Draft for ballot #5791

Well Control Equipment Reliability Modeling

API TR16G
FIRST EDITION, XXXX 2021

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Contents

Page

1 Scope 1

2 Informative Reference 1

3 Terms, Definitions, and Abbreviations 1
3.1 Terms and Definitions 1
3.2 Abbreviations 3

4 Reliability Analysis 4
4.1 Introduction 4
4.2 Objectives 4
4.3 Reliability Tools 5
4.4 Assumptions 15
4.5 Methodology 17
4.6 Operational Risk Analysis Use of Reliability Models 18
4.7 Data Sources 19

5 Model Results and Examples 20
5.1 Pressure and Function Test Frequency Analysis 20
5.2 Operator's Ability Sensitivity Analysis 21
5.3 Failure Rate Sensitivity Analysis 22
5.4 Fluid Quality Sensitivity Analysis 24
5.5 Common Cause Sensitivity Analysis 24

Annex A: Use of minimal cut sets in Reliability Estimation 26

Annex B: DP MODU Fault Tree 28

Annex C: Moored DU Fault Tree 28

Annex D: Surface DU Fault Tree 28

Introduction

This technical report documents the results of an industry led well control equipment systems reliability model. This technical report is under the jurisdiction of the API Committee on Standardization of Oilfield Equipment and Materials.

The objective of this technical report is to assist the oil and gas industry in promoting personnel safety, public safety, integrity of the drilling equipment, and preservation of the environment for land and marine drilling operations. In the context of well control equipment systems, this objective is best attained through a combination of equipment reliability and management of risk. This technical report is published to provide direction and guidance to analyze reliability in design, installation, and operation of well control equipment. Analysis of model through reliability engineering will also provide insight for redundancy, testing and maintenance frequency that could be utilized by other API work groups to improve our industry standards, making a positive impact on equipment reliability to reduce risk. This report models typical system designs and does not account for all system designs that can be employed to successfully install and operate well control equipment systems in drilling, completions, and well testing operations.

Well Control Equipment Systems Reliability Model

1 Scope

The purpose of this technical report is to document methods of reliability analysis for well control equipment systems installed for drilling wells.

Well control equipment systems are designed with components that provide wellbore pressure control in support of well operations. As an example, the following typical systems were modelled and analyzed:

— Surface On-Shore BOP Systems.

— Surface Off-Shore BOP Systems.

— Subsea BOP System with Discrete Hydraulic Control System.

— Offshore DP MODU with a Subsea BOP System with Electro-hydraulic/Multiplex Control System.

Fault trees were developed based on generic (non-original equipment manufacturer specific), and limited to, well control equipment components with a top event of “failing to seal and secure the well” (see Annex C, Annex D, and Annex E). This technical report did not include consequence analysis. The intent of the models is to identify the system’s ability to perform its intended function and document the individual components importance and percentage failure contribution to the top event.

The fault trees only analyze the probability of sealing a well, and do not address non-productive time.

2 Normative References

There are no normative references.

3 Terms, Definitions, and Abbreviations

3.1 Terms and Definitions

For the purposes of this standard, the following terms and definitions apply.

3.1.1
Availability
Ability to be in a state to perform as required.

3.1.2
Autoshear
System designed to automatically shut in the wellbore in the event of a disconnect of the lower marine riser package.

3.1.3
Common Cause Failures
CCF
Failures of multiple items, which would otherwise be considered independent of one another, resulting from a single cause.

3.1.4
Common Mode Failures
Failures of different items characterized by the same failure mode.

3.1.5
Critical
Element or system that is deemed by the organization, product specification, or customer as mandatory, indispensable, or essential, needed for a stated purpose or task.

3.1.6
Deadman System
System designed to automatically shut in the wellbore in the event of a simultaneous absence of hydraulic supply and control of both subsea control pods.

3.1.7
Demand
Activation of the function (includes functional, operational and test activation).

3.1.8
Failure
Loss of ability to perform as required.

3.1.9
Failure Mode
Manner in which failure occurs.

3.1.10
Fault
Inability to perform as required, due to an internal state.

3.1.11
Pivotal Event
Generally, the specific steps that must fail for the top event to fail.

3.1.12
Redundancy
Existence of more than one means for performing a required function of an item.

3.1.13
Reliability
Probability of an item to perform a required function under given conditions for a given time interval.

