any instant of time.
b. To *shut in the well flow* in case of a dangerous incident on the downstream side of the x-mas tree. The well shut-in function is an *on demand* function activated in a random critical situation.

This PhD work belongs to the field of applied science, meaning research aiming directly at practical application. The thesis is build up by a main report and a series of papers. The main report addresses primarily personnel involved with risk control of offshore wells in the operational phase. The papers describe methods primarily for personnel performing quantitative reliability analysis.

An extensive list of definitions is included at the end of the main part of the thesis. The definitions are either discussed directly in the text or included as footnotes when the term occurs the first time.

Professor Marvin Rausand, Department of Production and Quality Engineering at NTNU, has been supervisor during the work. I am grateful for his valuable assistance and support, and also for his cooperation in writing Paper 5.

Research cannot be carried in isolation. It is not only a result of my own efforts but also affected by related research activities carried out by my colleagues. I want to thank former colleagues at SINTEF Industrial Management, Department of Safety and Reliability, and current colleagues at ExproSoft AS, for their collaboration and support during the PhD study. Especially, I want to thank Per Hokstad for the cooperation in writing paper Paper 2 and Geir-Ove Strand for the cooperation with the method described in chapter 6. Thanks also to Hilde Brandanger Haga, Eli Tenold and Gustav Rundgren from Norsk Hydro, and Kåre Kopren for valuable support and cooperation.

I also want to thank fellow PhD students for fruitful discussions of research challenges and comfort in common destiny. In particular, I would like to thank Snorre Sklet for the cooperation in writing Paper 3, and for the company when sharing office the first scholarship period.

At last I thank my wife and children for having patience with me.

Trondheim, March 2006.

Kjell Corneliussen

Table of content

1. Introduction

This chapter describes the background and motivation for the PhD project, along with the objectives and the limitations. The scientific approach adapted is discussed and the structure of the thesis is outlined.

1.1 Background and motivation

The essential function of an oil and gas producing well is to transport hydrocarbons from the reservoir to the processing equipment in a cost effective and safe manner.

The importance of well safety has been recognized and accepted for a long time, and significant improvements concerning both design and operating procedures have been made. In spite of these improvements, failures still occur and will most likely continue to occur in the future. The need for continued focus on well safety is exemplified by the gas blowout in 2005 on the Snorre tension leg platform operating on the Norwegian Continental Shelf (NCS). According to the Petroleum Safety Authority (PSA) in Norway the accident[1] could have resulted in a major accident with the loss of many lives (PSA, 2005). Two of the conclusions drawn from the investigation were:

- Deficient assessments of overall risk.
- Breach of the requirements to well barriers.

A well barrier is an envelope of one or several dependent barrier elements preventing fluids or gases from flowing unintentionally from the formation into another formation or to surface (NORSOK D-010). The well barriers are means to reduce

[1] *Accident* - An unintended event or sequence of events that causes death, injury, environmental or material damage (DEF-STD 00-56).

overall risk. How well barriers influence on well risk in the operational phase is focused on in this thesis.

Technology trends

The industry continues to develop new well designs for challenging reservoir conditions. In Norway, most of the profitable fields are in production. The industry now focuses on finding and developing the smaller/marginal fields in the southern part of the NCS. In search for new large and profitable fields, the industry moves north and into deeper water. This development results in production in more environmentally sensitive areas and in operations under more hostile weather conditions. A similar development is seen, e.g., in Russia where offshore fields in the Barents region are being planned.

To develop the marginal fields it is expected that the operators of offshore fields will be more directed towards subsea systems and investments in new development concepts and technologies. An example is subsea high integrity pressure protection systems (HIPPS), where the pipeline is not rated for the full pressure and a safety instrumented system (SIS) is installed on the seafloor to close the flow if high pressure above acceptable level occurs. The first subsea HIPPS on the NCS is the Kristin field. The field started production October 2005 (Statoil, 2005).

The trends mentioned above indicate that new technology applied in more challenging fields will require continued focus on well risk management[2] in the future.

Supply and demand

According to Hirsch, et al (2005) the oil production will soon peak and there may be a mismatch between the demand for and the supply of petroleum, and this situation will not be temporary. Peaking will create a severe liquid fuel problem for the transportation sector. Peaking will result in dramatically higher oil prices, which will cause economic hardship in the industrial countries, and even worse problems in the developing countries. The study concludes that the problem of peaking of world conventional oil production is unlike any yet faced by modern industrial society. With the expected

[2] *Risk Management* - Systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating and controlling risk (IEC 60300-3-9).

mismatch between demand and supply it is likely that there will be an increased pressure on safety.

Increased focus on well age and life extension

In Norway, the NORSOK D-010 standard describes well integrity requirements, where *well integrity* is "the application of technical, operational, and organizational solutions to reduce risk of uncontrolled release of formation fluids throughout the life cycle of the well." Well integrity has always been focused on in the design of new wells, but well integrity in the operational phase is now of increasing concern. Because of high oil prices, new technology for increased recovery, and government incentives, it is now possible and profitable to extend production beyond the assumed design life[3]. However, life extension may result in more frequent critical failures involving leakages to the environment. The outcome of such leaks can be catastrophic. According to Burton (2005) 10% of the wells on the United Kingdom Continental Shelf (UKCS) were shut-in due to well integrity problems during the last five years. The article refers to a study based on interviews with 17 UKCS operators. Approximately 83% of these operators experienced well integrity problems. Other topics highlighted in Burton (2005) are:

- Little is known about the implications of operating wells beyond their design lives, and UK operators found growing concern about the safety, environmental, and economic standards associated with well structural integrity.
- More subsea wells will have implications on the identification and remediation of integrity problems.
- 32% of UKCS completed or suspended wells are more than 20 years old, with some over 38 years old.
- Well lives are being extended, older assets are being sold to smaller operators, and the number of subsea wells is increasing.
- Erosion, corrosion, and fatigue problems associated with prolonged field life are thought to have led to more frequent well integrity problems.

[3] *Design life* - Planned usage time for the total system (NORSOK O-CR-001).

- Some operators believe that well functionality can be maintained, regardless of age, through inspection, monitoring, and maintenance. Nevertheless, 87% of the operators questioned believe that the incidence of structural integrity problems is increasing and will continue to do so.

It is likely that the NCS situation is comparable to the UKCS situation because there are many similarities in field age, type of installations, operating practice, etc. Well integrity is also a major concern in the United States Gulf of Mexico (US GoM). A study carried out on behalf of the Mineral Management Services (MMS) concludes that more than 8000 wells on the US GoM Outer Continental Shelf experience well completion leaks (Bourgoyne et al 2000).

The increased emphasis on well integrity in the operational phase is reflected in recent regulations and standards. In Norway, NORSOK D-010 describes requirements for "*Well Integrity in drilling and well operations*", while the American Petroleum Institute (API) currently develops a recommended practice for handling of annular casing pressure in the US GoM. The working title is API RP90[4] – Annular Casing Pressure Management for Offshore Wells.

Independent of industry sector, there is a global trend towards functional requirements (what is to be achieved) rather than deterministic/rule based requirements (what to do) in high-risk industries. A main reason for this change is to enable the industry to cope with new technology rather than restricting the development. As a consequence of more functional requirements there is an increased focus on risk assessment methods to demonstrate acceptable risk.

The well as part of a safety instrumented system (SIS)

On offshore installations leaks or other hazardous events[5] may occur that make it necessary to isolate the wells. In this situation the well safety function is to "shut-in the

[4] No official version of this recommended practice (RP) is available yet

[5] *Hazardous event* - Event which can cause harm (IEC 60300-3-9).

well". This safety function[6] will reduce the consequences[7] of the initiating event. The well shut-in function is the "protection layer" closest to the reservoir, and the availability[8] of this function contributes significantly to reducing the total risk on the installation.

The well shut-in function is part of a SIS. On offshore installations a SIS has traditionally been designed in accordance with ISO 10418 (or API RP14C), which gives rules for how to design such systems. In Norway and in the UK there has been a change towards the IEC 61508 and IEC 61511 standards, which describe a risk-based approach to determine the design, and quantitative[9] reliability[10] requirements for safety functions. Overall, it is expected that these standards will contribute to a more systematic safety work and increased safety in the industry. In Norway, the new IEC standards have resulted in a guideline for the application of the standards in the Norwegian petroleum industry (OLF, 2004). The guideline states a quantitative reliability requirement to safety functions. One of the safety functions described in OLF (2004) is the "isolation of well" function. The "isolation of well" function comprises the well safety valves and the control logic that actuates the valves.

[6] *Safety function* - Function to be implemented by a SIS (Safety Instrumented System), other technological safety-related system or external risk reduction facilities which is intended to achieve or maintain a safe state for the process in respect to a specific hazardous event (IEC 61511)

[7] *Consequence* - A possible result of an undesired event. Consequences may be expressed verbally or numerically to define the extent of injury to humans, or environmental or material damage (NS 5814).

[8] *Availability* - The ability of an item under combined aspects of its reliability, maintainability, and maintenance support) to perform its required function at a stated instant of time or over stated period of time (BS 4778).

[9] *Quantitative* - The property of anything that can be determined by measurement. The property of being measurable in dimensions, amounts, etc., or in extensions of these that can be expressed by numbers or symbols. A quantitative statement describes "how much", while a qualitative statement answers the question, "what kind is it?" or "how good is it?" (Tarrants 1980).

[10] *Reliability* - The ability of an item to perform a required function, under given environmental and operational conditions, and for a stated period of time (ISO 8402).

Motivation

The industrial and technological development, the extended lifetime of wells and, the recent regulations and standards imply that there is a need for a systematic approach towards well safety during the entire life cycle of a well.

Both well integrity and the well system[11] as part of a SIS are essential to the total risk on an installation. Further, design and operation of the well and the SIS are traditionally the responsibility of organizational units with different focuses. In well system design the ability to contain and transport well fluids from the reservoir to the rest of the process system is emphasized. In SIS design the ability to close in the well when demanded is focused on. Traditionally well integrity and the well system as part of a SIS are handled separately. However, well system failures may have an effect on both well integrity and the ability to shut-in the well when required.

The application of risk assessment in design of wells and of SIS is not new. However, descriptions and guidelines on how to control risk from a well design perspective are fragmented. In particular, this limitation applies to risk assessment in the operational phase.

IEC 61508 and IEC 61511 focus on the use of field specific reliability data. How to collect and include field specific reliability input data in risk assessment need to be focused on.

1.2 Objectives

The overall objective of the PhD project is to develop a systematic approach for risk assessment and control of offshore wells in the operational phase. The main focus is on the two main safety functions of the well:

a. To prevent uncontrolled leakage of well fluids from the well to the environment. This function is usually referred to as *well integrity* and is a *continuous* safety function that may fail at any instant of time.

[11] *System* - A bounded physical entity that achieves in its domain a defined objective through interaction of its parts (DEF-STD 00-56).

b. To *shut in the well flow* in case of a dangerous incident on the downstream side of the x-mas tree. The shut in function is an *on demand* function activated in a random critical situation.

The overall objective is split into the following sub-objectives:

1. Describe the state of the art related to analysis and control of the functions mentioned above.
2. Describe regulations, standards, and industry practice, giving requirements to well safety in the operational phase.
3. Identify commonly accepted analysis[12] methods applied in risk assessment of wells, with focus on quantitative analysis techniques.
4. Identify input reliability data[13] available for quantitative well safety analyses and discuss the quality of the data.
5. Assess the applicability of existing well safety analysis methods and, if necessary, suggest improvements.
6. Suggest improvement in application of reliability input data.
7. Develop a systematic approach for risk assessment of oil and gas wells in the operational phase. In this context a systematic approach means to assess well risk when a well component failure occurs in the operational phase. The basis for the risk assessment is the quantitative analysis techniques identified.

1.3 Delimitation

The PhD work focuses on well safety. Safety is defined by IEC 61508 as “freedom from unacceptable risk”, while IEC 60300-3-9 defines risk as a “combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.” The same standard defines a hazardous event as an “event which can cause

[12] *Analysis* - An examination of a complex, its elements, and their relations; the use of methods and techniques of arranging facts to assist in deciding what additional facts are needed, establish consistency, validity and logic, establish necessary and sufficient events for causes, and guide and support inferences and judgments (Johnson 1980)

[13] *Reliability data* - Reliability data is meant to include data for reliability, maintainability and maintenance supportability.

harm." A well has the potential to create hazardous events, and hence well risk must be acceptable. The risk should be acceptable throughout the lifetime of the well.

For a well the main hazardous event is a blowout. The acceptable mean time between blowouts is very long compared with the lifetime of a well. In such situations Rasmussen (1994) states that the risk involved in operation has to be predicted analytically from the first beginning and the proper defenses have to be designed from this prediction. The thesis focuses on predictive analysis methods.

The work is limited to offshore wells and the two functions described in section 1.2. Another limitation is that the work focuses on the operational phase of the well lifecycle. The operational phase typically starts after the well is handed over to production operations. The operational phase involves a long-term operation where failures may develop over time and result in unacceptable changes in risk. The well operations before the well is in production (i.e., drilling and completion) or operations to repair[14] or maintain the well (i.e., workover and wireline operations) are not covered.

Holand (1997) describes two main types of barrier situations; static and dynamic. A static barrier situation is a situation where the same well barrier will be available over a "long" period of time. In a dynamic situation the well barrier varies over time. This situation is typical for well drilling, workover, and completion operations. With focus on the operational phase, the thesis treats static barrier situations. Appropriate analysis techniques for dynamic well situations are discussed in Holand (1997).

It is not within the scope to assess the effect of major modifications, e.g., to convert the well from a production to an injection well. Such changes are known in advance and may be handled as a new design.

Risk can be related to losses comprising:

- Loss of human life.
- Environmental damage.
- Material and production loss.

[14] *Repair* - The part of corrective maintenance in which manual actions are performed on the entity (IEC 50(191)).

Severe accidents may impair the reputation of the operating company, and risk management is therefore important in the entire life cycle of the offshore installation. Through design, operation, and maintenance the aim is to minimize risk. However, risk is not only about losses. Effective risk management may provide a significant business advantage by contributing to increased business performance and reputation. This thesis focuses on risk related to losses with focus on loss of human life risk. The possible side-effect that the proposed method(s) contribute to a business advantage is not treated in the thesis.

The total risk will be a combination of risk from several potential hazardous events, where the hazardous events result from different hazards. According to EN 12100-1, there may be mechanical, radiation, chemical, biological or electrical hazardous energy sources. Even if a well may include aspects of the hazardous energy sources above, the release of inflammable/explosive fluids (hydrocarbons) to the surroundings is by far the most significant risk factor. This risk factor is focused on in the thesis.

A blowout may be caused by a well component failure or an external event directly affecting the well, both situations resulting in loss of control. Well component failures are focused on in this thesis. The frequencies of external events that result in well failure are not covered.

The thesis is limited to the technical factors. Organisational and human factors are not covered. Neither is the risk associated with occupational accidents.

The thesis focuses on the use of quantitative risk analysis methods. If existing methods suited for the purpose are identified, these methods are used as basis. In this case improvement of, e.g., input data is focused on rather than suggesting new methods.

The well shut-in function comprises three basic parts, namely detection (sensors), logic actuator and actuation (the well safety valves). The thesis focuses on the well components that are part of the well shut-in function, but the results may serve as input to the design and follow-up of the entire function.

The need for risk acceptance criteria[15] are described and discussed. However, explicit risk acceptance criteria are not within the scope. To establish acceptance criteria is seen as the responsibility of the operator.

1.4 Scope of work and principal results

A clear understanding of the system and the system boundaries is a key factor in any analysis, and consequently also in any risk analysis[16]. By the system understanding, suitable risk analysis methods and input data can be identified. The results from the risk analyses should provide an appropriate basis for risk evaluation[17] to make decisions concerning risk.

An offshore installation is a complex system. Figure 1 illustrates the system breakdown structure used as basis for further discussion. Three system levels are defined, namely installation, well, and well component level. Figure 1 illustrates the conceptual model[18] for the design phase. This phase is a typical top-down process where the tasks on installation level determine the boundary conditions for the lower system levels. On each level typical *design tasks* are illustrated with boxes in greyscale. Within each *design task* a set of *safety* tasks are performed. The *safety* tasks are illustrated with white boxes. The focus in the thesis is on the well system level, and the *safety tasks* with letters in bold face indicate the main safety tasks performed on well system level. Arrows illustrate the information flow (or boundary conditions) transferred from one task to another. The dotted lines indicate risk results on well system level that may serve as input to the installation level. This feedback loop is, however, not treated specifically in the thesis.

[15] *Acceptance criteria* - Criteria based on regulations, standards, experience and/or theoretical knowledge used as a basis for decisions about acceptable risk. Acceptance criteria may be expressed verbally or numerically (NS 5814)
Risk criteria - A qualitative or quantitative statement of the acceptable standard of risk with which the assessed risk needs to be compared (The Royal Society 1992).

[16] *Risk Analysis* - Systematic use of available information to identify hazards and to estimate the risk to individual or populations, property or the environment (IEC 60300-3-9).

[17] *Risk Evaluation* - Process in which judgments are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects (IEC 60300-3-9).

[18] *Model* - Simplified representation of a phenomenon or object where some aspects are highlighted whereas other are left out (e.g., causal models) (Hellevik 1999).

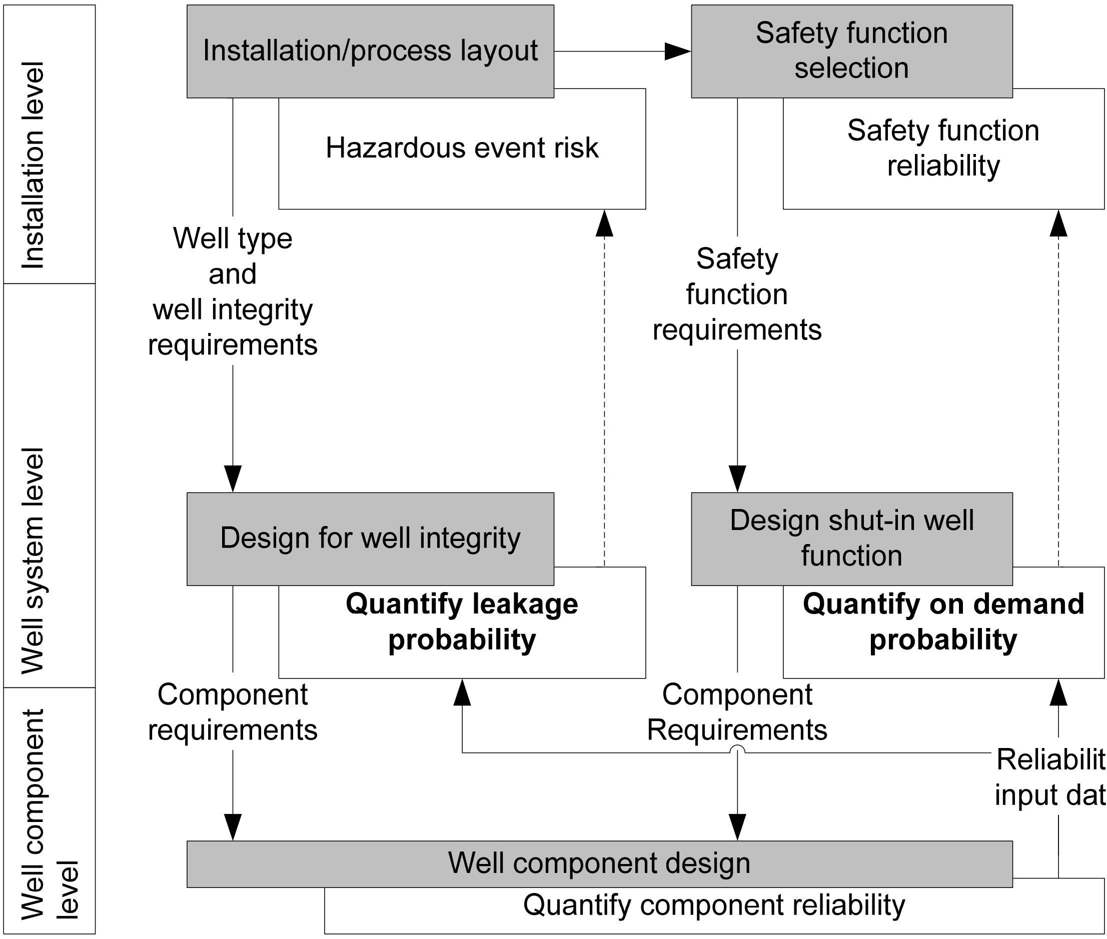

Installation level
Well system level
Well component level
Installation/process layout
Safety function selection
Hazardous event risk
Safety function reliability
Well type and well integrity requirements
Safety function requirements
Design for well integrity
Design shut-in well function
Quantify leakage probability
Quantify on demand probability
Component requirements
Component Requirements
Reliability input data
Well component design
Quantify component reliability

Figure 1 Well risk assessment in the design phase

IEC 61508, Part 4 defines equipment under control (EUC) as "equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities". On offshore installations the EUC will vary from the entire installation to components. It is impossible to develop one risk method that covers all risk aspects of the installation. Risk analyses are therefore performed on various system levels (EUCs).

Risk analyses (QRA) are commonly performed on the installation level. The QRA methods applied differ from country to country. The discussion is based on the practice on the NCS. However, the approach and the limitations highlighted have similarities with the approach used in other countries.

In Norway, the QRA is used to quantify the installation risk. The QRA identify a set of hazardous events, and model the frequency and consequence of the hazardous events. The QRA is a tool used to assess the layout of the installation, placement of main safety functions, and dimensioning accident loads. The QRA as of today tend to model the consequences of the hazardous events in a very detailed manner, whereas the frequency of the hazardous events is modeled in a very rough manner. One of the hazardous events included in the QRA is blowouts. Even if blowout events contribute to a high share of the risk on the NCS, the blowout frequencies used as input to the QRA are based on coarse analysis. In most cases the estimates are based on the historic occurrence of blowouts, where the basis is the work of Holand (1997). For the consequence of a blowout however, a range of models exist. The QRA is therefore a useful tool to identify and compare solutions aimed at reducing the consequence of a blowout. The QRA is not suited (and not used) for reduction of the blowout frequency for a single well. The thesis therefore focuses on risk analysis of single wells rather than using the QRA as basis for modeling well risk.

Ideally, the QRA may be used to establish quantitative requirements to the lower systems levels on the installation. It could, e.g., be possible to set a target value for the blowout frequency for a single well or to the well shut-in function. However, according to OLF (2004) "the level of detail of the QRA as it is performed today makes it more appropriate for evaluating conceptual options and for verification purposes, than for stating absolute criteria." The thesis therefore includes a description of other regulations and requirements that include criteria for wells in the operational phase.

On installation level the first design task is to determine the field and installation layout, including type and number of wells. On well system level this means that the consequences of a hydrocarbon leak is determined too a large degree by decisions made on installation level and by the field properties in general (reservoir conditions). On well system level the role of the risk assessment is restricted to leak frequency analysis of alternative well designs (configurations) to select the well design with the lowest risk. The role of the risk evaluation is to assess if the estimated leak frequency can be accepted.

The same principle is applicable to the well shut-in function. On installation level the risk analysis (QRA) includes a range of hazardous events and safety functions are included to reduce the hazardous event risk. One of the safety functions is the well shut-in function. In the QRA it assumed that the well is able to shut-in with a certain on-demand probability. This probability then becomes the boundary condition for the designers of the well shut-in function. The safety task on well system level is to verify that the well shut-in function is able to function with the required on-demand probability. This requirement should be followed up in the operational phase.

On well system level the component level boundary conditions are determined. Based on the input from the well level, the well components are selected and qualified for use in the specific well. Reliability input data on well component level may then be fed back to well system level.

Different types of risk evaluation are made in the design phase and in the operational phase. In the design phase, several configurations and well component alternatives are evaluated. In this phase the role of the risk analysis is to present a basis for comparison and ranking of the alternatives. In the operational phase the well design is fixed, and risk control[19] should be performed throughout the life of the well. The role of the risk analysis in this process is to illustrate changes in risk and to present alternatives for reducing risk. The risk evaluation should conclude whether the change in risk is acceptable or not.

Figure 2 illustrates the conceptual model for the operational phase. In contrast to the design phase, the operational phase is a typical bottom-up process where well component failures influence the higher levels in the hierarchy. The PhD project includes a risk assessment[20] method to be applied on the well system level. The method includes both well integrity and the well shut-in function. The basis for the risk assessment method is the quantitative analysis and well level requirements identified as suited for use in the design phase. The quantitative analysis are used to measure the

[19] *Risk Control* - Process of decision-making for managing and/or reducing risk; its implementation, enforcement and re-evaluation from time to time, using results of risk assessment as one input (IEC 60300-3-9).

[20] *Risk Assessment* - Overall process of risk analysis and risk evaluation (IEC 60300-3-9).

increase in well integrity risk and the well shut-in function on-demand probability as a result of well component failures that occur in the operational phase.

The risk assessment method is used to control well risk in the operational phase. It is assumed that if the well risk is acceptable on single well level, the risk change will not be reflected in the QRA on installation level. A possible extension not covered in this thesis is to implement the method as part of a tool to update the QRA in the operational phase (indicated with dotted lines in Figure 2).

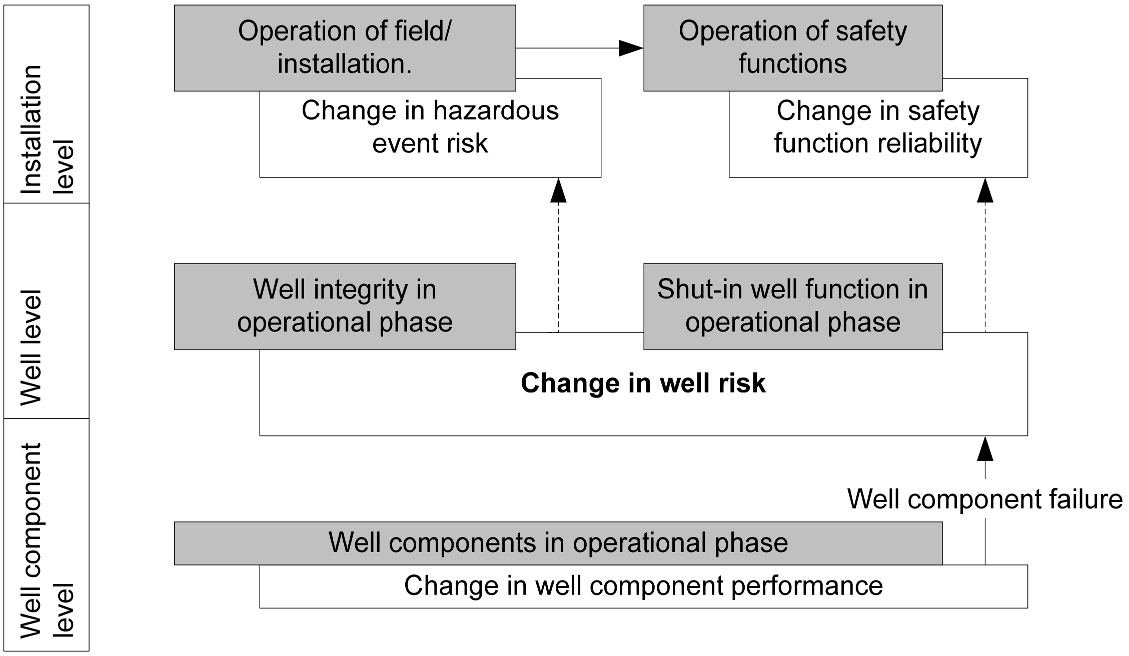

Installation level
Well level
Well component level
Operation of field/ installation.
Change in hazardous event risk
Operation of safety functions
Change in safety function reliability
Well integrity in operational phase
Shut-in well function in operational phase
Change in well risk
Well component failure
Well components in operational phase
Change in well component performance

Figure 2 Well risk assessment in the operational phase

1.5 Scientific approach and verification

This PhD project belongs to the field of applied science, meaning research aiming directly at practical application. Applied research can be exploratory but are often descriptive. Applied science is an activity of original character to gain new knowledge and insight, primarily to solve specific, practical problems. This means that the quality of the research must be considered not only from a scientific point of view, but also from a user point of view. Applied research "asks questions" and in this context the thesis objective may be stated as "how can well risk be controlled by risk assessment?".

The general basis for the thesis is established through extensive literature surveys. These surveys represent the starting point for the research, and support all subsequent activities. In addition the professional experience from SINTEF and ExproSoft, input from my advisor Marvin Rausand, co-operation with industry representatives from Norsk Hydro, and co-operation with colleagues from ExproSoft and SINTEF have contributed to valuable input to the identification of problem areas, comments and subjects to be focused on.

To prove its validity, the empirical verification of the research is one of the cornerstones in many scientific disciplines. However, direct verification of the full extent of the methodology in the thesis may be unrealistic. Due to many influencing factors both in the design phase and in the operational phase, a new method may improve safety but cannot guarantee it. Consequently, it is difficult to separate the effects of a certain method from other factors, or to prove afterwards that other methods would have led to a better result (Roozenburg and Eekels, 1995). As an alternative, Vatn (1996) describes some basic principles to ensure a scientific approach to the development of procedures and methods. The principles followed to the extent possible are:

1. *Defining and limiting the problem*. As part of a procedure or a method, the principal problem it is developed for and the limitations shall be clearly defined.
2. *Stringency*. Rules must be obeyed. Because most methods within applied science are cross-disciplinary, the rules or the scientific standards vary among the disciplines. For example, the predictive part of a method will often require an understanding of the world in terms of cause-effect models.
3. *Accuracy*. The method shall be careful and exact.
4. *Correctness*. Deductive reasoning shall be correct according to formal logic. If an argument cannot be defined from a formal logic point of view, this should be stated.
5. *Thoroughness*. The method shall explore how all important aspects of a problem can be treated. If some aspects are left out from the analysis, this shall be stated and justified. A key question is “Can the method handle this and that?”.
6. *Traceability*. In this context traceability means that arguments leading to the proposed procedure or method should be stated as part of the procedure/method, or

as a supplement to the method. This involves demonstrating how the method relates to a theoretical basis, and literature references should be made to relevant work.

7. *Order and system*. The procedures and methods shall have a high degree of order and system to ensure that 1) critique can be raised against the method, and 2) it is easy to understand and use the method to solve real problems.
8. *Critique*. Arguments against the procedure and methods shall also be identified and discussed.

The thesis consists of a main report that describes a framework for use of well risk assessment in the operational phase. A set of papers is included as appendixes to the main report. The papers describe detailed methods or procedures that are part of the framework. The criteria listed above have been followed as far as possible both in the main report and in the papers.

The risk assessment procedure presented in the main report is developed in co-operation with Norsk Hydro. The risk assessment procedure is now being implemented by Norsk Hydro. The plan is to conduct a series of courses to get user feed-back before the method is implemented as an internal procedure. Paper 2 is published in a journal. Paper 1 and Paper 3 are presented in conferences.

1.6 Structure of the thesis

The thesis consists of a main report and enclosed papers. The main report provides a framework to the work presented in the thesis together with summary and discussion. The main report provides references to specific topics presented in the papers. The content of the main report are described in more detail below.

Chapter 1 describes the background and motivation for the PhD project, along with the objectives and the limitations. The scientific approach adapted is discussed and the structure of the thesis is outlined.

Chapter 2 describes the main characteristics of an offshore well. The chapter forms a basis for the discussions and evaluations later in the report. A base case well is described, as well as different well types and well operations. Finally, well integrity and the well shut-in function are discussed.

In *Chapter 3* the boundary conditions for risk assessment of single wells are discussed. The boundary conditions are conditions or limitations determined by the higher levels in the offshore installation system hierarchy or by specific well integrity and well shut-in function requirements. With basis in the boundary conditions, suited types of risk analysis and risk measures are discussed.

In chapter 3 it is identified that the IEC 61508/61511 standards require risk analysis to be performed to determine the required protection from safety functions, while a risk analysis normally not is required is Norway. In *Paper 1* the difference between the two approaches is discussed in more detail.

Chapter 4 describes well configuration and well component characteristics. The discussion includes functionality requirements, failure modes, failure causes, and reliability data. Different types of safety critical well barrier failures require different types of detection strategies and follow-up, and in Paper 3 strategies for revealing safety critical failures are discussed. C*hapter 4* presents a failure classification scheme that is useful when performing quantitative reliability analysis. The basis for the classification scheme is described in Paper 5.

Chapter 4 also presents barrier diagrams as a method to illustrate the possible leak paths between the reservoir and the environment. Barrier diagrams are useful for keeping an overview of the well barriers when analyzing various well barrier arrangements. Barrier diagram construction rules are described in *Paper 4*.

In *Chapter 5* the quantitative reliability analysis applied on well system level are discussed. On well system level the designers/user can primarily influence 1) the blowout and/or well release frequency and 2) the probability of failure on demand (PFD) for the well shut-in function. In chapter 5 the two reliability measures are presented, together with suitable analytic method.

Paper 5 describes models to calculate the unavailability for different Surface Controlled Subsurface Safety Valve (SCSSV) configurations. In Paper 2 a common cause failure model is described. The models described in paper 2 and 5 are supplements to the methods described in Chapter 5.

Chapter 6 describes a method for risk assessment of a single well. The method is to be applied in the operational phase when a failure of a well component has occurred.

Chapter 7 provides a brief evaluation of the research process, a discussion of the results of this thesis, and recommendations for further work.

2. Well system description

To establish a basis for the discussions and evaluations later in the report this chapter describes the main characteristics of an offshore well A base case well is described, together with different well types and well operations. Finally, well integrity and the well shut-in function are discussed.

2.1 Well system, well types and well operations

A well consists of a x-mas tree, a wellhead, a well completion, and a casing program, where:

- The *well completion* is the assembly of tubing hanger, downhole tubular, safety valve, production packer, and other equipment placed inside the production casing to enable safe and efficient surface access to a (pressurized) formation.
- The *x-mas tree* is an assembly of valves, pressure gauges and chokes fitted to the wellhead to control the well flow.
- The *wellhead* is the surface/seabed termination of a wellbore that incorporates facilities for installing casing hangers during the well construction phase and for hanging the production tubing and installing the x-mas tree.
- The *casing program* encompasses all casing and liner strings, including hangers and cement, in a wellbore.

The *well* as defined above is the system boundary in this report. An example well is included as a basis for discussion and exemplification later in the report. Figure 3 shows a sketch of the well, which is a typical surface oil production well. On a surface well the wellhead, the x-mas tree, and the production control system are positioned on the platform. On subsea wells these systems are located on the seabed and the reservoir fluids are transported from the well through a flowline and a riser to the platform. On subsea wells there are two main x-mas tree types. Vertical subsea x-mas trees are in principle similar to the surface x-mas tree, while a horizontal x-mas tree is configured with the master valves and flow-control equipment on a horizontal axis (the PMV is located horizontally).

The well completion gives access to the reservoir. The well completion part below the tubing hanger is commonly called the tubing. The tubing is an assembly of tubing joints and other completion components. The reservoir fluids (oil, gas and water) flow from the reservoir through the tubing to the x-mas tree and to surface. The components selected for any well completion should be compatible with the wellbore geometry, well pressure, reservoir fluids, etc.

The casing program consists of different types of casing strings. The casing program has several functions. The production casing is set across or at the start of the reservoir and allows installation of the well completion. The intermediate casing string provides protection against caving of weak or abnormally pressured formations and enables the use of drilling fluids of different density necessary for the control of lower formations. The surface casing string provides structural strength so that the inner casing strings and the well completion can be installed.

The space between the tubing and the production casing is called A-annulus in the report. The annuli outside the A-annulus are called B- and C-annulus, respectively.

Several components with different functions are integrated into a well. Some commonly installed component types and associated functions are[21]:

- *Tubing hanger and tubing head.* The tubing hanger is located in the tubing head. The tubing head provides a means of attaching the x-mas tree to the wellhead. Both components ensure that the tubing and annulus are hydraulically isolated.
- *Production packer.* The production packer isolates the annulus and anchors the bottom of the production tubing string.
- *Seal assembly.* The seal assembly is a component with seals that engages in a sealbore to isolate the production tubing conduit from the annulus.

[21] See the Definitions chapter for detailed function description

- *Surface controlled subsurface safety valve (SCSSV)*[22]. The SCSSV is a downhole safety valve, which is operated from the surface through a control line. The valve is able to shut-in the well when demanded. The valve is fail-safe[23], i.e., the valve closes with loss of hydraulic control pressure. Two basic types of SCSSV are common: wireline retrievable (WR), whereby the principal safety-valve components can be run and retrieved on wireline, and tubing retrievable (TR), in which the entire safety-valve assembly is installed with the tubing string. TR-SCSSV valves are most common in use. The WR-SCSSV are in some cases installed to replace a failed TR-SCSSV.
- *Production master valve (PMV).* The PMV is located on the x-mas tree and controls the flow from the wellbore. The PMV also has a safety function and is fail-safe close if control pressure is lost. On surface wells also a manual master valve is usually installed.
- *Production wing valve (PWV).* The PWV is located on the side of the x-mas tree. The PWV is used to control and isolate production. In addition a service (kill) wing valve is available for treatment or well-control purposes.
- *Swab valve.* The swab valve is located on the top of the x-mas tree and provides access to the wellbore if repair or inspection is required.

[22] Other types of Downhole Safety Valves (DHSV) are available but the dominating type is SCSSV and only this type is included in the thesis.

[23] *Fail safe* - A design feature that ensures the system remains safe or, in the event of a failure, causes the system to revert to a state that will not cause a mishap (MIL-STD 882D).

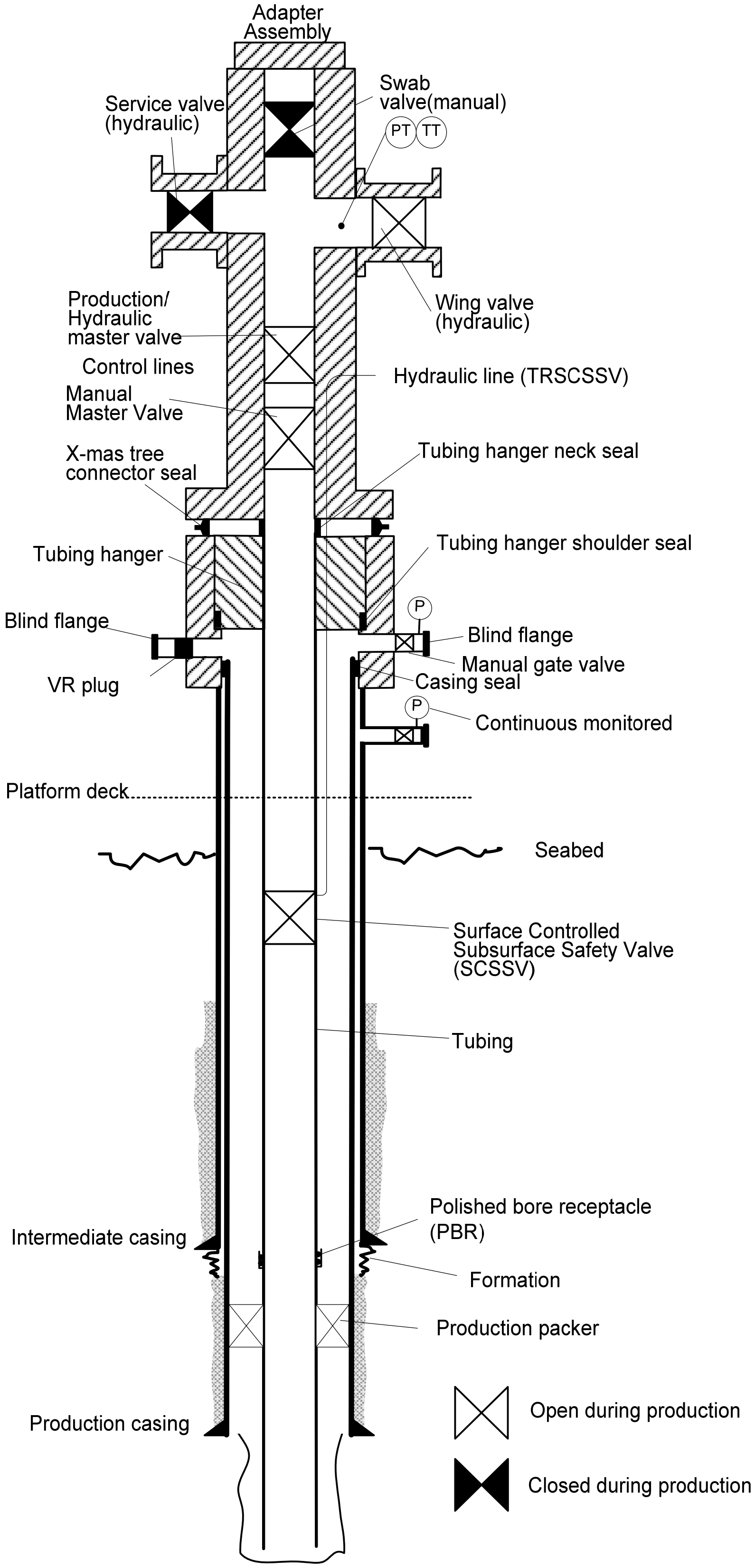


Figure 3 Typical surface oil production well

2.1.1 Well types

A well may be a production or an injection well. Production wells produce well fluids, while injection wells are used to inject gas or water to the reservoir to maintain reservoir pressure.

Production wells

A production well transports well fluids from the reservoir to the rest of the process facilities on the installation. In addition to oil, an oil well almost always produces some gas and frequently water. A gas well produces natural gas, and frequently some condensate (natural gas liquids such as propane and butane) and occasionally some water.

In a naturally flowing production well the formation pressure is sufficient to produce oil at a commercial rate. In the North Sea most reservoirs are initially at pressures high enough to allow a well to flow naturally. After a period of time the pressure may decrease and it is required with artificial lift to continue production. Artificial lift means any system that adds energy to the fluid column in a wellbore with the objective to improve production from the well. Artificial-lift systems use a range of operating principles, such as rod pumping, gas lift, and electrical submersible pumps (Podio et al, 2001). Gas lift is the most common type of artificial lift in the North Sea.

Injection wells

In a gas injection well, separated gas from production wells or imported gas is injected into the upper gas section of the reservoir. The injected gas is used to maintain the pressure in the oil reservoir. In most cases, a field will incorporate a planned distribution of gas-injection wells to maintain reservoir pressure.

Water injection wells are common offshore, where filtered and treated seawater or produced water is injected into a lower water bearing section of the reservoir. Water production can be significantly higher than oil production from a field. Consequently, treatment and disposal of produced water, especially in remote locations, have a significant impact on the feasibility of a project.

2.1.2 Well operations in the operational phase

In the operational phase major maintenance or remedial treatments may be necessary. Eventually, the well will be terminated. Through-tubing workover is a common term for coiled tubing, snubbing or wireline operations conducted for treatment or service of the well. Wireline operations are most common. In this operation a piece of equipment is run inside the tubing string on a wireline either to make a replacement in the well, to install new equipment or to perform well surveys. Tubing access through vertical subsea trees and surface threes is achieved by simply opening the valves in the tree, while on horizontal subsea trees a set of plugs need to be retrieved to gain access to the well bore. Wireline operations are relatively routinely performed on platform wells, while a vessel or a rig must be contracted to do the same wireline operation on subsea wells. A through-tubing workover may avoid a full workover, which is more time and cost consuming.

A full workover means that parts of or the complete tubing string is removed and replaced with a new. A full workover may be required due to necessary corrective maintenance[24] or productivity problems. On surface wells and vertical subsea x-mas trees a failure of the tubing string will require pulling of the x-mas tree. On horizontal subsea x-mas trees the tubing string can be pulled without pulling the x-mas tree. Workovers on subsea wells are normally more time consuming than on platform wells because a workover rig must be contracted.

To kill a well means to stop a well from flowing reservoir fluids. In the case of a producing well, a kill fluid with sufficient density to overcome production of formation fluid is pumped into the well.

The well may be closed-in because of operational reasons. To close-in the well means to close one or several valves in the well.

If the well is non-productive, the well will be abandoned. Before abandonment the well is plugged with cement plugs and recoverable equipment is removed.

Workover operations are dynamic situations and are not covered directly in the report. Indirectly, such operations are included in the quantitative reliability analyses

[24] *Corrective maintenance* - The maintenance carried out after a failure has occurred and intended to restore an item to a state in which it can perform its required function (BS 4778).

described later in the report because expected time to repair safety critical failures is included in the analysis. The risk of performing such operations are however not included.

2.2 Well integrity

NORSOK D-010 defines well integrity as "the application of technical, operational and organizational solutions to reduce risk of uncontrolled release of formation fluids". The SINTEF offshore blowout database (SINTEF, 2005) defines a *blowout* as "an incident where formation fluid flows out of the well or between formation layers after all the predefined technical well barriers or the activation of the same have failed". In addition to blowout the SINTEF offshore blowout database (SINTEF, 2005) has defined a second event called well release. A *well release* is a "an incident[25] where oil or gas flow from the well from some point were flow was not intended and the flow was stopped by use of the barrier system that was available in the well at the time the incident started". A typical well release will be a leak through a component in the x-mas tree and the SCSSV is activated. As seen, NORSOK D-010 defines well integrity as the solutions available to prevent a blowout (uncontrolled release). However, it is chosen to also include well releases in the thesis. Therefore the following well integrity definition is used:

- The application of technical, operational and organizational solutions to reduce risk of blowout *and* well release.

A well should be designed and operated to minimize the blowout and well release risk. Safety is defined by IEC 61508 as "freedom from unacceptable risk". Safety related to well integrity may therefore be defined as "freedom of unacceptable blowout or well release risk".

A blowout or a well release may consist of salt water, oil, gas or a mixture of these. A blowout that flows into another formation and not to the surface is called an underground blowout. A blowout or well release may be caused by a well component

[25] *Incident* - Any unplanned event resulting in, or having potential for, adverse consequences (ISO/TMB WG 1998).

failure or an external event directly affecting the well, both situations resulting in loss of control.

2.2.1 Well integrity and well barriers

The technical means of avoiding a blowout are well barriers. A well barrier is defined by NORSOK D-010 as "an envelope of one or several dependent barrier elements preventing fluids or gases from flowing unintentionally from the formation into another formation or to surface". The same standard defines a well barrier element (WBE) as an "object that alone cannot prevent flow from one side to the other side of it self". A well barrier can be viewed as a pressurized vessel (envelope) capable of containing the reservoir fluids. The two barrier principle is followed in Norway and in most oil producing countries. This principle means that there should be at least two well barriers in a well. A well can therefore be considered as a system of two or more pressurized vessels (envelopes) that prevent the fluid from entering the surroundings. Figure 4 illustrates the well barrier system as pressure vessels. In Figure 4, the well tubulars and the x-mas tree body constitute the vessel walls while the SCSSV and x-mas tree valves are illustrated as the outlet valves from the vessel. The innermost vessel illustrates the well barrier closest to the reservoir while the outer vessels illustrate the consecutive well barriers.

A well release will typically be an incident where the outer vessel leaks, and the inner well barrier stops the leak. In a blowout situation all the predefined technical well barriers or the activation of the same in one possible leak path have failed.

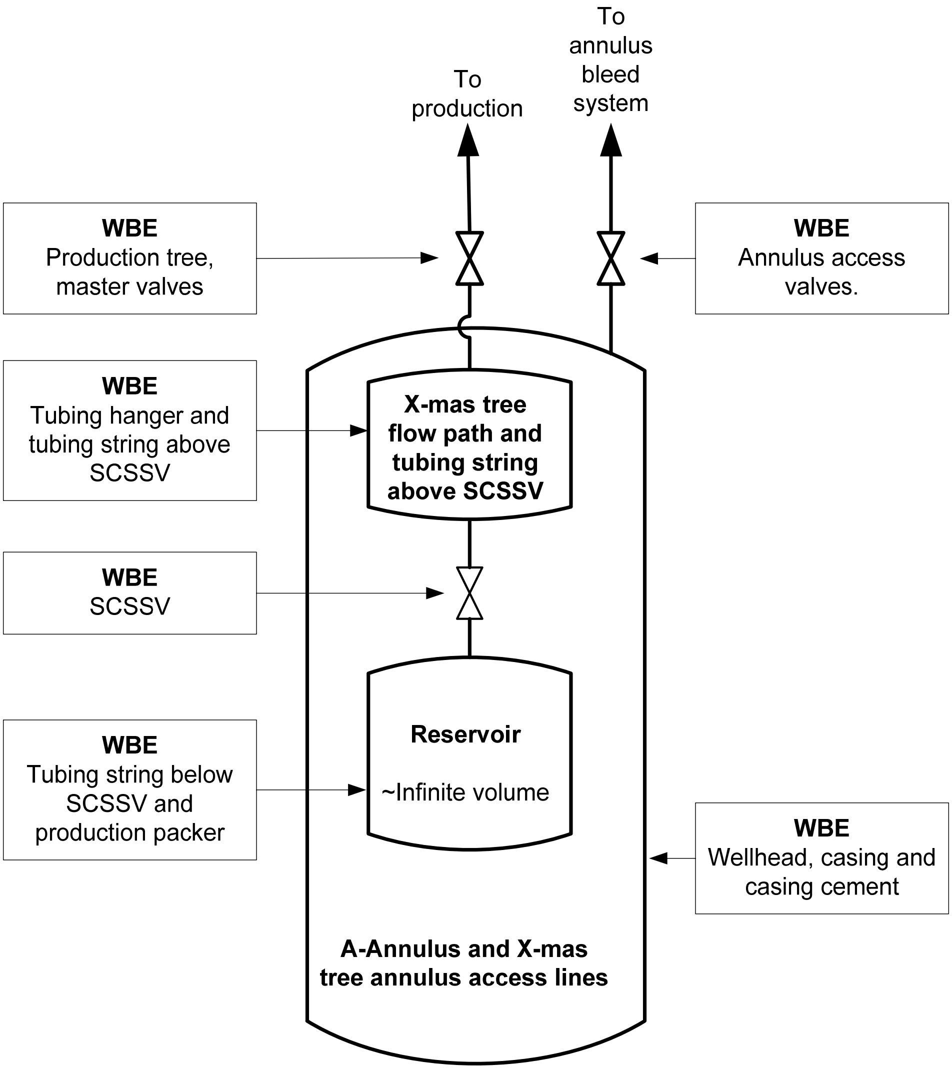

To production
To annulus bleed system
WBE Production tree, master valves
WBE Annulus access valves.
WBE Tubing hanger and tubing string above SCSSV
X-mas tree flow path and tubing string above SCSSV
WBE SCSSV
WBE Tubing string below SCSSV and production packer
Reservoir
~Infinite volume
WBE Wellhead, casing and casing cement
A-Annulus and X-mas tree annulus access lines

Figure 4 Illustration of well barriers to achieve well integrity

2.2.2 Well integrity risk

Blowouts (and well releases) can be catastrophic and lead to loss of life, material loss, and severe environmental impacts. Depending on installation type, location of wells, well type, etc., blowouts represent an important contribution to the total fatality risk in offshore oil and gas exploration activities. A measure for the fatality risk is the fatal accident rate (FAR), which is a frequency rate[26] defined as the expected number of

[26] *Frequency rate* - The number of occurrences of a given type of event expressed in relation to a base unit of measure (for example, accidents per 1 million miles traveled (Tarrants 1980)

fatalities per 10^8 hours of exposure. The FAR contribution from blowouts in all well phases is discussed in Holand (1997), where it is estimated that blowouts represent between 3.5% and 7.2 % of the total fatality risk in offshore oil and gas exploration activities in the US GoM outer continental shelf and the North Sea regions.

Blowout and well release frequencies

Blowout frequencies and failure causes are presented in Holand (1997). Holand (1997) include blowouts from the period 1 January 1980 until 1 January 1994 in US GoM outer continental shelf and the North Sea (Norwegian, UK waters). Holand (1997) is based on data from the SINTEF offshore blowout database, and this database is continuously updated (SINTEF, 2005). The database is available to the sponsors of the project.

Two main potential blowout situations are reported in the operational phase:

- Blowout during normal operation caused by well equipment failures.
- Blowout caused by an external hazardous event. In such situations the external hazardous event damages the well components above the ground or on the seabed (wellheads and x-mas trees).

Holand (1997) discusses 12 production blowouts, where six blowouts are caused by well equipment failures, and six blowouts are caused by external loads damaging well equipment with subsequent failure to close in the well, e.g., storm, earthquake, naval vessel collision, dropped objects, fire and explosion loads. All the production blowouts originate from platform completed wells. Holand (1997) did not distinguish between blowout and well release. This differentiation is now made in the SINTEF Offshore Blowout Database (SINTEF, 2005). It is reason to believe that many of the external load events now would have been classified as well releases.

Further from Holand (1997), most of the production blowouts are caused by failure to take action after well equipment failures. Typically, production has continued with tubing or casing failure, or the SCSSV has been left in failed condition (or failed when activated).

As input to risk analyses Holand (1997) recommends a well blowout frequency of 5.0 10^{-5} blowouts per well year for wells in the operational phase (production and injection wells). This blowout frequency is likely to be conservative due to outdated well design, operating practices, and the broad definition of blowout (include well releases). For example, modern SCSSVs are in general regarded to be far more reliable than SCSSVs used in the 80-ties and early 90-ties (Molnes and Strand, 1999).

In Norway hydrocarbon leaks above 0.1 kg/s must be reported. According to PSA (2003) a total of 228 significant hydrocarbon leaks (i.e., leak rate above 0.1 kg/s) occurred from permanent and mobile installations on the NCS during the period 1996-2002. None of the significant hydrocarbon leaks ignited. Valve faults and incorrect operational actions account for most of the leaks. No blowouts where reported in the same period.