3.1.14
Root Cause
Set of circumstances that leads to failure.

3.2 Abbreviations

For the purposes of this standard, the following abbreviations apply.

BOP	blowout preventer
BSR	blind shear ram
CCF	common cause failure
CSR	casing shear ram
DMAS	deadman / autoshear function
DP	dynamically positioned
FMECA	failure mode, effects, and criticality analysis
ETA	event tree analysis
FTA	fault tree analysis
HPU	hydraulic pumping units
MODU	mobile offshore drilling unit
PRA	probabilistic risk assessment
RBD	reliability block diagram
TE	top event
UBSR	upper blind shear ram
WCE	Well Control Equipment

4 Reliability Analysis

4.1 Introduction

Reliability engineering is a discipline focused on assuring the ability of equipment to function without failure. Reliability analysis uses both qualitative and quantitative methods to evaluate a system and its components ability to function under stated conditions over a specific period. Depending on how complex the system is, and the type of system, a variety of techniques can be applied such as reliability block diagram (RBD), failure mode and effects analysis, reliability prediction, and fault tree analysis (FTA) to mention the most popular ones.

The blowout preventer (BOP) FTA technique presented in this report was performed to better understand the contribution of individual component and subsystem failures to the top event (TE) described as “BOP System Failure to Shear and Seal the Wellbore”. This model will further allow evaluation of how various changes, in either BOP system configuration or operation, could affect its ability to shear and seal the wellbore. This BOP analysis reflects API Standard 53 requirements for well control barriers and their control systems.

A fault tree represents multiple scenarios depicting the failure propagation from the lowest maintainable component(s) to the TE during the typical BOP well control operations. This analysis relies exclusively on the well control equipment failure data from the RAPID-S53 database for rigs operating in Gulf of Mexico. The data from RAPID-S53 was used as an input for the fault tree’s components failure rates. The FTA allowed quantification of fault propagation due to single and multiple failure events so accumulative risk contribution towards the TE could be assessed.

This analysis uses a “typical” BOP configuration and does not represent a specific rig or rig specific configuration. For a specific application, the process described in Section 4 can be applied to both identifying various ways a component failure can cause failure of the BOP. This type of analysis can provide a better understanding of a fault propagation, combination of various component failures, common cause failures (CCF’s), component failure contribution, etc. The results of such analysis can be used in support of decisions to improve reliability including configuration improvements, balanced test interval strategy, operator performance, improved maintenance strategy and intervals, and better understanding of operational risks.

4.2 Objectives

To define a methodology of conducting a reliability analysis for BOP Systems. The method described herein is a Fault Tree analysis. The Fault Tree’s TE being fail to seal and secure the well. Failure modes of the following subsystems and components should be included in the analysis.

a) mechanical components;

b) pneumatic components;

c) operator initiated functions;

d) electrical/electronic components; and

e) hydraulic components.

The failure modes of the components and subsystems above were used to perform the following analyses:

a) pressure and function testing intervals;

b) redundancies analysis (main control, secondary and emergency control);

c) CCF's (hydraulic and electronics components and software);

d) operator's ability to recognize an event and initiate the appropriate function;

e) fluid quality;

f) identification of critical components; and,

g) failure rate.

4.3 Reliability Tools

There are many tools and techniques that can be used in reliability analysis of engineering systems. Some of the techniques include failure mode effects and criticality analysis (FMECA), RBD analysis, FTA, physics of failure, petri nets, and Markov analysis. With computer-based analysis it is possible to explore variations in component reliability or failure and observe sensitivity in the model's execution. It is also possible to run a full-scale uncertainty analysis using Monte Carlo or other sampling simulations.

Most of the reliability techniques use bottom-up inductive reasoning when a specific observation leads to a broader finding or generalization (from a cause to consequence). FTA, on the other hand, is a top-down deductive method used for identification a variety of causes (basic events) leading or contributing to the final consequence or a TE (from consequence to causes). It also allows for modeling the relationship between basic events (individual and combination of failures) and their contributions to the TE. In a fault tree, functional and component level redundancies and operational sequence leading to TE could be modeled and assessed. Another technique, often used in combination with FTA, is the event tree analysis (ETA). ETA assesses propagation of the accident scenarios, due to various initiating events, that lead to potential catastrophic consequences. ETA combined with FTA technique are part of the probabilistic risk assessment (PRA) methodology that encompasses all other reliability methods and provides a broader picture of the system's resilience.

RBD is a tool that represents a system using interconnected blocks arranged in combinations of series and/or parallel configurations. In RBD the individual BOP functions or components can be modeled as individual blocks. The subsystems or components can be arranged via series and parallel blocks to represent redundancies or active and standby states. FTA and RBD are both analytical logic techniques that can be applied to analyze system reliability and related characteristics. However, RBD may be difficult to construct for very complex systems.

To conduct a reliability analysis of such a complex system as BOP, the selected tool needs to be able to represent the system logic and compute the failure rate combinations of individual component failure modes to quantify probability of the TE occurrence. Since the TE is failure to close and seal the BOP, and not quantification of availability to drill, the FTA was the tool selected from the suite of available reliability tools.

4.3.1 Basic Reliability Math

Reliability is defined as the probability an item will provide its intended function under given conditions for a given time interval. This definition states that the measure of reliability is a probability function. Therefore, the math used to compute reliability is based in statistical probability concepts.

Since the math has its foundations in probability the reliability function R(t) will always be a value between zero and one. The complement of the reliability function is the failure function F(t). The failure function will also always be a value between zero and one. The failure and reliability functions are related by the following relationships: Equation 1 for reliability as a function of the failure function, and Equation 2 for failure as a function of the reliability function.

$$R(t) = 1 - F(t) \quad \text{Equation 1}$$

$$F(t) = 1 - R(t) \quad \text{Equation 2}$$

The system logic of a series or parallel configuration can be described using Boolean variables in either success or failure space. RBDs rely on a component reliability number (probability of success) while FTAs use component failure rate (probability of failure), see Figure 1 and Figure 2. Both methods are probabilistic in nature, but FTA is better suited for modeling complex systems and has enhanced capabilities to include other factors such as common cause failures.

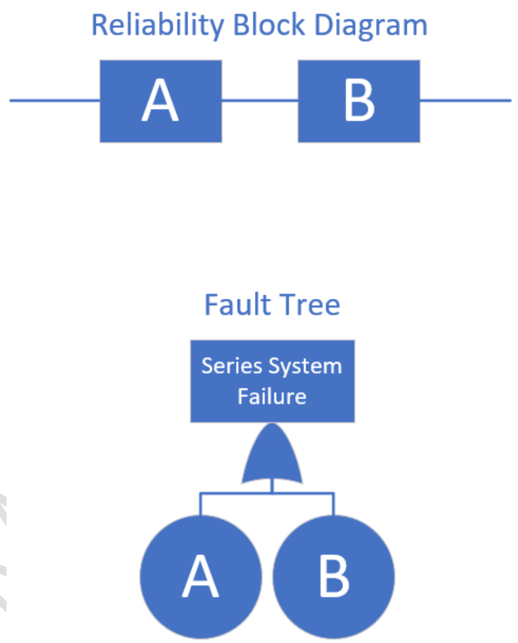


Figure 1. Series Reliability Diagrams

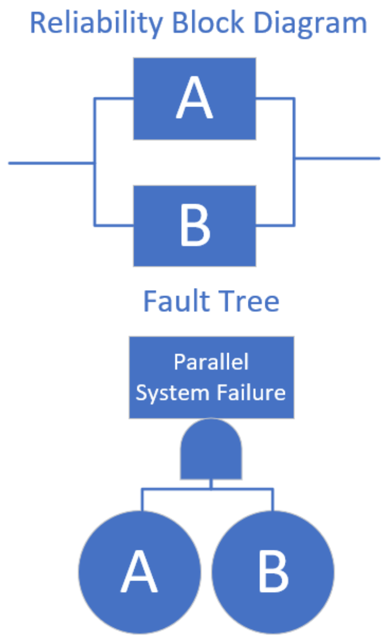


Figure 2. Parallel Reliability Diagrams

Systems generally consist of more than one component or subsystem. When a system is designed such that any failure in the system constitutes a system failure, the configuration is considered series reliability. System reliability, for a series system, is computed as the product of the component reliabilities as seen in Equation 3.

$$R_s(t) = R_1(t) * R_2(t) * \ldots * R_N(t) \qquad \text{Equation 3}$$

Since the transfer function for a series reliability system is known, and the relationship between the failure function and reliability function are known, the system series unreliability can be expressed as in Equation 4. System reliability is generally modeled in RBD's, whereas system unreliability is generally computed using FTA.