The blowout and well release frequencies presented above illustrate that the mean times between blowouts and major releases are long, and that the mean time between worst case consequences because of a major hydrocarbon release is even longer. Therefore, the risk (frequency and consequence) must be predicted.

Blowout and well release consequences

A well blowout or well release (or a hydrocarbon release in general) may have severe consequences for personnel and material assets caused by release of toxic substances (e.g., H_2S), instability of platforms, or ignition resulting in fire and explosion loads.

In the UK, the RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations) classification (HSE, 2002) is used to categorize the criticality of hydrocarbon leaks. The categorization is presented in Table 1. A blowout from a typical production well in the North Sea belongs to the RIDDOR “major releases” category.

Table 1 The RIDDOR classification of hydrocarbon releases (adapted from HSE, 2002)

Fluid[1]	Category[2]	
	Major	Minor
Gas and 2-Phase	EITHER Quantity released > 300 kg OR Mass release rate >1kg/s and duration >5 min	EITHER Quantity released < 1 kg OR Mass release rate < 0.1 kg/s and duration < 2 min
Liquids[3]	EITHER Quantity released > 9000 kg OR Mass release rate >10kg/s and duration >15 min	EITHER Quantity released < 60 kg OR Mass release rate <0.2 kg/s and duration < 5 min
Remark / Scenario	*Gas*: Capable of jet fire over 10 meters length (>1kg/s) capable of causing significant escalation after 5 minutes duration, or a flash fire/explosion on reaching LFL. Where 300 kg equates to approx. 3000 m^3 explosive cloud at NTP, enough to fill an entire module or deck area, and to cause serious escalation if ignited. *Liquids*: This could result in a pool fire over 10 meters in diameter (>10kg/s) filling a module or cutting off a deck, hindering escape and affecting more than one person directly if lasting for over 15 minutes duration.	*Gas*: This could result in a jet fire of less than 5 meters length (< 0.1 kg/s), which is unstable (< 2 min duration) and therefore unlikely to cause significant escalation, or a flash fire/explosion on reaching LFL. Where <1 kg equates to <10 m3 explosive cloud at NTP, probably insufficient to cause a significant hazard if ignited. *Liquids*: This could result in a pool fire smaller than 2 meters in diameter (< 0.2 kg/s) unlikely to last long enough to hinder escape (< 5 min), but could cause serious injury to persons nearby

1) For 2-phase Releases combinations of the gas and liquids scenarios described are possible, depending on the gas to oil ratio (GOR) involved.
2) A third category called Significant is described as a scenario between major and minor
3) Oil / Condensate / Non-process

From the RIDDOR classification, it is seen that compared with gas a higher volume or leak rate of liquids is defined within each category. Empirically based ignition models (Cox, 1991) also indicate the ignition probability for a gas leak to be at least five times higher than for an oil leak.

In Norway, a quantitative risk analysis (QRA) is used to quantify the installation risk. The QRA includes a range of hazardous event frequencies and models how safety functions contribute to reducing the consequences of the hazardous events. The results from the QRA are typically presented as estimated FAR values. The QRA is used as input to decisions concerning system layout, and type of safety functions to be implemented (placement of living quarter, dimensioning of structures, etc.). NORSOK

Z-013 describes requirements to the QRA performed on the NCS. The starting point for consequence calculations is a distribution of hole sizes. Based upon the pressure in the system, initial leak rates should be calculated and classified according to a leak rate distribution. In NORSOK Z-013 the following narrow leak rate categories are used (all values in kg/s): 0.1-0.5; 0.5-1; 1-2; 2-4; 4-8; 8-16; 16-32; 32-64: > 64. NORSOK Z-013 use the leak rates as a starting point for modeling the consequences of a blowout. For a blowout event NORSOK Z-013 describes the following factors that should be taken into account in the consequence model:

- Blowout location.
- Flow rate as a function of time and bridging possibilities.
- Medium (e.g., gas or oil).
- Operation (e.g., drilling, completion, maintenance, production, injection).
- Reservoir conditions (e.g., shallow gas).
- Probability of ignition, time of ignition.
- Probability of explosion, impact of explosion.
- Effect of fire fighting system, heat load.
- Wind conditions.
- Escalation of accident.
- Escape and evacuation.
- Simultaneous operations (e.g., drilling, production).

In contrast to the RIDDOR classification, NORSOK Z-013 does not describe typical consequences of ignited leaks. As seen, NORSOK Z-013 requires modeling of hydrocarbon leak consequences. A detailed description of fire and explosion models is given in, e.g., SINTEF/Scandpower (1992) and in Hekkelstrand and Skulstad (2004). A blowout may also result in environmental damage, and in Norway the MIRA[27] method (OLF, 2001) is a widely accepted method for environmental risk analysis. This method describes a quantitative approach to the assessment of environmental risk from offshore petroleum activities. The consequences of hydrocarbon releases are often difficult to

[27] *MIRA* - Method for Environmental Risk Analysis (translated from Norwegian)

measure directly, and Lygner and Solli (2001) describe how risk indicators[28] can be used to measure environmental risk.

2.3 Well shut-in function

PSA (2001b) state that “Facilities shall be equipped with necessary safety functions which at all times are able to:

a. detect abnormal conditions,
b. prevent abnormal conditions from developing into situations of hazard and accident,
c. limit harm in the event of accidents.”

In general, two main safety functions are required in a hazardous process.

- Process control, which means to maintain equipment under control with minimum deviation[29] from specifications (category a and b in PSA (2001b) requirements above).
- Process safety, which mean to prevent and minimize damage upon loss of control (category c in PSA (2001b) requirements above).

A general event sequence with process safety functions implemented to minimize damage upon loss of control is illustrated in Figure 5. The process safety functions are illustrated as barriers to mitigate the consequences of hazardous events.

[28] *Indicator* - A measurable/operational variable that can be used to describe the condition of a broader phenomenon or aspect of reality (Øien 2001)

[29] *Deviation* - Departure from a norm (criterion) (Johnson 1980).

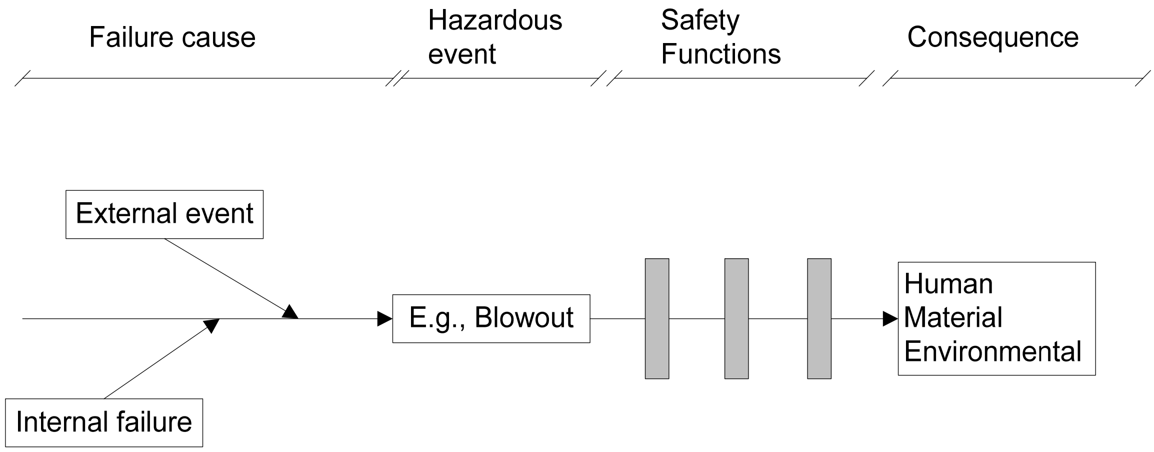


Figure 5 **A general event sequence with process safety functions implemented to minimize damage upon loss of control**

The well shut-in function is a process safety function. The well shut-in function is required if a given hazardous event occurs elsewhere on the installation (e.g., fire on the installation or blowout from another well). The valves in the well must close and shut-in the well and thereby reduce the consequences of the hazardous event. For a standard production well, the *well shut-in* function consists of the following components (OLF, 2004):

- Emergency ShutDown (ESD) logic
- Production wing valve (PWV)
- Production master Valve (PMV)
- Surface controlled subsurface safety valve (SCSSV)
- Solenoid valves

A typical configuration of the well shut-in function is illustrated in Figure 6. The well safety valves are fail-safe, i.e., they will close when hydraulic pressure is lost. In addition to automatic bleed down via the ESD logic, there may be additional means for removing the hydraulic power to the valves. Depending on the scenario that triggers the demand for shut-in, one of the three valves will be sufficient to isolate the well.

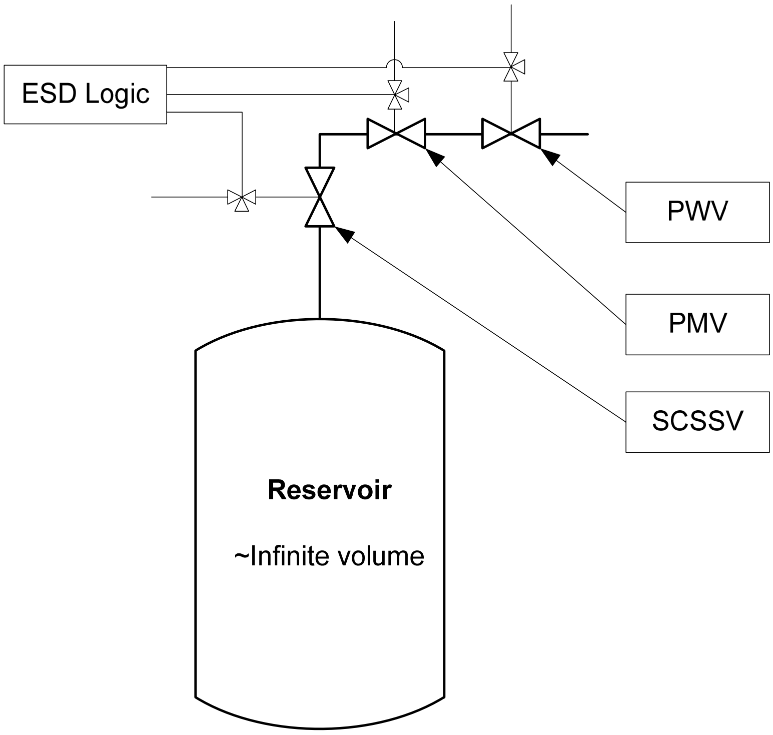


Figure 6 Well shut-in function for a typical surface production well

Hazardous events may also affect the well directly. For surface wells the main source of external hazards will, e.g., be dropped objects on the platform with a potential for hitting and causing damage to the x-mas tree. Other events may be fire or explosion loads acting on the x-mas tree. For subsea wells the main source of external hazards will likely be dropped objects from vessels with a potential for hitting and causing damage to the subsea x-mas tree. In this case the well must close in on the SCSSV (placed below surface and assumed not affected by the external events). This well shut-in function is illustrated in Figure 7. For this function it is assumed that the control line is ruptured and that the SCSSV close due to loss of hydraulic pressure.

According to the PSA (2003) statistics, more than half of the hydrocarbon leaks on the installations are discovered by automatic detection equipment, while personnel in the relevant area discover the remaining leaks. Information on how many of these events that required activation of the well shut-in function is not readily available in the PSA statistics. Some typical average demand rates are given in OLF (2004), where 3 isolations per well-year due to ESD segregation are assumed. However, the number of demands will vary depending on the type of installation.

The two well shut-in functions described above are one of the most important safety functions on an installation. The potential volume released from a production well related to a major accident scenario is "infinite" and the ability to shut-in the well is therefore important to the overall installation risk.

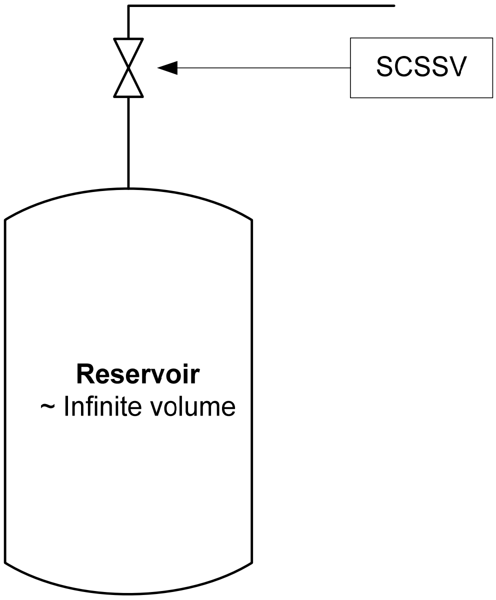


Figure 7 Well shut-in function given an event that result in x-mas tree failure (ESD logic not included, assume control line rupture)

2.4 Main well risk factors

Well integrity and well shut-in function risk factors are illustrated in Table 2. The risk factors are categorized in frequency and consequence factors.

In the design phase the consequence factors are mainly controlled by decisions made on installation level or by reservoir properties (see discussion in section 1.4). The frequency factors, however, are strongly influenced by the decisions made on well system level in the design phase.

In the operational phase a well component failure may result in changes in blowout and well release risk (well integrity). How to assess increased risk after a well component failure is focused on in this thesis. The risk increase will be a combination of frequency and consequence factors. Figure 8 illustrate an example where a well component has failed (leak indicated in figure). The failure is located above the SCSSV. In this situation the well barrier system is degraded (frequency factor) and the well release risk has increased due to storage of hydrocarbons in the A-annulus. Both well shut-in functions is unaffected by the failure since the valves are functioning. However, the volume stored in the A-annuli will be released if the x-mas tree is damaged.

Table 2 Main well blowout and well release risk factors in the well operational phase

Frequency factors
Well barrier system design *Number of well barriers and WBEs in each leak path.* **Well barrier element (WBE) availability factors** *Functionality, reliability, detection of failures, repair of failures.* **External hazards** *Mudslide, fault slippage, extreme weather conditions, dropped/swinging objects (BOP, riser, container, pipe), collisions (icebergs, trawls, naval- and air traffic), fire or explosion loads and resulting fire/explosion resistance, operator/human errors.*
Consequence factors
Installation type *Platform/surface/subsea.* **Installation design /layout** *Protected subsea wellheads, templates, safety functions, placement of living quarter, evacuation routes* **Installation activity type and level** *Manned/unmanned.* **Well leakage fluid(s)** *Condensate/gas//oil/water/other.* **Well leakage characteristics** *Rate/quantity/duration.* **Well leakage exit point** *Casing/formation/wellhead/x-mas tree.* **External factors (not controlled by installation/well design)** *Weather conditions/location/nearby installations/external support*

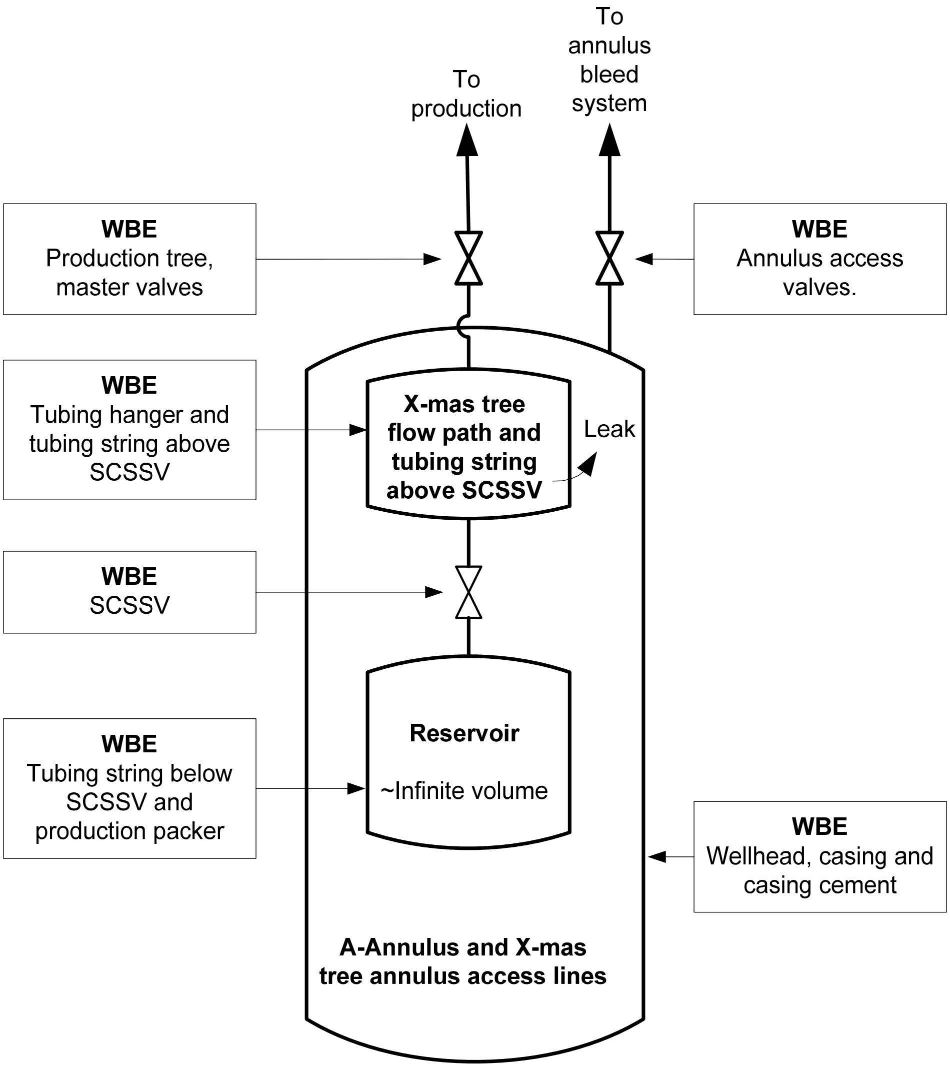

To production
To annulus bleed system
WBE Production tree, master valves
WBE Annulus access valves.
WBE Tubing hanger and tubing string above SCSSV
X-mas tree flow path and tubing string above SCSSV
Leak
WBE SCSSV
Reservoir
~Infinite volume
WBE Tubing string below SCSSV and production packer
WBE Wellhead, casing and casing cement
A-Annulus and X-mas tree annulus access lines

Figure 8 Well component failures influence on blowout and well release risk

3. Well risk assessment boundary conditions

In this chapter the boundary conditions for risk assessment of single wells are discussed. The boundary conditions are conditions or limitations determined by specific well integrity and well shut-in function requirements. With basis in the boundary conditions, suited types of risk analysis and risk measures are discussed.

3.1 Boundary conditions

Well integrity and the well shut-in function are handled by different regulations, standards, guidelines, and recommended practices. The well integrity and well shut-in function boundary conditions from regulations and standards are discussed in sections 3.2 and 3.3, respectively. In section 3.4 required risk analysis measures and risk assessment results based on the review of the requirements are summarized.

3.2 Well integrity requirements

This section gives a review of well system requirements in Norway and in the US GoM. In Norway PSA issues health, environment, and safety regulations. The basis for the regulations is functional requirements. It is left to the operator to find solutions (organizational and technical) that are in accordance with the regulations.

The Framework regulation (PSA, 2001c) describes the overall framework and principles for the other regulations issued. In section 9, "Risk reduction principles" it is stated that "*Harm or danger of harm to people, the environment or to financial assets shall be prevented or limited in accordance with the legislation relating to health, the environment and safety, including internal requirements and acceptance criteria. Over and above this level the risk shall be further reduced to the extent possible. Assessments on the basis of this provision shall be made in all phases of the petroleum activities.*"

On well system level this means that blowout and well release risk should be minimized to the extent possible. The use of risk assessment is a means to achieve this objective.

The Management regulations (PSA, 2001a) describe the operator management principles. In section 2 the principles for management of barriers is described, and it is stated that "*It shall be known what barriers have been established and which function they are intended to fulfill, and what performance requirements have been defined in respect of the technical, operational or organizational elements which are necessary for the individual barrier to be effective.*" Related to well system design this means that the well barriers shall be known, and it should be clearly defined what is required for the well barrier to be effective.

Further in the Management regulations (PSA, 2001a), section 2, it is stated that "*It shall be known which barriers are not functioning or have been impaired. The party responsible shall take necessary actions to correct or compensate for missing or impaired barriers.*" Hence, it is left to the operator to take "necessary actions". A possible approach to provide arguments for "necessary actions" is the use of risk assessment in the operational phase.

In the US GoM the regulations are issued by the MMS. An overall safety requirement policy from MMS is found in the 30 CFR 250 on "Production Facilities". The regulations are built up of "parts", where each part addresses rather specific topics. Many of the same operating principles used in Norway are found in the MMS regulations. This relationship is natural because US oil and service companies dominated the industry, at least in the early years of the "oil age".

An important difference is that the use of rules (what to do) is dominating in the MMS regulations while a practice with use of risk analysis to demonstrate acceptable risk is accepted in Norway. This difference is exemplified by the handling of sustained casing pressure (SCP) in the MMS regulations. SCP often results from tubing leaks (leak in well barrier). A failure of, e.g., the production casing may then result in an underground blowout. According to Bourgoyne et al (2000) the SCP requirements were consolidated in 1988 and included in 30 CFR 250.517. In 1991 MMS issued a letter that dictated changes in the SCP policy.

The requirements for continued operation with SCP were as follows:

1. The SCP is less than 20% of the minimum internal yield pressure, AND
2. The casing pressure bleeds to zero during the diagnostic tests.

A "departure" (deviation from rule) is automatically granted to wells, which meet the criteria above. If not, a request for departure must be submitted to MMS. In the US, API RP 90 – Annular Casing Pressure Management for Offshore Wells is being developed to provide guidance on how to deal with SCP. The API standard is scheduled for completion in 2006 (no official version is available to the public). The standard will likely result in changes in the MMS regulations. An early draft included use of risk analysis to demonstrate acceptable risk. But the risk analysis approach seems to have been abandoned in later draft versions.

As a conclusion, the regulations in Norway require that the operator develop internal procedures based on the principles in the regulations. The role of the authorities is to control that the operators follow their own procedures. The operator must 1) minimize the blowout risk by use of well barriers, 2) control the well barrier status when in operation, and 3) take necessary actions given unacceptable risk. Risk assessment in the design and the operational phase is accepted.

Both the MMS and the PSA regulations frequently refer to international standards, like IEC, ISO and API standards. In Norway a range of NORSOK standards are developed and accepted by the PSA.

The NORSOK standard D-010 defines the minimum functional and performance oriented requirements and guidelines for well design, planning and execution of safe well operations in Norway. NORSOK D-010 states that "*Upon confirmation of loss of the defined well barrier, the production or injection shall be suspended and shall not re-commence before the well barrier or an alternative well barrier is re-established*". However, in the next paragraph it is stated that "*If for any reason the well is contemplated for continued operation, the following shall apply:*

a. *any well with a potential to flow to surface or seabed shall have two independent well barriers. If the well barrier status, availability or monitoring*[30] *ability is altered, any continued use shall be supported by the subsequent points;*

b. *a risk assessment shall be performed based on current reservoir/well condition and time factors in any continued use;*

c. *any deterioration of the leak, or additional failure of a WBE, shall not significantly reduce the possibility of containing the hydrocarbon/pressure and normalising the well;*

d. *a formal deviation process shall be implemented;*

e. *any deviation from the original two defined well barriers shall be presented to the authorities for information and/or approval for further use.*"

In conclusion, the NORSOK D-010 standard opens for a risk-based approach to show that risk is within acceptable limits if deviations occur in the operational phase. The standard does not explicitly state that risk analysis have to be performed in the design phase. In practice quantitative risk analysis are often performed in the design phase to compare the blowout frequency of alternative well system alternatives.

3.3 Well shut-in function requirements

The PSA regulation requirements referred in section 3.2 also apply to process safety functions. In addition, in the guideline to section 7 in the Facilities regulations (PSA, 2001b), it is stated that "... *the IEC 61508 standard and OLF guideline No. 70 should be used where electrical, electronic and programmable electronic systems are used in constructing the functions.*" So, IEC 61508/61511 and OLF (2004) are preferred for design and operation of safety functions implemented by a Safety Instrumented System (SIS).

The IEC 61508/61511 requirements are given as a Safety Integrity Level (SIL). Safety Integrity is the *"probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time"*. SIL is introduced for specifying the target level of safety integrity, and numerical

[30] *Monitoring* - Activity, performed either to manually or automatically, intended to observe the state of an item (IEC 50(191).

target failure measures are linked to the safety integrity levels. Here, it is distinguished between two types of SIS, depending on if the system is “operated in low demand mode of operation” or “operating in high demand or continuous mode of operation”. The well shut-in function will be of the first category. For “low demand” functions safety integrity is given as “average probability of failure to perform its design function when demanded”. The defined SIL levels of the “low demand mode of operation” type systems are given in Table 3.

Table 3 Safety integrity levels: target failure measures for a safety function, allocated to an SIS operating in low demand mode of operation (IEC 61508)

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

In contrast to the IEC 61508/61511 approach, where the SIL level is determined by the use of risk analysis, OLF (2004) does not require a risk analysis to be performed. OLF (2004) defines typical safety functions on an offshore installation and recommends a minimum SIL for each function. In Paper 1 the difference between the approaches in OLF (2004) and IEC 61508/61511 is discussed in more detail.

Independent of approach chosen, both the OLF (2004) and IEC 61508/61511 result in a SIL requirement to the well shut-in function. In Norway, the well shut-in function is assigned a SIL 3 requirement, which means that the probability of failure on demand (PFD) should be 10^{-3} or lower (OLF, 2004). On well system level a risk analysis must be performed to demonstrate that this quantitative requirement can be achieved.

IEC 61508/61511 describes a “safety life cycle” and describes requirements to the entire life of the safety function. This life cycle perspective also means that the PFD requirement must be followed up in the operational phase.

MMS requirements to safety-systems are found in 30 CFR 250. Identified parts related to safety functions are:

- 250.801 Subsurface safety devices.
- 250.802 Design, installation, and operation of surface production-safety systems.
- 250.804 Production safety-system testing and records.

In these parts it is often referred to API RP 14C for requirements to *safety-systems.* API RP 14C is widely accepted in the offshore industry, and the design principles in API RP 14C are established as “standard” safety function designs also in the UK and in Norway. So, even if the risk based approach in IEC 61508/615011 now is preferred both in the UK and in Norway the “tradition” from API RP 14C is still followed when designing the safety systems. The typical API 14C safety function designs are actually the basis for the minimum SIL requirements in OLF (2004).

3.4 Well risk assessment requirements

Based on the review in the previous sections in this chapter it can be concluded that risk assessment is accepted both in the design phase and in the operational phase. For the well shut-in function it is required to perform quantitative analysis to calculate the PFD and verify compliance with the SIL requirements. Related to the well integrity function no explicit blowout frequency requirements on single well level are identified.

The well level risk assessment boundary conditions are summarized in Table 4. Table 4 shows that different risk measures are used for the well integrity and well shut-in function. Also the risk assessment will have different objectives.

Table 4 Summary of well level risk assessment boundary conditions

Risk objectives	Well integrity	Well Shut-in function
Risk assessment objective in the design phase	Risk assessment not explicitly required by regulations, but risk assessment frequently used to, e.g., evaluate alternative well designs.	Verify that SIL requirement (e.g., SIL 3) can be achieved (i.e., PFD < 10^{-3})
Risk assessment objective in the operational phase	It shall be known which barriers are not functioning or have been impaired. Two well barriers must be intact. Risk assessment must be performed before continued use if a well barrier have failed.	Verify that SIL requirement is fulfilled.

4. Well barriers, well barrier elements, and barrier diagrams

In this chapter well barriers and well barrier elements (WBE) are discussed. The discussion includes functionality requirements, failure modes, failure causes, and WBE reliability data. Barrier diagram is presented as a method to illustrate the possible leak paths between the reservoir and the environment. Barrier diagrams are useful when assessing well integrity for alternative well designs.

4.1 Well barriers

A well barrier system should prevent uncontrolled outflow from the borehole/well to the external environment (NORSOK D-010). The well barrier and WBE definitions in NORSOK D-010 are used in the thesis (see section 2.2.1, page 26). A well barrier is dependent on one or several WBEs to fulfill its function. A failure of one WBE results in a failure of the well barrier. A system that is functioning if and only if all of its components are functioning is called a series structure. The well barrier series structure is illustrated as a *reliability block diagram* (RBD) in Figure 9. A RBD is a success-oriented network describing the function of the system. It shows the logical connections of (functioning) components needed to fulfill a specific system function. If we consider a well barrier we have connection between the end points *a* and *b* (the well barrier is functioning) if and only if we have connection through all the *n* blocks representing the WBEs (components), i.e., all WBEs are functioning.

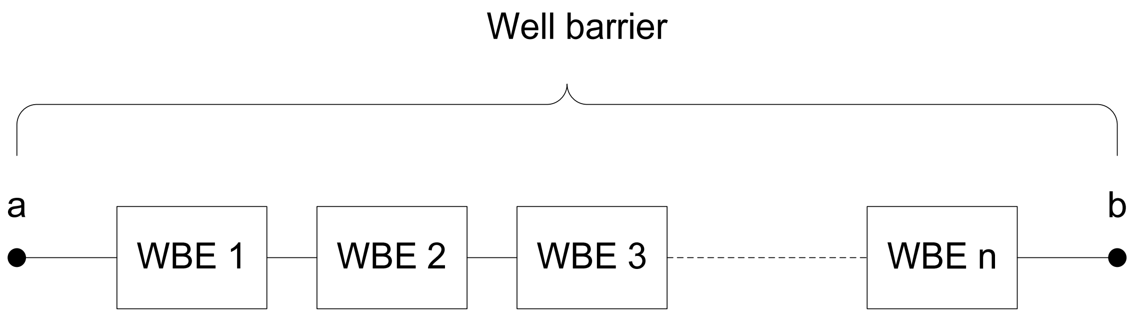


Figure 9 Reliability block diagram of a well barrier

4.1.1 Two well barriers principle

According to NORSOK D-010 there must be "at least two well barriers available during all well activities and operations, including suspended or abandoned wells, where a pressure differential exists that may cause uncontrolled outflow from the borehole/well to the external environment." This two barrier principle is established throughout the oil industry. The well barrier closest to the reservoir is often called the primary well barrier, while the secondary well barrier is the second object that prevents flow from the source. A system that is functioning if at least one of its components is functioning is called a parallel structure. Therefore, a system with a primary and secondary well barrier is a parallel structure (i.e., a redundant[31] system). Redundancy is used to obtain high system availability. A system with a primary and secondary well barrier is illustrated in Figure 10. The well barrier system is functioning if we have connection either through the secondary or the primary well barrier, or both.

The principle of two independent barriers is also important from a robustness[32] point of view. For example, if the wellhead on a production well is severely damaged the only remaining well barrier against a severe blowout is the primary well barrier, namely the SCSSV and the tubing components below the SCSSV (see Figure 3, page 22).

[31] *Redundancy* - In an entity, the existence of more than one means of performing a required function (IEC 50(191)).

[32] *Robustness* – The ability to function under given accident conditions (PSA, 2002).

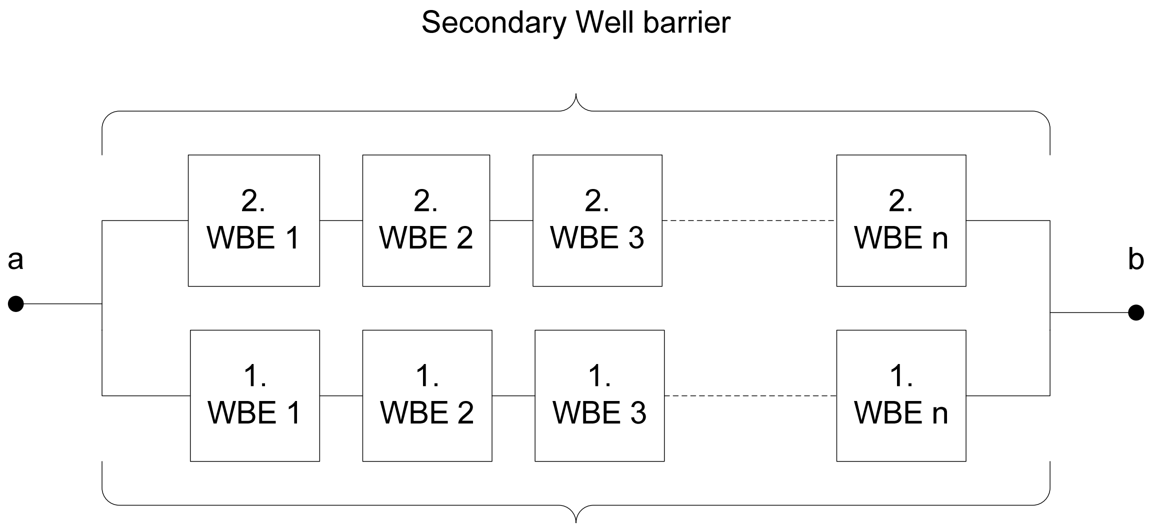


Figure 10 Reliability block diagram of primary and secondary well barrier

4.1.2 Passive vs. active well barrier elements

CCPS distinguishes between passive and active independent protection layers (IPL) (CCPS, 2001). A *passive* protection layer is a protection layer that is not required to take an action to achieve its function in reducing risk. An active protection layer is required to move from one state to another in response to a change in a measurable process property (e.g., temperature or pressure), or a signal from another source (such as a push-button or a switch). A well barrier can be viewed as a protection layer with the objective to prevent flow from the reservoir. A well barrier will however be a combination of passive and active protection layer "elements". The protection layer categorization in CCPS (2001) is used in this thesis to distinguish between passive and active WBEs. Typical passive WBEs are the production packer, the seal assemblies and the tubing string. Active WBEs are the PMV, the PWV, and the SCSSV. For these valves a signal has to be sent (input) to close the valve (change state). A combination of passive and active WBEs constitutes a well barrier and may be illustrated as the series structure in Figure 11.

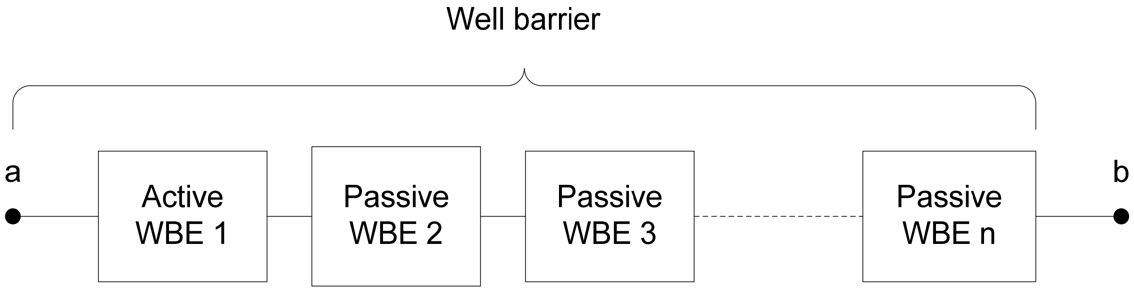


Figure 11 Reliability block diagram of well barrier with one active WBE and "n" passive WBEs

4.1.3 Well barrier system and interfaces

The availability of a well barrier system (or any system) depends on its interfaces with the rest of the world. It is necessary to study how the interfaces influence the system. A clear understanding of system interfaces is essential both in the design phase and the operational phase. In the operational phase the interfaces may change, or a well barrier failure results in changes to the remaining well barrier system. In Rausand and Høyland (2004) a generic technical system and interfaces are illustrated as shown in Figure 12. This generic presentation is used to describe the well barrier system and interfaces.

The elements illustrated in Figure 12 are discussed in detail in Rausand and Høyland (2004) and an extract is given here:

1. System; the technological system that is subject to analysis (and design). The system usually comprises several functional blocks.
2. System boundary; the system boundary defines elements that are considered part of the system and elements that are outside.
3. Outputs; the outputs (wanted or unwanted) are the results of the required functions (like materials, information, etc.).
4. Inputs; the inputs to the system (unwanted or wanted) are the materials and the energy the system is using to perform its required function. Unwanted input may be particles, scale build-up, excessive pressure, etc.

5. Boundary conditions; the operation of the system may be subject to many boundary conditions, like risk acceptance and environmental criteria set by authorities or by the company.
6. Support; the system usually needs support functions, like cleaning, lubrication, maintenance and repair.
7. External threats; the system may be exposed to a wide range of external threats. Some of these threats may have direct affect on the system, others threats may affect the system inputs. Examples of external threats are earthquake, falling loads, loss of energy supply, sabotage, impact from other systems. The distinction between unwanted inputs and external threats may not always be clear. However, the classification in itself is not important. What is important is that all inputs and threats are identified.

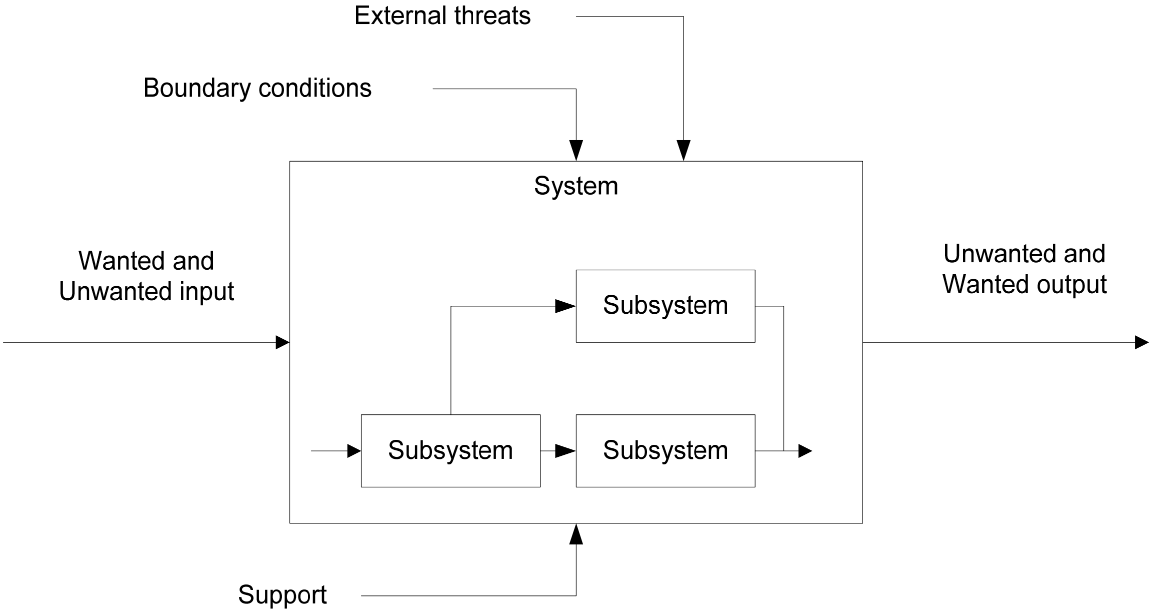


Figure 12 Systems and interfaces (Rausand and Høyland, 2004)

As a supplement to the categorization above, PSA (2002) identifies three elements that describe the performance of safety barriers in general:

1. *Functionality/efficiency*; the ability to function as specified in the design requirements.
2. *Reliability/availability*; the ability to function on demand or continuously.
3. *Robustness*; ability to function as specified under given accident conditions.

With basis in the general system and interface model presented by Rausand and Høyland (2004) a well barrier system and its interfaces are illustrated in Figure 13. The figure is modified to include the PSA (2002) elements also. *Robustness* is included as the ability to function given external threats, while *availability* is illustrated as a RBD, and underlines the importance of the well barrier system to "function over time". *Functionality* is seen as part of the design process where all interfaces are considered and are not included explicitly in the figure. A list of generic well barrier requirements is given in NORSOK D-010. The requirements are grouped into the different system interface categories and included in Figure 13.

A well barrier failure situation may result in a revision/re-assessment of the boundary conditions (acceptance criteria) and the interfaces. For example, a risk assessment after a WBE failure has occurred may conclude that production can continue given that pressure limits (input) and/or test frequency[33] (support) are changed.

[33] *Test frequency* - The number of tests of the same type per unit time interval; the inverse of the test interval (IEEE Std. 352).

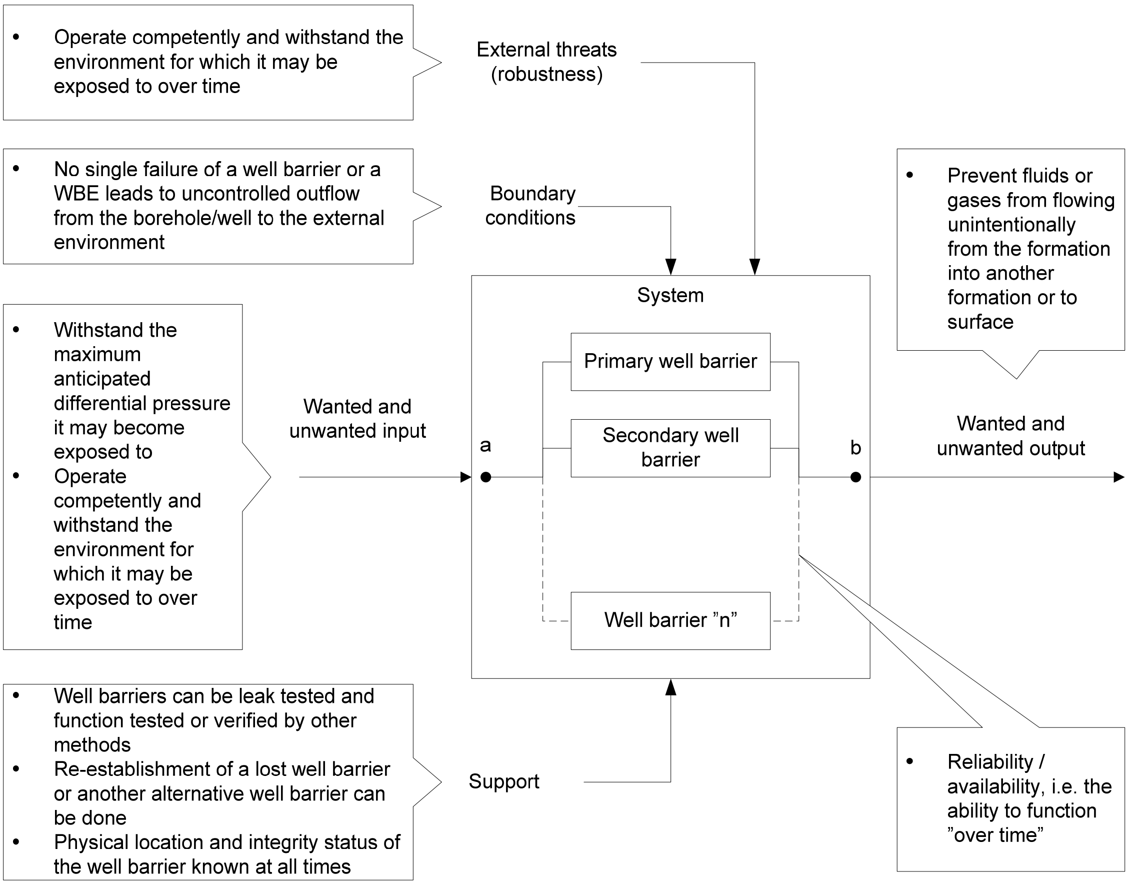

Operate competently and withstand the environment for which it may be exposed to over time
External threats (robustness)
No single failure of a well barrier or a WBE leads to uncontrolled outflow from the borehole/well to the external environment
Boundary conditions
Prevent fluids or gases from flowing unintentionally from the formation into another formation or to surface
System
Withstand the maximum anticipated differential pressure it may become exposed to
Operate competently and withstand the environment for which it may be exposed to over time
Wanted and unwanted input
Primary well barrier
Secondary well barrier
Well barrier ”n”
a
b
Wanted and unwanted output
Well barriers can be leak tested and function tested or verified by other methods
Re-establishment of a lost well barrier or another alternative well barrier can be done
Physical location and integrity status of the well barrier known at all times
Support
Reliability / availability, i.e. the ability to function ”over time”

Figure 13 Well barrier system and interfaces (NORSOK D-010 requirements included)

Figure 13 illustrates how the identified interfaces may be used to categorize the generic well barrier requirements. Below the interface categories are used to group requirements to well barriers found in regulations and standards[34]:

1) Wanted and unwanted input
    a) *A well barrier should withstand the environment and maximum anticipated differential pressure it may be exposed to over time (NORSOK D-010)*. Changes in input during the well life must be frequently assessed (change in well fluid composition, excessive pressure, scale, particles in the flow, etc.). It is also

[34] Text in italic are quotations from standards and regulations. Text not in italic are derived from standards and regulations.

important to consider unwanted input. For example, failure of the primary well barrier might result in high pressure on a secondary well barrier.

2) Wanted and unwanted output
   a) *The acceptable leak rate shall be zero, unless specified. In situations where the function of the well barrier is weakened, but are still acceptable should be defined (NORSOK D-010).* A specific leak rate criterion[35] for the SCSSV and the SCASSV[36] (Surface controlled annular safety valve) is specified in NORSOK D-010, which originates from API RP 14B. API RP 14B defines an acceptable leak rate, which is 15 SCF/min (~0.42 SCM/min) for gas, and 400cm^3/min for liquids[37].
3) Boundary conditions
   a) Two well barriers shall be available during all well activities and operations (NORSOK D-010 and industry practice). In addition NORSOK D-010 states that "*No single failure shall lead to uncontrolled outflow from the borehole/well to the external environment".*
   b) *SCSSV and SCASSV valves should be placed minimum 50 m below seabed (NORSOK D-010).* The setting depth requirement makes the SCSSV less vulnerable to external events. The setting depths of the SCSSV and the SCASSV are primarily dictated by the pressure and temperature conditions in the well. However, deep-set valves make the primary well barrier less vulnerable to tubing leaks (assuming that the failure rate[38] increases with increasing length).
4) External threats (robustness)
   a) *The well barriers shall be designed, selected and/or constructed such that it can operate competently and withstand the environment for which it may be exposed to over time (NORSOK D-010).* In addition to long term environmental exposure, robustness include the ability to function under all accident conditions,

[35] *Criterion* - A norm, i.e., rule or test against which (the quality of) performance can be measured (Johnson 1980).

[36] SCASSV - Same functionality as SCSSV but installed in annulus between production string and production casing. The valve is normally installed in a packer (Schlumberger, 2005).

[37] Assuming a density of methane gas of 0.7 kg/m^3, this gives a leak rate ~0.3 kg/min or 0.005 kg/s. Assuming a density of oil of 840 kg/m3, this gives a leak rate ~0.34 kg/min or 0.006 kg/s

[38] *Failure rate* - The rate at which failures occur as a function of time.

and events like earthquake, fire, loss of energy supply, sabotage, falling loads, etc. should also be assessed.

5) System (availability)
    a) *The primary and secondary well barriers shall, to the extent possible, be independent of each other (NORSOK D-010).* Independence makes the system more robust, and also increases the availability.
    b) A SIL requirement to the well shut-in function should be established. It should also be controlled that the well shut-in function is able to fulfill this requirement in the well life (see section 2.3, page 32).
6) Support
    a) In the Facilities regulations (PSA, 2001b), section 47 it is stated that "*Well barriers shall be designed so that their performance can be verified.*" According to NORSOK D-010 "*The physical location and the integrity status of the well barrier shall be known at all times".* Verification of the performance of well barriers may be based on functional testing and condition monitoring (e.g., monitoring of changes in pressure). More specific, NORSOK D-010 states the following requirements to well barriers:
        i) *A well barrier shall be leak tested, function tested or verified by other methods (NORSOK D-010).* NORSOK D-010 also requires that "*The SCSSV, the production tree valves and the annulus valves shall be leak tested regularly".* Common practice on the NCS is to test valves every 6 months.
        ii) *The pressure in all accessible annuli (A, B and/or C annuli) shall be monitored and maintained within minimum and maximum pressure range limits (NORSOK D-010).*

The requirements listed reflect the requirements in Norway. The list is not complete when looking at a specific well. However, the categorization above gives an overview of the most important requirements and how the requirements influence the system. The categorization may also be used to include additional requirements from other countries or from internal operator guidelines.

For a specific well situation the system and interfaces must be assessed before a well risk assessment is performed.

4.2 Well barrier failures

BS 4778 defines availability as "The ability of an item[39] under combined aspects of its reliability[40], maintainability[41], and maintenance support to perform its required function[42] at a stated instant of time or over a stated period of time." Availability is a measure of the ability of a well barrier system to function over time. In this section well barrier failures and well barrier maintenance are discussed in more detail.

Different types of well barrier failures are reviewed and fitted into a common terminology. The IEC 61508 terminology is used as a basis. In IEC 61508 safety critical failures are called dangerous failures, while non-safety critical failures are called safe failures. Only dangerous failures influence safety and are included in the discussion. Typical dangerous failures are failure to close the SCSSV, leak through production packer, etc. An example of a safe failure is a failure to open a SCSSV. This failure will not affect the ability to prevent a blowout or to shut-in the well when demanded.

4.2.1 Failure definition

A failure is usually described by a failure mode. IEC 50(191) defines a failure mode as one of the possible states of a faulty item, for a given required function. For example, one SCSSV function may be expressed as *close SCSSV*. A loss of this function may therefore be defined as the failure mode *Failure to close SCSSV*.

According to IEC50(191) failure is the *event* when a required function is terminated (exceeding the acceptable limits), while *fault is "*the state of an item characterized by inability to perform a required function, excluding the inability during preventive

[39] *Item* - Any part, component, device, subsystem, functional unit, equipment or system that can be individually considered (IEC 50(191)).

[40] *Reliability* - The ability of an item to perform a required function, under given environmental and operational conditions, and for a stated period of time (ISO 8402).

[41] *Maintainability* - The ability of an item, under stated conditions of use, to be retained in, or restored to, a state in which it can perform its required functions, when maintenance is performed under stated conditions and using prescribed procedures and resources (BS 4778).

[42] *Required function* - A function or combination of functions, of an entity, which is considered necessary to provide a given service (IEC 50 (191).

maintenance[43] or other planned actions, or due to lack of external resources." A fault is hence a state resulting from a failure.

According to IEC 50(191) an *error* is a "discrepancy between a computed, observed or measures value or condition and the true, specified or theoretically correct value or condition." An error is (yet) not a failure because it is within the acceptable limits of deviation from the desired performance (target value). The relationship between these terms is illustrated in Figure 14.

A clear distinction between error and failure is important for the planning of corrective measures. For example, an error may call for increased monitoring, while a failure results in a corrective measure, e.g., a workover.

Each WBE has different functions, and therefore different acceptable deviations (or performance criteria[44]). Examples of the relation between WBE functions, failure modes, and acceptable deviations are given in Table 5. The table illustrates that active WBEs change state and therefore the acceptable deviation for the state transition must be defined in addition to the acceptable deviation in the passive state (leak rate in closed position).

For example, the target value for an SCSSV in closed position is no leak. However, a certain leak rate is accepted (API RP 14B), and this leak rate is the acceptable deviation from the target value. If the leak rate exceeds this limit, the valve is regarded to be in a fault (state). The standard was initiated after an incident where a jet fire took off on a x-mas tree. The incident was used to model jet fire heat exposure to neighboring x-mas trees. The maximum allowable leakage rate was then estimated from how much heat load the neighboring trees could carry. The acceptance criteria stated in the API RP 14B does not reflect that risk levels vary among installations and well types (e.g., platform vs. subsea wells, injectors vs. producers, etc.).

[43] *Preventive maintenance* - The maintenance carried out at predetermined intervals or corresponding to prescribed criteria and intended to reduce the probability of failure or performance degradation of an item (BS 4778)

[44] *Performance criteria* - Operational standards for use in determining effectiveness or efficiency (Tarrants 1980)

The experience from reliability data collection work in the UK is that the leak rate criterion in API RP 14B is sometimes used as a leak rate criterion across other well barrier elements.

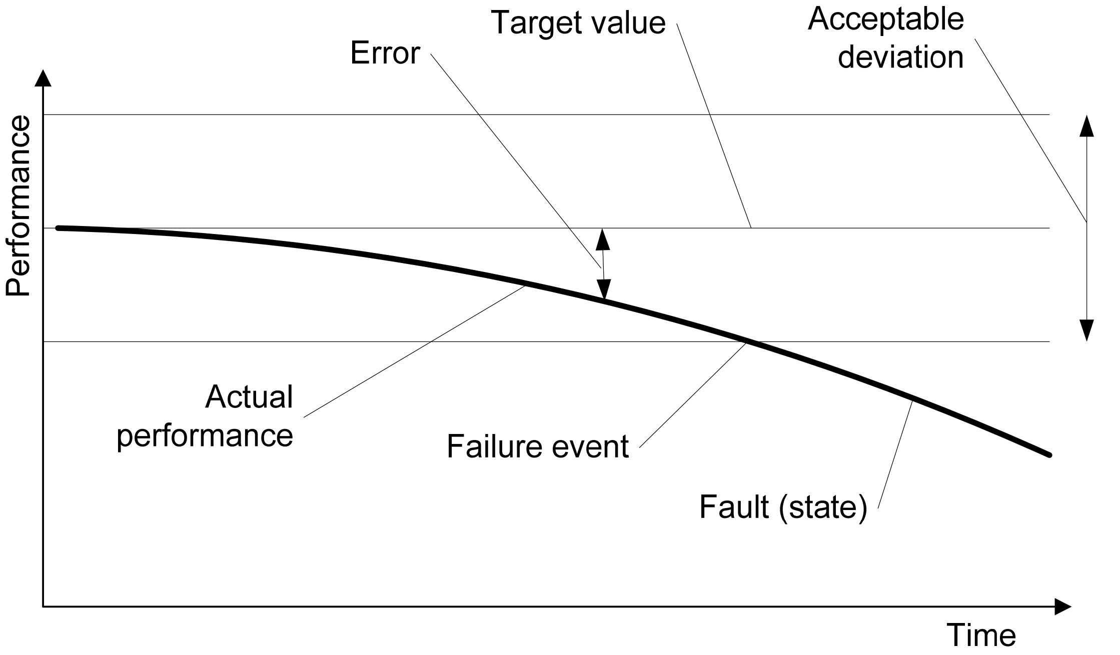


Figure 14 **Illustration of the difference between failure, fault and error (adapted from Rausand and Høyland, 2004)**

Table 5 **WBE functions and corresponding failures**

WBE type	Function	Failure mode	Acceptable deviation
Passive	Contain fluid, i.e. prevent leak across WBE	Leak across WBE	Leak rate (kg/s)
Active	Close WBE	Fail to close WBE	Closure time (s)
	Prevent leak (in closed position)	WBE leak in closed position	Leak rate (kg/s)

4.2.2 Well barrier element failure classification

A failure may result from different failure causes[45] (reasons why a component fails). A clear understanding of the failure cause is important to select countermeasures to avoid failures.

Random hardware and systematic failures

According to IEC 61508 a failure of a safety-related system can be classified as either a *random hardware* or a *systematic* failure. A random hardware failure is a "failure, occurring at a random time." A systematic failure is a "failure related in a deterministic way to a certain cause, which can only be eliminated by a modification[46] of the design or the manufacturing process, operational procedures, documentation or other relevant factors". A systematic failure may be interpreted as a failure of the component to fulfill the intended function without any physical degradation. Systematic failures may be introduced in the entire life cycle of the component (design, operation, maintenance). In the thesis it is assumed that systematic failures remain undetected, and results in a "baseline" unavailability. This baseline unavailability is not quantified explicitly in the thesis. This approach is in line with IEC 61508, which states that random hardware failures should be quantified, while systematic failures should not.

Random hardware failures occur because a physical property influences on the WBE function. Random hardware failures may result from various reasons. Typical reasons are physical loads (e.g., pressure, temperature), human errors (e.g., scratches during installation), and design factors (e.g., choice of materials). Random hardware failures may also occur as a result of s*tress* failures, which are failures that lay outside the component design limit.

Dependent failures

So far single independent WBE failures have been discussed. Failures in a system may also be dependent and result in common cause failures (CCF) or cascading failures. A

[45] *Failure cause* - The circumstances during design, manufacture, or use which have led to a failure (IEC 50(191)).

[46] *Modification* - The combination of all technical and administrative actions intended to change an item (IEC 50(191)).

common cause event is, according to NUREG/CR-6268, a *"dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause"*. NASA (2002) state that a common design or material deficiency, a common installation error, a common maintenance error, or a common harsh environment may cause common cause failures.

According to Rausand and Høyland (2004) cascading failures are multiple failures initiated by the failure of one component in the system that result in a chain reaction or domino effect. Malfunction of a component may, for example, lead to a more hostile working environment for the other components through increased pressure, higher temperature, and so on. For a well barrier system, failure of one of the WBEs in the primary well barrier may result in failure of one of the WBEs in the secondary well barrier if, for example, the pressure contained by the primary well barrier is higher than the secondary well barrier design limit.

The relationship between independent and dependent failures is illustrated in Figure 15. The figure shows that the dependent failures may have a significant effect on the well barrier system.

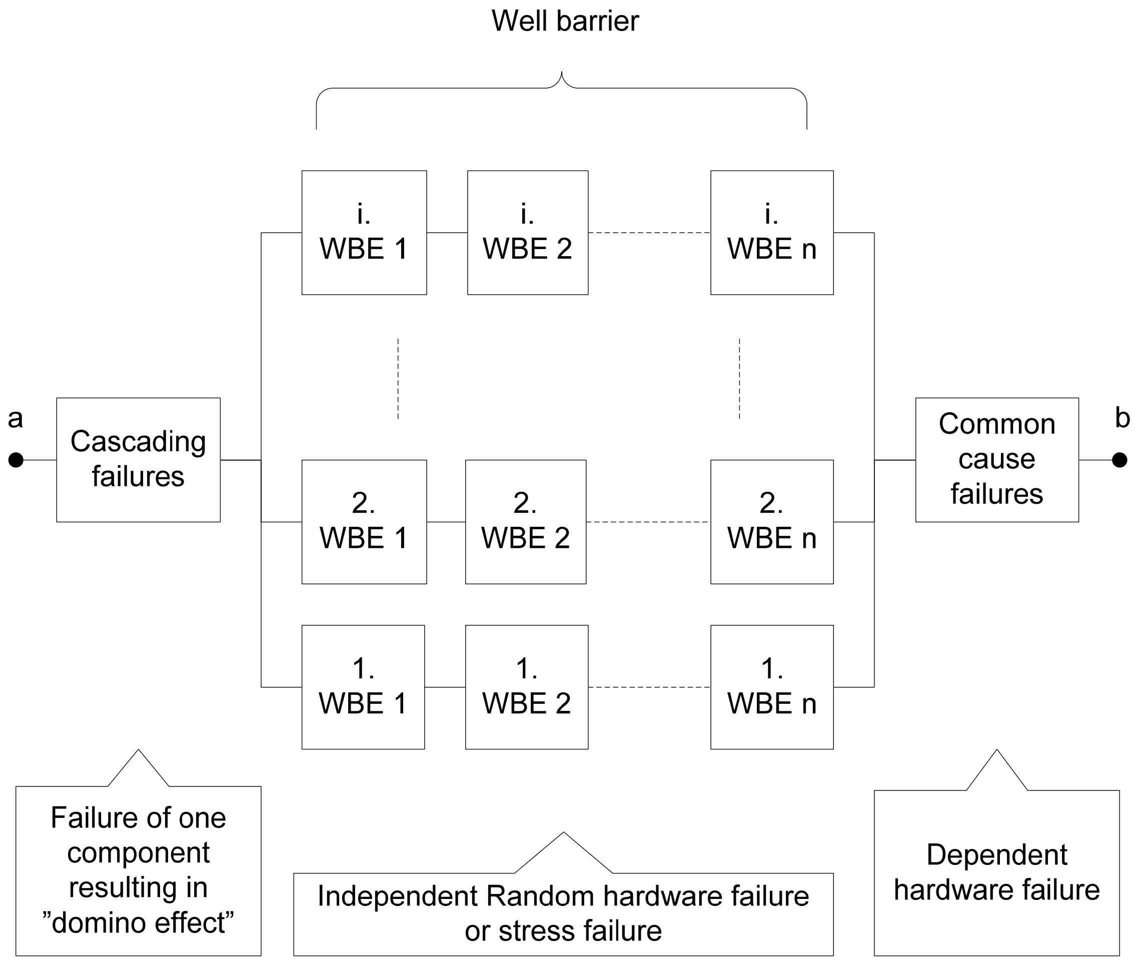

Well barrier
a
Cascading failures
i. WBE 1
i. WBE 2
i. WBE n
2. WBE 1
2. WBE 2
2. WBE n
1. WBE 1
1. WBE 2
1. WBE n
Common cause failures
b
Failure of one component resulting in ”domino effect”
Independent Random hardware failure or stress failure
Dependent hardware failure

Figure 15 Relationship between independent and dependent well barrier failures

Detected and undetected failures

Common to all types of WBEs is that they "*shall be designed so that their performance can be verified (PSA, 2001b).* IEC 61508 differs between detected and undetected failures. Detected failures are normally detected immediately without any specific testing, while undetected failures (also called hidden failures[47]) can only be revealed through functional testing. For active WBEs (SCSSV, PMV, and PWV) the dangerous hardware failures are undetected failures, while the safe failures are detected failures (a spurious closure of the SCSSV will be detected immediately). For active WBEs the

[47] *Hidden failure* - A failure not evident to crew or operator during the performance of normal duties (MIL-STD-2173(AS)).

dangerous hardware failures may occur at any time in the interval between consecutive tests. The failure is, however, not manifested and discovered until a test is carried out or the valve is to be closed because of some operational reasons. Tests of active WBEs are carried out at regular intervals. The length of the test interval varies from installation to installation, but is usually one, three or six months. The test interval is partly decided by the authorities.

For passive WBEs, the dangerous hardware failures may be detected by continuous monitoring (e.g., pressure and temperature) or by monitoring/readings at regular intervals.

Restoration

When a WBE failure is detected the critical time with respect to safety is the time from the failure is detected until the well is brought to a safe state. For some of the restoration time it is known that the failure is present but the state is still dangerous, while after some time the WBE is still not repaired but the well is brought to an equally safe or safer state than before the WBE failed. Hence, the dangerous repair time is usually much lower than the actual time used to restore the well barrier.

If assuming that once the well is brought to a safe state, the remaining repair time is equally safe or safer than before the WBE failure was detected, this means that the critical time to include in the availability calculations is the time from a failure is detected until the well is brought to a safe state. The mean value of this time is called the Mean Dangerous Waiting Time (MDWT) in this thesis

Well barriers can be repaired by various means and operations (see section 2.1.2, page 24). For a failed WBE the most common repair action is to perform a workover and replace the failed component. This type of repair is both costly and time consuming. Sometimes a through-tubing workover may be sufficient to restore the well barrier. If the failure is caused by, e.g., scale build-up it is often possible to inject fresh water, acid or chemicals or alternatively perform milling to clean the well. Wireline tools utilizing ultrasound are also available to remove scale.

The MDWT may vary considerably depending on the type of well and installation. On surface wells repair of the x-mas three may be performed on the same shift. Repair of a well completion on a surface well takes longer time but the well may be brought to a safe state by setting, e.g., a wireline plug. If a workover rig is installed on the installation, a surface well wireline operation may be performed within days. On subsea wells the repair involves contracting of a vessel. The repair of subsea wells will therefore take significantly longer time (from weeks to months). However, a subsea well may also be brought to a safe(r) state when a failure is detected. It may, e.g., be possible to close the well on the x-mas tree. Whether this state is safe or not depends on the distance to the neighboring platform, the additional valves available on the subsea template, etc. The risk of external damage of the x-mas tree must also be conidered. A compensating measure may be to reduce the vessel activity above the wellhead.

Failure causes

The classification into hardware and systematic failures, dependent and independent, and restoration types are used to discuss different hardware failure causes and failure mechanisms. The failure classification is discussed in more detail in Paper 5. The paper also describes a method that uses the failure classification to calculate the availability of SCSSVs. The following broad failure cause categories are suggested:

- Hardware failures dependent on standby period. Moving parts relative to each other may reduce the effect of some failure mechanisms[48], and therefore increased testing may improve the reliability of the component.
- Hardware failures dependent on demands/tests. The effect of some failure mechanisms may be increased by testing (e.g., wear-out and hydrate formation).
- Hardware failures independent of WBE operation. The failure mechanisms acting on the WBE are unaffected by the operation of the valve.
- Stress failures (outside design limit) induced on the valve. Stress outside the design envelope of the valve result in an immediate failure (shock failure).

[48] *Failure mechanism* - The physical, chemical or other process, which has led to a failure (IEC 50(191)).

All four categories apply to active WBEs, while only *stress* and *hardware failures independent of WBE operation* applies to passive WBEs, which not is function tested at regular intervals (passive WBEs do not change state).

Hardware failures that can be prevented by exercising the WBE are typically mechanisms influenced by loads like scale, debris, sand build up or sticking seals. Hardware failures dependent on testing or actual demands are typically wear out effects on the dynamic surfaces (e.g. because of "slamming" of the valve or friction between moving parts). Failure mechanisms not influenced by testing are ageing mechanisms (propagation of scratches, corrosion, etc). Stress failures typically occur because of a wireline operation where the wireline tool damages the WBE or a well pressure exceeding the WBE design limit. The total failure rate of a WBE will be a function of all these mechanisms.

Figure 16 summarizes the discussion above and illustrates that different strategies must be used to address different types of failure causes. The figure also includes a division into systematic failures that occur in the design or operational phase. Even if systematic failures are not quantified they may be equally important, in particular for redundant systems. Hence, both hardware and systematic failures must be focused on when designing and operating the well.

Within the industry the effect of testing is discussed. Some operators argue not to test the active WBEs (in particular the SCSSV). The argument is that testing has a wear out effect or may lead to hydrate formation during testing. However, the most operators have the opinion that the valve should be actuated in order for the valve to function appropriately and to reveal dangerous undetected failures. Even if the hardware failures for active WBEs may be dependent on the operation (length of test interval/number or tests) all dangerous hardware failures will be detected during test. Hence, the assumption that no testing will increase the overall availability requires a large proportion of the failures to be caused by the testing itself. For most active WBEs increased testing will result in increased availability.

In relation to the suggested failure classification it is assumed that the hardware failures influenced by demands/tests or standby period and stress failures are more prone to dependent failures than the hardware failures not influenced by the functional tests and demands, or stress outside the design envelope.

The findings reported in Molnes and Strand (1999) underline the importance of controlling different types of failures. In this report a failure is categorized as an "item failure" when it has been confirmed that the cause of the failure lies within the item itself. If the failure is confirmed as being caused by another item, the failure is classified as "non-item failure." For example, the observed TR-SCSSV[49] distribution between "item failures" and "non-item failures" found in Molnes and Strand (1999) is 23% and 47%, respectively (remaining failures categorized as "unknown"). This distribution shows that many failures are reported as failures not directly caused by the valve itself. Non-item failure causes are therefore important to consider when designing and operating a well. The data shows that hydrates, asphaltenes, erosion and scale in addition to through-tubing well operations are contributors to the non-item failures. Such non-item failures also contribute to dependent failures.

In the design phase possible failure causes and loads that may lead to dependent or independent failures should be thoroughly assessed with the objective to:

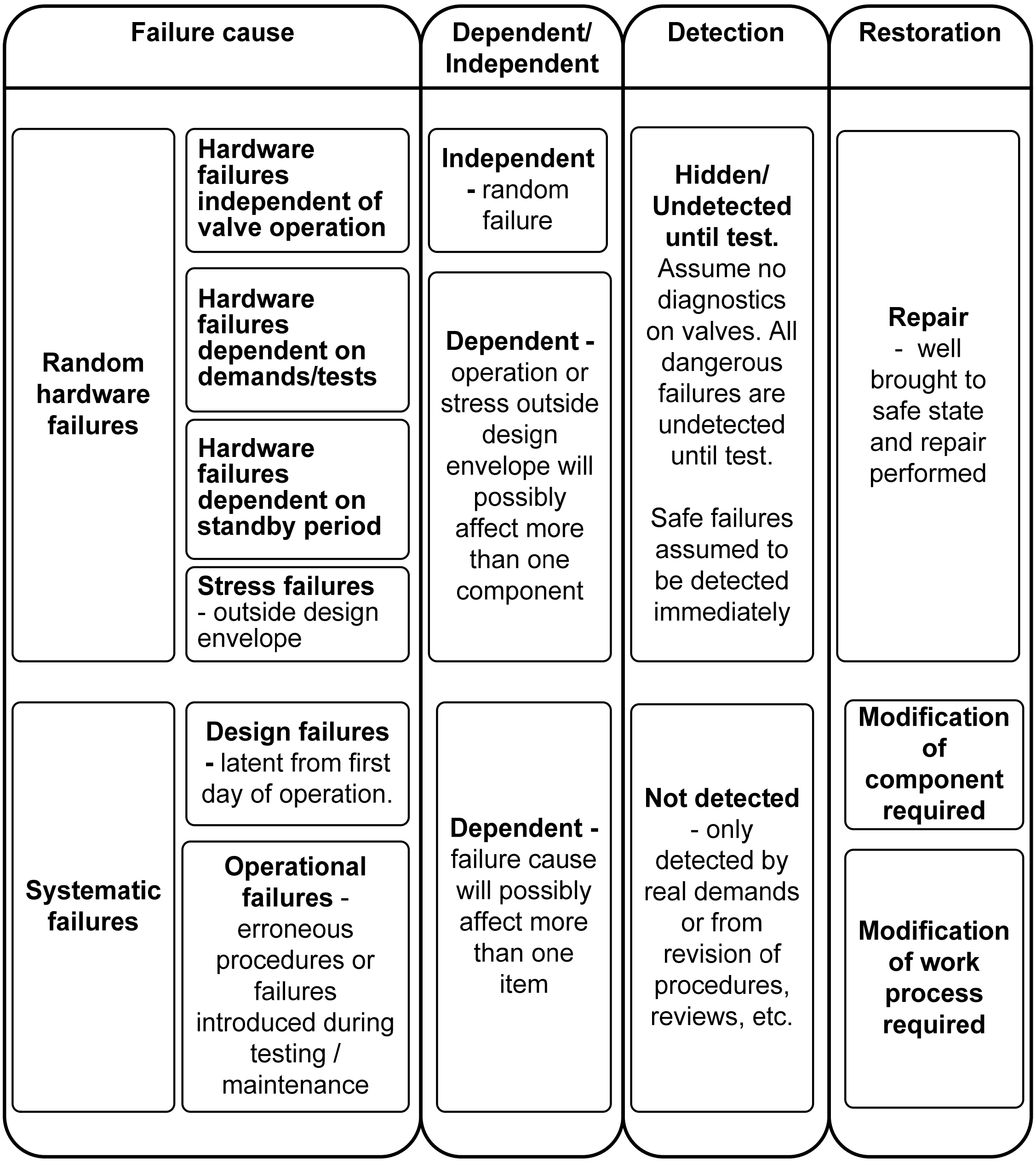
1. Reduce the overall number of hardware and systematic failures.
2. Maximize the independence of the components to avoid dependent failures (CCF).
3. Minimize the likelihood of cascading failures.

The design phase should result in an understanding of the optimal design and operation of the well to avoid failures. In the design phase it is also important to study foreseen changes in well conditions in the entire well life cycle. Molnes and Strand (1999) describe the experience from Statoil's Gullfaks field, and states; "This field is experiencing an increasing number of failures, primarily caused by scale build-up with frequent remedial action taken in terms of chemical (acid washing) and mechanical (brushing) scale removal."

In the operational phase, it should be controlled that the assumptions made in the design phase still are valid, that unforeseen failure causes do not occur, and that risk

[49] *TR-SCSSV* - Tubing Retrievable Surface controlled subsurface safety valve

related to cascading failures is controlled (e.g., caused by changes in pressure regimes or degradation of components).



Failure cause		Dependent/ Independent	Detection	Restoration
Random hardware failures	**Hardware failures independent of valve operation**	**Independent -** random failure	**Hidden/ Undetected until test.** Assume no diagnostics on valves. All dangerous failures are undetected until test. Safe failures assumed to be detected immediately	**Repair** - well brought to safe state and repair performed
	Hardware failures dependent on demands/tests	**Dependent -** operation or stress outside design envelope will possibly affect more than one component		
	Hardware failures dependent on standby period			
	Stress failures - outside design envelope			
Systematic failures	**Design failures -** latent from first day of operation.	**Dependent -** failure cause will possibly affect more than one item	**Not detected** - only detected by real demands or from revision of procedures, reviews, etc.	**Modification of component required**
	Operational failures - erroneous procedures or failures introduced during testing / maintenance			**Modification of work process required**

Figure 16 Failure classification scheme

4.3 Well barrier element reliability data

Well component reliability data are used as input to the quantitative risk analysis performed on well system level. The importance of well component reliability data has been recognized in the oil industry. Extensive data collection projects are therefore established and have been running for many years.

The well barrier system availability is a function of the configuration of the well barriers, and the reliability and restoration of the WBEs that constitute the well barriers. It is therefore necessary to use reliability data on WBE level as input to the reliability analyses.

Input reliability data[50] of high quality is essential to any reliability analysis. For example, Holand (1997) describes a case with two tension leg platforms (TLPs) in the Norwegian sector. The installations are in principle similar. Risk assessments were carried out for both installations to decide whether or not fire insulation of the risers was required to keep the risk within the acceptable levels. The objective in both analyses was to assess the blowout risk. Two different consultants performed the analyses. For one of the TLPs it was selected to include fire insulation and for the other not. The total investment cost was reduced with at least 120 million US dollars for the TLP without fire insulation (Molnes, 1995). This TLP was installed two years later than the first one. The availability of updated SCSSV reliability data was the main reason for arriving at the different conclusions, i.e., the updated reliability data showed that the SCSSV reliability had improved compared with previous experience.

The basis for the discussion of input reliability data is illustrated in Figure 17. The figure illustrates the interfaces to be considered when establishing input reliability data for a specific well barrier system analysis. This section includes a discussion of generic failure rate estimates provided from publicly available databases or handbooks (i.e., support). Such reliability data must always be assessed related to the interfaces indicated in Figure 17 before use in specific application. The assessment should include aspects like well fluids, pressure limits, acceptable leak rates, common cause failures, and cascading failures (see section 4.2, page 56).

[50] *Reliability data* - Reliability data is meant to include data for reliability, maintainability and maintenance supportability (NORSOK O-CR-001).

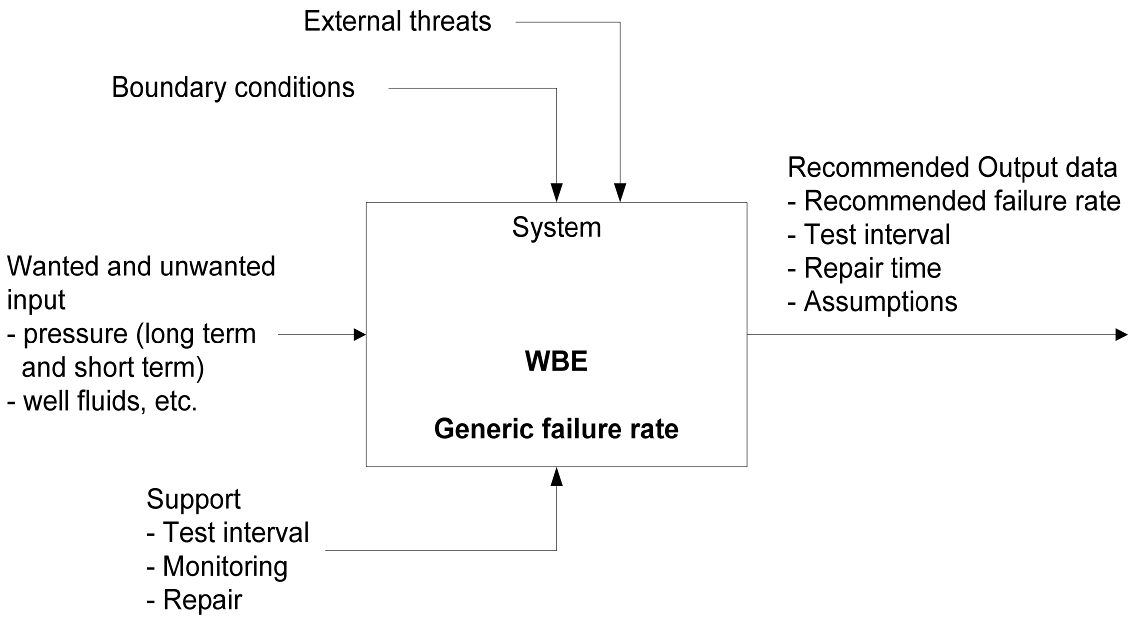


Figure 17 WBE failure data framework

For well systems there are three main databases available:

- The *WellMaster* (2006) project has run a more or less continuous data collection since the Bravo blowout on the Ekofisk field in the North Sea in 1977. The database is accessible only for the oil companies sponsoring the project, but some reports with aggregated data have been published. The most recent publicly available data are Molnes and Strand (1999). The database covers the well completion and the casing program.
- The *SubseaMaster* (2006) project collects failure data on subsea production systems, including the subsea x-mas tree. The project was started in 1999. The database is accessible only for the oil companies sponsoring the project No publicly available data yet.
- The *OREDA* (2002) project collects failure data on offshore subsea and topside equipment. The project is sponsored by several oil companies. Publicly available information is presented in the OREDA handbook (OREDA, 2002).

In addition to well system components, the well shut-in function consists of the process control system (control logic and solenoids), which actuate the safety valves in the well (see section 2.3, page 32). The following reliability data collection projects are identified that may contribute with input data:

- *Reliability Data for Control and Safety Systems (Albrechtsen and Hokstad, 2002).* The report presents reliability data/for computer-based process safety systems (i.e, SIS). The report includes both random hardware and systematic failure data. The report is based on review of oil company data files, workshops with technical experts, and questionnaires.
- *OLF (2004).* The guideline presents recommended reliability data for SIS on offshore installations. Values for well system components are also presented.

The reliability data collection projects above present reliability data for random hardware as a failure rate, where the failure rate is presented as an average frequency of failure (i.e., the number of failures per unit of time). The data are assumed to represent independent random hardware failures. In addition, Albrechtsen and Hokstad (2002) and OLF (2004) present values for systematic failures, and for dependent failures (the common cause contribution). The dependent and systematic failures values are based on expert judgment and not on reported failures in databases. The difficulty with establishing dependent and systematic failure values are discussed in more detail in paper 3.

Table 6 presents a comparison of components covered in the databases. The components are divided into input devices (senors, transmitters), control logic units and output devices/WBEs (valves and passive WBEs). As seen only WellMaster (2006) includes the well completion and casing program.

Table 6 Well integrity and well shut-in function components covered in different reliability databases

Project and industry sector	Components		
	Input devices	Control logic Units	WBEs (Output devices)
OREDA (2002)	Fire/gas detectors, pressure senors	Control logic units (subsea and topside) and pilot valves	x-mas tree valves and passive x-mas tree components
Reliability Data for Control and Safety Systems (Albrechtsen and Hokstad, 2002) and OLF (2004)	Same as above	Same as above	PMV, and PWV and SCSSV
WellMaster (2006)	Downhole cauges (pressure and/or temperature)	Not included	Well completion components (including SCSSV and SCASSV and casing program
SubseaMaster (2006)	Pressure and temperature sensors	Subsea control logic	x-mas tree valves and passive x-mas tree components

Table 7 presents data for important WBEs in a well. The table includes the recommended reliability data in OLF (2004) and in Molnes and Strand (1999). The reliability data is only included for illustrative purposes and should not be regarded as recommended values. To perform a quantitative analysis a more detailed assessment of well component reliability data must be performed (see discussion in section 5.2, page 77). Table 7 includes components from the reservoir through the tubing string and the x-mas tree production bore. In blowout risk assessments the leak paths via the annuli must be included also (e.g., casing and annuli access valve failures).

Functional tests of active WBEs reveal random hardware failures but will not differentiate between independent and common cause failures. Consequently, the reliability databases will not make this distinction. There are several methods available for modeling CCF failures. The most common in use is the β-factor method. The β-factor is a measure of the fraction of common cause failures. For analysis purposes this fraction must be analyzed through use of, e.g., expert judgment. Many sources suggest ranges for the value of β. IEC 61508-6 describes a separate methodology to arrive at a specific β, where the β range from 1 to 10% for final elements (valves). Table 7 also includes values for the common cause factor, β. The β–factor model is discussed in section 5.3.

Table 7 Typical input data for WBE and well shut-in function components

Components and dangerous hardware failure modes[1]	Well safety function[4]	Generic failure rate (failures per 10^6 hours)[5]	Common cause, β[6]
Topside PMV/PWV – FTC[1] or LCP[2]	WI/WS	0.8	2%
Subsea PMV/PWV - FTC or LCP[1]	WI/WS	0.1	2%
SCSSV – FTC or LCP	WI/WS	2.5 *(2.2 -2.5)*	-
Production packer – LTA[1]	WI	*0.2*	-
Seal Assembly (conventional) – LTA	WI	*0.5*	-
Tubing – LTA	WI	*0.4 (per km)*[3]	-
Programmable safety system/logic (ESD) – FTO[1]	WS	1	1%
Solenoid/pilot valve – FTO	WS	0.9	2% - 10%[2]

1) FTC – Fail to close, LCP – Leakage in closed position, FTO- Fail to operate, LTA – Leak to annulus
2) 10% for pilot valves on same valve. 2% otherwise
3) The failure rate must be multiplied with length of tubing
4) WI – Well integrity, WS – well shut-in function
5) Numbers in *italic* from Molnes and Strand (1999). Numbers not in italic from OLF (2004)
6) β-factor model used to model common cause failures

Table 7 illustrates that the difference between passive and active WBEs quite commonly is two to three orders of magnitude. This difference is natural because active WBEs involve many parts, where different failure mechanisms (erosion, chemical and temperature effects, etc.) act on each part.

The failure rate may even for "simple" components be sensitive to the well conditions. Molnes and Strand (1999) report a failure rate ranging from 0.1 to 0.7 failures per 10^6 hours per km for water injectors and gas/condensate tubing, respectively.

There are several challenges and general concerns regarding reliability databases. Such limitations are thoroughly discussed by Rausand and Høyland (2004), by Cooke (1996), and by Cooke and Bedford(2002). A main concern is that to apply the data in the databases subjective judgments have to be made. In most cases acceptable limits/deviations (see section 4.2.1, page 56) are not defined and/or it is not possible to measure the degree of failure. Normally, the databases include reliability data from different sources (operators and installations) and the criteria for failure reporting may vary significantly. This is a problem difficult to overcome since the databases covers equipment used in different applications (safety, control, auxiliary) or operators with different acceptable limits for the same application. Therefore, the databases should include a description of the boundary conditions and a definition of the acceptable limits to the greatest possible extent.

The variation in acceptable limits may be less for some types of equipment. The acceptable leak rate for SCSSVs stated in API RP 14B is widely accepted as an acceptable limit in the industry, and this is also a benefit to the uniformity of the SCSSV reliability data found in the WellMaster database (WellMaster,2006).

The reliability databases provide estimates of a failure rate[51] or a mean time to failure (MTTF[52]) for specific component types. For analysis purposes it is assumed that the reliability data fit the exponential distribution[53], i.e., a constant failure rate. However, it is possible to perform life data analysis to obtain information about the life distribution for a component. Life data analysis is, e.g., used to determine if a Weibull distribution fit to the failure data, i.e., an increasing failure rate with time. Life data testing is described in Rausand and Høyland (2004).

For new components (or an existing component in a new application or environment), where the existing failure data are inadequate it is possible to perform life testing to determine the life distribution. Life testing is expensive and normally performed for products produced in large quantities, like consumer electronics. Life testing is therefore seldom performed on well equipment. Life testing is discussed in Rausand and Høyland (2004).

In lack of reliability data or as a supplement it is also possible to perform expert judgment to arrive at a recommended failure rate. Expert judgment methods are presented in Øien (1998).

[51] *Failure rate* - The rate at which failures occur as a function of time.

[52] *MTTF* - Let T denote the time to failure of an item. The mean time to failure is the mean (expected) value of *T*

[53] Consider a random variable *X*. the distribution function of *X* is

$F_X(x) = P_r(X \leq x)$ (Rausand and Høyland 2004)

4.4 Barrier diagrams

Barrier diagrams are used in static barrier situations to illustrate well barrier systems. Barrier diagrams have been used in various forms for some 10-15 years to assist in well risk analysis.

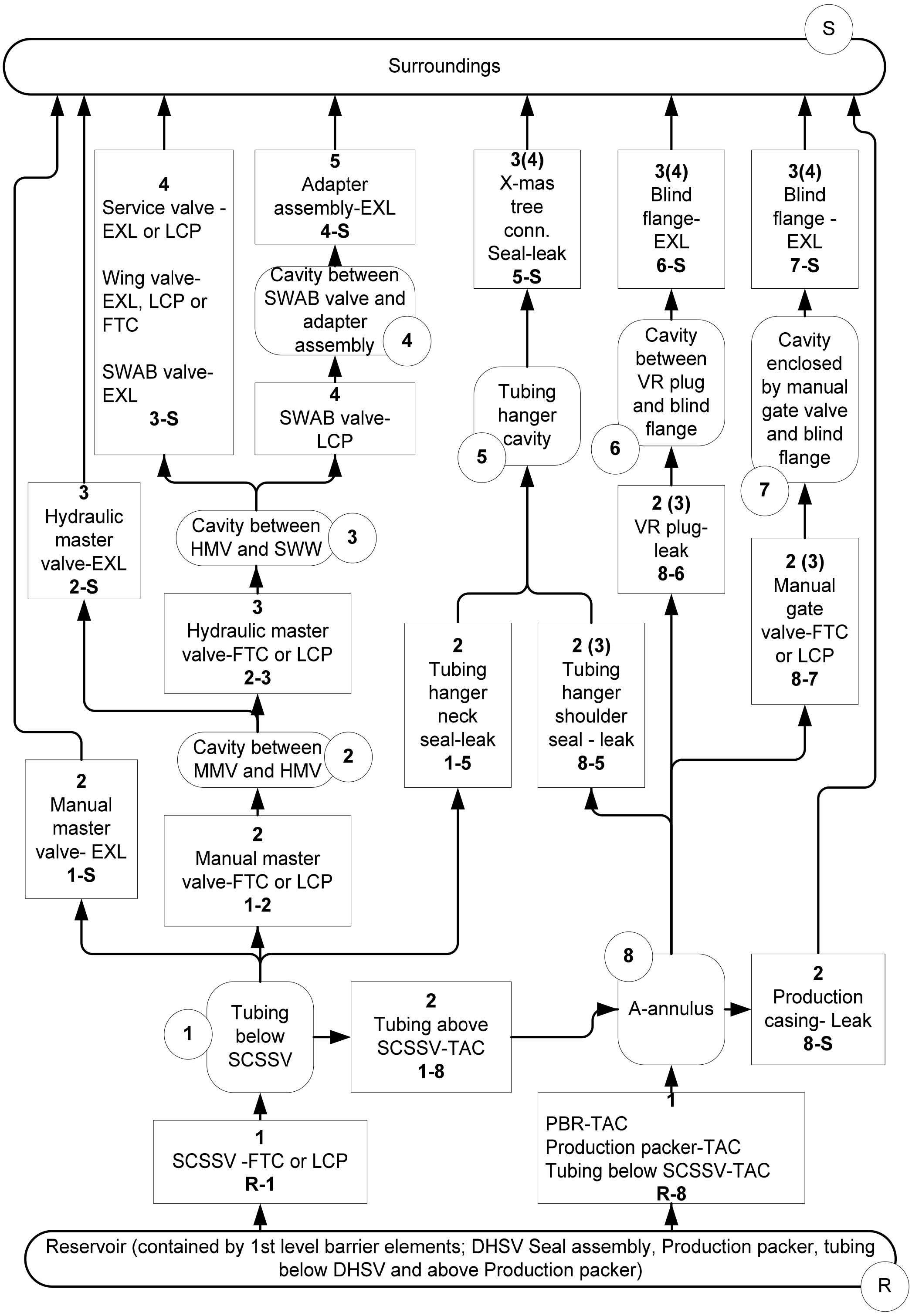
Barrier diagrams have been constructed in a variety of forms but no formal construction rules have been presented. Therefore, a method for constructing barrier diagrams is established. The method is described in Paper 4. The construction rules facilitate the possibility to make simple quantitative calculations directly from the barrier diagram. Alternatively, the barrier diagram construction rules assist in "automatic" transition to a Fault Tree Analysis (FTA) structure.

An example barrier diagram is shown in Figure 18. The basis for the barrier diagram is the well illustrated in Figure 3, on page 22. The construction of the barrier diagram and further transfer of the diagram into quantitative models or construction of fault trees are described in Paper 4, and only a brief description of the barrier diagram symbols are given here:

- A rounded rectangle illustrates a cavity (or the reservoir) enveloped by well components. Top and bottom rounded rectangle illustrate the reservoir and surroundings, respectively. The lines between the cavities illustrate possible flow paths from one cavity to another. The arrows describe the flow direction.
- In each line a rectangle is included. The rectangle includes the well component failures (components not qualified as a WBE may also be included) that can result in flow from one cavity to another.
  - The text part describes the well components failure modes.
  - The upper number describes the number of well components in each flow path. For example, the SCSSV, the seal assembly, the production packer, and the tubing string below the SCSSV are the well components closest to the reservoir (indicated with **1** in the rectangle).
  - The lower number describes the start and en point "cavity" if the well component (s) fails.

Benefits of the established barrier diagram construction rules are:

- Possible flow paths from the reservoir to the surroundings are easily identified.
- Number of well components in each flow path is easily identified.
- The well barrier system is easily communicated to both well design and reliability personnel.
- Easy to perform "what-if" analysis, e.g., what is the consequence if the tubing below the SCSSV fails.
- The cavities can be used to identify the boundary conditions on both sides of the well components (pressure, fluids, temperature, etc.).
- Simple quantitative reliability analysis may be performed directly from the barrier diagram.
- Easy and consistent transfer of the barrier diagram to a FTA. Rules for transfer to FTA are presented in paper 4.


S
Surroundings
4
Service valve - EXL or LCP
Wing valve- EXL, LCP or FTC
SWAB valve- EXL
3-S
5
Adapter assembly-EXL
4-S
Cavity between SWAB valve and adapter assembly
4
4
SWAB valve- LCP
3(4)
X-mas tree conn. Seal-leak
5-S
3(4)
Blind flange- EXL
6-S
3(4)
Blind flange - EXL
7-S
Tubing hanger cavity
5
Cavity between VR plug and blind flange
6
Cavity enclosed by manual gate valve and blind flange
7
3
Hydraulic master valve-EXL
2-S
Cavity between HMV and SWW
3
3
Hydraulic master valve-FTC or LCP
2-3
2 (3)
VR plug- leak
8-6
2 (3)
Manual gate valve-FTC or LCP
8-7
2
Tubing hanger neck seal-leak
1-5
2 (3)
Tubing hanger shoulder seal - leak
8-5
Cavity between MMV and HMV
2
2
Manual master valve- EXL
1-S
2
Manual master valve-FTC or LCP
1-2
8
A-annulus
2
Production casing- Leak
8-S
1
Tubing below SCSSV
2
Tubing above SCSSV-TAC
1-8
1
SCSSV -FTC or LCP
R-1
1
PBR-TAC
Production packer-TAC
Tubing below SCSSV-TAC
R-8
Reservoir (contained by 1st level barrier elements; DHSV Seal assembly, Production packer, tubing below DHSV and above Production packer)
R

FTC-Fail to close
LCP-Leakage in closed position
EXL-External leakage
INL-Internal leakage
TAC-Tubing to annulus leakage

Figure 18 Example barrier diagram

5. Well system reliability analysis

Earlier in the thesis it is concluded that the engineers on the well system level primarily can influence 1) the blowout and/or well release frequency and 2) the probability of failure on demand (PFD) for the well shut-in function. In this chapter the two reliability measures are presented in more detail, together with suitable analytic method.

5.1 Reliability analysis and risk analysis

A quantitative risk analysis is based on various models and risk input data. Both the models and the data may be incomplete. It is essential that the analysis reflects the real risk picture, and that it is possible to identify and rank major risk contributors.

In chapter 2 it was concluded that in the design phase, the risk analyses on the well system level primarily are used to:

1. Demonstrate that the blowout frequency from a specific well is acceptable.
2. Verify through quantitative analysis that the required probability of failure on demand (PFD), stated through the SIL requirement, can be achieved for the well shut-in function.

The analytical methods discussed in this chapter are methods used to provide quantitative measures for frequency or probability, and the common term used is reliability analysis.

5.2 Basic component types used in reliability analysis

As discussed in section 4.2.2, only dangerous hardware failures are included in the thesis. Four basic well component types are discussed:

- Test interval components

- Repairable components
- Non-repairable components
- On demand components

Test interval

Test interval components are tested periodically with test interval τ. A failure may occur anywhere in the test interval. For such components dangerous hardware failures may be further split into (Hokstad and Corneliussen, 2003):

- *Dangerous Undetected (DU).* Dangerous hardware failures not detected by automatic self-tests (i.e. revealed by a functional test or by demands). The reliability parameter is the dangerous undetected failure rate λ_{DU} (expected number of dangerous undetected hardware failures per hour).
- *Dangerous Detected (DD).* Dangerous hardware failures detected by automatic self-test. The reliability parameter used is the failure rate λ_{DD} (expected number of dangerous detected failures per hour).

The dangerous hardware failure rate, λ_D *(*expected number of dangerous hardware failures per hour) will then be $\lambda_D = \lambda_{DU} + \lambda_{DD}$. This situation is typical for many types of detectors, process sensors, and safety valves. The active WBE's (i.e., the SCSSV, the PMV and the PWV) in a well barrier system are such test interval components. The active WBEs do not have any automatic self-test functionality. Some sensors and the logic that actuate the valve have this functionality. Typically, it is assumed that the ESD logic self-test functionality will reveal more than 90% of the dangerous failures. The remaining 10% will be dangerous undetected failures. The ability to detect dangerous hardware failures is called diagnostic coverage.

For active WBEs, a dangerous hardware failure will not be detected until a functional test is carried out or the component is needed. All dangerous hardware WBE failures are therefore undetected, and resulting in $\lambda_D = \lambda_{DU}$.

Following the PDS definition (Hokstad and Corneliussen, 2003), the safety unavailability measure for *random hardware failures* are PFD. The PFD measure is split in two parts:

- PFD_{UK} is the "unknown unavailability" and includes the unavailability due to dangerous undetected failures *during the period when it is not known that the function is unavailable.*
- PFD_K is the "known unavailability". This includes the unavailability due to dangerous hardware failures *during the period when it is known that the function is unavailable.*

Assuming an exponential failure distribution (i.e., constant failure rate), the reliability parameters entered are the failure rate λ_{DU} (expected number of dangerous undetected failures per hour), λ_D (expected number of dangerous hardware failures per hour), the test interval τ (in hours) and the mean dangerous waiting time MDWT (in hours). The (average) probability of a test interval component not functioning may then be calculated by[54]:

$$PFD = PFD_{UK} + PFD_K \approx \frac{\lambda_{DU}\tau}{2} + \lambda_D MDWT$$

Assuming no automatic self-test λ_D=$\lambda_{DU,}$ the PFD is then calculated by:

$$PFD \approx \frac{\lambda_D\tau}{2} + \lambda_D MDWT$$

Repairable components

Repairable components are repaired when a failure occurs. If the dangerous hardware failure rate is denoted λ_D and the mean time to repair MDWT, the probability of the component not functioning at time t, p(t), may be approximated by the formula:

$$p(t) = \frac{MDWT}{MDWT + MTTF}$$

[54] This is a simplified formula and main limitation is that the term $\lambda_{DU} \cdot \tau$ should be small enough to allow $\exp(-\lambda_{DU} \cdot \tau) \approx 1 - \lambda_{DU} \cdot \tau$.

where $MTTF = \frac{1}{\lambda_D}$

Non-repairable

Non-repairable component failures are not detected. If the dangerous hardware failure rate of the component is denoted by λ_D, then the probability that the component is not functioning at time *t*, p(t), may be calculated by (exponential distribution):

$$p(t) = 1 - e^{-\lambda_D t}$$

Note that non-repairable components cannot be defined as part of a well barrier, since the failure of the component cannot be detected. According to NORSOK D-010 "*A well barrier shall be leak tested, function tested or verified by other methods*".

On demand

On demand is used for components that have a certain probability to fail when they are required and are represented by:

p = Constant, where the constant is a value between 0 and 1.

Summary of basic component types and input parameters

To summarize, the necessary input parameters for the basic component types included in quantitative reliability analyses are:

- *Failure rate* (λ) presented as an average frequency of failure (i.e., number of failures per unit of time). In the thesis λ presents the dangerous random hardware failure rate.
- *Detection* is the way the failure is detected (undetected (until test), detected, or not detected).
- *Repair time* is the time used to restore/repair a failed component. The safety critical time is the time until the well is brought to a safe state. The term used in the thesis is the MDWT.

Table 8 shows a summary of the component types, the necessary input parameters and corresponding reliability measure used in quantitative reliability analyses.

Table 8 Component types, necessary input parameters and reliability measures

Component types	Input parameter			Reliability measure
	Dangerous hardware failure rate	Detection time	Repair time	
Test interval components	λ	$\tau/2$	MDWT	PFD
Repairable components	λ	Immediate	MDWT	p(t)
Non-repairable components	λ	Not detected	-	p(t)
On demand components	-	-	-	p

The repair time and detection (e.g., the test interval) are determined by the specific well subject to analysis. The generic failure rate may be extracted from failure databases. For a specific well, field a recommended failure rate must be determined by well specific conditions. The classification in section 4.2.2 is useful in this process.

5.3 The β-factor model

As discussed in section 4.2.2, the most commonly used model for common cause failures is the β-factor model. To illustrate the general model, consider a system with N=2 components with the same constant failure rate, see Figure 19. Letting λ_{DU} be the relevant failure rate for each component, we have

$\lambda_{1\cdot 2} = 2 \cdot (1-\beta) \cdot \lambda_{DU}$ = rate of single (independent) failures for duplex system

$\lambda_{2\cdot 2} = \beta \cdot \lambda_{DU}$ = rate of double failures (CCFs) for duplex system

β can therefore be given the following interpretation; given A has just failed, β is the conditional probability that B fails at the same time.

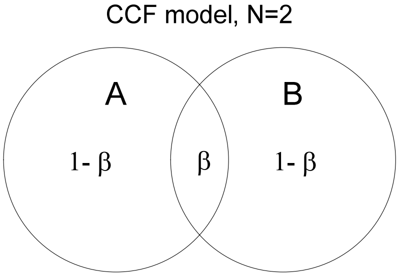


Figure 19 Beta factor model for a duplicated system (N=2)

The limitation of the β-factor is that the method does not distinguish between different parallel structures (see section 4.1.1, page 48), and the same result is obtained e.g. for a parallel structure with 2 and 3 components. So, e.g., the contribution to PFD_{UK} from CCFs simply equals $PFD_{UK} = \beta \cdot \lambda_{DU} \cdot \tau /2$ for parallel structures. The reason why it still can make sense to apply this model is that the reliability engineer can come around (or at least reduce) this problem by using different βs, e.g., with β=1% for a parallel structure with 3 components, and β=5% for a parallel structure with 2 components.

IEC 61508-6 introduces an "application specific" β, which to *some extent* depends on the redundancy. However, the rate of system CCFs does only to a very slight degree depend on the system configuration. In Paper 2 a more general CCF model is suggested. The model is a *simple,* direct generalisation of the β-factor model that distinguishes between the performance of different parallel structures.

5.4 Well integrity and well shut-in function reliability measures

In this section well integrity and well shut-in function reliability measures are presented.

Well integrity reliability measures

The well integrity reliability analysis on well system focuses on the blowout frequency The reliability measure typically comprises the estimated average number of well blowouts per time unit (normal operation blowout frequency) and may be described as:

Blowout frequency caused by inherent failure cause (per time unit) $=F_{All\ well\ barriers}$

Other useful reliability measures for blowout analysis are:

- R(t)[55] = P("Blowout will not occur in the time interval [0,t]"). R(t) is the survival function of the system with respect to the non-occurrence of blowout.
- MTTF[56] = mean time to first occurrence of blowout

Well shut-in function reliability measure

The required level of protection from the well shut-in function is given as a SIL requirement (see section 3.3, page 42), and an associated PFD requirement. The reliability measure for the well shut-in function is therefore:

$PFD_{Well\ shut\text{-}in}$ *= Average proportion of time the well is unable to shut-in*

If the hazardous event affects the integrity of the well itself, e.g., caused by fire in the wellhead area, the well must be shut-in by closing the SCSSV (the function is illustrated in Figure 7, on page 35). The reliability measure for this function is:

*Blowout frequency caused by external event(s) (per time unit) = Frequency of external event(s) damaging x-mas tree * Average proportion of time the SCSSV is unable to shut-in =* $F_{External\ event} * PFD_{SCSSV}$

For this well shut-in function, the personnel responsible for the wellhead area layout should focus on measures to avoid dropped objects and to protect the wellhead area against fire explosion loads. The personnel responsible for the well system should focus on selecting the best available SCSSV, where to place the SCSSV in the tubing string (e.g., to avoid scale), and recommend SCSSV operational procedures (testing, repair).

[55] *Survivor function* - Let *T* denote the time to failure of an item. The survivor function *R(t)* of the item is $R(t) = \Pr(T > t)\ for\ t \geq 0$. R(t) is sometimes called the *reliability function* or the *survival probability* at time t of the item (Rausand and Høyland 2004).

[56] *MTTF* - Let T denote the time to failure of an item, with probability density *f*(t) and survivor function *R*(t). the mean time to failure is the mean (expected) value of *T* which is given by $MTTF = \int_0^\infty t \cdot f(t)dt = \int_0^\infty R(t)dt$ (Rausand and Høyland 2004).

5.5 Reliability analysis procedure

In this section a procedure for performing reliability analysis is presented. The procedure is generic, but the reliability analysis techniques used are different. Therefore the procedure for well integrity is presented first, then specific well shut-in function conditions that differ from the well integrity procedure is presented in section 0.

5.5.1 Well integrity reliability analysis

The procedure includes the use of barrier diagrams and FTA. Barrier diagrams were presented in section 4.3. FTA is a well-known analysis technique and several software versions are available, like CARA Fault tree (2004). See, e.g., Rausand and Høyland (2004) for a more detailed description of FTA. The FTA technique is well suited for quantitative analysis and for assessing alternative well designs. The suggested procedure include the following activities:

1. *System understanding/design basis*. To perform quantitative analysis recommended reliability data must be established for each of the WBE failure modes. For each component it should be identified if the component is of the test interval, repairable, non-repairable or on demand type (see section 5.2, page 77). The activity should also include an assessment of potential failure causes, the possibility of cascading failures, and common cause failures. Systematic failures should also be discussed.
2. *Barrier diagrams*. The relationship between the well barriers is visualised in a barrier diagram. The barrier diagram for the example well (Figure 3, on page 22) was illustrated in Figure 18, on page 75. The barrier diagram is used to discuss the well barrier system between well design and reliability personnel.
3. *Quantitative analysis*. Based on the barrier diagram and input reliability data a fault tree can be constructed, and the blowout frequency calculations can be carried out. The first page of the fault tree for the example well is shown in Figure 20. The figure illustrates the leak paths from the reservoir via the tubing side to the surroundings. The leak paths from the reservoir via the annulus side are modelled in the same way.
4. *Present and evaluate results*. Results from the analysis must be presented. The alternative reliability measures was presented in section 5.4. In addition, the effects

of various risk reduction measures and the sensitivity of various input data must be evaluated. Such an evaluation typically includes:

a. Improved ability to detect dangerous WBE failures. E.g., through more frequent testing, condition monitoring, remotely operated vessel (ROV) surveys / other type inspections.
b. Reduced WBE downtimes[57], e.g., shorten repair times or time to kill the well.
c. Sensitivity analysis by, e.g., altering input failure data for critical components and components with high uncertainty.

5. *Conclusions/present results.* The analysis ends up with a conclusion, and typically includes recommended well design (e.g., casing program), and operation (e.g., monitoring, test interval, etc.). The conclusion should include the uncertainties in the calculations to allow for peer review. Recommendations for further work may be included.

There should be a strategy for how to present the analysis results. Two possible presentation strategies are:

- Present the blowout frequency as a relative difference between well alternatives, where one alternative may be a standard accepted solution.
- Present the blowout frequency for one alternative and evaluate the result against a fixed frequency requirement, e.g. not more then 10^{-4} blowouts per well year

The first option is the preferred because this allows for relative comparison between alternatives rather than a quantitative reliability result measured against an absolute requirement. Relative comparison between alternatives gives more robust results than giving “absolute” frequency numbers.

As an illustrative example, it may, e.g., be an alternative to design the surface well presented in Figure 3, on page 22 either 1) as a well with the intermediate casing *not* qualified as a well barrier or 2) as a well with the intermediate casing qualified as a well

[57] The period of time during which an item is not in a condition to perform its required function (BS 4778).

barrier. The results will show that the blowout frequency will be higher for the alternative with intermediate casing *not* qualified as a well barrier. The result can be further evaluated and include sensitivity analysis with respect to repair time, detection and altering of input failure data for safety critical components and components with high uncertainty.