$$F_s(t) = 1 - (1 - F_1(t)) * (1 - F_2(t)) * \ldots * (1 - F_N(t)) \qquad \text{Equation 4}$$

Systems that are designed such that all the subsystems or components in a circuit branch need to fail to constitute a system failure are known as parallel reliability. Similar to the series systems, parallel systems can have their transfer function expressed in terms of reliability or unreliability as shown in Equation 5 for system parallel reliability and Equation 6 for system parallel unreliability respectively.

$$R_s(t) = 1 - (1 - R_1(t)) * (1 - R_2(t)) * \ldots * (1 - R_N(t)) \qquad \text{Equation 5}$$

$$F_s(t) = F_1(t) * F_2(t) * \ldots * F_N(t) \qquad \text{Equation 6}$$

As an example, consider a reliability analysis of a system consisting of three components. These components are structured in reliability series (in terms of a fault tree, all three inputs would feed an OR gate). The reliability of the components is given as: $R_1(t) = 0.9$, $R_2(t) = 0.95$, $R_3(t) = 0.96$. Therefore, the system reliability example is shown in Equation 7.

$$R_S(t) = 0.82 = 0.9 * 0.95 * 0.96 \quad \text{Equation 7}$$

Note that a series configuration (i.e. an OR gate configuration in a fault tree) will always result in a reliability that is lower than the worst component in the system.

Consider a second example of a reliability analysis of a system consisting of three components. These components are structured in reliability parallel (in terms of a fault tree, all three inputs would feed an AND gate). The reliability of the components is given as: $R_1(t) = 0.9$, $R_2(t) = 0.85$, $R_3(t) = 0.86$. Therefore, the system reliability example is shown in Equation 8.

$$R_P(t) = 0.998 = 1 – (1 – 0.9) * (1 – 0.85) * (1 – 0.86) \quad \text{Equation 8}$$

Note that a strictly parallel configuration (i.e., an AND gate configuration in a fault tree) will always result in a reliability that is higher than the best component in the system.

Series-parallel systems can also be analyzed following the same logic. Generally, the parallel branches are computed first to create a series equivalent value. The series equivalent value is then inserted into the remaining strictly series configuration to compute an overall system reliability. The same analysis can be done with failure probabilities using a FTA.

Parallel systems generally represent redundancy. Redundancy is an important concept in the practice of reliability engineering. It is important to understand how much improvement in reliability is useful, and where redundancy meets the law of diminishing returns. As a final example for this section consider the comparison of two subsystem implementations on a BOP system (e.g., pods, annulars, valves or other examples). The first implementation has two subsystems in reliability parallel in Equation 9. The second implementation has three systems in reliability parallel in Equation 10. All the subsystems are identical, and each is 99.2% reliable as a standalone subsystem (this is illustrative example only).

$$0.999936 = 1 – (1 – 0.992) * (1 – 0.992) \quad \text{Equation 9}$$

$$0.999999488 = 1 – (1 – 0.992) * (1 – 0.992) * (1 – 0.992) \quad \text{Equation 10}$$

Assuming a failure were to happen during the useful life of the subsystem (i.e. the system is properly maintained and not worn out), the exponential distribution in Equation 11 can be used to convert the reliability function to MTBF.

$$R(t) = EXP(-t / MTBF) \quad \text{Equation 11}$$

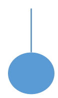
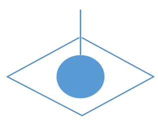
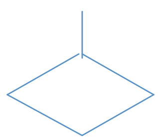
Since failure rate is 1 / MTBF, a failure rate can be computed. The result of the comparison is the dual redundant system had an MTBF of 2,624,916 hrs which translates to a failure rate of 3.8E-7. Whereas the triple redundant system had an MTBF of 328,124,916 hrs which translates to a failure rate of 3E-9. While the triple redundant system results in a much better numerical result, the duration between function tests of a BOP system is only 168 hrs (i.e., 7 days) therefore in practice, a triple redundant system may not provide a measurable improvement over the dual redundant system.

4.3.2 Fault Tree Analysis

Each pivotal event in the top-level fault tree has its probabilities informed by a lower-level fault tree. Fault trees are generally constructed starting with the TE using Boolean logic methods. The Boolean approach allows logical combination of subsystem/subcomponent failures. Once the fault tree is constructed it can then be used to combine the probabilities of failure of the lower levels to the probability of failure of the TE.