CARA Fault Tree version 4.1 (c) Sydvest Sotfware 1999
Licensee: ExproSoft AS, Norway
Supplied by Sydvest, Norway

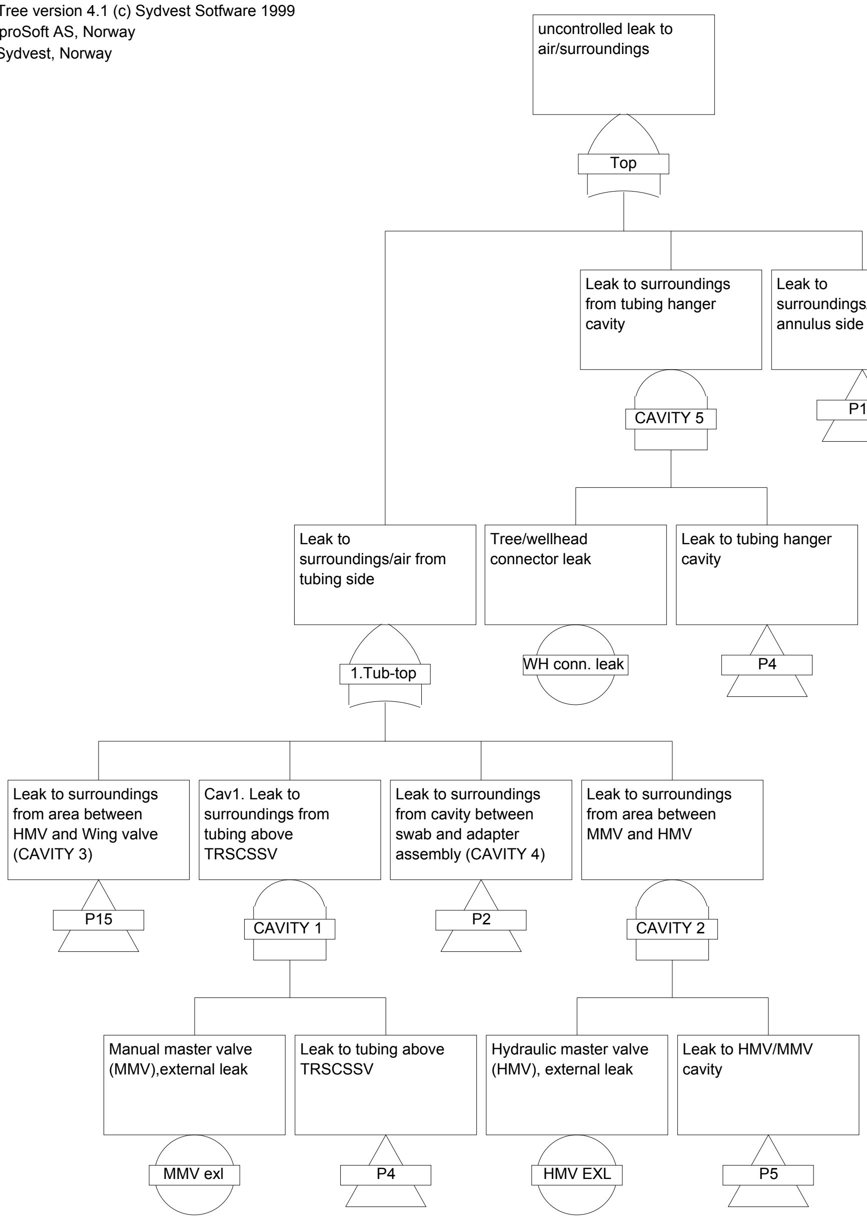

uncontrolled leak to air/surroundings
Top
Leak to surroundings from tubing hanger cavity
Leak to surroundings/air from annulus side
CAVITY 5
P14
Leak to surroundings/air from tubing side
Tree/wellhead connector leak
Leak to tubing hanger cavity
1.Tub-top
WH conn. leak
P4
Leak to surroundings from area between HMV and Wing valve (CAVITY 3)
Cav1. Leak to surroundings from tubing above TRSCSSV
Leak to surroundings from cavity between swab and adapter assembly (CAVITY 4)
Leak to surroundings from area between MMV and HMV
P15
CAVITY 1
P2
CAVITY 2
Manual master valve (MMV),external leak
Leak to tubing above TRSCSSV
Hydraulic master valve (HMV), external leak
Leak to HMV/MMV cavity
MMV exl
P4
HMV EXL
P5

Figure 20 Example well - Fault tree layout

5.5.2 Well shut-in function reliability analysis

As described in section 2.3, the well shut-in function is comprised of the SCSSV, the PMV, and the PWV. In addition the control system that actuates the valves must be included. This function only includes active WBEs, i.e., test interval components.

Several reliability quantification methods are suited for modeling of active components. Rouvroye and Brombacher (1999) present a comparison of quantitative analysis techniques, and in Rouvroye and Bliek (2002) the discussion is further extended to a comparison of quantitative and qualitative safety analysis techniques. Both papers conclude that one of the methods best suited for the purpose is the PDS[58]-method (Hokstad and Corneliussen, 2003). In this thesis the PDS-method is used as a basis.

The procedure for quantification and evaluation of the well shut-in function follows the same steps as described for the well integrity function in the previous section. The main exception is that only active WBEs are included in the model, and that the PDS-method is used to quantify the reliability. Hence, barrier diagrams and FTA are not used. Additional differences are:

- In addition to active WBEs, the ESD logic and solenoid valves are included in the safety function.
- The common cause contribution is an essential contributor to the ability to shut-in on demand. Common cause failures should therefore be paid particular attention.

The PDS-method use reliability block diagrams (RBD) to illustrate the safety function (RBD was described in section 4.1, page 47). Figure 21 illustrates a typical well shut-in function, while the RBD for the function is shown in Figure 22. The function has a high degree of redundancy. However, if including common cause failures between the solenoid valves and the PMV and the PWV, the PFD contribution from the solenoids and the x-mas tree valves will be dominated by the common cause

[58] *PDS* - Reliability of computer-based safety systems (Norwegian)

contribution, and the RBD will change into the RBD shown in Figure 23. The total PFD for the function then becomes:

$$PFD_{Total} = PFD_{ESDlogic} + PFD_{\beta\ Solenoid} + PFD_{\beta PMV/PWV\ AND\ SCSSV}$$

With the same data as presented in Table 7, and a 6 months test interval for all components, the PFD_{Total} will be dominated by the ESD logic contribution and result in a total PFD = 4.4 * 10^{-3}. Note that this result is above the SIL 3 requirement stated in OLF (2004), and OLF therefore recommend a redundant ESD logic to comply with the SIL 3 requirement.

For a detailed description of the PDS-method and calculation formulas it is referred to Hokstad and Corneliussen (2003) and Paper 2. In addition, Paper 5 presents a model for SCSSV PFD calculations.

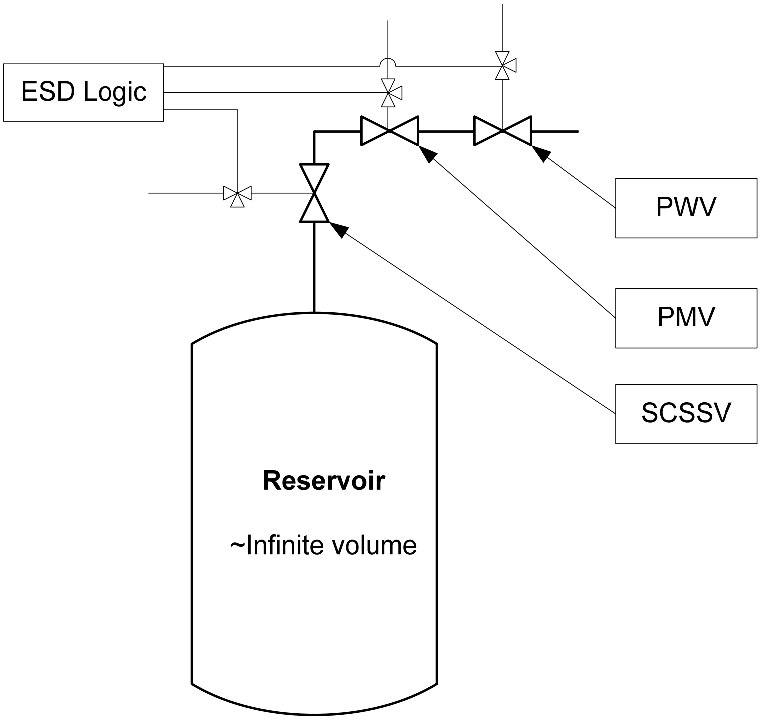


Figure 21 Illustration of typical well shut-in function for a surface well

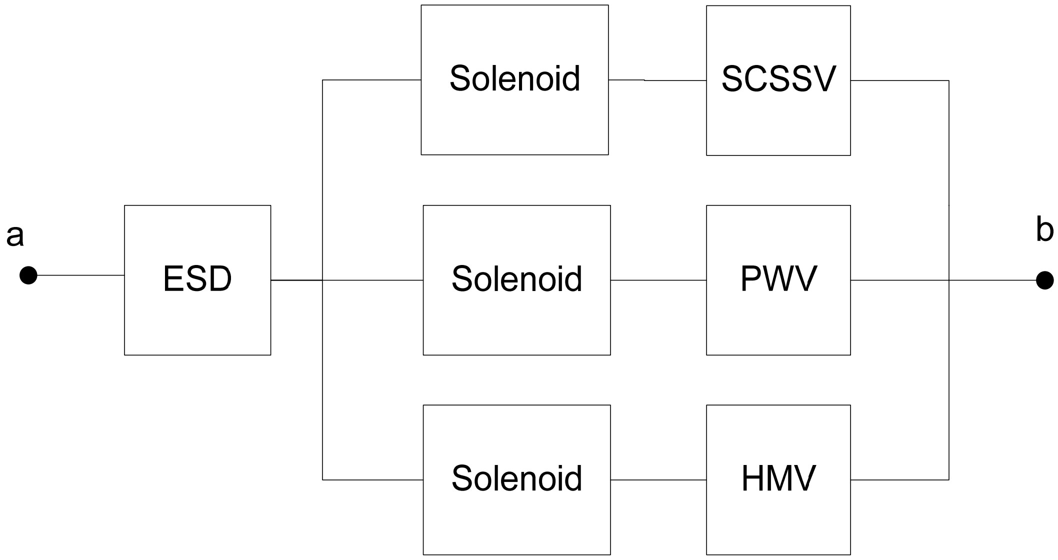


Figure 22 RBD for the example well shut-in function

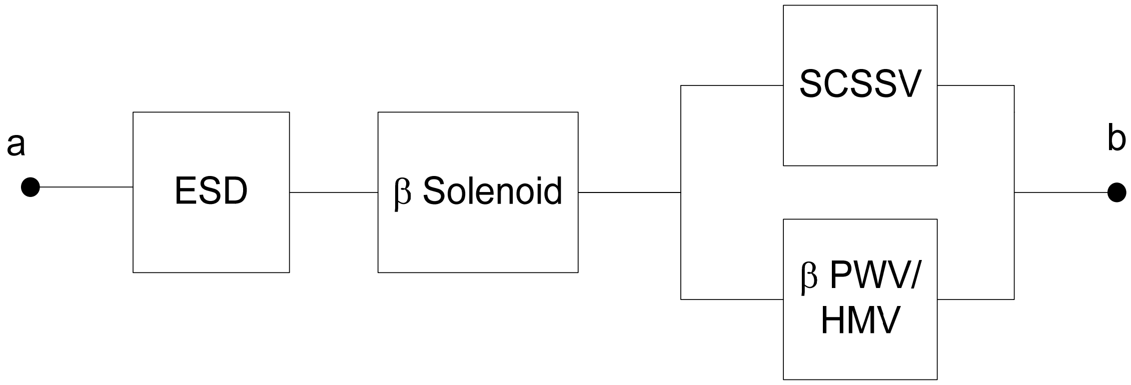


Figure 23 RBD including common cause failures for well shut-in function

5.6 Reliability analysis discussion

A model tries to represent the real world. However, any model has its limitations. This section discusses main limitations of the methods presented above. General to both the well shut-in function PFD calculations and the blowout frequency calculations are that:

- Many systems are highly inter-linked, and a deviation at one of them may have a cause elsewhere. Many accidents have occurred because small local modifications had unforeseen knock-on effects elsewhere.

- The success of the analysis depends on the experience and interaction among team members.
- The risk analysis only considers parts that appear on the design representation.

5.6.1 WBE input parameters

The reliability input data will highly influence the result. The uncertainty in failure rates is an important contributor to the results. However, relevant date may not always be available, e.g., because of new components, little operational experience or application of existing components in new well conditions. In this case sensitivity analysis is important.

The awareness of different types of failure causes and mechanisms is important when establishing the field specific reliability data. Different failure causes require different strategies for detection and repair.

Common cause failures may significantly reduce the reliability of a system, especially of systems with a high degree of redundancy.

The models do not include cascading effects. It is assumed that the probability of such failures is negligible. However, such failures may have severe consequences. The likelihood of such failures must therefore be emphasized in the design process. The risk analysis should include a discussion of the likelihood of cascading failures.

Most quantitative reliability methods only include random hardware failures. Actually IEC 61508 argues not to include systematic failures because it is not possible to collect data on systematic failures. However, the PDS-method (Hokstad and Corneliussen, 2003) does attempt to quantify systematic failures. The values for systematic failures in the PDS-method are based on, e.g., expert judgment.

5.6.2 SIL budget

The SIL requirements apply to entire safety functions, and the role of the reliability analysis is to validate that the SIL for the function can be achieved. Alternatively a “SIL budget” for the input, logic and output of the safety function may be established. For example, the PFD requirement to a SCSSV may be set to 5.5 10^{-3} (PFD = $\lambda_{DU}*\tau/2$ = 2.5

10^{-6} failures/hours* 4380 hours/2 = 5.5 10^{-3})[59]. This result implies that the SCSSV should not fail more than once every 181 demands/tests. A similar approach may be used for the PMV and PWV. With the OLF assumptions, the PFD for a single PMV/PWV[60] is 3.5 10^{-3}, and this gives a "success criterion" of 285 demands/tests. This "SIL budget" approach is based on the historic occurrence of failures. Follow-up of such a "SIL budget" in the operational phase requires a large number of similar valves operated under comparable conditions. In the design of a new well this type of SIL budget may be used as a target value. The role of the engineers will then be to validate that the PFD for the valves can be fulfilled.

5.6.3 Blowout versus leakage

In the blowout frequency calculations it is assumed that all dangerous hardware failures may lead to a blowout. However, most WBE failure combinations may be controlled rather fast and will not be regarded a blowout. If, for instance, a leak to the annulus occurs and is followed by a leak in the flange of the annulus access valve, this will not be regarded a blowout as long as the annulus pressure can be bled down and the leak is stopped.

For a leak to result in a blowout, a fairly rapid development of the failure has to occur, or the presence of a failure in the well barrier is undetected. A leak in a casing or tubing string caused by corrosion will likely develop more rapidly than a leak in a threaded connection. For a valve a fail to close failure is more serious than a failure where the valve leaks in closed position.

In general, leaks to annulus below the SCSSV are important contributor to blowout risk because valves in the tubing cannot stop such leaks. If high pressure occurs in the annulus, a large leak may result if the casing or the formation behind the casing cannot withstand the pressure build up.

Most leaks/blowouts will likely be leakages that can be controlled. This presupposes that when failures are detected proper steps need to be taken to bring the

[59] Same assumptions as in OLF (2004) are used. The repair time is not included, 6 months test interval, and the SCSSV failure rate used in OLF (2004)

[60] OLF(2004) assumptions for PMV/PWV PFD calculations are λ=0.8*10^{-6} failures/hour and test interval = 12 months.

well to a safe state. However, for shorter periods (while preparing for an intervention) risk analyses often indicate that continued production can be accepted. This situation is further discussed in the next chapter.

6. Well risk assessment in the operational phase

This chapter describes a method for risk assessment of a single well. The method is to be applied in the operational phase when a failure of a well component has occurred.

6.1 Introduction

This chapter describes a method for risk assessment of wells in the operational phase. When a well is installed, the well risk is regarded to be acceptable. In the operational phase failures may occur, and these failures will usually result in an increased risk. The risk increase is influenced by which component has failed, the failure mode, and the extent of the failure (see the error versus failure discussion in section 4.2.1, page 56).

The upstream industry tends to treat well integrity differently among countries, operators and even on fields/installations operated by the same company. This diversity in practice was, e.g., discussed at a SPE workshop held in Scheveningen, Netherlands in November 2005[61]. To address this issue, Norsk Hydro wanted to develop a risk based procedure for handling of well leaks. The objective was to establish a uniform approach able to handle well annular leaks for different well types.

The method described in this thesis is based on the procedure developed on behalf of Norsk Hydro. The primary user of the method is the operator. The method basis is the definition of a set of standard well types and possible well component failures for each well type. When a real failure occurs, Norsk Hydro operating personnel should then be able to perform an internal risk assessment. The benefit is that the defined failures for the standard well types are treated consistently and within a short time. After the risk assessment is performed, the operator may continue production given certain risk

[61] No papers were released from the workshop

reducing measures that not involve repair of the failed well component, or decide to shut-in the well and perform more detailed risk assessment, or decide to shut-in and repair the well.

The method described in this thesis covers the following well component failures:

- Well component failures that influence the well shut-in function. In practice, this means that dangerous SCSSV and PMV hardware failures are included. Failures of x-mas tree components other than the PMV are not included.
- Failure of passive well components in well completion and casing program.

For other well component failures detailed and specific risk analyses must be performed. Also, the method only covers failures of one well barrier. Failure of more than one well barrier is an indication of a significant increase in risk, and should be treated accordingly.

The Norsk Hydro procedure also includes guidelines for detection, diagnosis, and implementation of corrective measures. Only the risk assessment part is described in detail.

6.2 Acceptance criteria

Risk assessment is defined by IEC 60300-3-9 as an "Overall process of risk analysis and risk evaluation", where NS 5814 defines risk evaluation as "A comparison of the results of a risk analysis with the acceptance criteria for risk and other decision criteria." NS 5814 defines acceptance criteria as "Criteria based on regulations, standards, experience and/or theoretical knowledge used as a basis for decisions about acceptable risk. Acceptance criteria may be expressed verbally or numerically." This definition of acceptance criteria is in line with The Royal Society (1992) that defines risk acceptance criteria as "A qualitative or quantitative statement of the acceptable standard of risk with which the assessed risk needs to be compared." Hence, a risk assessment must include a risk analysis and acceptance criteria to compare the result from the risk analysis. A set of acceptance criteria must therefore be developed.

According to Hokstad et al (2003) the rationale behind the use of risk acceptance criteria could be:

- To control the risk to a level that is accepted.
- Improved efficiency of decision process.

Further from Hokstad et al (2003), a successful implementation of such risk acceptance criteria requires that the criteria represent a direction for improvement and hence should be difficult to meet. However, setting ambitious risk acceptance criteria could also be difficult because this may substantially increase the ownership cost. The acceptance criteria must balance these considerations, and will be a trade-off between production and safety.

Functional requirements versus rules

Traditionally, well designs and well component failures have been treated by rules like the leak rate criterion for SCSSVs in API RP14B and the sustained casing pressure rule stated by the MMS (see section 3.2, page 39). The two barrier principle is also well established in the industry. Such rules are often based on sound engineering judgment, and should not be abandoned unless there is a documented reason for it. The use of rules can be a benefit, but the rules tend not to reflect variations in risk level and may therefore also limit the development.

The method described in this chapter attempts to balance the rules established in the industry against a risk based approach for assessment of well component failures. A set of risk factors is identified, while it is left to the operator to define explicit acceptance criteria for each risk factor.

6.3 Well risk factors

In section 2.2, well integrity was defined as "The application of technical, operational and organizational solutions to reduce risk of blowout *and* well release". A well component failure may increase both the blowout and well release risk. In the event of a dangerous SCSSV or PMV failure the reliability of the well shut-in function is also reduced.

A set of risk factors is identified that has a potential influence on well integrity risk and/or the reliability of the well shut-in function. It is assumed that the wells that experience a well component failure are designed, completed and operated according to an accepted risk level. Therefore, the method only threats risk factors that may change significantly after a well component failure has occurred. The risk factors are called well risk factors (WRF), where a WRF is defined as “an aspect of a well component failure that affects the well risk level during the operational phase”. It is assumed that by performing an assessment of each WRF separately all well risk aspects are covered, which may change significantly during the operational. The following WRFs are identified:

1. *Blowout consequence (acceptable deviation)*. The leak rate across a failed well component will influence the consequences of a blowout in the leak path(s) the failed component is part of.

2. *Well shut-in function and well integrity fault tolerance*. The two barrier principle is a established rule in the industry and an alternative acceptance criterion resulting in a deviation from the two barrier principle is not considered realistic. This WRF assess if a well component failure result in failure to comply with the two barrier principle. The assessment includes both the well shut-in function and well integrity.

3. *Blowout frequency*. The location of the leak/failure may influence the probability of a blowout because of reduced number of WBEs in the leak path(s) the failed component is part of.

4. *Well release consequences*. A leak to annulus results in well fluids stored in the annuli. The increase in well fluids stored in the annuli will increase the potential consequences of a well release. The amount of fluid, fluid type, fluid toxicity, etc., influences the well release consequences.

So far the influence on well integrity and the well shut-in function is treated. In addition, the following WRFs are identified to account for changes in the well design assumptions or well operation as a result of the well component failure:

5. *Failure cause*. This WRF examines if further development of the failure is likely or if other well components may be influenced by the same failure cause. If the situation is likely to escalate or if the failure cause is uncertain, the risk of continued operation may be unacceptable.
6. *Well barrier system and interfaces*. The well barrier system and interfaces (see section 4.1.3, page 50) may be changed as a result of a well component failure. The well component failure may, e.g., result in increased risk of cascading failures unless the operation of the well is changed (e.g., by reducing injection pressure in a injection well).
7. *Operations in the well*. A well component failure may result in increased risk when performing operations in the well (see section 2.1.2, page 24, for description of well operations). The well component failure may, e.g., result in reduced ability to kill the well in the event of an additional well component failure or in a blowout situation.

The basis for the method is a comparison with a base case well without failure. The relative increase compared with the base case well is a measure for the increased risk. For each WRF separate acceptance criteria for the relative increase in risk should be defined. The acceptance criteria may be established separately and may be revised when experience is gained. The description in this thesis discusses the framework for the acceptance criteria for each WRF. The operator should establish explicit acceptance criteria.

6.3.1 WRF 1 – Blowout consequence (acceptable deviation)

Compared to a well without failures, failure of a well component may increase the consequences of a blowout. This WRF relates to the failure versus error discussion in section 4.2.1, and criteria for when a WBE is regarded to be in a failed state. The basis for the WRF is a scenario where a blowout is controlled by the well barrier the “failed” WBE is part of. Given this scenario, the following question(s) must be answered:

1. What is the acceptable leak rate across the WBE?
2. If the WBE is active, what is the acceptable closure time?

Specific acceptance criteria are not given here, but the SCSSV leak rate criterion in API RP 14B (see section 4.1.3, page 50) is far less than the leak rate included in the QRAs performed in Norway (see section 2.2.2, page 27). The SCSSV leak rate criterion is also below the hydrocarbon leak rates reported in the UK and Norwegian sectors (see section 2.2.2, page 27). The SCSSV leak rate criterion may therefore be relevant to use also for other well components.

The API RP 14 B criterion does not distinguish between well types (as discussed in section 3.2). Different well types include different aspects of risk (human, environmental) and a differentiation in leak rate criterion should be possible for, e.g.:

- Subsea vs. surface wells, since the consequences of a blowout will be different.
- Non-natural flowing or non-hydrocarbon flowing wells vs. hydrocarbon flowing wells. Non-natural flowing wells will not be able to “produce” in the event of a blowout, while non-hydrocarbon wells will not have the same fire and explosion consequences as a hydrocarbon well.

It should also be possible to establish different criteria for closure time of active WBEs. For example, to close in a subsea well will probably not be as time critical as for a surface well because of the distance from personnel.

A well component that leaks externally or leaks to a volume not enveloped by a qualified well barrier will likely not be accepted independent of leak rate. This situation is comparable to a situation with an external leak from the process system on an offshore installation..

6.3.2 WRF 2 - Well shut-in function and well integrity fault tolerance

IEC 61508, Part 4 defines fault tolerance as “Ability of a functional unit to continue to perform a required function in the presence of faults or errors”. The two barrier principle is a fault tolerance requirement. An alternative acceptance criterion resulting in a deviation from the two barrier principle is not considered realistic. It is therefore assumed that the acceptance criterion for the well shut-in function and the well barrier system will be that there should be at least two well barriers in all foreseen situations.

For the well shut-in function, the PMV are regarded as the outlet from the secondary well barrier, while the SCSSV is the outlet from the primary barrier (production/injection well). If the failed WBE not is part of these two envelopes, the failure does not influence the ability to shut-in the well on demand, and the well shut-in function complies with the two barrier principle.

The two barrier principle also applies to well integrity, i.e., there should be two well barriers to prevent a blowout in normal operation. Two or more WBEs should therefore be intact in all leak paths.

In addition to the two well barrier requirements is it is assumed that the primary barrier always must be intact. This primary barrier must be intact to allow for isolation of the well in the event of an external event damaging the wellhead.

6.3.3 WRF 3 - Blowout frequency

If the two barrier principle is fulfilled, this WRF assess the relative increase in blowout frequency. The location of a well component failure may result in increased blowout frequency because of reduced number of WBEs to prevent a blowout, and a quantitative reliability analysis (FTA) is used to measure the relative increase in blowout frequency.

The following reliability analyses (see section 5.5.1, page 84) are performed:

1. Base case well blowout frequency. The base case well is a well with no failures operated according to normal industry (Norsk Hydro) practices. This well is considered to represent the “acceptable blowout frequency” level.
2. Base case well with well component failure. This well is similar to the base case well but with the failed well component included in the model.
3. Base case well with well component failure and with risk reduction measures. This well is similar to the failed well, but risk reducing measures not involving repair of the failed well component are included in the model. Examples of such measures are monitoring of outer annuli, increased test frequency, shorter well kill time, and shorter repair times (MDWT) for the remaining WBEs.

In this situation acceptable risk (blowout frequency) is achieved if the quantitative reliability analysis (i.e., the FTA) can demonstrate that the “acceptable blowout frequency” represented by the base case well can be achieved for the well with the well component failure without repair of the failed well component, but with increased testing, increased maintenance support (reduce repair time), and/or increased monitoring.

For example, “Leak 2” in Figure 24 illustrates a situation with a leak in the tubing above the SCSSV. In this situation it will often be possible to include risk reducing measures that reduce the blowout frequency to the same level as the base case well (i.e., the “acceptable blowout frequency”). The reason why this can be achieved is that the primary well barrier and secondary well barrier are intact. In contrast, “Leak 1” in Figure 24 shows a situation where the primary well barrier has failed. In this situation the two well barrier principle will not be fulfilled, and at the same time it will be difficult or impossible to verify by use of FTA that the blowout frequency can be reduced to the base case frequency without repair of the failed component.

In the Norsk Hydro project a “library” of standard well types was established. The library included a set of given “standard” Norsk Hydro wells. For each well FTA for the three base case well scenarios were performed for different leak locations (tubing leak above SCSSV, casing leaks, etc.). This library is used by Norsk Hydro to assist in the well risk assessment and recommend risk reducing measures.

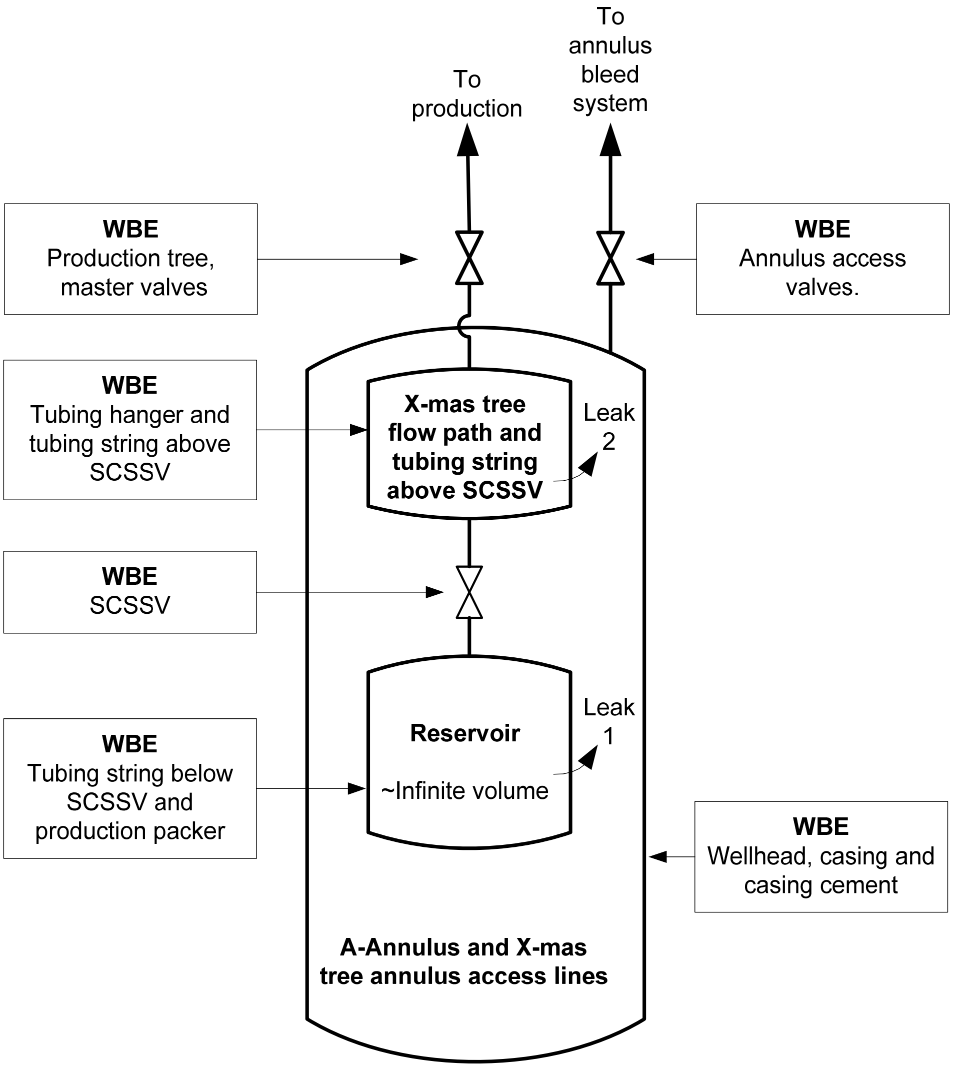

To production
To annulus bleed system
WBE Production tree, master valves
WBE Annulus access valves.
WBE Tubing hanger and tubing string above SCSSV
X-mas tree flow path and tubing string above SCSSV
Leak 2
WBE SCSSV
Reservoir
~Infinite volume
Leak 1
WBE Tubing string below SCSSV and production packer
WBE Wellhead, casing and casing cement
A-Annulus and X-mas tree annulus access lines

Figure 24 Well component failures/leaks with different influence on the blowout frequency

6.3.4 WRF 4 - Well release consequences

A well component failure resulting in a leak to annulus results in well fluids stored in the annuli. The increase in well fluids will increase the potential consequences of a well release compared with a base case well without failure. For example, "Leak 2" in Figure 24 may be acceptable from a blowout frequency perspective, but the increased volume stored in the A-annulus must also be assessed.

The extra volume of well fluids stored in the annuli represents an additional risk mainly related to increased well release consequences. The increase in well release consequences (hazardous fluids stored in well annuli) primarily depends on:

- Release fluid type.
- The amount of fluids stored.
- Toxicity of fluids.

The factors above are the immediate factors that influence the well release consequences. After a period of time the annuli will be drained, and the leak will be controlled by the leak rate. The leak rate risk (blowout consequences) was discussed in section 6.3.1 (WRF 1).

A leak to annulus will cause gas to segregate and be “stored” below the tubing hanger, while the oil and water fractions stabilize lower in the well. This situation applies even for wells with liquid type reservoir fluids. Hence, there will always be an increased risk of a gas leak from the well. Gas is more volatile and has a higher ignition probability than oil (see section 2.2.2, page 27).

The operator should establish explicit acceptance criteria related to allowable storage of well fluids. Possible “minimum storage criteria” may be a comparison between conventional wells and the typical volume of gas stored above a functioning SCASSV in a gas lift wells. In Norway, the SCASSV should be placed at least 50 m below mudline (minimum packer type SCASSV setting depth), and the typical gas lift injection pressure is 180 Bar pressure.

In addition, the *Guideline for protection of pressurized systems exposed to fire* (Hekkelstrand, B. and P. Skulstad, 2002) may contribute with additional input. According to this guideline exceedance of either of the following criteria is considered to make a vessel rupture unacceptable:

- Released quantity of hydrocarbons (the sum of gas and liquid) > 4 tons.
- Released quantity of the sum of gas/initially flashed fraction of condensate/LPG > 1 ton.

Other criteria that may be used are the sustained casing pressure criteria for departure in the US GoM (see section 3.2, page 39) or the RIDDOR classification given in Table 1, on page 36.

For subsea wells the release quantity criterion may be linked to environmental consequences rather than personnel risk.

For platform wells, factors such as toxicity (H_2S in gas) may override fire/explosion criteria, and lead to a more stringent requirement related to the consequence of a well release.

6.3.5 WRF 5 - Failure cause

This WRF assess the failure cause (see section 4.2, page 56), and the likelihood that similar WBEs in the well will fail or the likelihood of further degradation of the WBE (if WBE not in fault state yet (see WRF 1)). The main criterion for this WRF is that further escalation, which cannot be controlled, should not be accepted. If the failure cause can be determined, and if further escalation/degradation of the well can be controlled, the risk can be accepted.

6.3.6 WRF 6 - Well barrier system and interfaces

The well barrier system and interfaces (see section 4.1.3, page 50) may change because of a well component failure. NORSOK D-010 states that if the well barrier status, availability or monitoring ability is altered, any continued use shall be supported by a risk assessment based on current reservoir/well condition and time factors. Hence, the change in boundary conditions for the remaining well barrier system must be assessed.

For example, the well component failure may expose other well components to well conditions that result in new failures or escalation of failure mechanisms. The well componet failure may also result in increased risk of dependent failures. For example, the failure may result in changes in pressure regimes and thereby increase the risk of cascading failures.

The main criterion for this WRF is that the well barrier boundary conditions must be within acceptable limits. For example, establishing new annulus pressure limits, decrease of injection pressure, etc., may reduce increased risk of cascading failures.

6.3.7 WRF 7 - Operations in the well

During the operational phase, several types of (dynamic) operations are performed in the well (see section 2.1.2, page 24). A well component failure may result in increased risk when performing such operations. The risk associated with such dynamic operations should not be increased as a result of a well component failure.

In addition the ability to perform operations to mitigate a blowout or well releases should not be reduced. In particular, the ability to kill the well is of vital importance if well control is lost. Also, the ability to kill the well if an additional WBE fails should be assessed before deciding to continue production without repair of the failed well component.

6.4 Risk assessment framework

The risk assessment is part of an overall framework for detection of abnormal well behavior, diagnosis, risk assessment and implementation of risk reducing measures. The framework is illustrated in Figure 25. After abnormal well behavior is detected, the framework includes three tasks, which are diagnosis, risk assessment, and implementation of risk reduction measures.

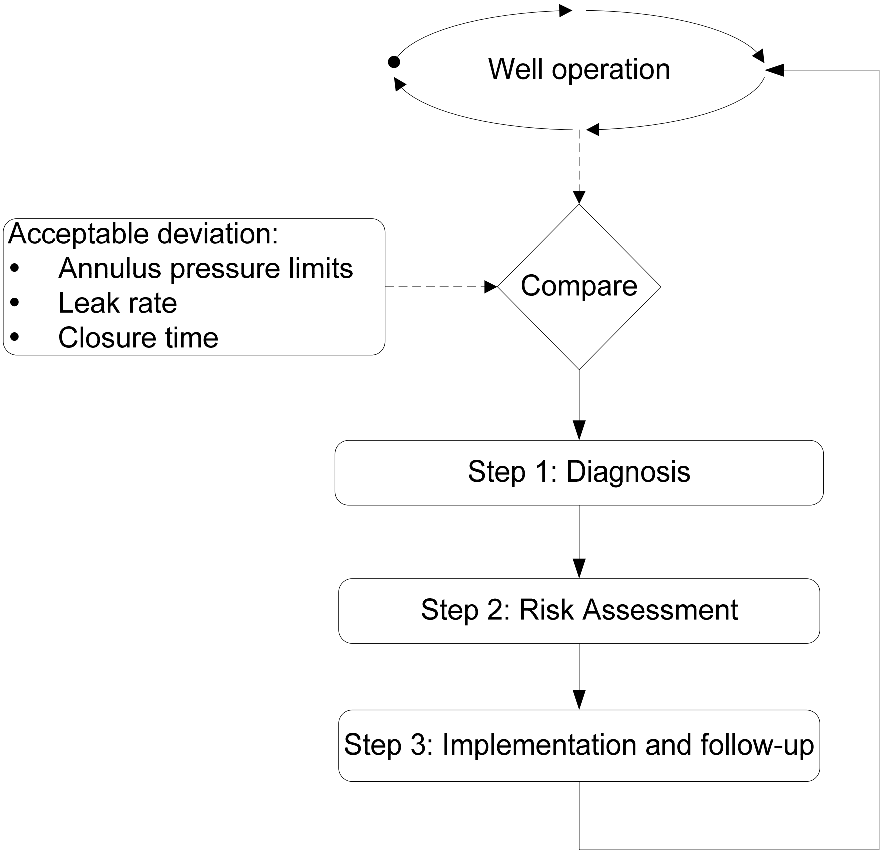


Figure 25 Risk assessment framework

Boundary conditions for normal well operation

A clear understanding and follow-up of the boundary conditions for normal well operation is a prerequisite for determining abnormal well behavior. The boundary conditions must be established early in the operational phase and continuously updated throughout the well lifetime. This work involves identification of general well data and well design limitations. In addition, allowable annulus pressure domains and allowable pressure alarm limits must be identified. The pressure alarm limits are used as criteria for normal well pressure behavior. Failure/leak symptoms can thus be identified by pressure readings outside these alarm limits. Similarly, the acceptable leak and closure times for the active WBEs must be determined (see Table 5, page 58). Key well data that should be available are:

- Basic well data for leak detection and input to quantitative risk assessment (e.g., well fluids, pressure behavior).

- WBE design data, barrier diagrams, well schematics, etc.
- Short-term/long-term allowable annuli pressures.
- B-annulus well barrier design limitations.
- Normal A-annulus pressure behavior and pressure alarm setting.

Step 1; Diagnosis of well behavior outside boundary conditions

This task includes three consecutive activities for diagnosis of abnormal annulus pressure behavior. Firstly, data collection for diagnosis must be initiated. Recommended maximum and minimum allowable annulus pressures must be identified to perform the diagnosis operation safely. Then the diagnosis work starts with an 'external' factors diagnosis with the objective to determine if the abnormal pressure reading is caused by factors other than a change in the downhole well components. If the external factor investigation is inconclusive, a well investigation must be performed to determine the 'internal' factor that contributes to abnormal well behavior. The internal diagnosis work should establish the following properties of the downhole failure:

- Location (depth)
- Direction
- Leak rate
- Volume/mass influx to annulus
- Probable cause

It must be possible to *verify* the leak location and leak rate, either by testing or by direct measurement. The ability to identify the location and to monitor the leak rate(s) is of key importance in order to verify leaks against a predetermined acceptance criterion. Without knowing the leak rate or location the risk level cannot be adequately controlled. If the leak diagnosis activities fails to establish location and leak rate of a detected leak this will in itself call for an intervention to provide more information about the leak or to restore the well to a state that can be verified as acceptable.

Step 2 Well risk assessment

With basis in the diagnosis results, the objective of this task is to evaluate the well state in respect of well risk. The assessment results in a risk status and required risk reducing measures. If risk is unacceptable, a workover must be performed. The method is described in section 6.5.

Step 3 Implementation and follow-up

After the risk assessment is performed, the required risk reducing measures must be implemented. The implementation is the responsibility of the operator and will vary depending on the overall risk management procedures of the company.

6.5 Risk assessment method

The risk assessment method is illustrated in Figure 26. Each WRF described in section 6.3 is assessed separately. For each WRF the well is assigned a risk status code (RSC). The RSC indicates the risk level and the necessary extent of risk reduction measures. Most severe RSC deduced from each WRF assessment step determines the overall RSC for the well.

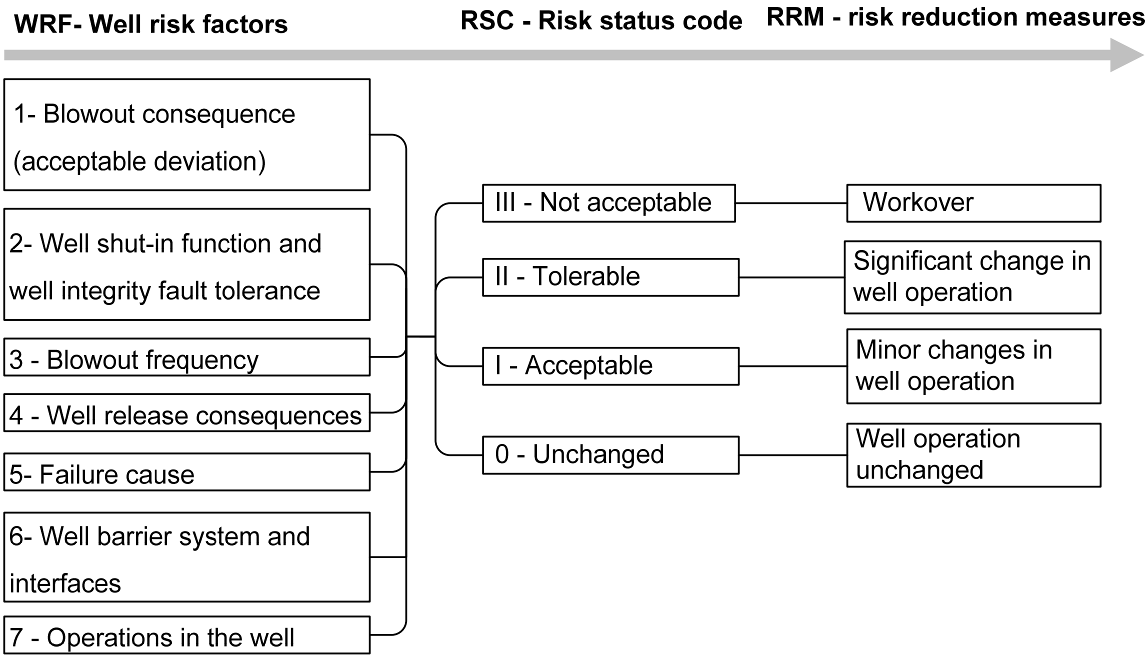

WRF- Well risk factors
RSC - Risk status code
RRM - risk reduction measures
1- Blowout consequence (acceptable deviation)
2- Well shut-in function and well integrity fault tolerance
3 - Blowout frequency
4 - Well release consequences
5- Failure cause
6- Well barrier system and interfaces
7 - Operations in the well
III - Not acceptable
II - Tolerable
I - Acceptable
0 - Unchanged
Workover
Significant change in well operation
Minor changes in well operation
Well operation unchanged

Figure 26 Risk assessment method principle

The risk status code indicates the relative change in risk compared with the original well conditions (well with no failure). The definition of each RSC is given in Table 9. The RSC refers to whether the WRF is above or below the acceptance criteria determined for each WRF. The operator must establish explicit acceptance criteria. The required type of acceptance criteria was discussed in section 6.3.

Table 9 RSC status code and influence on well risk and well functionality

RSC	Risk status	Well Status
0	Unchanged	No change in well functionality. No downhole leak.
I	Acceptable • Small/marginal increase in risk. • Risk can be controlled by minor changes in operational practice	Minor/marginal change in well functionality. • The well can be operated with minor operational changes
II	Tolerable • Acceptable only if risk factors can be controlled in remaining well life. • Risk reduction measures must be implemented	Degraded well functionality. • Major change in operation of well • Workover not necessary.
III	Not acceptable • Two well barrier principle not fulfilled • Primary well barrier has failed • Risk reduction measures not sufficient OR one or more WRFs cannot be controlled in remaining well life.	Well functionality not acceptable. • Increased blowout risk and/or ability to well shut-in. • Not possible to control risk without repair of failed component. • Workover must be performed.

A summary of the WRFs, the required acceptance criteria categories/format, and RSCs is given in Table 10. The summary illustrates that the assessment of the separate WRFs generate a set of remedial actions/risk reducing measures to be implemented. If risk cannot be controlled by the measures, a workover must be performed. Note that the acceptable deviation for the well component failure mode (see section 4.2, page 56) defined in WRF 1 will influence the assessment performed for WRF 2 and WRF 3. Other WRFs are not affected by the acceptable deviation defined in WRF 1.

Table 10 WRF and RSC summary

WRF	RSC		
	III – Not accepted	**II - Tolerable**	**I – Accepted**
1 - Blowout consequence (acceptable deviation)	Leak (any size) to a volume not enveloped by a qualified well barrier.	Well component failure. May be acceptable (given WRF2 or WRF3).	Leak rate or closure time acceptable. Well component error NOT a well component failure.
WRF 2 and 3 assessed if categorized as unacceptable deviation in WRF 1			
2 - Well shut-in function and well integrity fault tolerance	Two well barrier requirement not fulfilled. OR Failure of primary well barrier.		Two well barrier requirement fulfilled. AND Primary well barrier intact.
3 - Blowout frequency	Risk reduction measures cannot reduce relative (calculated) increase in blowout frequency to “base case frequency”. OR Risk reduction measures cannot be implemented due to operational reasons.	Risk reduction measures can reduce relative (calculated) increase in blowout frequency to “base case frequency” and risk reduction measures can be implemented.	
WRD 4 to 7 assessed independent of assessment in WRF 1			
4 - Well release consequences	Well fluids stored in well annuli > acceptance criterion (due to fire or toxicity) AND volume cannot be controlled.	Well fluids stored in well annuli > acceptance criterion (fire or toxicity criterion) AND volume can be controlled (no or few bleed offs).	Well fluids stored in well annuli < acceptance criterion.
5 - Failure cause	The failure cause cannot be controlled or not determined.	Failure cause can be controlled by countermeasures.	Otherwise (e.g., failure due to wireline operation).
6 - Well barrier system and interfaces	The well barrier system boundary conditions are changed and unacceptable (both wanted and unwanted input), AND measures cannot be implemented to reduce risk.	The well barrier system boundary conditions changed. Risk reducing measures must and can be implemented.	The well barrier system boundary conditions are not or marginally changed compared with original design assumptions.
7 - Operations in the well	Current well component failure OR an additional single component failure affect the ability to efficiently kill the well with mud. Corrective action cannot be implemented.	Current well component failure OR an additional single well component failure affect the ability to efficiently kill the well with mud. Corrective action can be implemented to kill the well equally effective as for the base case well.	Current well component failure OR an additional single well component failure do not affect the ability to efficiently kill the well with mud.

6.6 Risk assessment method benefits and limitations

In this section main benefits and limitations of the proposed risk assessment method are discussed.

The benefit of the proposed method is that it in a systematic order attempts to cover all well risk aspects of a well component failure. The method may also be used to establish specific acceptance criteria for different well types.

The method facilitates the use of a "library" with blowout frequency analysis of standard well types (WRF 2). This makes the method effective and reduces downtime when a failure occurs. Otherwise, the well must be shut-in and an extensive risk assessment study must be performed. At the same time, care should be taken in a real situation, because the standard well in the "library" may not reflect the actual well conditions. The assumptions and prerequisites for the analysis must therefore be clear to all involved parties. Otherwise, the use of standard well blowout frequency analysis may be misleading. The method should not be used for well component failures that are not defined or for "non-standard" well types. WRF 5 and WRF 6 are included to ensure that the assumptions for the quantitative analysis are assessed.

The risk assessment method depends on the ability to establish accurate diagnostic results. In particular leak rate estimation and location in the well are of critical importance. The ability to diagnose subsea wells in particular is limited. However, there are models/simulators available that may be utilized. In addition there are wireline tools available that are able to perform diagnostics of wells with a leak.

7. Summary and further work

This chapter provides a brief evaluation of the research process, a discussion of the presented results, and recommendations for further work.

7.1 Main contributions

The overall objective of the PhD project was to develop a systematic approach for risk assessment of oil and gas wells in the operational phase. In this context a systematic approach means to describe procedures for risk assessment, with focus on quantitative analysis as a means to provide input to the assessment. The risk assessment is based on existing and new methods and knowledge gained during the PhD project. The risk assessment includes the development of a set of procedures and methods to be applied in the design and operational phase. To arrive at such procedures and methods, it was necessary to:

1. Describe the state of the art related to analysis and control of the functions mentioned above.
2. Describe regulations, standards, and industry practice, giving requirements to well safety in the operational phase.
3. Identify commonly accepted analysis methods applied in risk assessment of wells, with focus on quantitative analysis techniques.
4. Identify input reliability data available for quantitative well safety analyses and discuss the quality of the data.
5. Assess the applicability of existing well safety analysis methods and, if necessary, suggest improvements.
6. Suggest improvement in application of reliability input data.

7. Develop a systematic approach for risk assessment of oil and gas wells in the operational phase. In this context a systematic approach means to assess well risk when a well component failure occurs in the operational phase. The basis for the risk assessment is the quantitative analysis techniques identified.

The use of risk analysis to assess well risk in the operational phase is not new. However, the risk assessment method for assessing well risk in the operational phase is new. More explicit the following contributions from the thesis are identified:

- A systematic approach for well risk assessment in the operational phase. A set of WRFs are identified that influence the total well risk. The procedure is aimed at risk assessment in the operational phase after a well component failure has occurred.
- A method for constructing barrier diagrams (paper 4). A barrier diagram is a structured way of describing a well as a barrier system. Barrier diagrams are used to 1) calculate failure probability directly or 2) converted to quantitative reliability analysis techniques.
- A framework for assessing well component failure causes, acceptable deviations in well component performance, and dependent failures.
- A method for calculating the safety unavailability of safety functions (paper 2), and a method for calculating the safety unavailability for different configurations of surface controlled subsurface safety valves (paper 5).

7.2 Evaluation of the research process

The theme for the PhD work has been risk control in the operational phase since the start of the scholarship period, and has been driven by the desire to extend the applicability of risk analysis to the operational phase. Traditionally, risk control in the operational phase has been less focused on than the risk assessment performed in the design phase. It was early realized that risk analysis in the operational phase has been suffering from lack of methodology. In particular well integrity is handled in different ways throughout the industry. In the industry SIS is treated in a more uniform way independent of country and operator.

The application area of the PhD work has, however, shifted during the PhD work. Initially the focus was on SIS in general, while after some period the focus shifted to wells as the system boundary. Therefore, the development of adequate procedures and methods has been more complex than what might be immediately apparent in the final work presented in the thesis. At the same time the focus on SIS initially in the process has contributed to valuable knowledge about how risk is modeled within other system disciplines, and has also contributed to a broader perspective when establishing the well risk factors.

To ensure the applicability of the procedures and methods, pragmatism has been important, but the procedures and methods presented are anchored in quantitative risk and reliability theory. To lend scientific credibility to the work, the criteria listed in section 1.5 have been followed as far as possible. Also the risk assessment method presented has been developed with strong involvement from the industry and colleagues mentioned in the preface.

7.3 Discussion of results

The petroleum activity gives extensive incomes to the operators and to the nations that possess the petroleum resources. At the same time the petroleum production may result in severe losses. It is therefore a pressure on the risk analysis to demonstrate acceptable risk. Freudenburg (2001) claims that there is a need to recognize that virtually all technological controversies inherently involves at least three sets of questions (Freudenburg, 2001):

- *How safe is it?* This includes factual or technical questions. On such factual questions the views of technical experts tend to be far more persuasive than do the views of most of their fellow citizens (lay people).
- *Is that safe enough?* This question involves not facts, but values – and when it comes to questions of values, another word for “scientist” is “voter”. For the value questions, in other words, ordinary citizens do indeed have just as much legitimacy as do scientist and engineers.
- *What have we overlooked?* Risk decisions – and indeed, a growing number of the challenging decisions in the 21st century – inherently involve complex mix of facts,

values and blind spots. For this question both experts and the non-experts have a great deal to contribute.

With these questions in mind the results are discussed.

7.3.1 Pressure on safety margins

Offshore systems in general have traditionally had an apparent degree of over dimensioning in the design. An example is the extensive use of redundancy in process control systems. The tradition has been to use a layer of protection philosophy to reduce the consequences of a hazardous event. Related to well systems there has also been a tradition for deterministic requirements stated in, e.g., API RP 14C and API RP 14B. However, there is trend towards functional requirements (what to achieve). Functional requirements give the engineers the possibility to develop a range of solutions to achieve the same function. It is the role of the engineers to decide if a solution achieves the required functional requirement and/or to compare alternative solutions. The risk assessment method proposed in the thesis is dominated by functional requirements. The exception is the two barrier requirement and the requirement that the primary well barrier should be intact (WRF 2 - Well shut-in function and well integrity fault tolerance).

Functional requirements may result in a move towards changes in well-proven safety philosophies for offshore design and operations. Arguments for this development are provided in the introduction to the thesis (see chapter 1). The question in the operational phase then is whether risk in operation is acceptable or not? This question is especially important if changes in design and operation philosophy mainly are motivated by cost reduction. Rasmussen (1997) comments on this, when he points out that commercial success in a competitive market, will lead to an exploration of the advantages of operating at the boundary of accepted praxis. By exploring and moving closer to the limit, one also run the risk of crossing the boarder of what can be said to be safe operation. Rasmussen also argues that commercial pressure force managers and key-decision makers to focus on short-term gains rather than longer-term criteria concerning e.g. safety. In his terms “managers runs the risk rather than taking risk”.

The presented risk assessment method attempts to control the risk by focusing on WRFs assumed to cover all important risk aspects resulting from a well component failure. The method focuses on functions, and functional requirements are dominating. However, it is proposed to keep established principles like the two barrier principle. Despite the combination of both rules and function requirements there is always a risk that the proposed risk assessment procedure does not cover all significant risk aspects.

The acceptance criteria applied will influence the well risk. The influence from different acceptance criteria is illustrated in Figure 27. In the figure it is assumed that the identified WRFs represent the total well risk. However, if the acceptance criteria are set to high, i.e., allow continued operation with to high risk, the operator will “run the risk”. On the other hand, too conservative acceptance criteria and risk reducing measures will result in “overprotective” operational philosophy. The reason for the elliptical form is that the deviation from the “optimal” philosophy is expected to be less for critical well component failures (e.g., failure of the primary well barrier) and for minor well component failures (minor leakage below leak rate criterion). For example, failure to close the SCSSV will in almost all cases result in a workover (or installation of a WR-SCSSV). The deviation from the “optimal” philosophy will be highest for well component failures where the influence on well risk are uncertain or may be reduced by different operational means, e.g., for leaks to the annulus above the SCSSV. By including several several WRFs in the risk assessment it is attempted to cover all risk aspects. There is therefore a risk of being overprotective. However, there is also a risk of running the risk if the acceptance criteria are set too high.

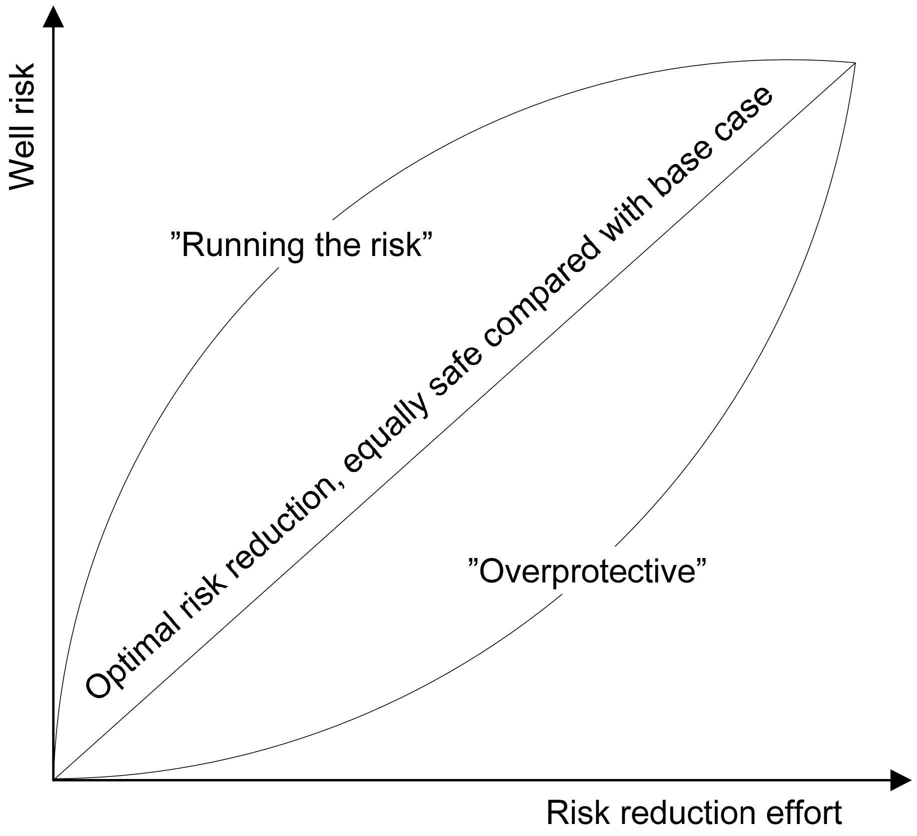


Figure 27 Risk assessment challenges

By applying the method suggested in the thesis there is also a risk that the well system moves closer to the edge, meaning that in the event of some sort of well system failure, there is less of safety margin for recovery to take place. This is similar to Perrow’s (1984) notion of “tight coupling” between systems. By the application of a wide range of WRFs this tendency is attempted reduced to a minimum. In particular WRF 7 – *Operations in the well* attempts to cover the recovery risk.

Another pitfall is the potential mismatch between the designer/method developer and user assumption. Designers are increasingly remote from the practitioner/operator of the system in many large-scale systems. A mismatch between designer and user expectations of how things should work may often occur. This mismatch may not be trivial, and sometimes may result in disaster (examples are given in Billings, 1996). Even if the procedure has been developed in close cooperation with the user (Norsk

Hydro), a mismatch between the method developers and the method users cannot be out ruled. A series of internal courses is planned in 2006 to reduce this risk.

When moving from rules to functional requirements, one could (simplified) say that one has moved from a regime with little degree of uncertainty to a regime with quantitative analysis to show acceptable safety margins. Included in such calculations are assumptions, (generic) reliability data, models, etc., which in sum gives an increased degree of uncertainty (especially when introducing new technology). This uncertainty can in most cases not be measured. In the worst case there is a risk of reducing the safety margin even if the probabilistic calculations do not show this decrease.

Because of this uncertainty a recommendation in NOU 2002:24 is to include some basic safety requirements with respect to barriers and redundancy from a precautionary principle. This strategy is also followed in the risk assessment method by including the two barrier principle and by recommending the leak rate criterion in API RP 14B. The recommended use of relative comparison with an accepted base case well also contributes to reducing the uncertainty.

7.3.2 Documentation of risk assessment process

There are problems related to verification of technology and assuring their safety. Kirwan (2001) highlights two main problems:

1. *Potential mismatch between the lifecycle of scientific investigation of new technology and the life cycle of the technological development itself.* Technology development used to take place over longer timescales, but this is no longer always the case. Underpinning research, checking the integrity of the new technology and looking for unwanted by-products may, take too long. It may cause a fatal delay of the technology's entry into the market. Given intense commercial pressure, a conflict of interest may then develop, with pressure to release the product into the market or industry.
2. *External regulations trying to control the fast developing products or systems*. External regulations should be able to question the emergence of the new technologies and limit their implementation until satisfactory research and testing has been completed. But many new products will not fit into existing and mature technology categories. The regulatory framework is at best a slow and bureaucratic

system, and may not be able to catch up with the new technology until it is already released.

Kirwan mainly focus on changes in technology, but the same points are relevant for changes in design and operating philosophy. Also, in the Norwegian oil sector there is increased focus on cost-effectiveness, resulting in introduction of new ways of both solving the technical issues and new ways of organizing the work. Kirwan (2001) gives an example from the introduction of new technology in aircraft cockpits. Experience has shown that there is a time lag between the introduction of new technology being implemented, and the occurrence and experience of system problems. Before these problems are known and the impact on the user of the system are realized, the design teams may be reduced and disbanded. This lag means that difficulties appear too late to be designed out, and therefore accidents may happen whereupon the industry is forced into costly refit. The same argument can be used for well systems, where new well designs constantly are being developed, and the life of existing wells is being extended. In this situation the risk assessment performed in the design phase and the changes in risk throughout the well life must be of high quality, have a broad scope and be well documented. In particular the "library" of standard well types may not capture all these aspects. The limitations in the analyses must therefore be known and criteria for when not to use the library should be clear. WRF 5 – *Failure cause* and WRF 6 – *Well barrier system and interfaces* are included to reduce this risk.

7.3.3 Well risk versus installation risk

Analysis and studies are performed on different system levels. Even if the proposed analyses and risk assessment method show that a given solution is acceptable on the well system level, the total risk on installation level is not modeled in this thesis. One problem is that a range of actors will be involved, and have different influence on the selected solution. As one of several possible approaches to this problem, Rasmussen (1997) recommends that the acceptable limits/level for safe operation of a system must be visible to the actors involved. The main challenge then becomes to identify the limits or barriers that actually exists in relation to different hazardous events and scenarios, and to make them known to the actors. In this perspective the methods and procedures suggested in this thesis may contribute to a better understanding of well risk for actors not only involved with well risk. For example, the barrier diagram method may contribute to better visualization and communication between well design and well operation personnel. Similarly the safety unavailability calculations may contribute with useful input to the actors involved with SIS design. The division into WRFs may contribute to visualize different risk aspects to different actors.

Often the methodology to show equality between technical solutions has a too narrow objective. This can also be claimed about analysis performed on well system level. The analysis might not be able to capture the spectrum of impacts a WBE failure has on safety. This argument can also be stated towards the risk analysis methods and risk assessment procedure described in this thesis. The thesis mainly covers technical aspects, and has in less degree assessed factors like operational complexity, more maintenance and the need for follow-up during operation. The influence from such factors must not be underestimated.

The well operator is supposed to intervene if there are deviations that exceed acceptable limits or due to abnormal incidents. In this situation the operator should be aware of the reason for the established limits, and have knowledge about how to handle deviations. The proposed risk assessment method may, e.g., result in increased dependence on pressure monitoring and/or changes in allowable pressure limits. Changes in established procedures may, e.g., influence on the operators ability to act when deviations occur. Another factor is that human under stress have a tendency not to act rational, but perform reflexive actions based on previous experiences from similar events (Reason, 1990). The risk assessment method proposed in the thesis does not cover the possible extra burden on the well operators. The risk assessment may result in risk reducing measures that might weaken the ability of the human to intervene if something unexpected happens. This factor may sometimes be important.

7.4 Further work

Well integrity is of increasing concern, and the field has gained more emphasis just over the past years. This is partly because of the growing number of mature fields and the application of technology, e.g. subsea and unmanned platform developments. Also, the regulations and standards governing the management of well integrity in various parts of the world are based on different approaches. In comparison the handling of SIS in high risk industries seems more uniform and has also been focused on over several years. A common best practice for well integrity is not established yet, and further work is necessary throughout the industry

This thesis do not attempt to cover all aspects of what is necessary to manage well risk, but may have contributed to bring the industry a step forward. Below suggestions to further improvements and work based on the PhD work are suggested.

Further testing of procedures and methods

The risk assessment method should be tested before implementation in the entire organization. Within Norsk Hydro, s series of courses is planned. The objective is to receive feedback from operational personnel before the method is implemented fully. In parallel with the courses case studies are performed within Norsk Hydro.

The methods applied in the risk analysis may also be further developed. For example the barrier diagram method may be further developed. In future, it should be possible to perform reliability analysis directly from the barrier diagram by, e.g., the development of a software tool.

Acceptance criteria

The acceptance criteria used by the operator are often generic and not flexible with respect to, e.g., well type. As an example today's API RP 14B leak rate requirements do not reflect that risk levels vary between installations and well types (platform vs. subsea wells, injectors vs. producers, etc.). Many operators have chosen to go beyond the acceptance criteria, more based on a perception of risk and/or convenience rather than actual verification of the required acceptance criteria. More research can be made on this area, and the split into WRFs may contribute to more focus on specific and diversified acceptance criteria.

Reliability data

One of the objectives in the thesis was to suggest improvement in the application of reliability input data. This is partly done by suggesting improved failure classification of

WBE failures (paper 5) and by improved analysis techniques (paper 5 and paper 2). However, the ambition was to perform detailed analysis of component failures, and, e.g., establish recommended reliability data and investigate failure causes in more detail. Due to limited access to field data this was not possible. However, this work will be increasingly important due to the increased average well age in the industry. The failure classification suggested in paper 5 and in section 4.2 may be a starting point for further research.

QRA and well risk assessment

In the start of the thesis it was stated that the QRA included coarse hazardous event frequency estimates. In the future it should be focused on how to improve these estimates both in the design and operational phase. One possible solution is to use quantitative analysis on well level as a supplement to the generic frequencies used today. One possible strategy is to develop a set (library) of well categories where the estimated blowout and well release frequency is compared relative to each other. The relative difference in blowout and well release frequency may be used as a supplement/correction factor to the historic blowout frequencies.

References

Albrechtsen, E. and P. Hokstad. 2002. *Reliability Data for Control and Safety Systems. 2002 Edition*. SINTEF report STF38 A02421, SINTEF, Trondheim, Norway.

API RP 14B. 1994. *Design, Installation, Repair and Operation of Subsurface Safety Valve Systems. 4th Edition*. American Petroleum Institute, Washington, DC.

API RP 14C/ISO 10418. 2001. Recommended practice for Analysis Design, Installation and Testing of Basic Surface Safety Systems for Offshore Production Platforms. 7th edition. (Note that the 4th Edition was issued as ISO 10418). American Petroleum Institute, Washington, DC.

Billings, C. 1996. *Aviation automation: The search for Human-Centered approach*. Lawrence Erlbaum Inc, New Jersey

Bourgoyne, A. T., S. L. Scott, and W. Manowski. 2000. *A Review of Sustained Casing Pressure Occurring on the OCS*, Louisiana State University, Baton Rouge.

BS 4778. British Standard: *Glossary of Terms Used in Quality Assurance Including Reliability and Maintainability Terms*. British Standards Institution, London.

Burton, K. 2005. Well structural integrity an increasing issue, Offshore Magazine, 2005, http://ogj.pennnet.com/

CARA Fault tree. 2004. CARA FaultTree. Computer program for fault tree analysis. Available from Sydvest Programvare AS. Internet address: http://www.sydvest.com.

CCPS. 2001. *Layer of Protection Analysis – Simplified Process Risk Assessment*. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York.

Cooke, R. and T. Bedford. 2002. Reliability databases in perspective. IEEE transactions on reliability **51:** 294-310

Cooke, R. M. 1996. The design of reliability databases. Part I and II. *Reliability Engineering and System Safety* **51**: 137-146 and 209-223.

Cox, A.W. 1991. *Classification of hazardous locations*, Institution of chemical engineers.

DEF-STD 00-56. 1996. *Safety Management Requirements for Defense Systems*. UK Defense Standardisation, Glasgow.

EIReDA. 1998. *European Industry Reliability Data Bank. Crete University Press*, Crete.

EN 12100-1. 2003. *Safety of Machinery. Basic concepts, general principles for design. Basic terminology and methodology*. European Committee for Standardization, Brussels.

Freudenburg, W. R. 2001. Risky thinking: facts, values and blind spots in societal decisions about risks. *Reliability Engineering & System Safety*, **72**: 125-130.

Hekkelstrand, B. and P. Skulstad. 2002. *Guideline for protection of pressurized systems exposed to fire.* Scandpower report no. 27.101.166/R1, Scandpower, Kjeller, Norway.

Hellevik, O. 1999. *Research Methodology in Sociology and Political Science (in Norwegian).* Unversitetsforlaget, Oslo.

Hirsch, R. L., R. Bezdek and R. Wendling. 2005. *Peaking of World Oil Production: Impacts, Mitigation & Risk Management*. United States Government, Washington DC. Internet: http://www.hilltoplancers.org/stories/hirsch0502.pdf

Hokstad, P. and K. Corneliussen. 2003. *Reliability Prediction method for Safety Instrumented Systems; PDS Method Handbook, 2003 Edition*. SINTEF Report STF38 A02420, SINTEF, Trondheim, Norway.

Hokstad, P., J.Vatn, T. Aven and M. Sørum. 2003. *Use of risk acceptance criteria in Norwegian offshore industry: dilemmas and challenges*. Proceeding of ESREL 2003, Balkema Publishers, Lisse, The Netherlands.

Holand, P. 1997. *Offshore Blowouts, Causes and Control*, Gulf Publishing Company, Houston.

HSE. 2002. *Offshore Hydrocarbon releases statistics*. HID statistics Report HSR 2001 002. Health and Safety Executive, Merseyside, UK.

IEC 50(191). 1990. *International Eletrotechical Vocabulary (IEV) – Chapter 191 – Dependability and Quality of Service*. International Electrotechnical Commission, Geneva.

IEC 60300-3-9. 1995. *International Standard on Dependability Management – Part 3: Application Guide – Section 9: Risk Analysis of Technological Systems.* International Standards Organization, Geneva.

IEC 61508. 1997. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Part 1-7. International Electrotechnical Commission, Geneva.

IEC 61511. 2003. *Functional Safety – Safety Instrumented Systems for the Process Industry*. International Electrotechnical Commission, Geneva.

IEEE Std. 352. 1982. *IEEE Guide for General Principles of Reliability Analysis for Nuclear Power Generating Stations*. Wiley, New York.

ISO 8402. 1986. *Quality Vocabulary*. International Standards Organization, Geneva.

ISO/TMB WG. 1998. *Risk Management Terminology – Guidelines for Use in Standards. First Working Draft*. ISO TMB Working Group on Risk Management Terminology, Secretariat: JISC, Japan.

Johnson, W.G. 1980. *MORT Safety Assurance Systems*. Marcel Dekker, New York.

Kirwan, B. 2001. Coping with accelerating socio-technical systems. *Safety Science*, Vol. **37:** 77-107.

Lygner, E. and A. Solli. 2002. Environmental Risk Indicators; Review and Proposal. Department of production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway.

MIL-STD 882D. 2000. *Standard practice for System Safety*. U.S. Department of Defense, Washington, DC.

MIL-STD-1629A. 1980. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*. U.S. Department of Defense, Washington, DC.

MIL-STD-2173(AS). 1986. *Reliability-Centered Maintenance. Requirements for naval Aircraft, Weapon Systems and Support Equipment*. U.S. Department of Defense, Washington, DC.

MMS 30 CFR 250 and 256. 2005. *Oil and Gas and Sulphur Operations in the Outer Continental Shelf*. The Minerals Management Services. (see http://www.gomr.mms.gov/)

Molnes, E. and G. O. Strand. 1999. Reliability of Well Completion Equipment – Phase III, Main Report. Exprosoft report 32.0898.00/04/99, ExproSoft, Trondheim, Norway.

Molnes, E., 1995. *Reliability analysis of subsea and well systems, Practical examples results and limitations,* Petrobras IV Technical meeting – Reliability engineering, Rio de janeiro, Brazil, 7-10 August 1995.

NASA. 2000. *Reliability Centered Maintenance Guide for Facilities and Collateral Equipment*. NASA Office of Safety and Mission Assurance, Washington, DC.

NASA. 2002. *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance, Washington, DC.

NORSOK D-010. 2004. *Well integrity in drilling and well operations. rev. 3.* (see http://www.standard.no/).

NORSOK O-CR-001. 1996. *Life cycle cost for systems and equipment. Rev. 1.* (see http://www.standard.no/).

NORSOK Z-013. 2001. *Risk and emergency preparedness analysis, revision 2.* (see http://www.standard.no/).

NOU 2000:24. 2000. *Et Sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Statens forvaltningstjeneste, Oslo.

NS 5814. 1991. *Requirements for Risk Analysis*. Norsk Standariseringsforbund, Oslo.

Øien, K. 1998. Improved quality of input data for maintenance optimization using expert judgment. Reliability Engineering and System Safety, **60**: 93-101.

Øien, K. 2001. *Risk Control of Offshore Installations – A framework for the Establishment of Risk Indicators.* PhD thesis, Department of production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway.

OLF. 2001. Veiledning for gjennomføring av miljøriskoanalyser for Petroleumsaktiviteter på norsk sokkel. Oljeindustriens landsforening (OLF), Oslo, Norway (see http://www.olf.no)

OLF. 2004. *Guideline on the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf.* The Norwegian Oil Industry Association, OLF Report 070 rev. 2 (see http://www.itk.ntnu.no/sil).

OREDA. 2002. *Offshore Reliability Data, 4th ed.* OREDA Participants. Available from: Det Norske Veritas, NO-1322 Høvik, Norway.

Perrow, C. 1984. *Normal accidents*. Basic Books, New York

Podio, A.L., J.N. McCoy, D.Becker, L.Rowlan and B. Drake. 2001. Total well Management II, SPE 67273, Society of petroleum engineers (SPE) production and operations symposium, Oklahoma.

PSA. 2001a. *Regulations relating to management in the petroleum activities (The management regulations)*, Petroleum Safety Authority, Stavanger, Norway. (see http:/www.ptil.no).

PSA. 2001b. *Regulations relating to design and outfitting of facilities etc. in the petroleum activities (the facilities regulations).* Petroleum Safety Authority, Stavanger, Norway. (see http:/www.ptil.no).

PSA. 2001c. *Regulations relating to health, environment and safety in the pteroluem activities (the framework regulations).* Petroleum Safety Authority, Stavanger, Norway. (see http:/www.ptil.no).

PSA. 2002. *The Risk Level on the Norwegian Continental Shelf* (In Norwegain - Risikonivå på norsk sokkel). Petroleum Safety Authority, Stavanger, Norway.

PSA. 2003. *Offshore Norway NPD's annual report 2002*. Petroleum Safety Authority, Stavanger, Norway.

PSA. 2003. *Trends in Risk Levels on the Norwegian Continental Shelf, Phase 3 Summary Report 2002*. Petroleum Safety Authority, Stavanger, Norway.

PSA. 2005. Press release from 10.3.2005 regarding the Snorre incident. (see www.ptil.no).

Rasmussen, J. 1997. Risk management in a dynamic society: a modeling problem. *Safety Science*, **27:** 183-213, 1997, Elsevier.

Rausand, M. and A. Høyland. 2004. *System Reliability Theory. Models, Statistical methods, and Applications. Second Edition*. Wiley, New York.

Reason, J. 1990. *Human error*. Cambridge University Press, Cambridge.

Roozenburg, N. F. M and J. Eekels. 1995. *Product design; Fundamentals and Methods*. John Wiley, Chichester.

Rouvroye, J.L. and A.C. Brombacher, 1999. New quantitative safety standards: different techniques, different results? *Reliability Engineering & System Safety*, **66:** 121-125, Elsevier.

Rouvroye, J.L. and E.G: van den Bliek, 2002. Comparing safety analysis techniques *Reliability Engineering & System Safety*, 75**:** 289-294, Elsevier.

Schlumberger. 2005. Oilfield glossary. Internet: http://www.slb.com/

SINTEF. 2005. SINTEF Offshore Blowout Database, Internet: http://www.sintef.no/

SINTEF/Scandpower. 1992. *Handbook for fire calculations and fire risk assessment in the process industry*. Sale and distribution performed by Scandpower A/S, N-2007 Kjeller, Norway.

Statoil. 2005. *Information about the Åsgard and Kristin field (use of HIPPS)* (see www.statoil.com).

SubseaMaster. 2006. ExproSoft SubseaMaster project, http://www.exprosoft.com/

Tarrants, W.E. 1980. *The measurement of Safety Performance*. Garland STPM Press, New York.

T-book. 1992. *Reliability Data of Components in Nordic Nuclear Power Plants, Version 3.* ATV-kanseliet and Studsvik AB, published by Vattenfall, Sweden.

The Royal Society. 1992. *Risk: Analysis, Perception and Management. Report of a Royal Society Study Group*. Published by the Royal Society, London.

Vatn, J. 1996. *Maintenance Optimization Models and Methods*. PhD thesis, Department of production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway.

WellMaster. 2006. WellMaster project, http://www.exprosoft.com/

Definitions

A-annulus	A term used for the annulus between the production tubing and the production casing.
Acceptance criteria	Criteria based on regulations, standards, experience and/or theoretical knowledge used as a basis for decisions about acceptable risk. Acceptance criteria may be expressed verbally or numerically (NS 5814)
Accident	An unintended event or sequence of events that causes death, injury, environmental or material damage (DEF-STD 00-56).
Analysis	An examination of a complex, its elements, and their relations; the use of methods and techniques of arranging facts to assist in deciding what additional facts are needed, establish consistency, validity and logic, establish necessary and sufficient events for causes, and guide and support inferences and judgments (Johnson 1980)
Availability	The ability of an item under combined aspects of its reliability, maintainability, and maintenance support) to perform its required function at a stated instant of time or over stated period of time (BS 4778).
B-annulus	A term used for the annulus between the production casing and the intermediate casing (next outer casing string)
Barriers	The physical and procedural measures to direct energy in wanted channels and control unwanted release (Johnson 1980).
Blowout	A blowout is an incident where formation fluid flows out of the well or between formation layers after all the predefined technical well barriers or the activation of the same have failed (*SINTEF,* 2005)
C-annulus	A term used for the annulus between the intermediate casing and the surface casing (next outer casing string).
Casing	Large-diameter pipe cemented in place during the initial well construction process to stabilize the wellbore. The casing forms a major structural component of the wellbore and serves several important functions: preventing the formation wall from caving into the wellbore, isolating the different formations to prevent the flow or crossflow of formation fluids, and providing a means of maintaining control of formation fluids and pressure while the well is drilled. The casing string also provides a means of securing surface pressure control equipment and downhole production equipment, such as the drilling blowout preventer (BOP), x-mas tree or production packer.

Casing joint	A length of steel pipe, generally around 40 ft [13 m] long with a threaded connection at each end. Casing joints are assembled to form a casing string of the correct length and specification for the wellbore in which it is installed (Schlumberger, 2005).
Casing program	A collective term that encompasses all casing and liner strings, including hangers and cement, located in a wellbore.
Causal analysis	A systematic procedure for describing and/or calculating the probability of causes for undesired events (NS 5814).
Causal model	Specification of the influence relations assumed to exist between a set of variables, often illustrated graphically using boxes and arrows (Hellevik 1999).
Common cause failure	Multiple component faults that occur at the same time or that occur in relatively small time window and that are due to a common cause (NASA 2002). Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure (IEC 61508, Part 4). Failures of different items resulting from the same direct cause where these failures are not consequences of other failures (NORSOK O-CR-001). Note: Failures that are consequences of other failures are called cascading failures.
Conductor (-casing/-pipe)	The outermost casing string in a casing program set to support the surface formations. The conductor is typically a short string set soon after drilling has commenced since the unconsolidated shallow formations can quickly wash out or cave in. Where loose wellbore surface soil exists, the conductor pipe may be driven into place before the drilling commences.
Consequence	An outcome of an event (ISO/TMB WG 1998). A possible result of an undesired event. Consequences may be expressed verbally or numerically to define the extent of injury to humans, or environmental or material damage (NS 5814).
Consequence analysis	A systematic procedure to describe and/or calculate the possible extent of human injury, and environmental or material damage as a result of undesired events (NS 5814).
Corrective maintenance	The actions performed, as a result of failure, to restore an item to a specified condition (MIL-STD-2173 (AS)). The maintenance carried out after a failure has occurred and intended to restore an item to a state in which it can perform its required function (BS 4778).
Criterion	A norm, i.e., rule or test against which (the quality of) performance can be measured (Johnson 1980).
Design life	Planned usage time for the total system (NORSOK O-CR-001).
Deviation	Departure from a norm (criterion) (Johnson 1980).
Distribution function	Consider a random variable *X*. the distribution function of *X* is $F_X(x) = P_r(X \le x)$ (Rausand and Høyland 2004)
Downtime	The period of time during which an item is not in a condition to perform its required function (BS 4778).

Equipment under control (EUC)	Equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities (IEC 61508, Part 4).
Error	Any significant deviation from a previously established, required or expected standard of human performance that results in unwanted or undesired time delay, difficulty, problem, trouble, incident, malfunction or failure (Johnson 1980).
Fail safe	A design property of an item that prevents its failures being critical failures (BS 4778). A design feature that ensures the system remains safe or, in the event of a failure, causes the system to revert to a state that will not cause a mishap (MIL-STD 882D).
Failure	The termination of its ability to perform a required function (BS 4778). An unacceptable deviation from the design tolerance or in the anticipated delivered service, an incorrect output, the incapacity to perform the desired function (NASA 2002). A cessation of proper function or performance; inability to meet a standard; non-performance of what is requested or expected (NASA 2000)
Failure cause	The physical or chemical processes, design defects, quality defects, part misapplication, or other processes which are the basic reason for failure or which initiate the physical process by which deterioration proceeds to failure (MIL-STD-1629A). The circumstances during design, manufacture, or use which have led to a failure (IEC 50(191))
Failure effect	The consequence(s) a failure mode has on the operation, function, or status of an item (MIL-STD 1629)
Failure mechanism	The physical, chemical or other process which has led to a failure (IEC 50(191)).
Failure rate	The rate of which failure occur as a function of time. If *T* denotes the time to failure of an item, the failure rate *z*(t) is defined as $z(t) = \lim\limits_{\Delta t \to \infty} \dfrac{\Pr(t < T \le t + \Delta t \mid T > t)}{\Delta t}$ The failure rate is sometimes called “force of mortality (FOM)” (Rausand and Høyland, 2004).
Fault	A defect, imperfection, mistake, or flaw, of varying severity that occurs within some hardware or software component or system. “Fault” is a general term and can range from a minor defect to a failure (NASA 2002). Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (IEC 61508, Part 4)
Fault mode (failure mode)	One of the possible states of a faulty item, for a given required function (IEC 50(191)).
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508, Part 4)
Frequency rate	The number of occurrences of a given type of event expressed in relation to a base unit of measure (for example, accidents per 1 million miles traveled (Tarrants 1980)

Full workover	Preventive or corrective maintenance carried out on a well by pulling the X-mas tree and well completion string.
Functional unit	Entity of hardware or software, or both, capable of accomplishing a specified purpose (IEC 61508, Part 4)
Hazard	Source of potential harm or situation with a potential for harm (IEC 60300-3-9)
Hazard identification	Process of recognizing that a hazard exists and defining its characteristics (IEC 60300-3-9).
Hazardous event	Event which can cause harm (IEC 60300-3-9).
Hidden failure	A failure not evident to crew or operator during the performance of normal duties (MIL-STD-2173(AS)).
Hydraulic control line	A small-diameter hydraulic line used to operate downhole completion equipment such as the surface controlled subsurface safety valve (SCSSV). Most systems operated by control line operate on a fail-safe basis. In this mode, the control line remains pressurized at all times. Any leak or failure results in loss of control line pressure, acting to close the safety valve and render the well safe (Schlumberger, 2005).
Incident	Any unplanned event resulting in, or having potential for, adverse consequences (ISO/TMB WG 1998).
Indicator	A measurable/operational variable that can be used to describe the condition of a broader phenomenon or aspect of reality (Øien 2001)
Intermediate casing	A casing string that is generally set in place after the surface casing and before the production casing. The intermediate casing string provides protection against caving of weak or abnormally pressured formations and enables the use of drilling fluids of different density necessary for the control of lower formations.
Item	Any part, component, device, subsystem, functional unit, equipment or system that can be individually considered (IEC 50(191)).
Light intervention	Preventive or corrective maintenance carried out on a well without pulling the X-mas tree or any part of the completion string. It also covers other interventions, e.g., wireline logging operations and production operations such as testing, stimulations, chemical injection and perforation. Note: Often also called a thru-tubing intervention
Liner	A casing string in which the top does not extend to the wellbore surface but instead is suspended from inside of the previous casing string.
Maintainability	The ability of an item, under stated conditions of use, to be retained in, or restored to, a state in which it can perform its required functions, when maintenance is performed under stated conditions and using prescribed procedures and resources (BS 4778).
Maintenance	The combinations of all technical and corresponding administrative actions, including supervision actions, intended to retain an entity in, or restore it to, a state in which it can perform its required function (IEC 50(191)).

Master valve	A valve located on the x-mas tree that controls all flow from the wellbore. A correctly functioning master valve is important and most surface trees have two master valves fitted. The upper master valve is used on a routine basis, with the lower master valve providing backup or contingency function in the event that the normal service valve is leaking and needs replacement (Schlumberger, 2005).
Mean time to failure (MTTF)	Let T denote the time to failure of an item, with probability density *f*(t) and survivor function *R*(t). the mean time to failure is the mean (expected) value of *T* which is given by $MTTF = \int_0^\infty t \cdot f(t)dt = \int_0^\infty R(t)dt$ (Rausand and Høyland 2004).
Model	Simplified representation of a phenomenon or object where some aspects are highlighted whereas other are left out (e.g., causal models) (Hellevik 1999).
Modification	The combination of all technical and administrative actions intended to change an item (IEC 50(191)).
Monitoring	Activity performed either manually or automatically, intended to observe the state of an item (IEC 50(191).
Partial workover	Preventive or corrective maintenance carried out on a well by pulling the X-mas tree and/or a part of the well completion string.
Performance criteria	Operational standards for use in determining effectiveness or efficiency (Tarrants 1980)
Preventive maintenance	The maintenance carried out at predetermined intervals or corresponding to prescribed criteria and intended to reduce the probability of failure or performance degradation of an item (BS 4778)
Primary well barrier	First object that prevents flow from a source (NORSOK D-010)
Probability density	Consider a random variable *X*. The probability density function f_X(x) of X is $f_X(x) = \frac{dF_X(x)}{dx} = \lim_{\Delta x \to \infty} \frac{\Pr(x < X \le x + \Delta X)}{\Delta x}$ where F_X(x) denotes the distribution function of *X* (Rausand and Høyland 2004).
Production casing	A casing string that is set across or at the start of the reservoir interval, and within which the main well completion components are installed.
Production packer	A well completion device used to isolate the annulus between the production tubing and the production casing (A-annulus), and to anchor or secure the bottom of the well completion string.
Protected x-mas tree	A x-mas tree with probability less than 1x10-4 per installation-year for critical barrier function impairment due to external hazardous loads (explosions, fires, dropped objects, trawls, iceberg/vessel collisions, etc.). This criterion is based on requirements to main safety functions stipulated in the PSA (2001b) “Facilities Regulations”. The opposite of a protected wellhead is called an ‘unprotected X-mas tree’

Qualitative	The characteristic elements, attribute, kind, or degree of quality possessed by something. Refers to characteristics (physical or non-physical, individual or typical) that constitutes the basic nature of something or is one of its distinguishing features (Tarrants 1980).
Quantitative	The property of anything that can be determined by measurement. The property of being measurable in dimensions, amounts, etc., or in extensions of these that can be expressed by numbers or symbols. A quantitative statement describes "how much", while a qualitative statement answers the question, "what kind is it?" or "how good is it?" (Tarrants 1980).
Redundancy	In an entity, the existence of more than one means of performing a required function (IEC 50(191)). Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information (IEC 61508, part 4).
Reliability	The ability of an item to perform a required function, under given environmental and operational conditions, and for a stated period of time (ISO 8402).
Reliability data	Reliability data is meant to include data for reliability, maintainability and maintenance supportability (NORSOK O-CR-001).
Repair	The part of corrective maintenance in which manual actions are performed on the entity (IEC 50(191)).
Required function	A function or combination of functions, of an entity, which is considered necessary to provide a given service (IEC 50 (191).
Risk	Combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event (IEC 60300-3-9). Risk designates the danger that undesired events represent for humans, the environment or material values. Risk is expressed in the probability and consequences of undesired events (NS 5814).
Risk analysis	Systematic use of available information to identify hazards and to estimate the risk to individual or populations, property or the environment (IEC 60300-3-9). Systematic use of available information to estimate the likelihood and consequences of risks and their components (ISO/TMB WG 1998). A systematic approach for describing and/or calculating risk. Risk analysis involves the identification of undesired events, and the causes and consequences of these events (NS 5814).
Risk assessment	Overall process of risk analysis and risk evaluation (IEC 60300-3-9).
Risk control	Process of decision-making for managing and/or reducing risk; its implementation, enforcement and re-evaluation from time to time, using results of risk assessment as one input (IEC 60300-3-9).
Risk criteria	A qualitative or quantitative statement of the acceptable standard of risk with which the assessed risk needs to be compared (The Royal Society 1992).
Risk evaluation	Process in which judgments are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects (IEC 60300-3-9). A comparison of the results of a risk analysis with the acceptance criteria for risk and other decision criteria (NS 5814).

Risk management	Systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating and controlling risk (IEC 60300-3-9).
Safety	Freedom from unacceptable risk (IEC 61508) Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property (MIL-STD-882D). The expectation that a system does not, under defined conditions, lead to a state in which human life is endangered (DEF-STD 00-56)
Safety function	Function to be implemented by a SIS (Safety Instrumented System), other technological safety-related system or external risk reduction facilities which is intended to achieve or maintain a safe state for the process in respect to a specific hazardous event (IEC 61511)
Safety integrity	Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period of time (IEC 61508, Part 4).
Safety integrity level (SIL)	Discrete level (one out of a possible four) for specifying the safety integrity requirement of a the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level has the lowest (IEC 61508, Part 4).
Seal assembly	A system of seals arranged on the component that engages in a sealbore to isolate the production-tubing conduit from the annulus. The seal assembly is typically longer than the sealbore to enable some movement of the components while maintaining an efficient seal (Schlumberger, 2005).
Secondary well barrier	Second object that prevents flow from a source
Surface casing	A casing string set inside the conductor in shallow but competent formations. The surface casing protects onshore fresh-water aquifers, and it provides minimal pressure integrity and thus enables a diverter or a blowout preventer (BOP) to be attached to the top of the surface casing string after it is successfully cemented in place. The surface casing provides structural strength so that the remaining casing strings may be suspended at the top and inside of the surface casing.
Surface controlled annular safety valve (SCASSV)	Same functionality as SCSSV but installed in annulus between production string and production casing. The valve is normally installed in a packer (Schlumberger, 2005).
Surface controlled subsurface safety valve (SCSSV)	A downhole safety valve that is operated from surface facilities through a control line strapped to the external surface of the production tubing. Two basic types of SCSSV are common: wireline retrievable, whereby the principal safety-valve components can be run and retrieved on slickline, and tubing retrievable, in which the entire safety-valve assembly is installed with the tubing string. The control system operates in a fail-safe mode, with hydraulic control pressure used to hold open a ball or flapper assembly that will close if the control pressure is lost (Schlumberger, 2005).

Survivor function	Let *T* denote the time to failure of an item. The survivor function *R(t)* of the item is $R(t) = \Pr(T > t)\ for\ t \geq 0$ R(t) is sometimes called the *reliability function* or the *survival probability* at time t of the item (Rausand and Høyland 2004).
System	A bounded physical entity that achieves in its domain a defined objective through interaction of its parts (DEF-STD 00-56). Set of elements which interact according to a design, where an element of a system can be another system, called subsystem, which may be controlling system or a controlled system and may include hardware, software and human interaction (IEC 61508, Part 4).
Systematic failure	Failure related in a deterministic way to a cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other factors (IEC 61508, Part 4).
Test frequency	The number of tests of the same type per unit time interval; the inverse of the test interval (IEEE Std. 352).
Test interval	The elapsed time between the initiation of identical tests on the same senor, channel, etc. (IEEE Std. 352).
Tubing hanger	A device attached to the topmost tubing joint in the wellhead to support the tubing string. The tubing hanger typically is located in the tubing head, with both components incorporating a sealing system to ensure that the tubing conduit and annulus are hydraulically isolated. (Schlumberger, 2005).
Tubing head	A wellhead component that supports the tubing hanger and provides a means of attaching the x-mas tree to the wellhead (Schlumberger, 2005).
Tubing joint	A single length of the pipe that is assembled to provide a conduit through which the oil or gas will be produced from a wellbore. Tubing joints are generally around 30 ft [9 m] long with a thread connection on each end (Schlumberger, 2005).
Undesired event	An event or conditions that can cause human injury or environmental or material damage (NS 5814).
Wear-out failure	A failure whose probability of occurrence increases with the passage of time, as a result of processes inherent in the entity (IEC 50(191)).
Well	A collective term that encompass the main entities used to enable a contained and controlled access to a (pressurized) formation. For example, in the operational phase, well will typically encompass the x-mas tree, wellhead, well completion and casing program.
Well barrier	A well barrier is an envelope of one or several dependent barrier elements, which are designed to prevent unintentional flow of formation fluids between formations or to the surroundings (NORSOK D-010).
Well Barrier Element (WBE)	An object that alone cannot prevent flow from one side to the other side of it self (NORSOK D-010).
Well completion	A collective term that encompass the assembly of tubing hanger, downhole tubular, safety valve, production packer and other equipment placed inside the production casing to enable safe and efficient surface access to a (pressurized) formation.

Well Integrity	The application of technical, operational and organizational solutions to reduce risk of uncontrolled release of formation fluids throughout the life cycle of the well (NORSOK D-010).
Well release	The reported incident is a well release if oil or gas flowed from the well from some point were flow was not intended and the flow was stopped by use of the barrier system that was available in the well at the time the incident started (SINTEF, 2005).
Wellhead	The surface/seabed termination of a wellbore that incorporates facilities for installing casing hangers during the well construction phase. The wellhead also incorporates a means of hanging the production tubing and installing the x-mas tree or other flow-control devices in preparation for the production of the well.
Wing valve	A valve located on the side of the x-mas tree. Two wing valves are generally fitted to the x-mas tree. A flowing wing valve is used to control and isolate production, and the service (kill) wing valve fitted on the opposite side of the Christmas tree is available for treatment or well-control purposes. The term wing valve typically is used when referring to the flowing wing (Schlumberger, 2005).
x-mas tree	An assembly of valves, spools, pressure gauges and chokes fitted to the wellhead to control the well flow. Note: In the PSA regulations (2001b), Christmas trees also encompass wellheads, casing hangers and annular preventers.

Acronyms

API	American Petroleum Institute
CCF	Common cause failures
DD	Dangerous detected
DHSV	Downhole safety valve
DU	Dangerous undetected
EIReDA	European industry reliability data
EN	European Norm
ESD	Emergency shutdown
EUC	Equipment under control
FAR	Fatal accident rate
FTA	Fault tree analysis
FTC	Fail to close
FTO	Fail to operate
HIPPS	High integrity pressure protection system
HSE	Health and Safety Executive
IEC	International Electrotechnical Commission
IEC	International Electrotechnical Commission
IPL	Independent protection layer
ISO	International Organization for Standardization
LCP	Leakage in closed position
LTA	Leak to annulus
MDWT	Mean dangerous waiting time
MIRA	Method for environmental risk analysis (Norwegian)
MMS	Mineral Management Services
MTTF	Mean time to failure

Acronyms

NCS	Norwegian continental shelf
NORSOK	The competitive standing of the Norwegian offshore sector (Norwegian)
NTNU	Norwegian University of Science and Technology
OLF	Norwegian Oil Industry Association (Norwegian)
OREDA	Offshore reliability data
PDS	Reliability of computer-based safety systems (Norwegian)
PFD	Probability of failure on demand
PMV	Production master valve
PSA	Petroleum Safety Authority
PWV	Production wing valve
QRA	Quantitative risk assessment
RBD	Reliability block diagram
RIDDOR	Reporting of injuries, diseases and dangerous occurrences regulations
ROV	Remotely operated vessel
RSC	Risk status code
SCASSV	Surface controlled annular safety valve
SCP	Sustained casing pressure
SCSSV	Surface controlled subsurface safety valve
SIL	Safety integrity level
SINTEF	Foundation of Science and Technology at the Norwegian Institute of Technology
SIS	Safety instrumented system
TLP	Tension leg platform
TR-SCSSV	Tubing retrievable surface controlled subsurface safety valve
UK	United Kingdom
UKCS	UK continental shelf
US	United States
US GoM	US Gulf of Mexico
WBE	Well barrier element
WRF	Well risk factor
WR-SCSSV	Wireline retrievable surface controlled subsurface safety valve

Papers

Paper 1 Approaches to the determinations of safety integrity levels (SIL) for Safety Instrumented Systems (SIS); comparison and discussion

Kjell Corneliussen, “The Third Edinburgh Conference on RISK: Analysis, Assessment and Management”, April 2002

Approaches to the determination of safety integrity levels (SIL) for Safety Instrumented Systems (SIS); comparison and discussion

Kjell Corneliussen
Department of Production and Quality Engineering
Norwegian University of Science and Technology (NTNU)
NO 7491 Trondheim, Norway
E-mail: kjell.corneliussen@ipk.ntnu.no

Abstract

The generic standard IEC 61508 uses a risk-based approach to determine the safety integrity levels (SIL) for Safety Instrumented Systems (SIS). The same approach is used in the process industry specific standard IEC 61511. In Norway, the Norwegian Petroleum Directorate (NPD), refers to these standards in the new regulations. The application of IEC 61508/61511 is generally considered to be beneficial, but experience has revealed two main drawbacks; (1) extensive work is necessary to come up with the required SIL specification, and (2) the methodology does not necessarily preserve good working solutions. Therefore, a separate guideline for the application of IEC 61058/61511 has been developed by the Norwegian Oil Industry Association (OLF). In particular the determination of SIL for the safety functions in offshore oil/gas production is treated. This paper examines the risk-based approaches for determination of SIL levels outlined in IEC 61508/61511 and compares them with the approach in the OLF guideline.

1 Introduction

A safety system is installed to mitigate the risk associated with the operation of a hazardous process. The role of the safety systems is twofold: (1) to prevent and detect deviations in critical process parameters, and (2) to control accident sequences. A safety instrumented system (SIS) is a safety system comprising electrical and/or electronic components. A SIS is composed of a logic solver and related field devices.

The most important benefit of using a SIS is the increased flexibility to change the system and to introduce new functions. In some cases SIS may be the only alternative, e.g., for subsea HIPPS solutions [5]. SIS is a helpful commodity, but may also be a challenging consideration for the system developers and the regulatory authorities [6-7].

Requirements to such systems have traditionally been addressed through prescriptive requirements, for example, related to how a function shall be implemented. An example of a formulation may be: “all pressure vessels shall be protected against overpressure by installation of pressure safety valves (PSVs), and a protection system based on pressure transmitters and closure of inlet”. A typical example of such an approach from the Norwegian oil industry is ISO 10418 [8]. This type of standards offers little flexibility in realising safety functions. One of the arguments for developing risk-based standards is to meet the need for coping with rapidly developing technology and future developments. IEC 61508 [1] is an example of such a standard, and this standard is currently given the most attention within the SIS industry. This standard sets out a generic approach for all safety lifecycle activities for SIS. IEC 61508 is a generic standard common to several industries, and the process industry is currently developing their own sector specific standard for application of SIS, called the IEC 61511 [2]. The standards present a unified approach to achieve a rational and consistent technical policy for all SIS systems.

The application of IEC 61508/61511 is generally considered to be beneficial, but experience has clearly revealed two main drawbacks; (1) extensive work is necessary to come up with the requirements to the SIS for a specific application, and (2) the methodology does not necessarily preserve good working solutions [4]. The Norwegian Oil Industry Association (OLF) has therefore developed a guideline to support the use of IEC 61508/61511 [4]. In the new regulations from the Norwegian Petroleum Directorate (NPD) [3] specific references are given to the IEC standards and the guideline.

The OLF guideline do not describe a fully risk based approach according to IEC 61508, and the objective of this paper is to describe the two approaches, to illustrate the differences and to discuss the challenges and pitfalls involved with both approaches.

2 The IEC 61508 approach for determining SIL

IEC 61508/61511 consider all relevant hardware and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance, to decommissioning). The standards describe an overall safety strategy were all the safety-related systems are taken into consideration in order to ensure that the risk is reduced to an acceptable level. The standards distinguish between three different types of safety-related systems:

- SIS systems
- Safety-related systems based on other technology
- External risk reduction facilities, e.g., fire walls, physical distance/layout, manual intervention/procedures, etc.)

IEC 61508/61511 requirements are only given for instrumented safety systems. The necessary risk reduction will, however, also require that safety functions depending on “other technology”/”external risk reduction” are capable of providing a given protection level. Figure 1 illustrates some typical safety systems for pressure protection of a separator.

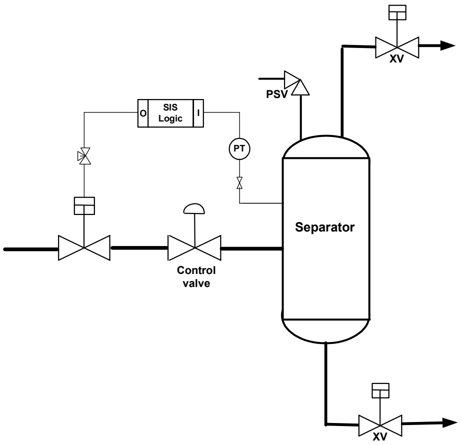


Figure 1 Example of safety-related systems

IEC 61508 focuses on safety functions, and the term “functional safety” is a characteristic of the safety-related system, whereas “safety” is a characteristic of the equipment that produces the risk. The focus on functional safety requires a performance measure to be introduced. Thus, “safety integrity” and safety integrity levels ("SIL") is introduced. SIL is introduced for specifying the target level of safety integrity. There are three main types of requirements that have to be fulfilled in order to achieve a given SIL:

- A quantitative requirement, expressed as a probability of failure on demand (PFD), or alternatively as the probability of a dangerous failure per hour.
- A qualitative requirement, expressed as architectural constraints on the subsystems constituting the safety function.
- Requirements concerning which techniques and measures should be used to avoid and control systematic faults.

The general risk assessment procedure is illustrated in Figure 2. The relations to the risk reduction framework in IEC 61508/61511 are also illustrated. The first step is to define the Equipment under control (EUC). This is the equipment to be protected. Initially, it is assumed that no safety-related systems are installed. The next step is to perform a hazard and risk analysis to identify hazardous events [1]. The standards do not prescribe any particular method to be applied, and may range from simple screening analysis to Hazard and Operability Study (HAZOP)[9]. When, e.g., the HAZOP is completed, the initial risk (“EUC risk) [1] should be understood. A risk acceptance criterion must be defined in order to determine the required risk reduction (ref. Figure 2). Acceptable risk would normally be defined by the user, and is outside the scope of IEC 61508/61511.

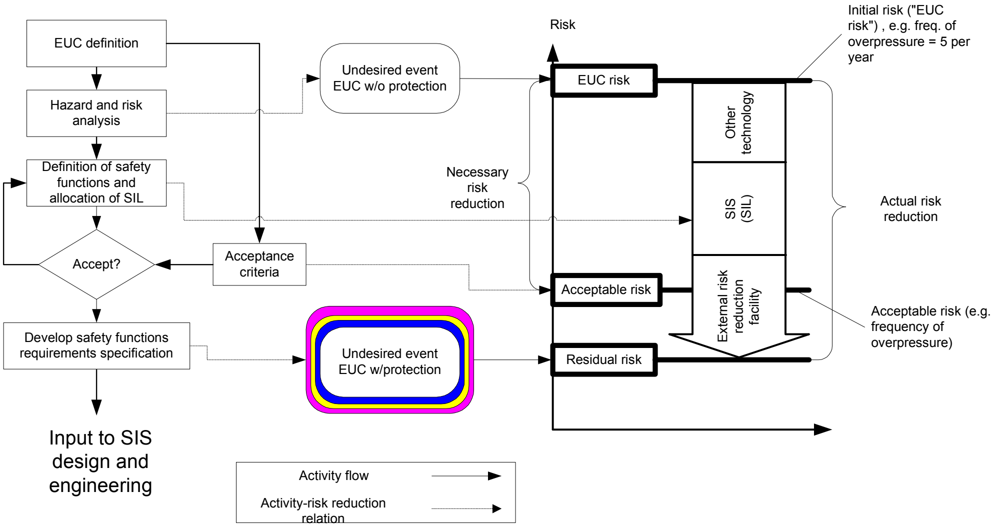

EUC definition
Hazard and risk analysis
Definition of safety functions and allocation of SIL
Accept?
Acceptance criteria
Develop safety functions requirements specification
Input to SIS design and engineering
Undesired event EUC w/o protection
Undesired event EUC w/protection
Risk
EUC risk
Other technology
SIS (SIL)
External risk reduction facility
Necessary risk reduction
Acceptable risk
Residual risk
Actual risk reduction
Initial risk ("EUC risk") , e.g. freq. of overpressure = 5 per year
Acceptable risk (e.g. frequency of overpressure)
Activity flow
Activity-risk reduction relation

Figure 2 **Generalized method for determination of SIL for SIS**

If the risk is found unacceptable, safety-related systems must be introduced to reduce the risk. If it is identified that a SIS is required, the safety integrity level (SIL) should be assigned. In the informative annexes to IEC 61511-3 [2] a number of alternative methods are presented. The methods are:

- The Semi-Quantitative Method is based on input from a hazard and risk analysis for identification of hazardous events, and different causes of these events. The resulting probability of an hazardous event is summarised in a fault tree, and the resulting consequences of the undesired event are summarised in an event tree. Safety-related systems are included in the event tree to reduce the probability of the hazardous event to occur. The method is of particular value when the acceptable risk is specified numerically (for example that a hazardous event should not occur with a greater frequency than 1 in 100 years).

- The Safety Layer Matrix Method [10] is applied after "safety-related systems based on other technology" have been included, and the need for an additional SIS has been identified. The method uses a matrix with frequency, severity and number of other safety related systems. The categories are described in general terms and must be calibrated to get consistent results.
- Calibrated Risk Graph is a semi-qualitative method that uses four parameters, which together describe the nature of the hazardous situation when safety instrumented systems fail, or are not available. The parameters are combined to decide the safety integrity level. The parameters are described in general terms and must be calibrated. As for the safety layer matrix, the need for SIS must be identified after other safety related systems have been included.
- Layer of Protection Analysis (LOPA) [11] is based on the hazardous events identified in the Hazard and Operability analysis (HAZOP). The total risk reduction from all safety related systems are included in a standard tabular form.

The approach above is iterative, and after the risk is found acceptable the required SIL is identified for the SIS. The next step is to establish the safety requirement specification for the SIS, and hand the specification over to the system developers for design.

3 IEC 61508 challenges and pitfalls

There is an obvious question how we, from a risk-based approach, can ascertain that SIS functions will perform satisfactorily, and whether the safety added by such systems is adequate and consistent. The process for SIL determination described above attempts to deal with the risk of each hazardous event and the capability of SIS and other safety-related systems to reduce the risk to an acceptable level. This process must be rational and consistent among risk analysis teams, development projects, companies, and industry sectors. It is important to have a clear understanding of (1) the risk assessment procedure (ref. Figure 2), (2) what is acceptable risk, and (3) how SIL determination should be performed. In order to achieve this, it is important to be aware of the challenges and pitfalls by using this approach. Some of the main challenges are:

- Compared to a deterministic approach, using the SIL allocation methods in IEC 61508/61511, the methods will introduce considerable amounts of additional analysis work. There is a risk of companies not realising the consequence of implementing the IEC approach. Experience has shown that the IEC approach for many industries require extensive additional analyses, and the risk assessment process should be designed to prioritise events with high severity and high likelihood. There is also a possibility of selecting sub-optimal safety integrity levels, when taking into consideration the numerous safety functions present, on e.g. an oil installation.
- When moving from a deterministic approach, with SIS solutions based on experience, with a design practice that has resulted in a safety level considered adequate, there is a risk of moving to a design practice that is not "proven in

use". The capability of each safety related system and the PFD estimate may be also be uncertain, and assumptions and uncertainties in the estimates must be documented. This uncertainty may also lead to a solution were the actual safety level is not acceptable.

- It is important that the companies define acceptable risk. If not there is a risk of selecting sub-optimal safety integrity levels.
- The risk assessment process is an iterative process that is performed until an acceptable risk level is reached, taking all risk reducing measures into consideration, and it is important that the results and assumptions are clearly documented. The risk assessment process should also facilitate for examination by other teams or later in the safety life cycle by people responsible for operation. In operation, it will be useful in order to handle safety functions that are taken out of service and also to verify that the initial risk assessment is in accordance with the operating conditions. Some of the methods for SIL determination do not deal with these factors explicitly.

The challenges above indicate that the risk assessment process, including the SIL allocation process must consider the risk of the hazardous events event, measure it against tolerable risk, and allocate SIL levels in a consistent way. The uncertainty in estimates should be documented in a way such that other teams or operating personnel can verify the results. Each company must consider these criteria when they develop individual risk assessment procedures. All the SIL allocation methods in IEC 61511 can be used in this process; the LOPA and the semi-quantitative method do, however, fit the criteria above more easily. The risk graph and the safety layer method require more calibration, and are applied only to decide the SIL for the SIS. These two methods are also not so explicit when considering acceptable risk, and the risk reduction from other safety-related systems.

4 The method for determining the required safety integrity level in the Norwegian oil sector

The offshore industry in Norway has been concerned with challenges discussed in the previous section, and the move from SIS solutions based on experience, with a design practice that has resulted in a safety level considered adequate, to a risk based approach adopted from IEC 61508/61511.

These concerns resulted in a compromise between the IEC approach and the previous deterministic approach for protection of process equipment, based on API 14C/ISO 10418 [8]. The approach is described in the OLF guideline [4], which describes an approach where minimum SIL requirements have been set to most common safety functions on an oil installation. The Norwegian Petroleum Directorate (NPD) has recently issued new regulations [3], were it is referred to the OLF guideline and the IEC standards. The background for establishing minimum SIL requirements is that application of IEC 61508/61511, although beneficial, is experienced to have two main drawbacks: (1) extensive work is necessary to come up with necessary SIL specification, and (2) the methodology does not necessarily preserve good working solutions[4].

Figure 3 illustrates the process for developing and allocating SIL requirements. This is not a fully risk based approach, and for most functions the OLF guideline gives minimum SIL requirements (i.e., fixed SILs are given independent of any risk analyses). These levels should be adhered to whenever possible and are based on, e.g.:

- Current practice,
- Available generic reliability data,
- What is technically possible with today's technology

Needs for deviating from these requirements will, however, arise, e.g., due to technological advances as well as special conceptual or operational aspects. Whenever identified, these "deviations" need to be treated according to IEC 61508/61511 methodology, i.e., the safety integrity level should be based upon a qualitative or quantitative risk based method.

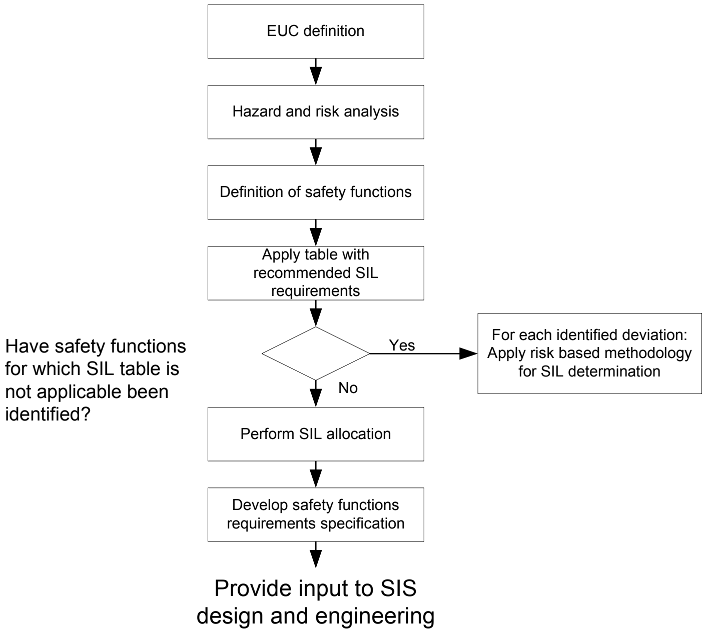

EUC definition
Hazard and risk analysis
Definition of safety functions
Apply table with recommended SIL requirements
Have safety functions for which SIL table is not applicable been identified?
Yes
For each identified deviation: Apply risk based methodology for SIL determination
No
Perform SIL allocation
Develop safety functions requirements specification
Provide input to SIS design and engineering

Figure 3 Flowchart for SIL development and allocation (OLF, 2000)

5 Challenges and pitfalls when using minimum SIL values

The OLF approach saves time in the hazard and risk analysis process, reduces documentation in justifying the SIL choice, and ensures consistency across process units. The process for SIL determination for SIS is, however, not fully in line with the risk based approach in IEC 61508/61511. The main challenges associated with the OLF approach are:

- For several safety functions it is difficult to establish generic definitions, due to process specific conditions, size of fire area, design and operational philosophies, etc., the number of final elements to be activated upon a specified cause will, for example, differ from case to case. There is therefore a risk of selecting a minimum SIL level that is not applicable for the actual application. The guideline have to some extent compensated for this by giving several of the requirements on a sub-function level rather than for an entire safety function.
- It is not necessary to define initial risk or acceptable risk, and hence the minimum SIL values are not related to the frequency or acceptance criteria of the hazardous event. It is therefore not possible to measure SIL level against acceptable risk. It is however stated in the guideline, that the minimum SIL requirements should be used as input to QRA (quantitative risk analysis, on

platform level), which will then represent a verification of the stated requirements. If the QRA reveals that the overall risk level is too high, then this could trigger a stricter requirement to one or more of the safety functions. Other types of analyses performed in the design phase may also introduce more stringent requirements than specified in the minimum SIL table.

- It is important to identify deviations from the assumptions the minimum SIL table is based on. The OLF guideline describes two types of deviations: (1) a functional deviations is a safety function not covered by the minimum SIL table, (2) an integrity deviation where an instrumented safety function as described in the minimum SIL table has been identified, but particular conditions imply a different integrity level requirement (e.g., related to the frequency of the associated hazard). To neglect such deviations, may result in applying the minimum SIL table based on wrong assumptions.
- The minimum SIL table is based on generic data, and this could give unrealistic SIL values. It is important that the input data for the minimum SIL table are realistic both with respect to the failure rates being representative for new equipment as well as the test intervals. When using "conservative" failure rates and/or long test intervals for calculating the failure probability of a given function, the resulting PFD ≈ $\lambda \cdot \tau / 2$, becomes "high" [12]. Accordingly, a "low" SIL value will be claimed for the function, resulting in a "non-conservative" requirement in the minimum SIL table. The applied failure rates are to a large degree based upon the PDS report "Reliability Data for Control and Safety Systems, 1998 Edition" [14] which is considered the most "up to date" database for the referred equipment. There are however "gaps" in the data, and there has been an increased the focus on collection of reliability data for SIS in the Norwegian sector, after the introduction of new NPD regulations and the OLF guideline.

6 Conclusions

In this paper the risk based approach outlined in IEC 61508/61511, and an alternative approach based on the Norwegian guideline for the application of the same standards, have been described. Both approaches must be rational and consistent among risk analysis teams, development projects, companies, and industry sectors, and important challenges in this respect have been discussed in the paper. A general conclusion is that the approaches must be thoroughly documented, so that the assumptions and uncertainties in the assessments are easily available for other parties. For future work it will be important to assess how the industry implements the approaches, both individually and also by comparing the approaches against each other.

Acknowledgements to fellow colleagues at SINTEF, who was involved in the development of the OLF guideline, and to Marvin Rausand for asking the right questions.

References

[1] IEC 61508. 2000. Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. International Electrotechnical Commission, Geneva.

[2] IEC 61511 (CDV). 2000. Functional safety: Safety Instrumented Systems for the process industry sector. International Electrotechnical Commission, Geneva.

[3] NPD Regulations. 2001. NPD Regulations relating to the Design and Outfitting of Facilities etc. in the Petroleum Activities (the Facilities Regulations). Norwegian Petroleum Directorate (NPD), Stavanger.

[4] OLF Recommended Guidelines, No.: 066, Revision no.: 01. 2000. OLF Recommended Guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf. Oljeindustriens Landsforening, Stavanger.

[5] Hokstad, P., S. Hauge and T. Onshus. 2001. Bruk av HIPPS for utstyrsbeskyttelse, STF38 A01422. SINTEF Industrial Management, Trondheim.

[6] Karydas, D. M., and A.C. Brombacher. 1999. Reliability certification of programmable electronic systems, *Reliability Engineering & System Safety*, 66, pp. 103-107. Elsevier, Oxford.

[7] Kirwan, B. Coping with accelerating socio-technical systems. *Safety Science*, Vol. 37, pp. 77-107. Elsevier, Oxford, 2001

[8] ISO/WD 10418 rev. 4. 1999. Petroleum and natural gas industries - Offshore production installations – Analysis, design, installation and testing of basic surface safety systems for offshore installations – Requirements and guidelines. International Standardisation Organization.

[9] IEC 61882. Hazard and operability studies (HAZOP studies) - Application guide. International Electrotechnical Commission, Geneva.

[10] Center for Chemical process Safety (CCPS). 1993. *Guidelines for Safe Automation of Chemical Processes*. American Institute of Chemical Engineers, New York.

[11] Dowell, A.M. 1998. Layer of protection analysis for determining safty integrity level. *ISA Transactions*, Vol 37, pp. 155-165. Elsevier, Oxford.

[12] Høyland, A. and M. Rausand. 1994. *System Reliability Theory; Models and Statistical Methods*. Wiley, New York.

[13] OREDA, Offshore Reliability Data Handbook - third Edition. 1997. Det Norske Veritas, Høvik.

[14] Aarø, R. and G.K. Hansen. 1998. Reliability Data for Control and Safety Systems – 1998 Edition, STF38 A98445. SINTEF Industrial Management, Trondheim.

Paper 2 Loss of safety assessment and the IEC 61508 standard

Per Hokstad and Kjell Corneliussen, Reliability Engineering and System Safety 83 (2004) 111-120.

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Reliability Engineering and System Safety 83 (2004) 111–120

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Loss of safety assessment and the IEC 61508 standard

Per Hokstad*, Kjell Corneliussen

Department of Safety and Reliability, SINTEF Industrial Management, Trondheim N-7465, Norway

Abstract

The standard IEC 61508 contains a lot of useful information and guidance for safety improvement regarding the use of safety systems. However, some of the basic concepts and methods for loss of safety quantification are somewhat confusing. This paper discusses the failure classification, the various contributions to the safety unavailability, and in particular the common cause failure (CCF) model presented in this standard. Suggestions for clarifications and improvements are provided. In particular, a new CCF model is suggested, denoted the Multiple Beta Factor model.

Keywords: IEC 61508; Safety unavailability; Failure classification; Common cause failures; Multiple beta factor model; Probability of failure on demand

1. Introduction

Today it seems evident that, at least in Europe, IEC 61508 [1] will become the central standard for specification, design and operation of Safety Instrumented Systems (SIS). Thus, the standard will have a major impact on the safety work, e.g. within the process industry. Whereas IEC 61508 is a generic standard common to several industries, the process industry is currently developing its own sector specific standard for application of SIS, i.e. IEC 61511 [2].

One recent indication is that the Norwegian offshore industry has now finalised guidelines for the use of the standards IEC 61508 and IEC 61511, see Refs. [3,4], (and will be revised in 2003). The Norwegian Petroleum Directorate refers to this guideline in their new regulations [5]. Overall, it is expected that these standards will contribute to a more systematic safety work in the industry and also to increased safety.

However, it has been realised that it may be difficult to apply the standard in a practical and useful way. Also, there seems to be a couple of ambiguities that impairs the usefulness of the standards, and may contribute to some confusion. These observations relate to the failure classification and to the quantification of Probability of Failure on Demand (PFD), which is the measure for loss of safety used in the standard.

The objective of the present paper is to present some suggestions for modification and clarification of the approach suggested in IEC 61508. The advantage of arriving at consensus on the main concepts and methods is obvious. So we maintain the IEC notation, but extend the notation by introducing some additional concepts not defined in the standard.

The paper has a focus not only on the quantification of loss of safety, but also considers related and more basic questions concerning failure classification. In the standard, there is an apparent inconsistency or at least ambiguity regarding the definition and use of the terms *random hardware failures* and *systematic failures*, and how these relate to Common Cause Failures (CCFs). This classification is discussed and some suggestions are given. Further, we discuss the different contributions to loss of safety from various failure categories, and suggest various measures for loss of safety.

Our major objective regarding the IEC approach for quantification of loss of safety relates to its suggestion to apply the β-factor (i.e. beta factor) model for quantification of CCFs. This β-factor method, as introduced in IEC 61508, will not distinguish between the performance of various voting logics like 1oo2 (1-out-of-2) and 2oo3. This is usually not satisfactory for the safety engineer of today, and an extended version of the β-factor model is presented, denoted the multiple beta factor (MBF) model.

Several suggestions presented in the paper can be traced back to the research project PDS (*Reliability and availability of computerised safety systems*) carried out for the Norwegian offshore industry some 10–15 years ago, see Refs. [6–9]. A forum succeeded the project, and this is still active [10–13]. This forum has recently modified

* Corresponding author. Tel.: +47-7359-2754; fax: +47-7359-2896.
E-mail address: per.hokstad@sintef.no (P. Hokstad).

0951-8320/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2003.09.017

Nomenclature

CCF	common cause failure
CSU	critical safety unavailability
D	dangerous failure (failure category in IEC standard)
DD	dangerous detected (failure category in IEC standard)
DU	dangerous undetected (failure category in IEC standard)
E/E/PES	electrical/electronic/programmable electronic system
IEC	International Electrotechnical Commission
MBF	multiple beta factor
MTTR	mean time to restoration
NSU	non-critical safety unavailability
PDS	Norwegian acronym for 'availability of computerised safety systems'
PFD	probability of failure on demand
PSF	probability of systematic failure
SIS	safety instrumented system
τ	Time elapsing between functional tests ($= T_1$ in the IEC notation)

the approach for loss of safety quantification, e.g. by adapting the notation to the IEC standard, and by incorporating the MBF model, see Refs. [13,14].

It is the intention that the results of the present paper will contribute to a better understanding of these fundamental issues, and that a more mature way to perform loss of safety quantifications will emerge. It is our hope that the paper can contribute to further discussions and eventually some consensus on the basic approach for safety calculations.

2. Failure classification

First we look at the failure classification as it appears in the standard [1] and then make some suggestions. According to the standard (see Note 4 in Section 3.6.6 of part 4), failures of a safety-related system can be categorised either as a random hardware failure or as a systematic failure. However, in a few places of the standard also, the term *hardware failure* is used (without attaching the term 'random'), e.g. see Annex B of Part 6. This introduces some inconsistency and makes the classification somewhat confusing, but probably the term *random hardware failure* is used synonymously with hardware failure. Finally, the standard also treats *software failures*, but we consider this as a subclass of the systematic failures, e.g. see Note 3 on p16 of IEC 61508-4 (i.e. part 4 of IEC 61508).

A random hardware failure is according to IEC 61508-4 (Section 3.6.5) a "failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware". From this definition, we could interpret the term *random hardware failure* as a failure that occurs without the failed component being exposed to any kind of 'excessive' stress, e.g. see the beginning of Section D.2 of IEC 61508-6. In the literature, this has also been referred to as 'natural ageing' failures. However, the standard may actually intend to include all hardware failures into this category.

IEC 61508-4 (Section 3.6.6) defines a systematic failure as a "failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or the manufacturing process, operational procedures, documentation or other relevant factors". So it includes all types of failures caused by design errors (e.g. inability of smoke detector to distinguish between smoke and steam, 'erroneous' location of gas detector and software errors). Further, these failures may be caused by operational errors (e.g. operator forgets to remove by-pass of the safety system after an inspection). Thus, modification rather than corrective maintenance of the hardware is required to eliminate these failures.

Note that the standard makes a clear distinction between these two failure categories, and it states that random hardware failures should be quantified, but systematic failures should not (IEC 61508-2).

The above classification and definitions should be compared with the description of hardware-related CCFs given in IEC 61508-6, Section D.2: "However, some failures, i.e. common cause failures, which result from a single cause, may affect more than one channel. These may result from a systematic fault (for example, a design or specification mistake) or an external stress leading to an early random hardware failure". As an example, the standard refer to excessive temperature of a common cooling fan, which accelerates the life of the component or takes them outside their specified operating environment.

So, the CCFs may either result from a systematic fault or it is a random hardware failure due to common excessive stress on the components. Apparently, only those CCFs arising from excessive stresses on the hardware are quantified. However, it could be somewhat confusing that these falls into the category 'random hardware failures'. We assume that several reliability engineers would delete the word *random* here. However, we will use random hardware failure to be in line with the standard. Below, we suggest a notation that makes a distinction between those random hardware failures that are caused by natural ageing and those which are caused by excessive stresses (and therefore, may lead to CCFs).

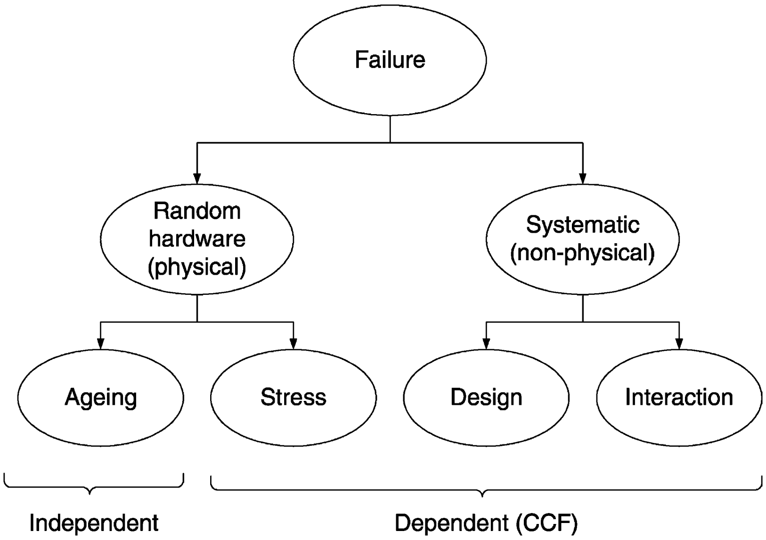


Fig. 1. Failure classification by cause of failure.

To be specific, the following concepts and failure categorisation are suggested, see Fig. 1:

1. *Random hardware failures* are *physical failures*, and are split into
   - ○ *Ageing* failures, which are failures occurring under conditions within the design envelope of the component.
   - ○ *Stress* failures, which occur when excessive stresses are placed on the component. The stresses may be caused either by external/environmental causes or by human errors during operation. An example is damage to gas detectors due to inadequate protection during sand blasting.
2. *Systematic failures* are *non-physical failures*, and are split into
   - ○ *Design* failures, which are initiated during engineering and construction, and may be latent from the first day of operation. Examples are software failures, sensors that do not discriminate between true and false demands, and erroneous location of fire/gas detectors.
   - ○ *Interaction* failures, which are initiated by human errors during operation or maintenance/testing. Examples are loops left in the override position after completion of maintenance, and erroneous calibration of sensors during testing. Another example is scaffolding that cover up sensors.

When there is a random hardware failure, the delivered service deviates from the specified service due to physical degradation. All random hardware failures are quantified, and a CCF model is introduced to account for the stress failures.

When there is a systematic failure, the delivered service deviates from the specified service, without a random hardware failure being present (i.e. no physical degradation). Then the failure can only be eliminated by a modification of the design or the manufacturing process, operating procedures, documentation or other relevant factors. The standard suggests that the systematic failures should not be quantified.

Note that random hardware failure could also be denoted physical failure, and systematic failure could be referred to as non-physical failure. Finally, the failures can be classified into the two categories:

- *Independent failures*, including the single category aging
- *Dependent failures* (or CCFs) including the three categories
  - ○ Stress
  - ○ Design
  - ○ Interaction

Following the standard, only the first category (stress) should be quantified, whereas interaction and design are systematic failures and thus are not quantified.

The above suggestion is a recent update (see Ref. [14]) of the failure classification previously introduced in the PDS project (see Refs. [6–10]), but now adapted to the IEC 61508 notation. We do not believe this categorisation to be in conflict with that of IEC 61508.

When it comes to quantification of loss of safety, the Standard introduces λ_{DU}, representing the rate of Dangerous Undetected (DU)[1] random hardware failures, i.e. including both ageing failures and stress failures. Now using the β-factor model, it follows that $(1-\beta)\lambda_{\mathrm{DU}}$ is the rate of independent failures, i.e. ageing failures. Similarly, $\beta\lambda_{\mathrm{DU}}$ is the rate those CCFs that are quantified, i.e. the random hardware failures due to excessive stress.

[1] DU failures are *Dangerous* failures (i.e. preventing shutdown on demand), which are *Undetected* by built in self-tests of the system. The DU failures are also denoted 'dormant'. Similarly, DD failures = *Dangerous* failures *Detected* by built in self-tests.

3. Contributions to loss of safety quantification

Before starting to discuss the quantification of loss of safety for a safety system, it is sensible to discuss the contributions to loss of safety from the various failure categories (causes) in Fig. 1. Actually it may be advantageous to introduce various measures for loss of safety, arising from the different contributions.

In addition to splitting the contributions according to failure cause, we suggest splitting the loss of safety contributions according to whether or not the unavailability is 'known'. The period of 'unknown' unavailability is here given as the period elapsing from a DU failure occurs, until it is detected by functional testing or possibly by a true demand. The period of known unavailability is the time elapsing from a dangerous (D) failure is detected, until it is restored. The known unavailability may also include the time needed to perform functional testing. During periods of known unavailability, alternative safety precautions may then be taken (e.g. shutting down), and hence is much less critical than the periods of unknown unavailability.

Following this argument, we suggest to make explicit the known and unknown contributions to loss of safety. This split is, however, introduced for random hardware failures only. For systematic failures, where there is no repair and no functional testing, we will (for simplicity) assume all unavailability to be unknown.

Thus, the total safety unavailability of a safety system is split into the following contributions:

1. *Unavailability due to random hardware failures*, split into
   (a) The unknown unavailability due to DU random hardware failures (of rate λ_{DU}). The average period of unavailability due to such a failure is $\tau/2$, where τ is the period of functional testing. In this period, the failure has not been detected, and it is not known that the component is unavailable
   (b) The known unavailability due to dangerous (D) random hardware failures. The average period of unavailability due to these events is equal to the mean restoration time, MTTR, i.e. time elapsing from the failure is detected until the situation is restored.
   (c) The known (or 'planned') unavailability due to the inhibition time during inspection/functional testing.
2. *Unavailability due to systematic failures.* Also this unavailability is caused by 'dormant' (dangerous and undetected) failures. Note that all the unavailability due to systematic failures is considered to be unknown.

Observe that the contributions to loss of safety of categories 1(b) and 1(c) will depend on the operating philosophy, e.g. whether any action is taken when a failure is detected. This provides a good reason to treat these contributions separately and not together with contribution 1(a). Often both the contributions 1(b) and 1(c) are very small compared to that of 1(a). That is, usually MTTR $\ll \tau$, but this is not always the case; e.g. for subsea equipment in offshore oil/gas production, the MTTR could be rather long. Category 1(c) is the least critical, as this represents a truly planned unavailability of the safety system.

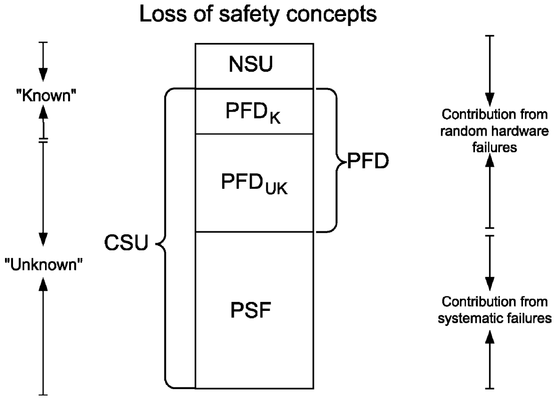

Loss of safety concepts
"Known"
"Unknown"
CSU
NSU
PFD$_K$
PFD$_{UK}$
PSF
PFD
Contribution from random hardware failures
Contribution from systematic failures

Fig. 2. Relations between loss of safety measures.

Below, we first introduce the loss of safety measures for random hardware failures, then for systematic failures, and finally the overall measure is given.

In IEC 61508, the parameter PFD is used to quantify loss of safety due to random hardware failures. According to the formulas given for PFD, see IEC 61508-6, it is obvious that this parameter includes the contribution from the categories 1(a) and 1(b). As explained above, we would like to separate out the various contributions, and now introduce

- PFD_{UK} is the unknown (UK) part of the safety unavailability (i.e. category 1(a)). It quantifies the loss of safety due to DU failures (with rate λ_{DU}), *during the period when it is not known that the function is unavailable*. The average duration of each unavailability period is $\tau/2$, giving the contribution $\lambda_{DU}\tau/2$ (for a single component without redundancy). PFD_{UK} is the most critical part of the PFD.
- PFD_K is the known (K) part of the safety unavailability (i.e. category 1(b)). It quantifies the loss of safety due to dangerous failures (with rate $\lambda_D = \lambda_{DU} + \lambda_{DD}$), *during the period when it is known that the function is unavailable* (i.e. failure has been detected). The average duration of the unavailability period is denoted MTTR, giving the contribution λ_DMTTR to PFD for a single system.

Observe that PFD now is given as; also see Fig. 2:

$$\mathrm{PFD} = \mathrm{PFD}_{UK} + \mathrm{PFD}_K$$

Next, systematic failures (category 2) is quantified by PSF, the Probability that a Systematic Failure causes the safety function to be unavailable.[2]

[2] This has also been denoted the probability of a Test Independent Failure (TIF), as it essentially is the probability that a component which has just been functionally tested will fail on demand.

Thus, the functional testing will not detect and prevent such a failure to occur if there should be an actual demand. As explained above, a design error or an interaction error may cause the systematic failure. The probability, PSF may be an important contributor to the overall safety unavailability, and the effect of this term is further elaborated, e.g. in Ref. [13,14].

As to the quantification of systematic failures, it is agreed that this is difficult. However, it is often experienced that systematic failures are a dominant contributor to the overall safety unavailability. Thus, attempts should also be made to quantify PSF and introduce safety unavailability measures that are more complete than PFD. Thus, we introduce

$$\mathrm{CSU} = \mathrm{PFD} + \mathrm{PSF}$$

where CSU, Critical Safety Unavailability is the probability that the component/safety system (either due to a random hardware failure or a systematic failure) will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event.

The last 'building block' for loss of safety quantification, see Fig. 2 is denoted as NSU, Non-critical Safety Unavailability which is the safety unavailability that occurs when the system is functionally tested, and equals the probability that it is known (actually planned) that the safety system is unavailable due to functional testing. This contribution to safety unavailability will depend on the frequency and duration of functional tests.

Our conclusion is that quantification of PFD alone is not sufficient for a proper evaluation of the loss of safety; rather one should assess various elements of the safety unavailability. The most critical part of PFD is $\mathrm{PFD}_{\mathrm{UK}}$, and could be stated separately. Further, one should attempt to perform an assessment of PSF. Thus, also CSU is considered an important measure for loss of safety, giving the total safety unavailability, except for the truly planned one which is denoted NSU.

4. The common cause failure modelling

In this section, we discuss the use of the β-factor model and suggest an extension of this. We restrict the discussion to the expression for $\mathrm{PFD}_{\mathrm{UK}}$, which for a 1oo1 voting is approximately equal to $\lambda_{\mathrm{DU}}\tau/2$.

4.1. The curse of the β-factor model

Some years ago there was in the reliability community a discussion regarding the 'curse of the exponential distribution'. Today we should perhaps look at the 'curse of the β-factor model'. The problem with the beta factor approach is of course that for any M-out-of-N ($M$oo$N$) voting ($M < N$) the rate of dependent failures (CCFs) is the same. If λ is the components failure rate, a system with $M$oo$N$ voting ($M < N$) has CCF rate equal to $\beta\lambda$. So the approach does not distinguish between different voting logics, and the same result is obtained, e.g. for 1oo2, 1oo3 and 2oo3 voting. So, e.g. the contribution to $\mathrm{PFD}_{\mathrm{UK}}$ from CCFs simply equals $\mathrm{PFD}_{\mathrm{UK}}(M\mathrm{oo}N) = \beta\lambda_{\mathrm{DU}}\tau/2$ for any $M$oo$N$ voting ($M < N$). The reason why it still can make sense to apply this model is that the sensible reliability engineer can come around (or at least reduce) this problem by using different β-s; e.g. using $\beta = 1\%$ for 1oo3, $\beta = 5\%$ for 1oo2 and $\beta = 10\%$ for 2oo3.

The approach suggested in the IEC standards the (IEC 61508-6 Annex D) introduces an 'application specific' β which to some extent depends on the voting logic $M$oo$N$ ($M < N$). However, the rate of system CCFs does only to a very slight degree depend on the system configuration. For instance, this approach does not distinguish at all between voting logics like 1oo2 and 2oo3. In most cases, this is hardly satisfactory.

Our goal is now to formulate a more general CCF model, requiring that this model shall both

- be a *simple*, direct generalisation of the β-factor model.
- clearly distinguish between the performance of voting logics like 1oo2, 1oo3 and 2oo3.

Of course there already exists a large number of generalisations of the β-factor model, e.g. see various references in Ref. [15]. In particular, the Multiple Greek Letter model [16] has certain similarities with the model suggested in the present paper. However, none of the previous generalisations seem to have gained widespread use.

4.2. A generalisation of the β-factor model

The reason for the success of the β-factor model is of course its extreme simplicity. So, it is very important that the generalised model also is simple to use in practice. We believe that this is best achieved by letting the CCF contribution to $\mathrm{PFD}_{\mathrm{UK}}$ for a $M$oo$N$ voting be calculate as

$$\mathrm{PFD}_{\mathrm{UK}}(M\mathrm{oo}N) = \beta(M\mathrm{oo}N)\lambda_{\mathrm{DU}}\tau/2 \qquad (M < N)$$

where $\beta(M\mathrm{oo}N)$ is the beta factor for a $M$oo$N$ voting. Further, this β-factor should be of the form

$$\beta(M\mathrm{oo}N) = \beta C_{M\mathrm{oo}N} \qquad (M < N)$$

where β is the beta factor as obtained from the IEC approach (see Appendix D of IEC 61508-6), and $C_{M\mathrm{oo}N}$ is a modification factor taking into account the voting logic ($M$oo$N$) of the system. The important thing to observe here is that the effect of the voting is singled out as a separate factor, valid for any value of β. So, just one assessment is carried out to assess the degree of dependence (β), to be used for all configurations. The result is modified by a separate factor $C_{M\mathrm{oo}N}$, independent of the chosen β. If now an argument can be provided to support the choice of $C_{M\mathrm{oo}N}$, a very simple and easy-to-use approach is provided.

Actually Refs. [3,4] present the above alternative formula for $\mathrm{PFD}_{\mathrm{UK}}$ of a $M$oo$N$ voting, and suggest values

Table 1
1Modification factors, C_{MooN}, based on system voting logic

Voting	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{MooN}	1.0	0.3	2.4	0.15	0.8	4.0

for C_{MooN} ($N = 2, 3, 4$), see Table 1 below. Observe here that $C_{1oo2} = 1$. Thus, for the 1oo2 voting we use the specified β-value without any modification. So the β obtained from the IEC approach is the one that is 'correct' for a 1oo2 voting. Thus, β is maintained as an essential parameter. However, its interpretation in the new model is entirely related to a double set of components.

Below we formulate a model, which allows us to motivate these values of C_{MooN}, and to derive C_{MooN} values for any N. This generalisation of the β-factor model is denoted the MBF model.

Of course there are some arbitrariness in the C_{MooN} values presented in Table 1. However, the C_{MooN} will be expressed in terms of parameters with a clear interpretation, allowing any user to calculate alternative values for C_{MooN}. However, the suggested values in Table 1 may be used as kind of generic starting values, which undoubtedly is much better than using $C_{MooN} \equiv 1$, as suggested by the IEC standard. Thus, it is our claim that this approach combines simplicity with a reasonable degree of realism. We can now see no good reason for using the β-factor model in the way suggested by the standard. Only in cases where just a rough analysis is required, without evaluation/comparison of various voting logics, the more simplistic β-factor model should apply.

4.3. The β-factor model for duplicated system

In order to motivate the generalised model, we first present well-known results for the β-factor model for $N = 2$ channels (components), see Fig. 3. So there are two components, A and B in parallel. Letting λ_{DU} be the relevant failure rate for each component, we have

$$\lambda_{1\cdot 2} = 2(1-\beta)\lambda_{DU} = \text{rate of single (independent) failures for duplex system}$$

$$\lambda_{2\cdot 2} = \beta\lambda_{DU} = \text{rate of double failures (CCFs) for duplex system}$$

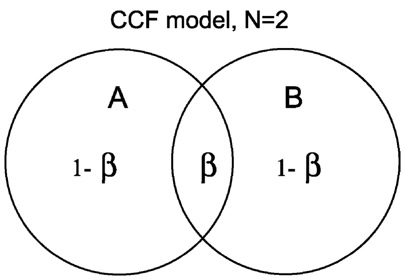


Fig. 3. Beta factor model for a duplicated system ($N = 2$).

So β can be given the following interpretation: Given A has just failed, β is the probability that B fails at the same time. We will relate this to the loss of safety probability, PFD_{UK} for duplicated systems. But for the present purpose, we ignore second order terms like $(\lambda_{DU}\tau)^2$, and thus the contribution to PFD_{UK} from two independent failures, i.e. $(\lambda_{DU}\tau)^2/3$, is not considered here. Further, PFD_K is ignored, (say we here assume MTTR = 0).

Let A also represent the event that component A has failed (at an arbitrary point of time), and let B be defined similarly. Further, the probability $Q = P(A) = P(B)$, where in our case $Q = \text{PFD}_{UK}(1oo1) \approx \lambda_{DU}\tau/2$; (as we know this can be considered the average probability over the interval $[0, \tau]$). Now by ignoring second order terms, we get

$$Q_{1\cdot 2} = \text{Probability of duplex system having single failure}$$
$$= 2(1-\beta)Q$$

$$Q_{2\cdot 2} = \text{Probability of duplex system having double failure}$$
$$= \beta Q$$

It directly follows that PFD_{UK} for the voting logics 1oo2 and 2oo2 equals, (still ignoring second order terms):

$$\text{PFD}_{UK}(1oo2) = Q_{2\cdot 2} = \beta Q \approx \beta\lambda_{DU}\tau/2$$

$$\begin{aligned}\text{PFD}_{UK}(2oo2) &= Q_{1\cdot 2} + Q_{2\cdot 2} = (2-\beta)Q \\ &\approx (2-\beta)\lambda_{DU}\tau/2 \approx 2\lambda_{DU}\tau/2\end{aligned}$$

The last expression is easily generalised to

$$\text{PFD}_{UK}(NooN) \approx N\lambda_{DU}\tau/2, \qquad N = 1, 2, 3, \ldots$$

Better approximations for $N$oo$N$ votings can obviously be given, but this is not the topic here. Our main objective is to generalise the approach to get simple expressions for $\text{PFD}_{UK}(MooN)$, when $M < N$.

4.4. The multiple beta factor model for $N = 3$ channels

Now consider a triplicated system with three components A, B and C. The situation is symmetric in these three components, and the probability of these to be in the failed state is denoted $P(A) = P(B) = P(C) = Q$. The parameter β has the same interpretation as given above when we consider just two of the three events. Further introduce β_2 = the probability that C fails, given that there has just been a dependent failure (CCF) affecting both A and B.

Then we have the following failure rates for the triplicated system:

$$\lambda_{1\cdot 3} = 3(1-(2-\beta_2)\beta)\lambda_{DU}$$
$$= \text{rate of single (independent) failures}$$

$$\lambda_{2\cdot 3} = 3(1-\beta_2)\beta\lambda_{DU} = \text{rate of double failures (CCFs)}$$

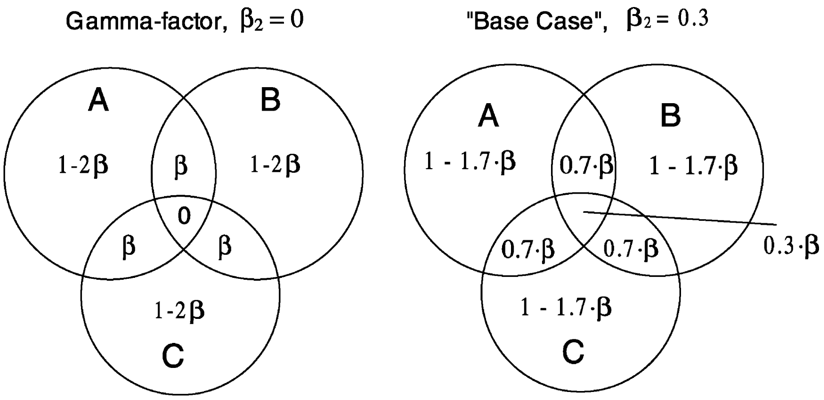


Fig. 4. Illustration of the multiple beta factor (MBF) model for a triplicated system ($N = 3$). Three different choices of the parameter β_2.

$\lambda_{3\cdot 3} = \beta_2\beta\lambda_{DU}$ = rate of triple failures (CCFs)

Now β_2 can take any value in the interval [0,1]. Illustrations are given in Fig. 4 for the cases, $\beta_2 = 0$, 0.3 and 1.0, respectively. Choosing the value $\beta_2 = 1$, we get the ordinary beta factor model; then any failure affecting two of the three components will also affect the third one. The other extreme is $\beta_2 = 0$. We also think this model should have a name and refer to it as the gamma factor (γ-factor) model. For this model all multiple failures are double ones, and thus none are triple.

We take it for granted that these two extremes, $\beta_2 = 0$ and 1.0, usually give quite unrealistic models. However, the knowledge about the 'true' β_2 would in many cases be very limited. So it would be useful to define some generic value as a 'Base Case', applicable when little information is available. We believe that this value usually is closer to 0 than 1, and rather arbitrarily choose the value $\beta_2 = 0.3$.

The general results for $N = 3$ channels are easily obtained for this parameterisation (ignoring second order terms):

$Q_{2\cdot 3}$ = Probability of triplicated system having double failure

$= 3(1 - \beta_2)\beta Q$

$Q_{3\cdot 3}$ = Probability of triplicated system having triple failure

$= \beta_2\beta Q$

For a 1oo3 voting, a system failure occurs if all three components fail, and thus $\mathrm{PFD_{UK}}(1\mathrm{oo}3) = Q_{3\cdot 3} = \beta_2\beta Q$, which directly gives $C_{1\mathrm{oo}3} = \beta_2$, (see definition of C_{MooN} in Section 4.2).

For a 2oo3 voting, there is a system failure if at least two components fail, and thus $\mathrm{PFD_{UK}}(2\mathrm{oo}3) = Q_{2\cdot 3} + Q_{3\cdot 3} = (3 - 2\beta_2)\beta Q$, directly giving $C_{2\mathrm{oo}3} = 3 - 2\beta_2$.

These results are now utilised to give the numerical values for $C_{1\mathrm{oo}3}$ and $C_{2\mathrm{oo}3}$, see Table 2. It is seen that the value of β_2 has a very significant impact on the results; for varying β_2 actually $C_{1\mathrm{oo}3} \in [0, 1]$ and $C_{2\mathrm{oo}3} \in [1, 3]$. However, except for the β-factor model ($\beta_2 = 1$), the values of $C_{1\mathrm{oo}3}$ and $C_{2\mathrm{oo}3}$ are indeed different. Thus, the β-factor model is very extreme by giving the same result for the 1oo3 and 2oo3 votings. So even if the 'Base Case' ($\beta_2 = 0.3$) is chosen rather arbitrarily, this should in most cases give much more realistic results than the β-factor model (and the γ-factor model). Assuming that we most often will have $\beta_2 = 0.3 \pm 0.2$, the values $\beta_2 = 0.1$ and 0.5 represent cases of sensitivity. These give values of $C_{2\mathrm{oo}3}/C_{1\mathrm{oo}3}$ ranging from 4 to 28, while the Base Case gives $C_{2\mathrm{oo}3}/C_{1\mathrm{oo}3} = 8$.

Observe that the results obtained for $C_{1\mathrm{oo}3}$ and $C_{2\mathrm{oo}3}$ for $\beta_2 = 0.3$ are in agreement with the suggestions presented in Table 1.

4.5. Summary of the MBF model

This approach for $N = 3$ can obviously be extended to cover any degree of redundancy (N). By increasing the number of channels (redundant components) from N to $N + 1$, we have to introduce each time a new parameter β_N. In order to cover $N + 1 = 4$, we need β_3 = probability of component D failing, given that there has occurred a CCF affecting both A, B and C. Proceeding as above, and inserting $\beta_2 = 0.3$ ('Base Case') we get

$C_{1\mathrm{oo}4} = 0.3\beta_3$

$C_{2\mathrm{oo}4} = 0.3(4 - 3\beta_3)$

$C_{3\mathrm{oo}4} = 3.6 + 0.9\beta_3$

Now a 'typical' value of β_3 should be chosen. In our judgement, it is natural to assume that the β_N-s may increase as N increases. Here we suggest the value $\beta_3 = 0.5$ as a 'Base Case'. The range of 'allowed' values (corresponding

Table 2
Values of $C_{1\mathrm{oo}3}$ and $C_{2\mathrm{oo}3}$

β_2	Description	$C_{1\mathrm{oo}3}$	$C_{2\mathrm{oo}3}$
0.0	Gamma (γ-) factor	0.0	3.0
0.1	Lower sensitivity	0.1	2.8
0.3	Base Case	0.3	2.4
0.5	Upper sensitivity	0.5	2.0
1.0	Beta (β-) factor	1.0	1.0

to $\beta_3 = 0$ and 1, but β_2 being fixed at 0.3) are given in parenthesis:

$$C_{1\text{oo}4} = 0.15 \in [0, 0.3]$$

$$C_{2\text{oo}4} = 0.75 \in [0.3, 1.2]$$

$$C_{3\text{oo}4} = 4.05 \in [3.6, 4.5]$$

The above 'Base Case' values are (essentially) in agreement with the suggestions of Table 1, and are located in the middle of the interval of allowed values (for β_2 fixed at 0.3). Observe that the above ranges are narrower than those for $C_{M\text{oo}3}$, see Table 1. When we step by step extend the model to higher N, it is actually a general tendency of getting less and less variation in the $C_{M\text{oo}N}$ (when previous β-s have been fixed).

To summarise, the $C_{M\text{oo}N}$ values presented in Table 1 are based on choosing $\beta_2 = 0.3$ and $\beta_3 = 0.5$. The basic assumption for the parameterisation of the MBF model is as follows:

Suppose we choose k components (from a total of $N > k$ redundant ones). Given that a failure has occurred, and that all k of these components are known to have failed, then β_k is the probability that also a specified one of the other $N - k$ components has failed at the same time. These probabilities (β_k) are not affected by the total number of components (N).

In particular, consider the definition of β_1. For a $M$oo$N$ voting system, we may specify one component amongst the total of N. If it is known that this one has failed, then β_1 is the probability that another specified component has also failed simultaneously. Thus, β_1 is identical to the parameter β, as used in the MBF model above. Further, note that this interpretation of $\beta = \beta_1$ in the MBF model is also valid for the β of the ordinary beta factor model (e.g. see Fig. 4).

Now the MBF model has proved successful with respect to satisfying the requirements stated at the beginning of Section 4.2. The clue to this success is that the parameterisation of the MBF model gives a result where all probabilities $Q_{k \cdot N}$ ($k > 1$) include the factor β, which can then be separated out. Thus, it is our claim that this model resolves the main objection against the standard β-factor model adopted in IEC. It is the intention to later provide a more comprehensive description of this model.

4.6. Extended PFD calculation formulas

The above formulas for PFD_{UK} account for the contribution of the CCFs only, and will for instance not take into account the possibility that there are two independent failures present simultaneously in a duplex system. The more complete quantification formulas for PFD become rather complex, in particular see formulas of Appendix B of IEC 61508-6. Now actually all such formulas are approximations, and below a couple of simplified but rather more transparent expressions for PFD_{UK} are presented, see Table 3. If the full $\text{PFD} = \text{PFD}_{\text{UK}} + \text{PFD}_{\text{K}}$ is required, the possible contribution from PFD_{K} could easily be obtained, given the operational philosophy for the chosen action when it is known that some (all) channels are unavailable (see Ref. [14]).

Table 3
Suggested (approximate) formulas for PFD_{UK}. Main terms in bold

Voting	Formula for PFD_{UK}
1oo1	$\boldsymbol{\lambda_{\text{DU}}\tau/2}$
1oo2	$\beta\boldsymbol{\lambda_{\text{DU}}\tau/2} + [(1-\beta)\lambda_{\text{DU}}\tau]^2/3 + 2(1-\beta)\lambda_{\text{det}}MTTR\lambda_{\text{DU}}(\tau/2)$
2oo2	$(\boldsymbol{2} - \beta)\boldsymbol{\lambda_{\text{DU}}\tau/2} + 2(1-\beta)\lambda_{\text{det}}MTTR\lambda_{\text{DU}}(\tau/2)$
2oo3	$\boldsymbol{2.4}\beta\boldsymbol{\lambda_{\text{DU}}\tau/2} + [(1-1.7\beta)\lambda_{\text{DU}}\tau]^2 + 3(1-1.7\beta)$ $\times\lambda_{\text{det}}MTTR\beta\lambda_{\text{DU}}(\tau/2)$

It is important to stress that the complete expression for PFD_{UK} requires assumptions regarding maintenance strategy and operational philosophy. The suggested formulas assume that a duplicated system is degraded to a 1oo1 system when there is a known failure of one channel. Similarly, a 2oo3 voting system is degraded to 1oo2 system when there is one known failure, and a shut down is initiated with known failures of two or more channels.

Note that λ_{det} in the table is the total rate of *detected* failures leading to degradation, i.e. both dangerous detected (DD) and safe detected failures.[3] MTTR is the duration of the degradation. Further comments to the formulas:

- The second term of 1oo2 and 2oo3 corresponds to the occurrence of two independent DU failures in the same test interval.
- The last term of 1oo2, 2oo2 and 2oo3 corresponds to one component having a detected single failure resulting in degraded operation, and then the (degraded) system getting a DU failure.
- The factor $C_{2\text{oo}3} = 2.4$ is introduced for the CCF term of 2oo3. Observe that for the 'second order terms' of the 2oo3 voting we use the factor $1 - 1.7\beta$ to get the rate of a single component failure, (cf. Fig. 4).

Any possible difference between β and β_D[4] is ignored in the formulas of Table 1. The effect of demands also serving as functional tests is not incorporated in the formulas. Similar formulas for other votings, including formulas for PFD_{K}, are suggested in Ref. [14].

4.7. Determination of application specific parameters

The IEC standard presents an approach to determine 'application specific' β, see tables in Appendix D of

[3] In the notation of IEC, we could say that λ_{det} is the sum of Dangerous Detected and Safe Detected, i.e. $\lambda_{\text{det}} = \lambda_{\text{DD}} + \lambda_{\text{SD}}$, (provided we interpret λ_{SD} to be the rate of 'safe' (trip) failures being detected and then causing degradation). The report [14] is a little more specific with respect to the concept of 'safe' failures.

[4] In the IEC standard β_{D} is the β-factor applicable for Detected failures (but unfortunately this notation could be mixed up with β for Dangerous failures).

IEC 61508-6. This approach follows the work of Humphrey [17], and is a sensible way of finding the degree of dependence for random hardware failures in a given application (the determination of the so-called Z-value in Ref. [1] is, however, questioned, see Ref. [13]).

Similarly, work should be initiated to give methods for assessment of an 'application specific' β_2, so that the values of C_{MooN} to some extent could be adapted to the actual system and application. Of course several factors contributing to a small $\beta = \beta_1$, would also contribute to a small β_2, so that in a more sophisticated modelling, these parameters are actually correlated.

Further, it is the recommendation of the present authors that systematic failures should also be quantified when the loss of safety is evaluated. It is believed that the importance of systematic failures is increasing; at least relatively speaking, as the reliability of hardware is improving. Thus, it is a serious drawback, e.g. when the SIL[5] requirements of IEC 61508 regarding systematic failures are rather vague. Requiring a qualitative evaluation of systematic failures only, necessarily implies that there will be less focus on these essential contributions.

Some work has been initiated to assess these application specific PSFs [11,12]. The first of these reports presents a method to assess the loss of safety due to systematic failures for gas detectors, and the second considers the PSF due to software errors. However, much work remains to be done in this area.

5. Conclusions and recommendations

The paper presents some recommendations regarding loss of safety quantification and further standardisation in safety/reliability modelling of safety systems:

1. A failure classification as given in Fig. 1 is suggested.
2. It is suggested that all the elements of the safety unavailability should be calculated as part of an overall evaluation of the safety system. Further, it is recommended to provide separate values for PFD_{UK}, PFD_{K} and PSF. As a minimum, PFD_{UK} should always be quantified. However, the importance of systematic failures is well documented, and also an assessment of PSF should be provided.
3. The standard β-factor model, as suggested in IEC 61508, will not allow a proper comparison of say the 1oo2, 1oo3 and 2oo3 voting logics. So this model should usually not be applied, unless a very rough analysis is required, (or the value of β is otherwise chosen to depend on the voting). We suggest the use of the MBF model introduced in Chapter 4. In this model, the β-factor of the $M$oo$N$ system is of the form $\beta_{MooN} = \beta C_{MooN}$. The β could be determined as suggested in the Standard (assuming a 1oo2 voting). For C_{MooN}, we suggest as a start to use the generic values given in Table 1.
4. The IEC approach to find application specific β-factors is a good principle. A similar approach should be developed to assess other application specific parameters, including the loss of safety of systematic failures.
5. The formulas for quantification of PFD given in IEC are rather complex, and it is suggested that these formulas are not the most sensible approximations. The formulas for PFD_{UK} presented above (Table 1) are considered simpler and more transparent, and these are suggested as a basis for the quantification of PFD_{UK} (and other measures for loss of safety).

Acknowledgements

We thank our colleagues Lars Bodsberg, Knut Øien, Terje Dammen, Tor Onshus and Sture Holmstrøm for fruitful discussions on this work. Further, we sincerely thank the members of the PDS forum for their continued contributions to the development of this area during several years, and also for funding to carry out the work on which this paper is based.

References

[1] IEC 61508. Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems. Part 1–7, Edition 1.0 (various dates).

[2] IEC 61511. Functional safety: safety instrumented systems for the process industry sector. Part 1–3, CDV versions.

[3] 070 OLF guideline on the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf, OLF, Rev. 01, 26-01-01, see http://www.itk.ntnu.no/sil.

[4] Hauge S, Hokstad P, Onshus T. The introduction of IEC 61511 in Norwegian offshore industry. Proceedings of ESREL, Torino, 16–20 September; 2001. p. 483–90.

[5] NPD2001. Regulations relating to management in the petroleum activities (The Management Regulations). The Norwegian Petroleum Directorate; September 2001.

[6] Bodsberg L, Hokstad P. A system approach to reliability and life-cycle cost for process safety systems. IEC Trans Reliab 1995;44(2): 179–86.

[7] Bodsberg L, Hokstad P. Transparent reliability model for fault-tolerant safety systems. Reliab Engng Syst Safety 1996;55: 25–38.

[8] Hokstad P, Fløtten P, Holmstrøm S, McKenna F, Onshus T. A reliability model for optimization of test schemes for fire and gas detectors. Reliab Engng Syst Safety 1995;47:15–25.

[9] Aarø R, Bodsberg L, Hokstad, P. Reliability prediction handbook; computer-based process safety systems. SINTEF report STF75 A89023; 1989.

[10] Hansen GK, Aarø R. Reliability quantification of computer-based safety systems. An introduction to PDS. SINTEF report STF38 A97434; 1997.

[5] Safety Integrity Level (see Ref. [1]).

[11] Hansen GK, Vatn. Reliability data for control and safety systems, 1998 edition. SINTEF report STF38 A98445; 1999.

[12] Vatn J. Software reliability quantification in relation to the PDS method. SINTEF report STF38 A0016; 2000.

[13] Hokstad P, Corneliussen K. Improved common cause failure model for IEC 61508. SINTEF report STF38 A00420; 2000.

[14] Reliability prediction method for safety instrumented systems. PDS method handbook, 2003 edition. SINTEF report STF38 A02420; 2003.

[15] Hokstad P. Common cause and dependent failure modelling. In: Misra KB, editor. New trends in system reliability evaluation. Amsterdam: Elsevier; 1993. p. 411–44. [chapter 11].

[16] Flemming KN, Mosleh A, Deremer RK. A systematic procedure for the incorporation of common cause events into risk and reliability models. Nucl Engng Des 1985;93:245–79.

[17] Humphreys RA. Assigning a numerical value to the beta factor common-cause evaluation. Proc Reliab '87, Proc Pap 2C 1987.

Paper 3 Challenges related to surveillance of safety functions

Kjell Corneliussen and Snorre Sklet, European Safety and Reliability Conference (ESREL), June 2003.

Challenges related to surveillance of safety functions

K. Corneliussen & S. Sklet
Dept. of Production and Quality Engineering, NTNU / SINTEF Industrial Management, Trondheim, Norway

ABSTRACT: One of the main principles for the safety work in high-risk industries such as the nuclear and process industry, is the principle of defence-in-depth that imply use of multiple safety barriers or safety functions in order to control the risk.

Traditionally, there has been a strong focus on the design of safety functions. However, recent standards and regulations focus on the entire life cycle of safety functions, and this paper focuses on the surveillance of safety functions during operations and maintenance. The paper presents main characteristics of safety functions, factors influencing the performance, a failure category classification scheme, and finally a discussion of challenges related to the surveillance of safety functions during operations and maintenance. The discussion is based on experiences from the Norwegian petroleum industry and results from a research project concerning the reliability and availability of computerized safety systems.

The main message is that there should be an integrated approach for surveillance of safety functions that incorporates hardware, software and human/organizational factors, and all failure categories should be systematically analyzed to 1) monitor the actual performance of the safety functions and 2) systematically analyze the failure causes in order to improve the functionality, reliability and robustness of the safety functions.

1 INTRODUCTION

One of the main principles for the safety work in high-risk industries such as the nuclear and process industry, is the principle of defence-in-depth or use of multiple layers of protection (IAEA 1999, Reason 1997, CCPS 2001).

The Norwegian Petroleum Directorate (NPD) emphasizes this principle in their new regulations concerning health, safety and environment in the Norwegian offshore industry (NPD, 2001a). An important issue in these new regulations is the focus on safety barriers, and in the first section of the management regulation, it is stated that "barriers shall be established which a) reduce the probability that any such failures and situations of hazard and accident will develop further, and b) limit possible harm and nuisance".

The IEC 61508 (IEC 1998) and IEC 61511 (IEC 2002) standards have a major impact on the safety work within the process industry, and describe a risk-based approach to ensure that the total risk is reduced to an acceptable level. The main principle is to identify necessary safety functions and allocate these safety functions to different safety-related systems or external risk reduction facilities. In IEC 61511 a safety function is defined as a "function to be implemented by a SIS (Safety Instrumented System), other technological safety-related system or external risk reduction facilities which is intended to achieve or maintain a safe state for the process in respect to a specific hazardous event". An important part of the standards is a risk-based approach for determination of the safety integrity level requirements for the different safety functions. IEC 61508 is a generic standard common to several industries, while the process industry currently develops a sector specific standard for application of SIS, i.e., IEC 61511 (IEC 2002). In Norway, the offshore industry has developed a guideline for the use of the standards IEC 61508 and IEC 61511 (OLF 2001), and the Norwegian Petroleum Directorate (NPD) refers to this guideline in their new regulations (NPD 2001a). Overall, it is expected that these standards will contribute to a more systematic safety work and increased safety in the industry.

Further, the NPD in section 7 in the management regulation (NPD, 2001a) requires that "the party responsible shall establish monitoring parameters within his areas of activity in order to monitor matters of significance to health, environment and safety", and that "the operator or the one responsible for the operation of a facility, shall establish indicators to monitor changes and trends in major accident risk". These requirements imply a need for surveillance of safety functions during operation. In accordance with these requirements, NORSOK (2001) suggests that "verification of that performance standards for safety and emergency preparedness systems are met in the operational phase may be achieved through monitoring trends for risk indicators. […] Examples of such indicators may be availability of essential safety systems". Also IEC requires proof testing and inspection during operations and maintenance in order to ensure that the required functional safety of safety-related systems is fulfilled (IEC 2002).

In order to monitor the development in the risk level on national level, the NPD initiated a project called "Risk Level on the Norwegian Continental Shelf". The first phase of the project focused on collection of information about defined situations of hazard and accident (DSHA), while the second phase also focus on collection of information about the performance of safety barriers (NPD/RNNS 2002). According to this project, the performance of safety barriers has three main elements: 1) functionality/efficiency (the ability to function as specified in the design requirements), 2) reliability/availability (the ability to function on demand), and 3) robustness (ability to function as specified under given accident conditions).

The NPD uses the term safety barrier in their regulations. However, they have not defined the term, and in a letter to the oil companies as part of the project "Risk Level on the Norwegian Continental Shelf" (NPD/RNNS, 2002), they have referred to the definition proposed by ISO (2000): "Measure which reduces the probability of realizing a hazard's potential for harm and which reduces its consequence" with the note "barriers may be physical (materials, protective devices, shields, segregation, etc.) or non-physical (procedures, inspection, training, drills, etc.)". Accordingly, the NPD uses the term barrier in an extended meaning and is therefore similar to other terms used in the literature, such as defence (Reason 1997), protection layer (CCPS 2001), and safety function (as used by IEC). The term safety function is used in this paper.

Surveillance of safety functions during operations in order to meet the requirements stated by the NPD (NPD 2001a) and IEC (IEC 1998 and IEC 2002) is not a straightforward task, but is a challenge for the oil companies. Therefore, several oil companies have initiated internal projects to fulfill the requirements (see e.g. Sørum & Thomassen 2002). This paper focuses on the surveillance of safety functions during operations and maintenance. The paper presents main characteristics of safety functions, factors influencing the performance, a failure category classification scheme, and finally a discussion of challenges related to the surveillance of safety functions during operations and maintenance. The discussion is based on experiences from the Norwegian petroleum industry and results from a research project concerning the reliability and availability of computerized safety systems.

2 CHARACTERISTICS OF SAFETY FUNCTIONS

Safety functions may be characterized in different ways, and some of the characteristics influence how the surveillance of the safety function is performed. The following characteristics are further discussed in this section: type of safety function, local vs. global safety functions and active vs passive systems.

IEC 61511 (IEC 2002) defines a safety function as a "function to be implemented by a SIS, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous events". By SIS IEC means an instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). Other technology safety-related systems are safety-related systems based on a technology other than electrical/electronic/programmable electronic, for example a relief valve. External risk reduction facilities are measures to reduce or mitigate the risk that are separate and distinct from the SIS. Examples are drain systems, firewalls and bunds.

A distinction between global and local safety functions is made by The Norwegian Oil Industry Association (OLF) (OLF, 2001). Global safety functions, or fire and explosion hazard safety functions, are functions that typically provide protection for one or several fire cells. Examples are emergency shutdown, isolation of ignition sources and emergency blowdown. Local safety functions, or process equipment safety functions, are functions confined to protection of a specific process equipment unit. A typical example is the protection against high level in a separator through the PSD (Process Shutdown) system.

CCPS distinguishes between passive and active independent protection layers (IPL) (CCPS 2001). A passive IPL is not required to take an action in order to achieve its function in reducing risk. Active IPLs are required to move from one state to another in response to a change in a measurable process property (e.g. temperature or pressure), or a signal from another source (such as a push-button or a switch). An active IPL generally comprises a sensor of some type (detection) that gives signal to a decision-making process that actuates an action (see Figure 1).

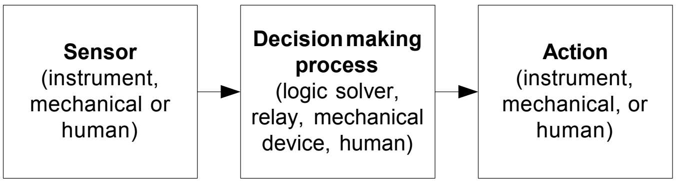

Sensor
(instrument, mechanical or human)
Decision making process
(logic solver, relay, mechanical device, human)
Action
(instrument, mechanical, or human)

Figure 1. Basic elements of active protection layers (CCPS, 2001)

3 SAFETY FUNCTIONS FOR PROCESS ACCIDENTS

The need for safety functions is dependent on specific hazardous events. Figure 2 gives a simplified illustration of the event sequence and necessary safety functions for "process accidents". The event sequence begin with the initiating event "leakage of hydrocarbons (HC)", and are followed by spreading of hydrocarbons, ignition, strong explosions or escalation of fire, escape, evacuation, and finally rescue of people. The main safety functions in order to prevent, control or mitigate the consequences of this accident are to prevent the hydrocarbon leakage, prevent spreading of hydrocarbons, prevent ignition, prevent strong explosion or escalation of fire, and to prevent fatalities. These safety functions may be realized by different kinds of safety-related systems. In this paper, we focus on the safety function "prevent spreading of hydrocarbons".

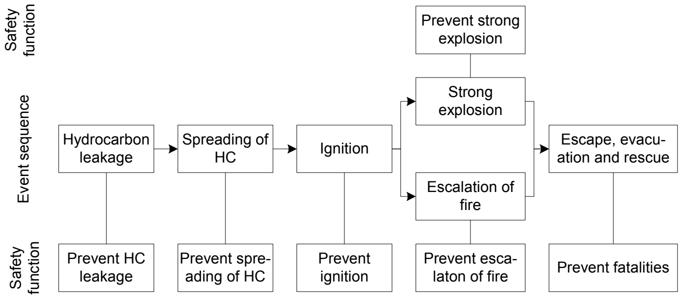


Figure 2. Event sequence for process accidents.

In principle, the safety function "prevent spreading of hydrocarbons" may be fulfilled in two different approaches, 1) stop the supply of HC, and 2) remove HC. In this paper, we focus on the former approach in order to illustrate some of the challenges related to the surveillance of safety functions.

The main elements of the active safety function "prevent spreading of hydrocarbons by stopping the supply" are shown in Figure 3. Firstly, the leakage of HC must be detected, either automatically by gas detectors, or manually by human operators in the area. Secondly, a decision must be taken, either by a logic solver or a human decision. The decision should be followed by an action, in this case, closure of an ESDV (Emergency Shutdown Valve). The action may either be initiated automatically by the logic solver, or by a human operator pushing the ESD-button, or manually by a human operator closing the ESD-valve manually.

There should be an integrated approach for surveillance of safety functions that incorporates hardware, software and human/organizational factors.

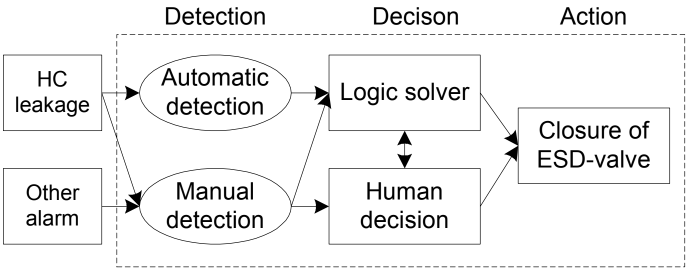


Figure 3. Safety function – prevent spreading of hydrocarbons.

4 FAILURE CLASSIFICATION

For safety functions implemented through SIS technology (as in Figure 3), IEC 61508 and IEC 61511 define four safety integrity levels (SIL). The SIL for each safety function is established through a risk-based approach. To achieve a given SIL, there are three main types of requirements (OLF, 2001):

- A quantitative requirement, expressed as a probability of failure on demand (PFD) or alternatively as the probability of a dangerous failure per hour. This requirement relates to random hardware failures.
- A qualitative requirement, expressed in terms of architectural constraints on the subsystems constituting the safety function.
- Requirements concerning which techniques and measures should be used to avoid and control systematic faults.

The requirements above influence the performance of the SIS, and in this section we present a failure classification scheme that can be used to distinguish between different types of failure causes (hardware and systematic failures). The scheme is a modification of the failure classification suggested in IEC 61508.

The basis for the discussion can be traced back to the research project PDS (Reliability and availability for computerized safety systems) carried out for the Norwegian offshore industry (Bodsberg & Hokstad 1995, Bodsberg & Hokstad 1996, Aarø et al 1989), and the still active PDS-forum that succeeded the project (Hansen & Aarø 1997, Hansen & Vatn 1998, Vatn 2000, Hokstad & Corneliussen 2000). The classification presented in this section is one of the results in the new edition of the PDS method (Hokstad & Corneliussen 2003).

According to IEC 61508 (Section 3.6.6 of part 4), failures of a safety-related system can be categorized either as random hardware failures or systematic failures. The standard also treats software failures, but we consider this as a subclass of the systematic failures (see Note 3 on p16 of IEC 61508-4). The standard makes a clear distinction between the two failure categories, and states that random hardware failures should be quantified, while systematic failures should not (IEC 61508-2, 7.4.2.2, note 1).

In IEC 61508-4 (Section 3.6.5), a random hardware failure is defined as a "failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware". IEC 61508-4 (Section 3.6.6) defines a systematic failure as a "failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or the manufacturing process, operational procedures, documentation or other relevant factors".

The standard defines "hardware-related Common Cause Failures (CCFs)" (IEC 61508-6, Section D.2): "However, some failures, i.e., common cause failures, which result from a single cause, may affect more than one channel. These may result from a systematic failure (for example, a design or specification mistake) or an external stress leading to an early random hardware failure". As an example, the standard refers to excessive temperature of a common cooling fan, which accelerates the life of the component or takes it outside it's specified operating environment.

Hokstad & Corneliussen (2003) suggest a notation that makes a distinction between random hardware failures caused by natural ageing and those caused by excessive stresses (and therefore may lead to CCFs). The classification also defines systematic failures in more detail. The suggestion is an update of the failure classification introduced in the PDS project, (Aarø et al 1989), but adapted to the IEC 61508 notation, and hence should not be in conflict with that of IEC 61508. The concepts and failure categorization suggested by Hokstad and Corneliussen (2003) is shown in Figure 4.

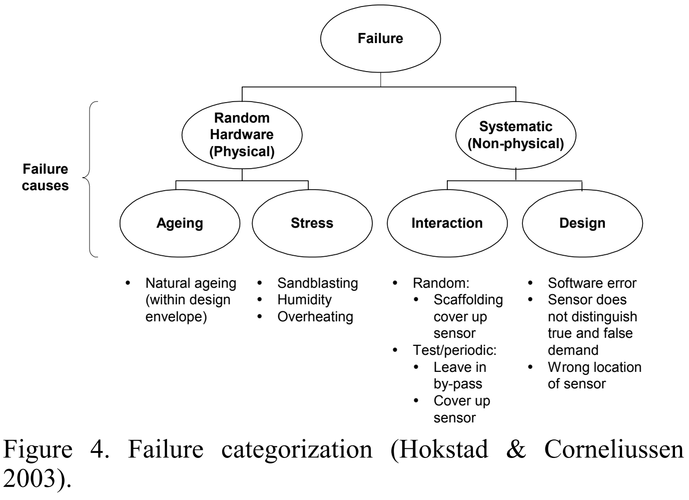

Failure
Random Hardware (Physical)
Systematic (Non-physical)
Failure causes
Ageing
Stress
Interaction
Design
• Natural ageing (within design envelope)
• Sandblasting
• Humidity
• Overheating
• Random:
• Scaffolding cover up sensor
• Test/periodic:
• Leave in by-pass
• Cover up sensor
• Software error
• Sensor does not distinguish true and false demand
• Wrong location of sensor

Figure 4. Failure categorization (Hokstad & Corneliussen 2003).

Hokstad & Corneliussen (2003) define the failure categories as:

- Random hardware failures are physical failures, where the delivered service deviates from the specified service due to physical degradation of the module. Random hardware failures are split into ageing failures and stress failures, where ageing failures occur under conditions within the design envelope of a module, while stress failures occur when excessive stresses are placed on the module. The excessive stresses may be caused either by external causes or by human errors during operation.
- Systematic failures are non-physical failures, where the delivered service deviates from the specified service without any physical degradation of the module. The failure can only be eliminated by a modification either of the design or the manufacturing process, the operating procedures, the documentation or other relevant factors. Thus, modifications rather than repairs are required in order to remove these failures. The systematic failures are further split into interaction failures and design failures, were interaction failures are initiated by human errors during operation or testing. Design failures are initiated during engineering and construction and may be latent from the first day of operation.

As a general rule, stress, interaction and design failures are dependent failures (giving rise to common cause failures), while the ageing failures are denoted independent failures.

To avoid a too complex classification, every failure may not fit perfectly into the above scheme. For instance, some interaction failures might be physical rather than non-physical.

The PDS method focuses on the entire safety function (Hokstad & Corneliussen 2003), and intends to account for all failures that could compromise the function (i.e. result in "loss of function"). Some of these failures are related to the interface (e.g. "scaffolding cover up sensor"), rather than the safety function itself. However, it is part of the "PDS philosophy" to include such events.

5 SURVEILLANCE OF SAFETY FUNCTIONS

This section discusses the surveillance of safety functions during operation related to the failure classification in the previous section.

The requirements for surveillance are related to the functional safety, and not only to the quantitative SIL requirements (see section 4). In IEC 61508-2, section 7.6.1 it is stated that one should "develop procedures to ensure that the required functional safety of the SIS is maintained during operation and maintenance", and more explicitly stated in IEC

61511-1, section 16.2.5, “the discrepancies between expected behavior and actual behavior of the SIS shall be analyzed and where necessary, modification made such that the required safety is maintained”. In addition to the quantitative (PFD) requirement, systematic failures and changes in safety system/functions should be considered. Also changes not explicitly related to the safety function may influence the safety level (number of demands, operation of the process, procedures, manning, etc.), however such conditions will not be treated in this paper. The discussion is limited to the boundary outlined in Figure 3.

In operation or during maintenance the performance of the safety functions or part of the functions may typically be observed by means of a range of activities/observations, Table 1 illustrates the relation between the failure cause categories (as discussed in section 4) and the main types of activities/observations.

Table 1. Different types of surveillance of safety functions.

Surveillance activity	Random hardware failures		Systematic failures	
	Ageing	Stress	Interaction	Design
Actual demand	x	x	x	x
Automatic self-test	x	x		
Functional test	x	x		
Inspection	x	x	(x)	
Random detection	x	x	(x)	

Not every failure encountered during the different surveillance activities may fit perfectly into the scheme, but it illustrates which failure categories that typically can be identified by use of different surveillance activities.

The actual demands of a function can potentially reveal both systematic and random hardware failures, provided that there is a systematic approach for registration of failures. The frequency of actual demands is, however, in most cases low, and it is therefore important that the organization focuses on the actions taken after an actual demand. As an example statistics from HSE (HSE 2002a) shows that gas detectors detected 59 % of 1150 gas leakages reported in the period 1-10-92 to 31-3-01, while the remaining releases were mainly detected by other means, i.e., equipment not designed for the purpose (visual means, by sound, by smell, etc.).

In addition to the actual demands, the SIS functions must be tested, and there are two types of testing: 1) functional tests and 2) automatic self-tests. These tests are essentially designed to detect random hardware failures. However, no test is perfect due to different factors as the test do not reflect real operating conditions, the process variables cannot be safely or reasonably practicably be manipulated, or the tests do not address the necessary functional safety requirements (e.g. response time and internal valve leak) (HSE 2002b).

Components often have built-in automatic self-tests to detect random hardware failures. Further, upon discrepancy between redundant components in the safety system, the system may determine which of the modules have failed. This is considered part of the self-test. But it is never the case that all random hardware failures are detected automatically (“Diagnostic Coverage”). The actual effect on system performance from a failure that is detected by the automatic self-test may also depend on system configuration and operating philosophy.

Functional testing is performed manually at defined time intervals, typically 3, 6 or 12 months intervals for component tests. The functional test may not be able to detect all functional failures. According to Hokstad & Corneliussen (2003) this is the case for:

- Design errors (present from day 1 of operation), examples are: software errors, lack of discrimination (sensors), wrong location (of sensor), and other shortcomings in the functional testing (the test demand is not identical to a true demand and some part of the function is not tested).
- Interaction errors that occur during functional testing, e.g., maintenance crew forgetting to test specific sensor, tests performed erroneously (wrong calibration or component is damaged), maintenance personnel forgetting to reset by-pass of component.

Thus, most systematic failures are not detected even by functional testing. In almost all cases it is correct to say that functional testing will detect all random hardware failures but no systematic failures.

The functional tests may be tests of:

- The entire system/function typically performed when the process is down, e.g., due to revision stops.
- Components or sub-functions. Component tests are normally performed when the process is in operation.

Component tests are more frequent than the system tests due to less consequences on production. Experience do, however, show that full tests (from input via logic to output device) “always” encounter failures not captured during component tests.

In IEC 61511-1, inspection is described as “periodical visual inspection”, and this restricts the inspections to an activity that reveals for example unauthorized modifications and observable deteriorations of the components. An operator may also detect failures in between tests (Random detection). For instance the panel operator may detect a transmitter that is “stuck” or a sensor left in by-pass (systematic failure).

6 DISCUSSION

The data from the various activities described above should be systematically analyzed to 1) monitor the actual performance of the safety functions and 2) systematically analyze the failure causes in order to improve the performance of the function. The organization should handle findings from all above surveillance activities, and should focus on both random hardware and systematic failures. The failure classification in PDS may assist in this work.

6.1 Performance of safety functions

As stated above, the performance of safety functions has three elements: 1) the functionality/efficiency, 2) the reliability, and 3) the robustness. The functionality is influenced by systematic failures. Since these failures seldom are revealed during testing, it is necessary to register systematic failures after actual demands or events that are observed by the personnel (inhibition of alarms, scaffolding, etc.).

Traditionally, the reliability is quantified as the probability of failure on demand (PFD) and is mainly influenced by the dangerous undetected random hardware failure rate (λ_{DU}), the test interval (τ) and the fraction of common cause failures (β).

The PDS-method (Hokstad & Corneliussen 2003), however, accounts for major factors affecting reliability during system operation, such as common cause failures, automatic self-tests, functional (manual) testing, systematic failures (not revealed by functional testing) and complete systems including redundancies and voting. The method gives an integrated approach to hardware, software and human/organizational factors. Thus, the model accounts for all failure causes as shown in Figure 4.

The main benefit of the PDS taxonomy compared to other taxonomies is the direct relationship between failure causes and the means used to improve the performance of safety functions.

The robustness of the function is defined in the design phase, and should be carefully considered when modifications on the process or the safety function are performed.

6.2 Analysis of random hardware failures from functional tests

Data from functional tests on offshore installations is summarized in a CMMS (computerized maintenance management system). The level of detail in reporting may vary between oil companies and between installations operated by the same company. Typically, the data is presented as failure rates per component class/type independent of the different safety functions which the components are part of. This means that the data from component tests must be combined with the configuration of a given safety function in a reliability model (e.g. a reliability block diagram or PDS) to give meaning with respect to SIL for that safety function. Alternatively a “SIL budget” for detection (input), decision (logic) and action (output) might be developed. This can be advantageous since tests of the components are more frequent, and data from tests can be used to follow up component performance independent of safety functions.

It is important to have a historical overview of the number of failures and the total number of tests for all the functional tests in order to adjust the test interval, but it is equally important to analyze the failure causes to prevent future failures. This is particularly the case for dependent failures (i.e. stress failures). An example is sensors placed in an environment that results in movements and temperature conditions that further may lead to stress failures on several sensors. The functional tests will reveal random hardware failures but will not differentiate between independent (ageing) and dependent failures, and the fraction between independent and dependent failures must be analyzed.

Common cause failures may greatly reduce the reliability of a system, especially of systems with a high degree of redundancy. A significant research activity has therefore been devoted to this problem, and Høyland and Rausand (1994) describe various aspects of dependent failures.

For the β-factor model we need an estimate of the total failure rate λ, or the independent failure rate (λ_I), and an estimate of β. Failure rates may be found in a variety of data sources. Some of the data sources present the total failure rata, while other present the independent failure rate. However, field data collected from maintenance files normally do not distinguish between independent failures and common cause failures, and hence presents the total failure rate. In this case, the β, and λ_I will normally be based on sound engineering judgment. An approach is outlined in IEC 61508 for determining the plant specific β(s).

The maintenance system (procedures and files) should be designed for assisting in such assessments, and it is especially important to focus on the failure causes discussed in this paper

The tests and calculated PFD numbers may be used as arguments for reducing the test interval or more critical, to increase the test interval. Such decisions should not be based on pure statistical evidence, but should involve an assessment of all assumptions the original SIL requirement was based on. OLF suggests an approach for assessment of the failure rate (OLF, 2001), but the oil companies have not implemented this approach fully yet.

6.3 *Analysis of systematic failures*

As described earlier, the systematic failures are almost never detected in the tests or by inspection, but it is important to analyze the systematic failures that occur in detail and have a system to control systematic failures.

Systematic failures are usually logged in other systems than the CMMS, but the information is normally not analyzed in the same detail as the data from functional tests. In particular, it is important to investigate the actions taken by the safety functions when an actual demand occurs. Systematic analysis of gas leaks is important for gas detection systems. Such analyses may indicate if the sensors have wrong location and do not detect gas leakages. In addition, other systems like incidents investigation, systems or procedures for inhibition of alarms, scaffolding work, and reset of sensors must be in place and investigated periodically. Another possibility that could be utilized more in the future, is to build in more detailed logging features in the SIS logic, to present the signal path when actual demands occur. This type of logging might give details about failed components and information about how the leak was detected.

6.4 *Procedure/system for collection of failure data*

Experiences from the failure cause analysis should be used to improve the procedures and systems for collection and analysis of failure data. A structured analysis of failures and events may reveal a potential for improvements in the actual maintenance or test procedures, or need for modifications of the safety-related systems to improve the functionality.

An important aspect regarding collection of failure data is the definitions of safety-critical failures. Ambiguous definitions of safety-critical failures may lead to incorrect registration of critical failures (e.g. failures that are repaired/rectified “on the spot” are not logged) or registration of non-critical failures as critical ones. The oil companies in Norway have initiated a joint project with the objective to establish common definitions of critical failures of safety functions.

6.5 *SIS vs. other types of safety functions*

Our case, “prevent spreading of HC by stopping the supply” is an active safety function, and we have not discussed challenges related to surveillance of passive safety functions. However, the functionality of passive safety functions is integrated in the design phase of the installation, and in practice, passive safety functions will be tested only during real accidents. Surveillance of passive safety functions may be carried out by continuous condition monitoring or periodic inspection.

The focus of this paper has been surveillance of SIS. However, surveillance of other safety functions as other technology safety-related systems and external risk reduction facilities is important to control the risk during operation. The failure classification and the surveillance activities presented above may also be used for other active, safety-related systems. Surveillance of some kinds of external risk reduction facilities in the form of operational risk reducing measures as operational procedures may require use of other kinds of surveillance activities.

7 CONCLUSIONS

Recent standards and regulations focus on the entire life cycle of safety functions, and in this paper we have focused on the surveillance of safety functions during operations and maintenance.

The main message is that there should be an integrated approach for surveillance of safety functions that incorporates hardware, software and human/organizational factors, and all failure categories should be systematically analyzed to 1) monitor the actual performance of the safety functions and 2) systematically analyze the failure causes in order to improve the functionality, reliability and robustness of safety functions.

Not all surveillance activities reveal all kind of failures, and a comprehensive set of activities should be used. Failures of safety functions should be registered during actual demands (e.g. gas leaks), testing (functional tests and self-tests), and inspection. The presented failure classification scheme can contribute to an understanding of which surveillance activities that reveal different types of failures.

8 REFERENCES

Aarø R, Bodsberg L, Hokstad P. *Reliability Prediction Handbook; Computer-Based Process Safety Systems*. SINTEF report STF75 A89023, 1989.

Bodsberg L, Hokstad P. A System Approach to Reliability and Life-Cycle Cost for Process Safety Systems. *IEC Trans. on Reliability*, Vol. 44, No. 2, 1995, 179-186.

Bodsberg L, Hokstad P. Transparent reliability model for fault-tolerant safety systems. *Reliability Engineering & System Safety*, 55 (1996) 25-38.

CCPS, 2001. *Layer of Protection Analysis – Simplified Process Risk Assessment*. ISBN 0-8169-0811-7, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, US.

Hansen GK, Aarø R. *Reliability Quantification of Computer-Based Safety Systems. An Introduction to PDS*. SINTEF report STF38 A97434, 1997.

Hansen GK, Vatn. *Reliability Data for Control and Safety Systems*. 1998 edition. SINTEF report STF38 A98445, 1999.

Hokstad P, Corneliussen K. *Improved common cause failure model for IEC 61508*. SINTEF report STF38 A00420, 2000.

Hokstad P, Corneliussen K. *PDS handbook*, 2002 Edition. SINTEF report STF38 A02420. 2003.

HSE 2002. *Offshore hydrocarbon releases statistics, 2001*. HID Statistics Report HSR 2001 002. Health & Safety Executive, UK.

HSE 2002b. *Principles for proof testing of safety instrumented systems in the chemical industry*, 2002. Contract research report 428/2002. Health & Safety Executive, UK.

Høyland A & Rausand M, 1994. *System Reliability Theory Models and Statistical methods*. ISBN 0-471-59397-4, Wiley-Interscience.

IAEA, 1999. *Basic Safety Principles for Nuclear Power Plants* INSAG-12, 75-INSAG-3 Rev. 1. IAEA, Vienna, 1999.

IEC 1998. IEC 61508 1998. *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission.

IEC, 2002. IEC 61511-1 2002. *Functional safety: Safety Instrumented Systems for the process industry sector Part 1: Framework, definitions, system, hardware and software requirements*, Version for FDIS issue 8/1/02. International Electrotechnical Commission.

ISO, 1999. ISO 13702:1999. *Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – requirements and guidelines*. International Electrotechnical Commission.

ISO, 2000. ISO 17776:2000. *Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment*.

NORSOK, 2001. *Risk and emergency preparedness analysis*, NORSOK standard Z-013 Rev. 2, 2001-09-01, NTS, Oslo, Norway.

NPD, 2001a. *Regulations relating to management in the petroleum activities (The Management Regulations)*. 3 September 2001, The Norwegian Petroleum Directorate

NPD, 2001b. *Regulations relating to design and outfitting of facilities etc. in the petroleum activities, (The Facilities Regulations)*. 3 September 2001, The Norwegian Petroleum Directorate.

NPD/RNNS, 2002. *The Risk Level on the Norwegian Continental Shelf* (In Norwegain - Risikonivå på norsk sokkel), Oljedirektoratet, Stavanger, Norway.

OLF, 2001. *Recommended Guidelines for the Application of IEC 61508 and IEC 61511 in the Petroleum Activities on the Norwegian Continental Shelf*. The Norwegian Oil Industry Association.

Reason, J. 1997. *Managing the risk of organizational accidents*, ISBN 1 84014 105 0, Ashgate Publishing Limited, England.

Sørum M, Thomassen O. 2002. *Mapping and monitoring technical safety*. SPE paper 739230.

Vatn J. *Software reliability quantification in relation to the PDS method*. SINTEF report STF38 A0016, 2000.

Paper 4 Barrier diagram of oil/gas wells - construction rules

Kjell Corneliussen

Barrier diagram of oil/gas wells – Construction rules

K. Corneliussen
Dept. of Production and Quality Engineering, NTNU /ExproSoft AS, Trondheim, Norway

Barrier diagrams have been used for some 10-15 years to assist in well risk analysis. However, the diagrams are constructed in a variety of forms and no formal construction rules have been presented.

This article describes a method to construct barrier diagrams. The barrier diagram is used to show the structural relationship between well barriers. Barrier diagram construction rules are presented together with a description of how to transfer the barrier diagrams directly to a fault tree or alternatively how to calculate leak probabilities directly from the barrier diagram.

The major uses of barrier diagrams are to prioritize the contributors leading to the blowout, contribute in communication between reliability and well design/operation personnel, assist in design of the well and easier modeling of the well with well-known and commercially available quantitative analysis techniques, like, e.g., fault tree analysis.

1 INTRODUCTION

The essential function of an oil and gas producing well is to transport hydrocarbons from the reservoir to the processing equipment in a cost effective and safe manner.

Safety is defined by IEC 61508 as “freedom from unacceptable risk”, while IEC 60300-3-9 defines risk as a “combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.”

The importance of well safety has been recognized and accepted for a long time, and significant improvements concerning both design and operating procedures have been made. In spite of these improvements, failures still occur and will probably continue to occur in the future. Also the industrial and technological development, the extended lifetime of wells and, recent regulations and standards with focus on functional requirements imply that there is a need for a systematic approach towards well safety during the entire life cycle of a well.

For a well the main risk contributor is blowout. The acceptable mean time between blowouts is very long compared to the lifetime of a well. In such situations Rasmussen (1994) states that the risk involved in operation has to be predicted analytically from the first beginning and the proper defenses designed from this prediction. Use of predictive methods in the well risk assessment is not new. However, descriptions and guidelines on how to apply the analysis techniques in the well lifecycle are fragmented.

The standard NORSOK D-010 – Well integrity in drilling and well operations, defines the minimum functional and performance oriented requirements and guidelines for well design, planning, and execution of safe well operations in Norway. The focus of the standard is well integrity, where well integrity is defined as application of technical, operational, and organizational solutions to reduce risk of uncontrolled release of formation fluids throughout the lifecycle of a well.

In NORSOK D-010 a well barrier is defined as an envelope of one or several dependent barrier elements preventing fluids or gases from flowing unintentionally from the formation, into another formation or to surface, while a well barrier element is defined as an object that alone can not prevent flow from one side to the other side of it self. Hence, a well barrier element will typically be of a physical nature (safety valves, tubing, seals, packers, etc.), while operational and organizational measures are used to ensure the integrity of the physical components. The terms well barrier and well barrier element (WBE) are used in this paper.

In the Norwegian oil industry a two barrier principle is followed. In NORSOK D-010 it is stated that there shall be two well barriers available during all well activities and operations, including suspended or abandoned wells, where a pressure differential exists that may cause uncontrolled outflow from the borehole/well to the external environment. In NORSOK D-010 the primary well barrier is defined as the first object that prevents flow from a source, while the secondary well barrier is the second object that prevents flow from the source.

Quantitative reliability analyses are often performed to assess alternative well designs. Quantitative analyses are performed to:

- Compare different well completion alternatives with respect to leak probabilities
- Identify potential barrier problems in specific well completions
- Assess the effect of various risk reduction measures
- Assess the effect of failed barrier elements with respect to leak probabilities and recommend risk reducing measures.
- Identify potential barrier problems during well interventions

To assist in this process a barrier diagram may be used to illustrate the structural relationship between well barrier elements. The major uses of barrier diagrams are:

- Prioritize the contributors leading to the blowout
- Contribute in communication between reliability and well design/operation personnel
- Assist in design of the well
- Easier to model the well with well-known and commercially available quantitative analysis techniques, e.g. FTA

Barrier diagrams have been used for some 20-25 years to assist in well risk analysis. However, the diagrams are constructed in a variety of forms and no formal construction rules have been presented. The main objective of this article is to present a barrier diagram method description. The article also describes how to transfer the barrier diagrams directly to a fault tree or to perform reliability calculations directly from the barrier diagram.

Holand (1997) describes two main types of barrier situations. That is static and dynamic barrier situations. A static barrier situation is a situation where the same well barrier will be available over a "long" period of time. Examples of static barrier situations are the production/injection phase or when the well is temporarily closed. In a dynamic situation the well barrier varies over time. This situation is typical for well drilling, well workover, and well completion operations. Barrier diagrams are best suited for static barrier situations.

The discussion is based on experiences from the Norwegian petroleum industry and results from several projects concerning blowout risk from well completions.

A typical oil production well is shown in Figure 1-1 as a basis for further discussion and exemplification. The well is a typical oil producing well with the x-mas tree located on the surface.

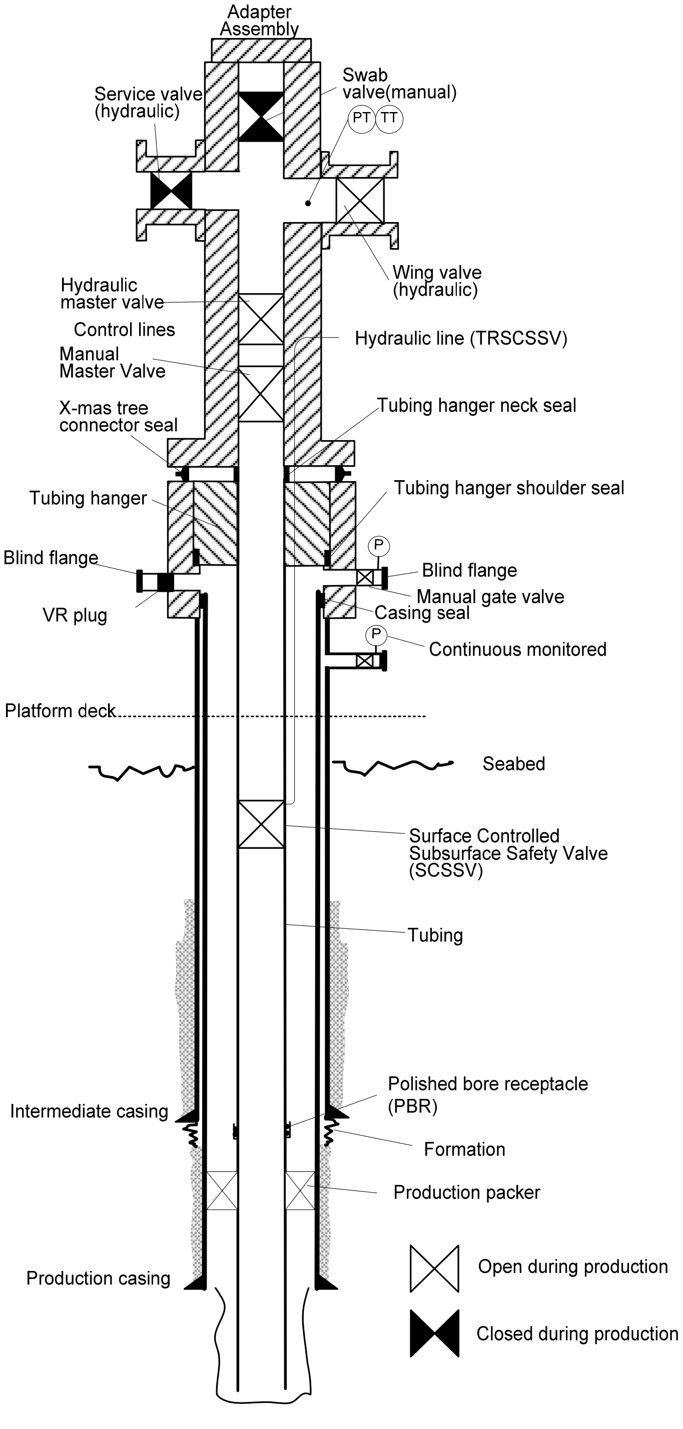


Figure 1-1 Example well

A well barrier can be regarded as a pressurized vessel (envelope) capable of containing the reservoir fluids. The two-barrier principle implies that it must be at least two well barriers in a well. A well can therefore be considered as several pressurized vessels (envelopes) that prevent the fluid from entering the surroundings, as illustrated in Figure 1-2. The well tubulars and the x-mas tree body constitute the vessel walls while the SCSSV and x-mas tree valves illustrate the outlet valves. The innermost vessel with the SCSSV illustrated as the outlet valve illustrates the primary well barrier closest to the reservoir while the outer vessels illustrate the consecutive well barriers.

A well release will typically be an incident where the outer vessel leaks, and the inner well barrier stops the leak.

The principle of viewing the well as several pressurized vessels is used when constructing a well barrier diagram.

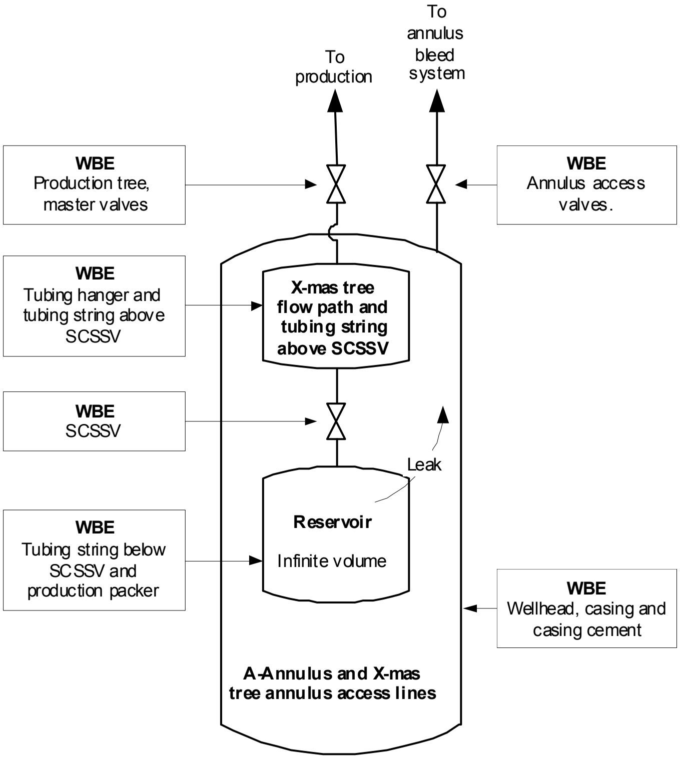

To production
To annulus bleed system
WBE Production tree, master valves
WBE Annulus access valves.
WBE Tubing hanger and tubing string above SCSSV
X-mas tree flow path and tubing string above SCSSV
WBE SCSSV
Leak
WBE Tubing string below SCSSV and production packer
Reservoir
Infinite volume
WBE Wellhead, casing and casing cement
A-Annulus and X-mas tree annulus access lines

Figure 1-2 Well illustrated as several vessels

CCPS distinguishes between passive and active independent protection layers (IPL) (CCPS, 2001). A passive protection layer is a protection layer not required to take an action to achieve its function in reducing risk. An active protection layer is required to move from one state to another in response to a change in a measurable process property (e.g. temperature or pressure), or a signal from another source (such as a push-button or a switch). This categorization is used in this article to distinguish between passive and active WBEs. Typical passive WBEs are the production packer, the seal assemblies and the tubing string. Active WBEs are the hydraulic master valve (HMV), the wing valve (WV) and the surface controlled subsurface safety valve (SCSSV). For these valves a signal has to be sent (input) in order to close the valve (change state). A combination of passive and active WBEs constitutes a well barrier.

2 BARRIER DIAGRAM CONSTRUCTION RULES

This section describes the barrier diagram construction rules. The well in Figure 1-1is used as example.

Main construction steps are:

1 Define the hazardous event
2 Define cavities where the pressure can be trapped between the reservoir and the surroundings
3 Identify the WBE failure modes and corresponding leak paths
4 Identify the fault tolerance of the well system
5 Identify barrier vectors
6 Identify minimal cut sets
7 Calculate leak probabilities

Each step is described in the following subsections. Step 2 and step 3 will be an iterative process. The steps are described separately to describe the construction principle.

2.1 Step 1 - Define the hazardous event

Before the diagram is constructed it is important to clearly define the hazardous event and the WBEs that is available to prevent the hazardous event.

The SINTEF blowout database (SINTEF, 2005) defines a blowout as “an incident where formation fluid flows out of the well or between formation layers after all the predefined technical well barriers or the activation of the same have failed”. In addition to blowout SINTEF (2005) has defined a second event called well release. A well release is defined as a “an incident where oil or gas flow from the well from some point were flow was not intended and the flow was stopped by use of the barrier system that was available in the well at the time the incident started”. A blowout will therefore be an uncontrolled flow from the reservoir. A well release may be a leak of gas lift gas that stops after the gas lift gas has escaped. The barrier diagram will not be the same for these two events.

Guidelines for defining the hazardous event are:

1. Define the criteria for the occurrence of the event by first defining the system success criteria.
2. Assure that the event is consistent with the problem to be solved and the objective of the analysis to be performed.
3. If unsure of the accidental event, provide alternative definitions that cover the event and assess the applicability of each one.

The hazardous event defined for the example well is:

- Formation fluid flows out of the well or between formation layers after all the predefined technical well barriers or the activation of the same have failed.

Together with the defined hazardous event a set of assumptions must be made, for example:

- Leaks from the reservoir via the wing valve into the flowline is regarded a hazardous event
- Leaks from the reservoir via the production casing is regarded a hazardous event
- Uncontrolled flow out of the well is defined as flow to the *surroundings*

2.2 Step 2 – Define cavities where the pressure can be trapped between the reservoir and the surroundings

As discussed a well barrier can be viewed as a pressurized vessel (envelope) capable of containing the reservoir fluids. In this step all "pressurized vessels" surrounded by WBEs able to contain the reservoir fluids are identified. The pressurized vessels are called cavities in this article. The cavities are placed between the reservoir and the surroundings. The cavities are enclosed by active WBEs in the final state (i.e., in closed position) in combination with passive WBEs, or cavities enclosed by passive WBEs only. The final stage of step 2 is illustrated in Figure 2-1.

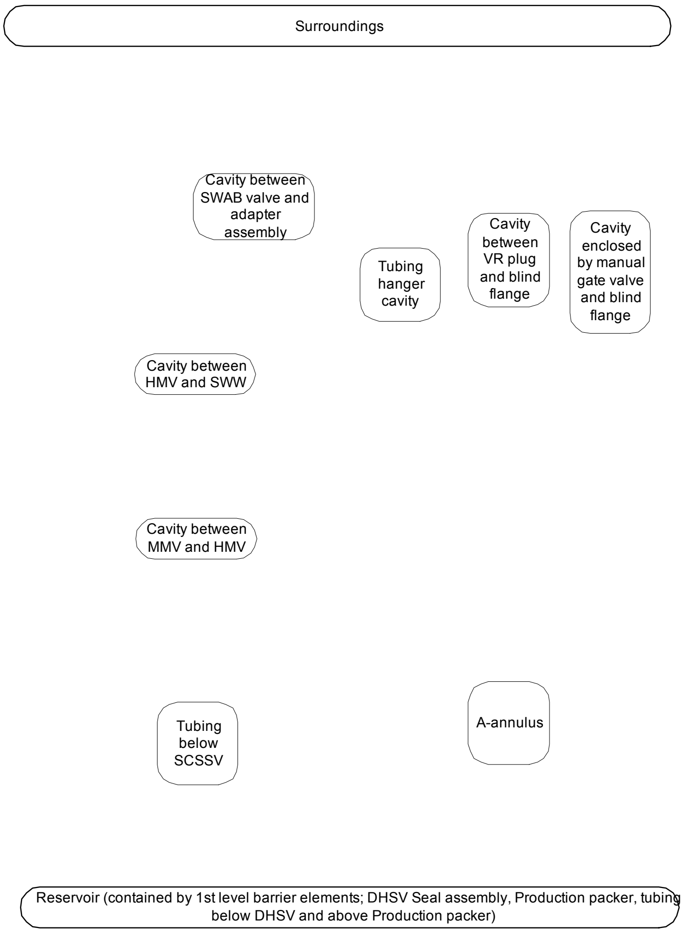

Surroundings
Cavity between SWAB valve and adapter assembly
Tubing hanger cavity
Cavity between VR plug and blind flange
Cavity enclosed by manual gate valve and blind flange
Cavity between HMV and SWW
Cavity between MMV and HMV
Tubing below SCSSV
A-annulus
Reservoir (contained by 1st level barrier elements; DHSV Seal assembly, Production packer, tubing below DHSV and above Production packer)

Figure 2-1 Cavities preventing reservoir fluid from reaching surroundings

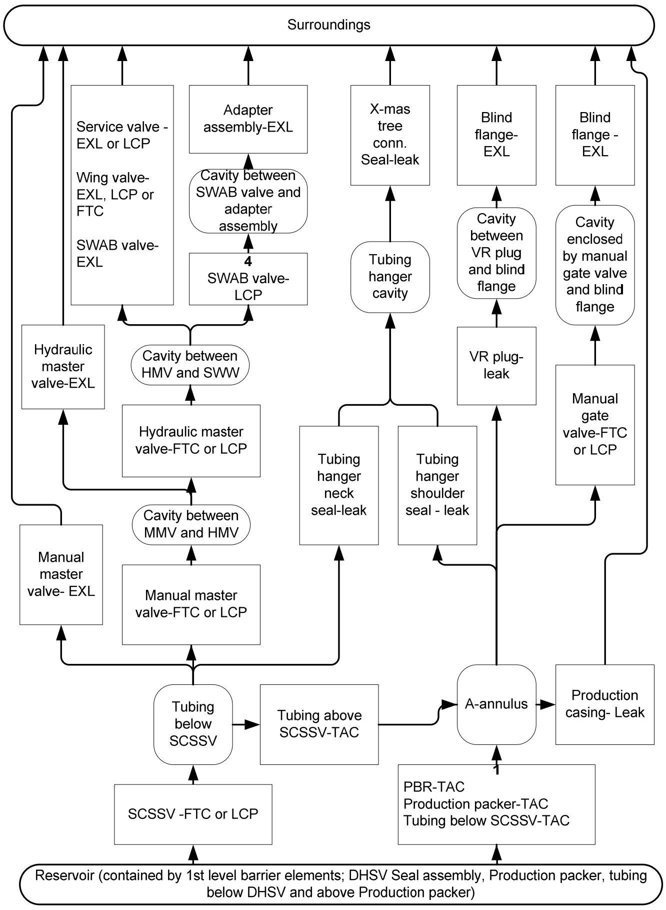
2.3 Step 3 – Identify WBE failure modes and corresponding leak paths

In this step all WBE failure modes and corresponding leak path are identified.

A failure is usually described by a failure mode and IEC 50(191) defines a failure mode as one of the possible states of a faulty item, for a given required function. As an example, one SCSSV function may be expressed as close SCSSV. A loss of this function may therefore be defined as the failure mode "Failure to close SCSSV".

A failure of a WBE may result in a leak path from one cavity to another or from one cavity to the surroundings.

All relevant failure modes and the corresponding leak paths should be entered into the barrier diagram. The result is illustrated in Figure 2-2. The leak paths are illustrated with lines with arrows. The arrows illustrate the leak direction. All leak paths include rectangles, where the WBEs and the related failure mode(s) that will result in the specific leak path are described.


Surroundings
Service valve - EXL or LCP
Wing valve- EXL, LCP or FTC
SWAB valve- EXL
Adapter assembly-EXL
Cavity between SWAB valve and adapter assembly
4
SWAB valve- LCP
X-mas tree conn. Seal-leak
Tubing hanger cavity
Blind flange- EXL
Cavity between VR plug and blind flange
VR plug- leak
Blind flange - EXL
Cavity enclosed by manual gate valve and blind flange
Manual gate valve-FTC or LCP
Hydraulic master valve-EXL
Cavity between HMV and SWW
Hydraulic master valve-FTC or LCP
Cavity between MMV and HMV
Manual master valve-FTC or LCP
Manual master valve- EXL
Tubing hanger neck seal-leak
Tubing hanger shoulder seal - leak
Tubing below SCSSV
Tubing above SCSSV-TAC
A-annulus
Production casing- Leak
SCSSV -FTC or LCP
PBR-TAC
Production packer-TAC
Tubing below SCSSV-TAC
Reservoir (contained by 1st level barrier elements; DHSV Seal assembly, Production packer, tubing below DHSV and above Production packer)

FTC-Fail to close
LCP-Leakage in closed position
EXL-External leakage
INL-Internal leakage
TAC-Tubing to annulus leakage

Figure 2-2 Leak paths and WBE failure modes

2.4 Step 4 – Identify the fault tolerance of the well system

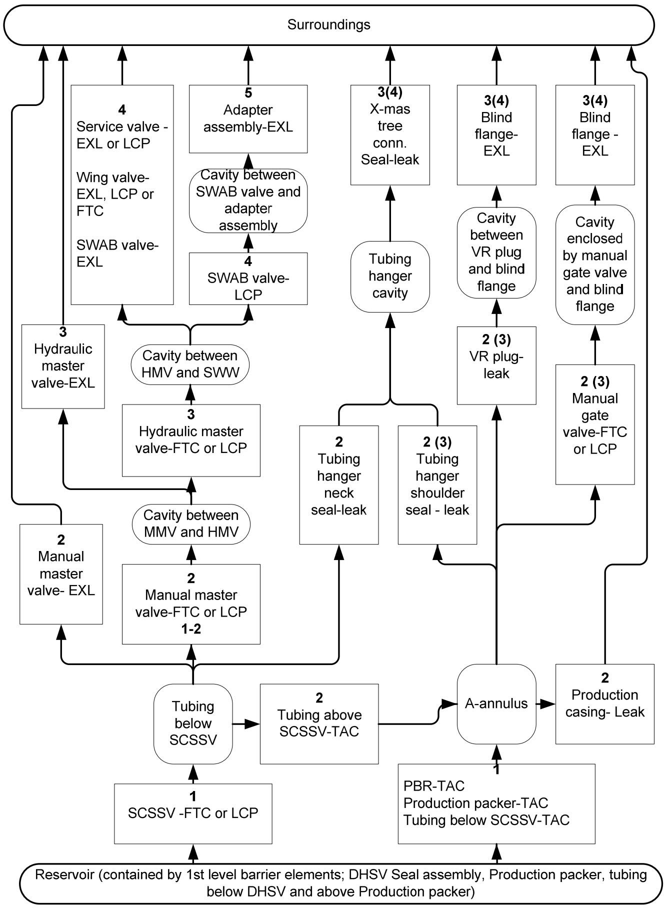
The number of WBEs failures that must occur before there is an uncontrolled leak from the reservoir to the surroundings indicates the fault tolerance of the well, where fault tolerance is defined by IEC 61508, Part 4 as "the ability of a functional unit to continue to perform a required function in the presence of faults or errors." The leak path with the fewest WBE failures has the lowest fault tolerance.

The number of WBE failures in each leak path is found by starting from the reservoir and by following the leak paths through the cavities to the surroundings. The primary WBE will be the WBE preventing leak from the reservoir to the first cavity after the reservoir. The secondary WBE will the WBE preventing flow from the first cavity after the reservoir, etc. Primary WBEs are marked with **1** in the upper part of the WBE failure mode rectangle, the secondary WBE is marked with **2**, etc. The final stage of step 4 is illustrated in Figure 2-3. As an example, it is seen from Figure 2-3 that a leak to the surroundings will occur if the SCSSV fails to close (FTC) or leaks in closed position (LCP) and if the manual master valve (MMV) leaks externally (EXL). The primary WBE failure will be that the SCSSV -FTC or LCP and is indicated with **1** in the diagram. The MMV-EXL failure is indicated with **2** in the barrier diagram.

From Figure 2-3 it is seen that the well have one leak path where only two WBEs must fail before a leak to surroundings occur, while for one leak path five WBEs must fail before a leak to surroundings occurs.

There may be several leak paths *to* one cavity. The WBE failure mode *from* the cavity may be part of a leak path with different fault tolerance. In the failure mode rectangle, all leak paths should be entered. The leak path with the highest fault tolerance should be entered in parenthesis. From Figure 2-3 it is seen that the X-mas tree connector seal will be part of a leak path with fault tolerance three if one of the WBEs between the reservoir and the A-annulus fails. If the leak path is from the reservoir via the SCSSV and the tubing above the SCSSV, the x-mas tree connector seal will be part of a leak path with fault tolerance four.

It is also seen from Figure 2-3 that the WBEs that form the primary well barrier are the SCSSV, the polished bore receptacle (PBR), the production packer and the tubing below the SCSSV.


Surroundings
4
Service valve - EXL or LCP
Wing valve- EXL, LCP or FTC
SWAB valve- EXL
5
Adapter assembly-EXL
Cavity between SWAB valve and adapter assembly
4
SWAB valve- LCP
3(4)
X-mas tree conn. Seal-leak
Tubing hanger cavity
3(4)
Blind flange- EXL
Cavity between VR plug and blind flange
2 (3)
VR plug- leak
3(4)
Blind flange - EXL
Cavity enclosed by manual gate valve and blind flange
2 (3)
Manual gate valve-FTC or LCP
3
Hydraulic master valve-EXL
Cavity between HMV and SWW
3
Hydraulic master valve-FTC or LCP
2
Tubing hanger neck seal-leak
2 (3)
Tubing hanger shoulder seal - leak
Cavity between MMV and HMV
2
Manual master valve- EXL
2
Manual master valve-FTC or LCP
1-2
Tubing below SCSSV
2
Tubing above SCSSV-TAC
A-annulus
2
Production casing- Leak
1
SCSSV -FTC or LCP
1
PBR-TAC
Production packer-TAC
Tubing below SCSSV-TAC
Reservoir (contained by 1st level barrier elements; DHSV Seal assembly, Production packer, tubing below DHSV and above Production packer)

FTC-Fail to close
LCP-Leakage in closed position
EXL-External leakage
INL-Internal leakage
TAC-Tubing to annulus leakage

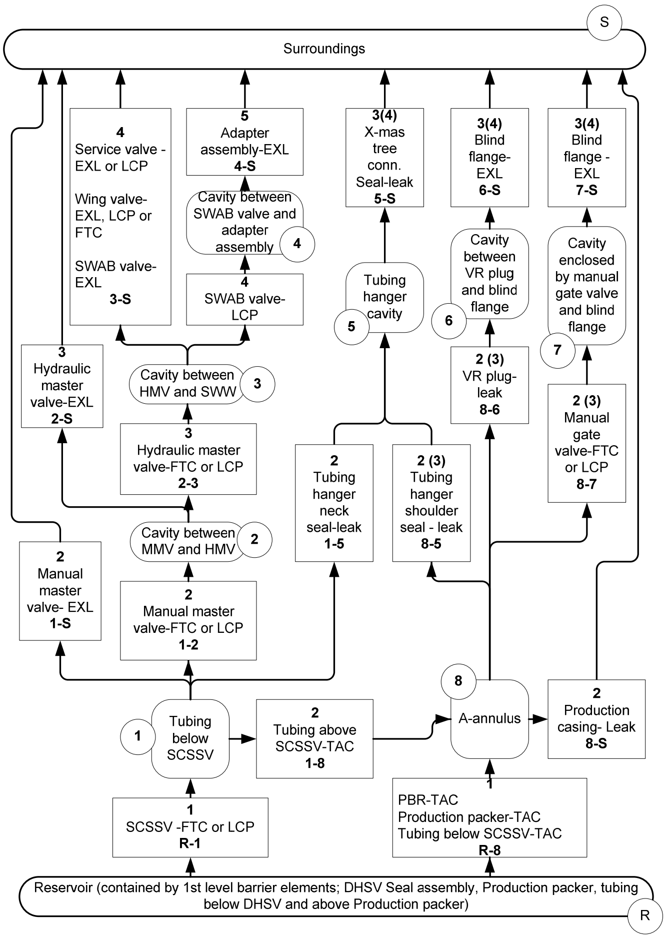
Figure 2-3 Well system fault tolerance

2.5 Step 5 – Identify barrier vectors

This step is an intermediate step that includes identification of barrier vectors. A barrier vector uniquely describes the start and end point (cavity) for each each leak path. The barrier vectors are used for quantitative and qualitative analysis in later stages.

The final stage of this step is illustrated in Figure 2-4. The step starts with labeling each cavity with a number, and by labeling the reservoir and surroundings with the letters R and S, respectively.

For each leak path, the barrier vector is entered in the lower part of the failure mode rectangle. The barrier vector identifier starts with the upstream cavity label and ends with the downstream cavity label. As an example, barrier vector for the leak path between the reservoir and the tubing below SCSSV cavity is identified as R-1.


S
Surroundings
4
Service valve - EXL or LCP
Wing valve- EXL, LCP or FTC
SWAB valve- EXL
3-S
5
Adapter assembly-EXL
4-S
3(4)
X-mas tree conn.
Seal-leak
5-S
3(4)
Blind flange- EXL
6-S
3(4)
Blind flange - EXL
7-S
Cavity between SWAB valve and adapter assembly
4
4
SWAB valve- LCP
Tubing hanger cavity
5
Cavity between VR plug and blind flange
6
Cavity enclosed by manual gate valve and blind flange
7
3
Hydraulic master valve-EXL
2-S
Cavity between HMV and SWW
3
2 (3)
VR plug- leak
8-6
2 (3)
Manual gate valve-FTC or LCP
8-7
3
Hydraulic master valve-FTC or LCP
2-3
2
Tubing hanger neck seal-leak
1-5
2 (3)
Tubing hanger shoulder seal - leak
8-5
Cavity between MMV and HMV
2
2
Manual master valve- EXL
1-S
2
Manual master valve-FTC or LCP
1-2
8
A-annulus
2
Production casing- Leak
8-S
1
Tubing below SCSSV
2
Tubing above SCSSV-TAC
1-8
1
SCSSV -FTC or LCP
R-1
1
PBR-TAC
Production packer-TAC
Tubing below SCSSV-TAC
R-8
Reservoir (contained by 1st level barrier elements; DHSV Seal assembly, Production packer, tubing below DHSV and above Production packer)
R

FTC-Fail to close
LCP-Leakage in closed position
EXL-External leakage
INL-Internal leakage
TAC-Tubing to annulus leakage

Figure 2-4 Barrier vectors

2.6 Step 6 – Identify minimal cut sets

In this step the barrier vectors are used to identify the minimal cut sets of the well system. A minimal cut set fails if and only if all the basic events in the set fail at the same time (Rausand and Høyland, 2001). Minimal cut sets are used as a basis for quantitative reliability analysis.

From the example, it is seen that the minimal cut set with the lowest fault tolerance is the leak from the reservoir to the surroundings via cavity number 1. The minimal cut sets will be 1) the SCSSV- FTC and MMV-EXL and 2) the SCSSV-LCP and MMV-EXL. These two minimal cut sets may be combined to a minimal cut set including the barrier vectors R-1 and 1-S.

The remaining minimal cut sets of barrier vectors are easily identified from the barrier diagram by following the different leak paths. The cut sets for the example well are given in Table 2-1. As seen, the minimal cut sets should always start with the letter S, be linked together with the same number and end with the letter R.

Table 2-1 Cut sets of barrier vectors

K1 = {R-1, 1-S}
K2 = {R-1, 1-2, 2-S}
K3 = {R-1, 1-5, 5-S}
K4 = {R-8, 8-5, 5-S}
K5 = {R-8, 8-6, 6-S}
K6 = {R-8, 8-7, 7-S}
K7 = {R-1, 1-2, 2-3, 3-S}
K8 = {R-1, 1-8, 8-5, 5-S}
K9 = {R-1, 1-8, 8-6, 6-S}
K10 = {R-1, 1-8, 8-7, 7-S}
K11 = {R-1, 1-2, 2-3, 3-4, 4-S}

It is possible to perform qualitative reliability analysis directly from minimal cut sets. However, barrier diagrams are frequently transformed to a fault tree for further qualitative analysis. The identified minimal cut sets make this transfer easy. An illustrative example of a fault tree is presented in Figure 2-5. Fault trees are constructed by definining a top event (TOP). In this article the top event will be the hazardous event defined in step 1. And-gates (K1, K2, KK) and or-gates (CI, C2, Cn) present the structural relationship of the system, while basic events (B1, B2, Bm) are the failure modes of the system. Fault tree construction rules are presented in many standards and books and will not be described further (see, e.g., Rausand and Høyland, 2001). The transition from barrier diagrams to fault trees is focused in this article.

Each minimal cut set identified from the barrier diagram can be represented as and-gates (K1, K2, etc) in the fault tree, while each barrier vector (cut) in the minimal cut set represents an or-gate (C1, C2, etc). The corresponding basic events (B1, B2, etc.) are the WBE failure modes in each barrier vector (cut). The transfer from minimal cut sets to a fault tree is illustrated in Figure 2-5.

It is also possible to calculate the leakage probability directly from the minimal cut sets. How to do this is described in the next step.

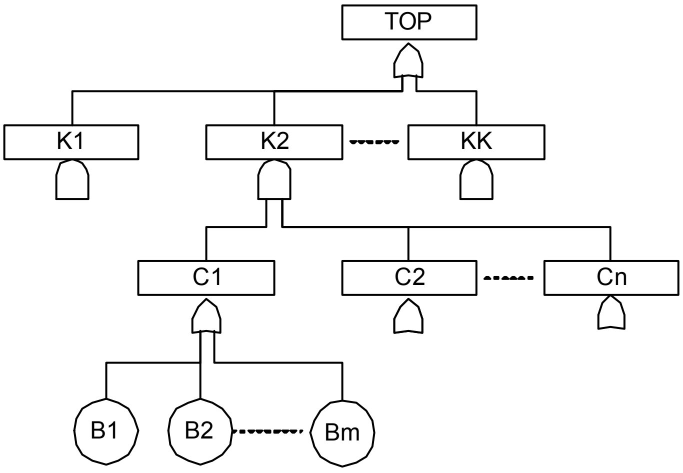


Figure 2-5 Fault tree constructed with the use of minimal cut sets

2.7 Step 7 - Calculate leak probabilities

From the cut sets, approximate formulas can be used to calculate the leak probability. A system that is functioning if and only if all of its components are functioning is called a series structure. Each barrier vector (cut) will be a series. A system that is functioning if at least one of its components is functioning is called a parallel structure, and a cut set will represent a parallel structure.

Rausand and Høyland (2001) describe how to calculate probability of failure (Q) based on minimal cut sets, and an extract is given here. Consider a system with k minimal cut sets K_1, K_2, …K_k. Let $\breve{Q}_j(t)$ denote the probability that minimal cut j fails at time t. If the basic events are assumed to be independent, then

$$\breve{Q}_j(t) = \prod_{i \in K_j} q_i(t)$$

Assuming that all the $\breve{Q}_j(t)$'s are so small that we can disregard their products. $Q_o(t)$, the probability that the top event occurs at time t, may be approximated by:

$$Q_0(t) \approx \sum_{j=1}^{k} \breve{Q}_j(t)$$

The CARA fault tree software tool (CARA FaultTree) uses four basic event types (assume exponential distribution, i.e., constant failure rate):

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

Test interval is used to describe components that are tested periodically with test interval t*. A failure may occur anywhere in the test interval. The failure will, however, not be detected until the test is carried out or the component is needed. This is a typical situation for many types of detectors, process sensors, and safety valves. The probability $q_i\ (t)$ is in this situation often referred to as the probability of failure on demand (PFD) or unavailability. The reliability parameters entered are the failure rate λ (expected number of failures per hour), the test interval t* (in hours) and the repair time τ (in hours). An approximate formula for the MFDT is:

$$q_i(t) \approx \frac{\lambda t^*}{2} + \lambda\tau$$

Note that this formula is only valid if we have independent testing of each component. If components are tested simultaneously, or if we have staggered testing, this formula will not be exactly correct, and the results will be too optimistic.

Repairable is used for components that are repaired when a failure occurs. If the failure rate is denoted λ, and the mean time to repair (MTTR) is denoted τ, $q_i(t)$ may be approximated by the formula:

$$q_i(t) \approx \frac{MTTR}{MTTR + MTTF} = \frac{\lambda\tau}{1+\lambda\tau}$$

where

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

The required reliability parameters are the failure rate λ (expected number of failures per hour) and the mean time to repair, MTTR (in hours).

Non-repairable is used to describe components where failures of single components will not be detected unless there is a leak to the surroundings. In this period the components may be considered as so-called *non-repairable* components. If the failure rate of the component is denoted by λ, then:

$$q_i(t) = 1 - e^{-\lambda t}$$

Where $q_i\ (t)$ denotes the probability that item no. *i* is not functioning at time *t*. The required reliability parameter is the failure rate λ (expected number of failures per hour). The time is represented by *t*.

On demand is used for components that have a certain probability to fail when they are required. In this study it has only been used in association with sensitivity analyses.

The four basic event types may be used to calculate the probability Q for each minimal cut set. Minimal cut set K1 is used to illustrate the principle. The SCSSV is a test interval component, which is tested every 4380 hours (6 months). The repair time is assumed to be 360 hours (15 days). The total failure rate for LCP and FTC failures is assessed to be 2.5 failures per 10^6 hours. The corresponding PFD (q_{SCSSV}) is then $4{,}92 * 10^{-6}$. An external leak from the MMV is assumed to be detected immediately, and repaired within 72 hours (3 days). The failure rate is assessed to be 0.02 failures per 10^6 hours. The corresponding $q_{MMV\text{-}EXL}$ is $7{,}19 * 10^{-6}$. When using these assumptions the leak probability, Q_1, to the surroundings via minimal cut set K1 is equal to $q_{SCSSV} * q_{MMV\text{-}EXL} = 5{,}65 * 10^{-6}$.

The remaining minimal cut sets may be calculated in the same way. The total probability will be the sum of all the cut sets.

3 SUMMARY AND CONCLUSIONS

In this article a method to construct barrier diagrams is described. The barrier diagram is used to illustrate the structural relationships between well barriers. Barrier diagram construction rules are presented together with a description of how to transfer the barrier diagrams directly to a fault tree or alternatively how to calculate leak probabilities directly from the barrier diagram.

The barrier diagram is a simplified representation of the real world. It is therefore important to validate the barrier diagram. This may not be an easy task and depends, e.g., on the experience of the personnel involved in the work, the input data used (if quantitative analysis is performed), etc. Some guidelines for validation are:

1. Obtain the minimal cut sets, and check if barrier vectors (cuts) are valid leak paths from the reservoir to the surroundings.
2. Identify WBE failure modes that have occurred from, e.g., failure databases. Check if the failure modes are included in the barrier diagram.
3. Check the ability of each WBE to function under given well conditions. This can, e.g., be performed by introducing failures downstream the cavity and by verifying that the WBE upstream the cavity can withstand the load.
4. Check the probabilities of the cut sets and their relative contributions to determine if the results are sensible.
5. Also, check the overall leak probability to see if it is realistic.

The method description in this article has only included single independent WBE failures. Failures in a system may also be dependent and result in common cause failures (CCF). The inclusion of common cause failures may be included in the future.

It should also be possible to develop a software tool to perform quantitative analysis directly from the barrier diagram. Such a program may ease the communication between the reliability engineer and the well design/operation personnel.

The author would like to thank Professor Marvin Rausand at NTNU, and my colleagues Per Holand, Einar Molnes and Geir-Ove Strand at ExproSoft.

4 REFERENCES

IEC 61508. 1997. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7. International Electrotechnical Commission, Geneva

IEC 60300-3-9. 1995. International Standard on Dependability Management – Part 3: Application Guide – Section 9: Risk Analysis of Technological Systems. International Standards Organization, Geneva.

Rasmussen, J. 1997. Risk management in a dynamic society: a modeling problem. Safety Science, 27: 183-213, 1997, Elsevier.

NORSOK D-010. 2004. Well integrity in drilling and well operations. rev. 3. (see http://www.standard.no/).

Holand, P. 1997. Offshore Blowouts, Causes and Control, Gulf Publishing Company, Houston.

CCPS. 2001. Layer of Protection Analysis – Simplified Process Risk Assessment. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York.

SINTEF. 2005. SINTEF offshore blowout database, Internet: http://www.sintef.no/

IEC 50(191). 1990. International Eletrotechical Vocabulary (IEV) – Chapter 191 – Dependability and Quality of Service. International Electrotechnical Commission, Geneva.

Rausand, M. and A. Høyland. 2004. System Reliability Theory. Models, Statistical methods, and Applications. Second Edition. Wiley, New York.

CARA FaultTree. 2005. Computer program for fault tree analysis. Available from Sydvest Programvare AS. Internet address: http://www.sydvest.com.

Paper 5 Reliability assessment of surface controlled subsurface safety valves

Kjell Corneliussen and Marvin Rausand

Reliability assessment of surface controlled subsurface safety valves

Kjell Corneliussen and **Marvin Rausand**
Department of Production and Quality Engineering
Norwegian University of Science and Technology
S. P. Andersens v. 5, NO 7491 Trondheim, Norway

Abstract

The surface controlled subsurface safety valve (SCSSV) is one of the most important barriers against blowouts on offshore oil and gas installations. This article suggests an SCSSV failure classification in line with the IEC 611508 terminology, discusses the various contributions to the safety unavailability, and describes a method for calculating the safety unavailability of different SCSSV configurations. The paper is based on data and experience from the WellMaster$^{\text{TM}}$ project.

1 Introduction

The subsurface controlled safety valve (SCSSV) is one of the most important barriers against blowouts on offshore oil and gas installations. In spite of improvements, SCSSV failures still occur, and will most likely continue to occur. New and complex well completion designs and more hostile reservoir conditions raise further challenges to the reliability of the SCSSV.

New regulations and standards have increased the focus on the reliability of barriers and safety functions. The IEC 61508 [5] and IEC 61511 [6] standards describe a risk-based approach to ensure that the total risk is reduced to an acceptable level. These standards require that a safety integrity level (SIL) is established for safety functions. The SIL requirements are partly quantitative and the standards focus on application of reliability data and modeling of common cause failures. The Norwegian Oil Industry Association (OLF) has developed a guideline [10] for using IEC 61508 and IEC 61511, and the Norwegian Petroleum Safety Authority refers to this guideline in their Management Regulations [11]. The OLF guideline sets minimum SIL requirements to safety functions where the SCSSV is part of the function. Requirements to the SCSSV are also given in the NORSOK D-010 standard [9], which covers all aspects of well integrity, i.e., technical, operational, and organizational means to reduce the risk of uncontrolled release of formation fluids throughout the life cycle of a well. The standard does not state any quantitative reliability requirements concerning the SCSSV, but gives physical requirements, e.g., related to acceptable leak rates.

It is expected that the new standards will contribute to more systematic work on safety and thereby increased safety in the industry. The requirements also imply that there is a need for continued focus on the SCSSV as a barrier element.

The objective in this paper is to discuss potential SCSSV failures and failure causes and to present a new model for SCSSV safety unavailability that is in compliance with the IEC approach. To be realistic, the model has to be based on a clear understanding of all potential failure modes and failure causes of the SCSSV. This is important both for the reliability modeling and also in the well design process.

The reliability of the SCSSV as a safety barrier is often measured by the *availability* of the valve, i.e., the probability that the SCSSV is able to function as required when if a demand occurs. The *unavailability* of the SCSSV is the probability that the SCSSV is unable to function upon a demand. The unavailability is often denoted *probability of failure on demand* (PFD).

The paper is based on data and experience from the WellMaster$^{\text{TM}}$ project and several other projects concerning blowout risk. The WellMaster project has run a more or less continuous data collection since the Bravo blowout on the Ekofisk field in the North Sea in 1977. The database is accessible only for the oil companies sponsoring the project, but some reports with aggregated data have been published. The data presented in the current paper is from one of these reports [8]. In this paper the data is used only to illustrate analytical problems, and the results should not be considered as representing the current status of SCSSV reliability.

2 SCSSV characteristics

This section describes the most important characteristics of the SCSSV.

2.1 SCSSV types and configurations

The SCSSV is located in the production tubing, 100 meters or more below the seabed. There are two main types of SCSSVs: wireline retrievable (WR) valves and tubing retrievable (TR) valves. The WR-valve is installed and retrieved by a wireline operation through the tubing and is locked to a landing nipple inside the tubing. The WR-valve reduces the tubing diameter and has to be pulled prior to wireline operations in the well. A TR-valve is an integral part of the tubing string and is installed together with the tubing. To replace a TR-valve, the tubing has to be pulled. The TR-valve does not reduce the tubing diameter, and wireline operations can therefore be carried out through the valve. The TR-valves have become increasingly popular in the last decades, and the rest of the paper is therefore restricted to TR-valves.

The SCSSV has a failsafe-close design, and is opened and held open by hydraulic pressure through a control line from the platform (or from the seabed control system for subsea wells). When the hydraulic pressure is bled off, the valve is designed to close by the force of an integrated spring. Two different closing principles are used: ball and flapper. Of these, the flapper valves are most common.

The SCSSV system may be configured in different ways. In Norway, the most common SCSSV configurations are:

- A single TR-valve with a single control line. When a TR-valve malfunction is detected, the crew will attempt to operate the valve by pressure manipulation or wireline operation to brush/clean the valve. If such manipulations are not successful, two options may be available. Either to install a WR-valve inside the failed TR-valve, or to pull the tubing and replace the TR-valve.

- Two TR-valves in series, making it a redundant system. When a failure of one valve is detected, this valve is locked open and the well is protected by the remaining valve. The tubing is pulled only when both valves have failed.

2.2 SCSSV safety functions

The main focus of IEC 61508 [5] and IEC 61511 [6] is on so-called safety instrumented systems (SIS). A SIS consists of sensor(s), logic solver(s), and final element(s). In this context the SCSSV is a final element that has to react on some specified hazardous events. The main functions of the SCSSV are:

1. To prevent well fluids to be released to the environment if there is a leakage on the downstream side of the SCSSV.

2. To shut-in the production from the well if there is an emergency on the installation, e.g., if a fire occurs on the installation.

In the first case the SCSSV is a barrier elements that has been installed to ensure well integrity. It is necessary to close the SCSSV when components on the downstream side of the SCSSV are leaking and when the X-mas tree or the wellhead area is damaged (e.g., because of a dropped object). In the second case the production has to be shut in because an emergency shutdown (ESD) action has been initiated on the installation. In this case the SCSSV together with the X-mas tree should stop the production in order not to escalate the critical situation.

A 'dual barrier philosophy' with the requirements of having two independent, testable well barriers in a well is laid down in §76 of the PSA Activities Regulations [12]. This is further elaborated in NORSOK D-010 [9] where it is explicitly stated that there should be two independent and tested barriers available. This means that the SCSSV will be a primary barrier while the X-mas tree valves will be a secondary barrier in order to shut-in the well. This is a deterministic requirement and hence deviates from the main principle of the PSA regulations where it is stated that 'the operator shall stipulate the strategies and principles on which the design, use, and maintenance of barriers shall be based' ([11], §2).

The SCSSV is a very important shut-in barrier in a platform well in case of fire in the wellhead area (ref. the Piper Alpha accident). The situation is different for a subsea well since there are several barriers in the production flow before hydrocarbons enter the riser termination area on the platform. However, the SCSSV in a subsea well is an important barrier against leakages to the environment, and will be the only barrier if the X-mas tree should fail. If the subsea well is located close to the installation, the loss of the secondary barrier (X-mas tree) may also result in severe personnel risk due to leakage below or close to the installation. Therefore, the SCSSV has an important role both for topside and subsea wells. However, the risk of fire or explosion will be lower for subsea wells than for platform wells.

Stringent requirements to prevent production leaks and blowouts lead to a rather high intervention frequency and correspondingly, a rather high intervention risk. Even if the dual barrier requirement is considered to be a minimum requirement, it may, in particular for subsea wells with low fire and explosion risk, be justifiable to assess the possibility of implementing risk reducing measures without shut-in of production until a workover can be performed. The risk reducing measures should then not be permanent and a time schedule for workover should be established. Some operators discuss whether or not it is necessary to install an SCSSV at all for some subsea wells [3]. This depends on a number of factors, like field layout, reservoir fluid, etc.

The reliability of the SCSSV system will depend on the configuration of the system. However, the reliability of the SCSSV as a final element will be independent of the safety function the SCSSV is part of. The SCSSV as a single barrier element is focused in the rest of the paper.

3 Failure classification

In this section the SCSSV failure modes are reviewed and fitted into the terminology of IEC 61508 [5]. The failure classification is also extended to reflect specific SCSSV characteristics and well conditions.

In IEC 61508 [5] safety critical failures are referred to as *dangerous* failures, while non-safety critical failures are referred to as *safe* failures. The standard also differs between detected and undetected failures. Detected failures are normally detected immediately without any specific testing, while undetected failures can only be revealed through functional testing.

For an SCSSV the dangerous failures are undetected failures, while the safe failures are detected failures. This means that dangerous failures may occur at any time in the interval between consecutive tests. The failure is, however, not manifested and discovered until a test is carried out or the valve is to be closed because of some operational reasons.

Tests of SCSSVs are usually carried out at regular intervals. The length of the test interval varies from installation to installation, but is usually either one, three or six months. The test interval is partly decided by the authorities.

The dangerous failure modes of the SCSSV are:[1]

1. *Fail to close on command* (FTC) is the most serious failure of an SCSSV. FTC failures are mainly caused by damage to certain steel parts of the valve, such as pistons, flapper hinge and pin or seat. The failure may also be caused by scale or hydrates preventing movement of the flapper. FTC failures may also be caused by a plugged control line.

2. *Leakage in closed position* (LCP) occurs when there is a leakage across the valve that is greater than a threshold value defined in API RP 14B [1]. LCP failures are detected during regular tests or by an unacceptable tubing pressure above the SCSSV for a well being shut in. LCP failures are normally caused by a damaged flapper, or scratches in the seat sealing area. Such damages may be caused by wireline or coiled tubing work through the valve. Contaminants in the tubing may also result in a leak above the threshold value (e.g., scale, hydrates).

A clear understanding of the failure cause is important to select countermeasures to avoid failures, and to understand how different failure causes influence on the reliability of the SCSSV as a safety barrier.

Failures of safety-related systems can, according to IEC 61508 [5], be classified as either *random hardware* or *systematic* failures. A random hardware failure is defined as a 'failure, occurring at a random time.' A systematic failure is defined as a 'failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or the manufacturing process, operational procedures, documentation or other relevant factors.' A systematic failure may therefore be seen as a failure of the component to fulfill the intended function without any physical degradation, and such failure may be introduced in the entire life cycle of the component (design, operation, maintenance). In this paper we

[1] The same failure modes are also used in WellMaster and in ISO 14224 [7]

assume that systematic failures will remain undetected until a real demand for the valve occurs, and will hence result in a ‘baseline’ unavailability.

Random hardware failures occur as a result of physical mechanisms influencing the valve function. Important mechanisms are physical loads (e.g., erosion due to sand particles in the fluid, corrosion due to high H_2S content, pressure, temperature), human errors (e.g., scratches during installation), design factors (e.g., choice of materials). A detailed FMECA should be performed to identify the failure causes and understand the failure mechanisms (e.g., see [13]).

The effect of testing is fiercely discussed within the industry. Some operators claim that the valve should not be tested since testing will cause wear-out of the valve, or may lead to hydrate formation during testing. Most operators, however, agree that the valve should be actuated to reveal dangerous undetected failures. Some operators also claim that the availability of the valve will be improved by the testing, since the testing can prevent sticking seals, etc. To elucidate this discussion we suggest to divide random hardware failures into the following broad failure categories:

- Hardware failures related to a long standby period. The effect of some failure mechanisms may be reduced by moving parts relative to each other, and the testing may therefore improve the reliability of the component.

- Hardware failures related to demands/tests. The effect of some failure mechanisms may be increased by testing (e.g., wear-out and hydrate formation).

- Hardware failures that are independent of valve operation. The failure mechanisms acting on the valve are unaffected by the operation of the valve.

- Stress failures (outside design limit) induced on the valve. Stress outside the design envelope of the valve that results in an immediate valve failure (shock failure).

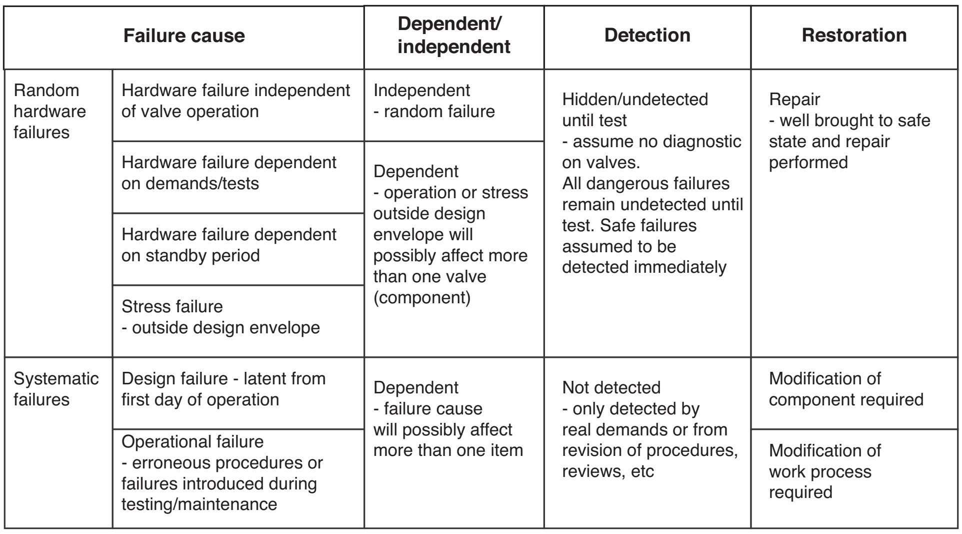
Stress failures will typically be due to (i) a wireline operation where the wireline tool damages the valve, or due to (ii) a well pressure exceeding the design limit. Hardware failures that can be prevented by exercising the valve are typically caused by scale, debris or sand build-up. Hardware failures caused by degradation due to testing (or real demands) are typically wear-out effects on the dynamic surfaces (e.g., due to ‘slamming’ of the valve or friction between moving parts). Failure mechanisms not influenced by testing are ageing mechanisms (propagation of cracks, corrosion, etc). The total failure rate of a valve will be a function of all these mechanisms (e.g., see [2]).

So far, we have discussed the SCSSV as a single element where SCSSV failures occur independent of each other. The SCSSV is also part of a system, and failures in the system may be dependent, and result in common cause failures (CCF). Fig. 2 illustrates some typical dependencies between components where the SCSSV is part of the safety function. IEC 61508 [5] requires that CCF failures are modeled by a β-factor model, where the parameter β denotes the fraction of common cause failures among all failures. The parameter β is also the conditional probability that a component failure is a common cause failure (e.g., see [13]). In relation to the failure classification above it is assumed that the hardware failures influenced by demands/tests or standby period and also stress failures are more prone to dependent failures than the hardware failures not influenced by the operation of the valve.

Fig. 1 summarizes the discussion above and also illustrates that different strategies should be used in order to address the various failure causes. Even if systematic failures are not quantified, they may be equally important, in particular for redundant systems. Hence, both hardware and systematic failures should be focused when planning the well. The different types of hardware failures should also be considered. Even if the hardware failures may be dependent on the operation of the valve (length of test interval or number or tests) all dangerous failures will be detected during testing. Hence, the assumption that no testing will increase the overall availability requires that a large proportion of the failures are caused by the testing itself. If the failures occur due to long standby times (no movement of the valve) or are independent of the test philosophy, no testing will result in an increased average unavailability.

4 Strategies for avoiding failures

To understand the factors that influence the likelihood of failures is important both during design and for reliability modeling purposes. The following approach is



Failure cause		Dependent/ independent	Detection	Restoration
Random hardware failures	Hardware failure independent of valve operation	Independent - random failure	Hidden/undetected until test - assume no diagnostic on valves. All dangerous failures remain undetected until test. Safe failures assumed to be detected immediately	Repair - well brought to safe state and repair performed
	Hardware failure dependent on demands/tests	Dependent - operation or stress outside design envelope will possibly affect more than one valve (component)		
	Hardware failure dependent on standby period			
	Stress failure - outside design envelope			
Systematic failures	Design failure - latent from first day of operation	Dependent - failure cause will possibly affect more than one item	Not detected - only detected by real demands or from revision of procedures, reviews, etc	Modification of component required
	Operational failure - erroneous procedures or failures introduced during testing/maintenance			Modification of work process required

Figure 1: Failure classification

suggested:

1. Perform a detailed FMECA to identify and understand failure mechanisms and failure causes and loads that may lead to dangerous failures. The FMECA should cover all parts of the safety function the SCSSV is part of. Generic failure rate estimates based on field experience may be used (e.g., from [8]).

2. Use the information from step 1 to prevent random hardware and systematic failures by focusing on the random hardware failure classifiaction discussed in section 3. Evaluate the generic failure rate with the actual valve and well conditions in order to reduce (or increase) the failure rate for a single component.

3. Maximize the independence of the components to prevent common cause failures. Establish β-factors for relevant dependent components.

This iterative process will improve the understanding of failure causes, and create a better basis for design of the valve, well operation procedures, and also to provide *specific* reliability data as input to unavailability calculations (as required in IEC 61508 [5]).

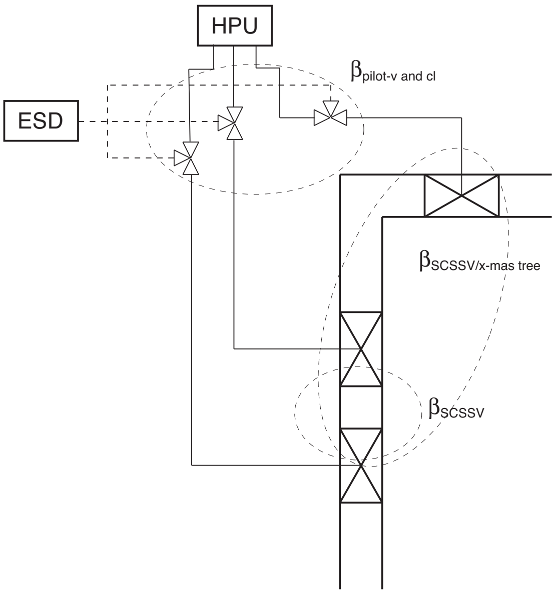

HPU
ESD
$\beta_{\text{pilot-v and cl}}$
$\beta_{\text{SCSSV/x-mas tree}}$
β_{SCSSV}

Figure 2: Examples of dependent failures in a well

There are several methods available for modeling common cause failures [13]. The most widely used model is the β-factor model. Many sources suggest ranges within which the value of β is likely to occur. The OLF guideline [10] has a data dossier where β is set to 2% for X-mas tree valves. Part 6 of IEC 61508 [5] suggests an approach to estimate a specific β (see also [15]). The approach will give β-values from 1 to 10% for final elements. Independent of which method that is used for arriving at β, the approach above should give a good basis for determining the β-factors.

The experience from WellMaster [8] may contribute in this process. The WellMaster database categorizes failures as *item failure* when the failure is caused by the item itself. If the failure is caused by another item or some external causes, the failure is classified as *non-item failure*. This would typically be the case if an SCSSV fails to open because of a control line rupture, or fails to close due to scale build-up. Non-item failures that include failures of other items should be modeled separately in a quantitative analysis, i.e., the control line and the valve should be modeled as separate items. However, the most significant part of the non-item failures are physical properties that do not directly degrade the valve parts, but prevent the valve from functioning (scale, hydrates, sand, debris) or due to stress failures. The observed distribution between item failures and non-item failures found in WellMaster are 45% and 55%, respectively, and shows that many failures are reported as failures not directly caused by the valve itself. This shows that the well conditions and operations in the well highly influence the reported failure rate and should be considered when designing a new well.

5 SCSSV restoration

The time after a failure is detected is important when considering safety unavailability, since the situation may be dangerous even if it is known that the valve has failed. NORSOK D010 [9] states that 'upon confirmation of loss of a defined well barrier, the production or injection shall be suspended and shall not re-commence before the well barrier or an alternative well barrier is re-established.'

An SCSSV can be repaired in different ways. For dangerous failures the most common repair action will be a workover, where the production string is pulled and the SCSSV is replaced with a new, or redressed, valve of the same type. This repair is both costly and time consuming. In some cases a through tubing repair may be sufficient to restore the valve function. If the failure is caused, e.g., by scale build-up, it may sometimes be possible to inject fresh water, acid or chemicals or alternatively perform wireline operations to clean the well. The repair times for the different intervention alternatives are highly influenced by the type of well. For a platform well the workover and also the wireline operation will be far less time-consuming than for a subsea well where all interventions must be performed from a workover vessel.

When a dangerous failure is detected, the important time with respect to safety is the time from the failure is detected until the well is brought to a safe state. During a part of the restoration time it will be known that the failure is present, but the state will still be dangerous, while after some time the valve is still not repaired but the well is brought to an equally safe or safer state than when the SCSSV was functioning as normal. Hence, the dangerous repair time is usually much lower than the actual time used to replace a failed valve. As an example, when an SCSSV failure is detected in a platform well, the well will normally be plugged below the SCSSV and also closed on the X-mas tree. This is considered safe until the actual repair of the valve is performed. It is also possible to plug a subsea well, but this requires a workover rig. Therefore, the well is normally closed on the X-mas tree until a workover to replace the SCSSV is performed. Whether or not this is safe depends on the distance to the neighboring platform (personnel risk in case of leak), the additional valves available on the template, etc. The risk of external damage to the X-mas tree must also be considered. Compensating actions may be to reduce the vessel activity above the wellhead.

Further in this paper it is assumed that when the well is brought to a safe state, the remaining repair time will be equally safe or safer than before the SCSSV failure was detected. This means that the critical time that should be included in the safety unavailability calculations is the mean time from a failure is detected until the well is brought to a safe state. This time is called the ‘mean dangerous waiting time’ (MDWT).

6 Safety unavailability models

In IEC 61508 [5] the probability of failure on demand (PFD) is used to measure the unavailability of a safety function. If a demand for the SCSSV as a safety barrier occurs, the PFD denotes the average probability that the SCSSV will not be able to fulfill its safety function. Since PFD is an average failure probability, it may also be interpreted as the mean proportion of the time where the SCSSV is not able to function as a safety barrier. This proportion of time is sometimes called the mean fractional down-time (MFDT).

In the following, three alternative PFD models are presented. The models are based on the classification discussed earlier in this paper. We assume that all time to failure distributions are exponential, which implies that failure rates are assumed to be constant.

Despite the huge amount of data in WellMaster [8], it has not been possible to decide with confidence whether or not the SCSSVs have constant failure rates. The main reason for this is that the data sets are inhomogeneous and represent valves operated under a variety of environmental conditions. The internal environment in each particular oil/gas well also changes during its lifespan. The usual assumption of independent and identically distributed lifetimes therefore does not hold. However, the exponential distribution is chosen because analysis of WellMaster data on SCSSV shows a fairly good fit to the exponential distribution. The SCSSV is usually replaced when a well workover is carried out. The time between well workovers varies significantly, with an average interval between 8 and 10 years. The average time in operation for an SCSSV is therefore 8–10 years.

A PFD model for deteriorating valves modeled by a Weibull distribution is suggested and discussed in [14].

Single SCSSV Let τ be the time interval between consequtive tests, and let λ_{D} be the rate of dangerous undetected failures of an SCSSV, i.e., failures that are not detected by diagnostic testing, and that may - or may not - be detected during periodic testing. For the SCSSV, no failures are supposed to be detected by diagnostic testing, which means that all dangerous failures are classified as undetected. Note that λ_{D} is the rate of all dangerous failures, be it item or non-item failures, and independent or common cause.

If we assume that *all* dangeous failures are revealed in each test, and we assume the the valve is ‘as good as new’ after each test, then the PFD within the test interval (of length τ) is (see [13])

$$\text{PFD} = \frac{1}{\tau}\int_0^{\tau} e^{-\lambda_{\text{D}} t}\, dt \approx \frac{\lambda_{\text{D}}\tau}{2} \tag{1}$$

In the WellMaster report [8] the SCSSV reliability is presented as a total mean time to failure, MTTF, for each of the valve makes presented in the study. The average MTTF for all SCSSVs was found to be 36.7 well-years, and 55.6% of all failures were dangerous failures. With this data, the dangerous failure rate λ_{D} is approximately $\lambda_{\text{D}} \approx 1.7 \cdot 10^{-6}$ (hours)$^{-1}$. With a test interval of, say, $\tau = 6$ months $= 4380$ hours, the PFD is equal to $3.8 \cdot 10^{-3}$. This means that we are unprotected by the valve in approximately 33 hours per year.

Non-perfect testing Often, the test is not fully realistic. In most cases the SCSSV is closed (smoothly) after the flow has been closed by the production wing valve. In a worst case real demand situation, the SCSSV has to be slam-shut, meaning that it will be closed against a flowing well. A slam-shut operation will give high stresses to the valve, and it may fail to close the well even if it passed a normal test just prior to the slam-shut.

To leak-test the valve the SCSSV has to be closed and pressure built-up on the downstream side has to be monitored. This test is sometimes imperfect, either because the crew does not wait long enough for the pressure to build up, or because of miscalibrated or defect pressure gauges.

The probability that a dangerous failure is present after a test is difficult to estimate. Let us assume that we, based on engineering judgement and observations, can estimate the probability θ that a failure persists after a test. The PDF within the test interval is therefore approximately

$$\mathrm{PFD} \approx \frac{\lambda_{\mathrm{D}}\tau}{2} + \theta \tag{2}$$

For simplicity, we assume that the probability θ is constant and independent of time. In the PDS project[4] the probability θ is called the probability of 'test independent failures' (TIF), or probability of systematic failures (PSF).

Down-time due to testing and repair The testing will, on the average, take the time MTTI (mean time to inspect). During the testing time the SCSSV is able to perform its function as a safety barrier if the valve is functioning when the test is initiated. Otherwise the SCSSV is not able to perform its safety function.

During the repair action the well will be unprotected during a part of the repair time as discussed in section 5. The unprotected time is denoted MDWT. If we assume that the tests are carried out after intervals of length τ irrespective of whether or not a failure has occurred, we get the overall PFD (i.e., the average proportion of time where the well is not protected by the SCSSV or an adequate substitute):

$$\mathrm{PFD} \quad \approx \quad \frac{\lambda_{\mathrm{D}}\tau}{2} + \theta + \frac{1 - e^{-\lambda_{\mathrm{D}}\tau}}{\tau}\,(\mathrm{MDWT} + \mathrm{MTTI})$$

$$\approx \quad \frac{\lambda_{\mathrm{D}}\tau}{2} + \theta + \lambda_{\mathrm{D}} \cdot (\mathrm{MDWT} + \mathrm{MTTI}) \qquad (3)$$

where $1 - e^{-\lambda_{\mathrm{D}}} \approx \lambda_{\mathrm{D}}\tau$ is the probability that a dangerous undetected failure is present when the test is initiated. We also note that $\lambda_{\mathrm{D}}\tau$ is the frequency of dangerous valve failures, i.e., the frequency of valve renewals due to dangerous failures.

If we use the same data as above, and assume that MDWT + MTTI is five weeks, i.e., 840 hours for a subsea well, then $\lambda_{\mathrm{D}} \cdot (\mathrm{MDWT} + \mathrm{MTTI}) \approx 1.5 \cdot 10^{-3}$.

Note that the PFD found by using eq. (1) or (2) is the unavailability of the valve in normal operation when we thrust that the valve is functioning. The contribution from $\lambda_{\mathrm{D}} \cdot (\mathrm{MDWT})$ in eq. (3) comes from the restoration action, when we *know* that we are unprotected by the valve. In some applications it is important to distinguish between these two contributions. Also note that the contribution from the MDWT is in the same order of magnitude as the *unknown* PFD. In the numerical example above we assumed MDWT to be five weeks for a subsea well. For many fields this is a rather low estimate and we may often see waiting times 2–3 times as high.

Standby redundancy So far, we have only considered a single SCSSV. Now, assume that two valves are installed in series. We assume that only one valve is in operation when the system is started up at time $t = 0$. The other valve is in standby position and may be activated by a dedicated mechanism. If the active valve fails, the standby valve will be activated. The well will not be re-completed until the second valve has failed. Only dangerous failures are considered. The active valve is tested at regular intervals of length τ. The standby valve is not possible to test while in standby position. The mean testing time is MTTI, the same as for a single valve. The mean dangerous waiting time, MDWT, is also the same as for a single valve.

The (initially) active valve has constant failure rate λ_{D1}. When the active valve fails, it is locked open and the standby valve is activated. The probability that this operation is successful is denoted $1 - p$. The standby valve has constant failure rate $\lambda_{\mathrm{D2}}^{s}$ in passive state, and failure rate λ_{D2} when activated. Common cause failures may be disregarded in this case since such failures are incorporated into the total dangerous failure rates of the two valves.

The survivor function $R_S(t)$ for the standby system with respect to dangerous failures is given by (see [13], p. 177)

$$R_S(t) = e^{-\lambda_{\mathrm{D1}} t} + \frac{(1-p)\lambda_{\mathrm{D1}}}{\lambda_{\mathrm{D2}}^s + \lambda_{\mathrm{D1}} - \lambda_{\mathrm{D2}}} \left(e^{-\lambda_{\mathrm{D2}} t} - e^{-(\lambda_{\mathrm{D1}} + \lambda_{\mathrm{D2}}^s)t} \right)$$

The mean time to the first dangerous system failure is

$$\mathrm{MTTF}_S = \frac{1}{\lambda_{\mathrm{D1}}} + (1-p) \cdot \frac{\lambda_{\mathrm{D1}}}{\lambda_{\mathrm{D2}}(\lambda_{\mathrm{D1}} + \lambda_{\mathrm{D2}}^s)}$$

The frequency of dangerous system failures, i.e., renewals due to dangerous system failures, is therefore

$$\nu_S \approx \frac{1}{\mathrm{MTTF}_S}$$

The standby system has only one active valve that is tested periodically. The PDF of the system during the test interval is therefore the same as for a single valve. The only difference is that the failure rate may change. From the start-up the failure rate is λ_{D1}. If the active valve fails, and the standby valve is activated, the failure rate will change to λ_{D2}. Assume that the time between workovers is t_0. The probability that the active valve survives a workover period is then equal to $R_{\mathrm{D1}}(t_0) = e^{-\lambda_{\mathrm{D1}} t_0}$. The 'average´failure rate is therefore approximately

$$\lambda_S \approx e^{-\lambda_{\mathrm{D1}} t_0} \cdot \lambda_{\mathrm{D1}} + \left(1 - e^{-\lambda_{\mathrm{D1}} t_0}\right) \cdot \lambda_{\mathrm{D2}}$$

The PFD_S of the standby system is

$$\mathrm{PFD}_S \approx \frac{\lambda_S \tau}{2} + \theta + \nu_S(\mathrm{MDWT} + \mathrm{MTTI})$$

Active redundancy Assume now that two SCSSVs of the same type are installed in series, and that both valves are active and tested at the same time after intervals of length τ. The total dangerous failure rate of a valve is λ_{D} and the two valves are exposed to common cause failures that can be modeled by a β-factor model. If one of the valves fails, this valve is left idle and the well is protected by the other valve. When both valves have a dangerous failure, the valves are renewed.

The survivor function of the valve system with respect to dangerous failures is (see [13], p. 220)

$$\begin{aligned} R_A(t) &= \left(2e^{-(1-\beta)\lambda_{\mathrm{D}}t} - e^{-2(1-\beta)\lambda_{\mathrm{D}}t}\right) \cdot e^{-\beta\lambda_{\mathrm{D}}t} \\ &= 2e^{-\lambda_{\mathrm{D}}t} - e^{-(2-\beta)\lambda_{\mathrm{D}}t} \end{aligned}$$

The mean time between dangerous system failures is hence

$$\mathrm{MTTF}_A = \frac{2}{\lambda_{\mathrm{D}}} - \frac{1}{(2-\beta)\lambda_{\mathrm{D}}}$$

The frequency of dangerous system failures is therefore

$$\nu_A \approx \frac{1}{\mathrm{MTTF}_A}$$

When both valves are functioning, the PFD_1 within the test interval can be approximated by (see [13], p. 444)

$$\mathrm{PFD}_1 \approx \frac{[(1-\beta)\lambda_{\mathrm{D}}\tau]^2}{3} + \frac{\beta\lambda_{\mathrm{D}}\tau}{2}$$

When only one valve is functioning, the PFD_2 within the test interval is approximately

$$\mathrm{PFD}_2 \approx \frac{\lambda_{\mathrm{D}}\tau}{2}$$

If we assume that the time between workovers is t_0, the probability that both valves will survive the whole interval without any dangerous failure is

$$R(t_0) = e^{-2\lambda_{\mathrm{D}}t_0}$$

The average PFD_3 in the test interval is then

$$\mathrm{PFD}_3 \approx e^{-2\lambda_{\mathrm{D}}t_0} \cdot \mathrm{PFD}_1 + \left(1 - e^{-2\lambda_{\mathrm{D}}t_0}\right) \cdot \mathrm{PFD}_2$$

The probability θ_A of test independent failures for the active redundancy system will be slightly lower that the corresponding probability θ for a single valve. The mean time to test the system, MTTI_A will be somewhat higher than MTTI for a single valve, and the mean dangerous waiting time, MDWT, will be unchanged.

The total PFD_A of the active redundancy system is hence

$$\mathrm{PFD}_A \approx \mathrm{PFD}_3 + \theta_A + \nu_A(\mathrm{MDWT} + \mathrm{MTTI}_A)$$

7 Concluding remarks

This article suggests a failure classification in line with IEC 611508 terminology, discusses the various contributions to the safety unavailability, and describes a model for calculating the safety unavailability for different SCSSV configurations. The model is based on the exponential distribution, even if we know that it might be unrealistic. In this paper we have presented a failure classification that divide hardware failures into failures influenced by the frequency of testing, failures not influenced by testing and stress failures. This classification may assist in more realistic input reliability data.

Several problems were not discussed, including interdependency between the various failure modes, and time-dependent variations in environmental and operational stresses. As an example, the presented failure classification suggests that some failures are influenced by the number of tests performed. This influence is not reflected in the unavailability model.

The model and approach for determining well specific reliability data requires access to detailed reliability data bases. Access to databases like the WellMaster project are, however, often restricted. Only publicly available information was used in this article.

Many of the ideas presented in the paper should also be applicable for other type of equipment like x-mas tree valves and subsurface controlled annulus safety valves (SCASV).

References

[1] API RP 14B. *API Recommended Practice for Design, Installation, Repair and Operation of Subsurface Safety Valve Systems, 4th edition*. American

Petroleum Institute, Washington, DC. 1994.

[2] Cooke, R. M. The design of reliability data bases, part 1: review of standard design concepts. *Reliability Engineering and System Safety*, **51**(2):137-146, 1996.

[3] Durham, C. J. and C. A. Paveley. Radical solutions required: Completions without packers and downhole safety valves can be safe. SPE 56934, Society of Petroleum Engineers, 1999.

[4] Hokstad, P. and K. Corneliussen. *Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook*. SINTEF report STF38 A02420, Trondheim, 2003.

[5] IEC 61508. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. Part 1-7. International Electrotechnical Commission, Geneva, 1997.

[6] IEC 61511. *Functional Safety - Safety Instrumented Systems for the Process Industry*. Part 1-3. International Electrotechnical Commission, Geneva, 2003.

[7] ISO 14224. *Petroleum and natural gas industries – Collection and exchange of reliability and maintenance data for equipment*. International Standards Organization, Geneva, 1999.

[8] Molnes, E. and G. O. Strand. *Reliability of well completion equipment – Phase III – Main report*. SINTEF report no. 32.0898.00, Trondheim, 1999.

[9] NORSOK D-010. *Well integrity in drilling and well operations (Rev. 3, August 2004)*. NORSOK Standard, 2004 (available on http://www.standard.no)

[10] OLF-G-070. *Guideline on the Application of IEC 61508 and IEC 61511 in the Petroleum Activities on the Norwegian Continental Shelf*. The Norwegian Oil Industry Association, 2001. (see http://www.itk.ntnu.no/sil)

[11] PSA. Regulations relating to management in the petroleum activities (The Management Regulations). Petroleum Safety Authority Norway, Stavanger, 2001.

[12] PSA. Regulations relating to conduct of activities in the petroleum activities (The Activities Regulations). Petroleum Safety Authority Norway, Stavanger, 2001.

[13] Rausand, M. and A. Høyland. *System Reliability Theory; Models, Statistical Methods, and Applications*. Wiley, New York, 2004.

[14] Rausand, M. and J. Vatn. Reliability modeling of surface controlled subsurface safety valves. *Reliability Engineering and System safety*. **61**:159-166, 1998.

[15] Smith, D. J. and K. G. L. Simpson. *Functional Safety*, Second ed. Elsevier, London. 2004.