Construction of a fault tree follows a standard set of symbols (O’connor, 2002). The symbology is found in Table 1. The analysis can be done many ways. For example, a small fault tree could be drawn in a simple drawing tool and the probabilities be manually computed. Real world problems are generally too complex to manage manually. Software tools are available to facilitate this type of analysis. The various tool suites on the market offer methods of drawing and managing the hierarchy of the tree as well as mathematical roll up of the probabilities. Most also offer Monte Carlo capabilities.

Table 1. Fault Tree Symbols

<table>
<tr><th>Symbol</th><th>Description</th><th>Boolean Relationship</th><th>Probability Calculation</th></tr>
<tr><td></td><td>A basic event that will not be developed further. This event is independent of other events</td><td>N/A</td><td>Data informed by data source such as field data, IADC, SINTEFF, etc.</td></tr>
<tr><td></td><td>A basic event that is developed in another fault tree. This is independent of other events</td><td>N/A</td><td>Data informed by lower-level fault tree</td></tr>
<tr><td></td><td>A dormant event is an event that is in an unknown state (failed or not) until it is tested</td><td>N/A</td><td></td></tr>
<tr><td></td><td>AND gate. A fault at the output indicates that both inputs are in a fault state</td><td><table><tr><td>P1</td><td>P2</td><td>Q</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td><td>Q = P1 * P2</td></tr>
<tr><td></td><td>OR gate. A fault at the output indicates that one or both inputs is in a fault state</td><td><table><tr><td>P1</td><td>P2</td><td>Q</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td><td>Q = 1 – (1-P1) * (1-P2)</td></tr>
<tr><td></td><td>XOR gate. A fault at the output indicates that one but not both inputs are in a fault state</td><td><table><tr><td>P1</td><td>P2</td><td>Q</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>0</td></tr></table></td><td>Q=1 - (1-P1) * (1-P2)-P1 * P2</td></tr>
<tr><td></td><td>Combination event. Shows the combinatorial output of lower-level gates</td><td>N/A</td><td>Data informed by gates connected to the event</td></tr>
</table>

Construction of a fault tree can be shown by example. The simple circuit in Figure 3 shows four relays that connect a transformer to a motor. In this example if relay K1 or relay K3 fail, the top branch of the circuit fails. If relay K2 or K4 fails, the second branch of the circuit fails. If both of those branches fail, or the motor fails, or the transformer fails then the circuit will not function.

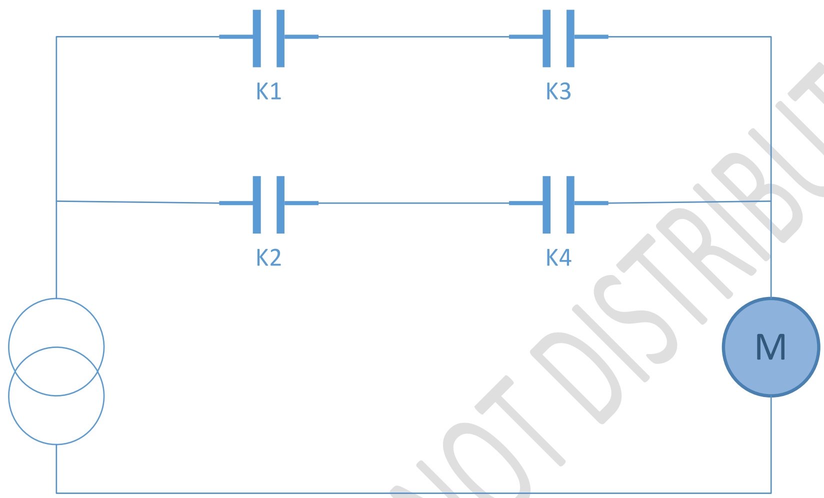


Figure 3. Simple Circuit

Analysis using a fault tree starts at the TE. See Figure 4. In this case the starting point is loss of circuit function. The analyst shows that if the motor fails or the transformer fails a loss of function will occur. The analyst also shows that if the switching network fails, a loss of function will also occur. These three lower-level failures are then combined with an OR gate (i.e., switching OR transformer OR motor results in failure).

The switching network has two series reliability paths that are placed in reliability parallel. The AND gate fed by the two OR gates on the left of the diagram handle the switching network.

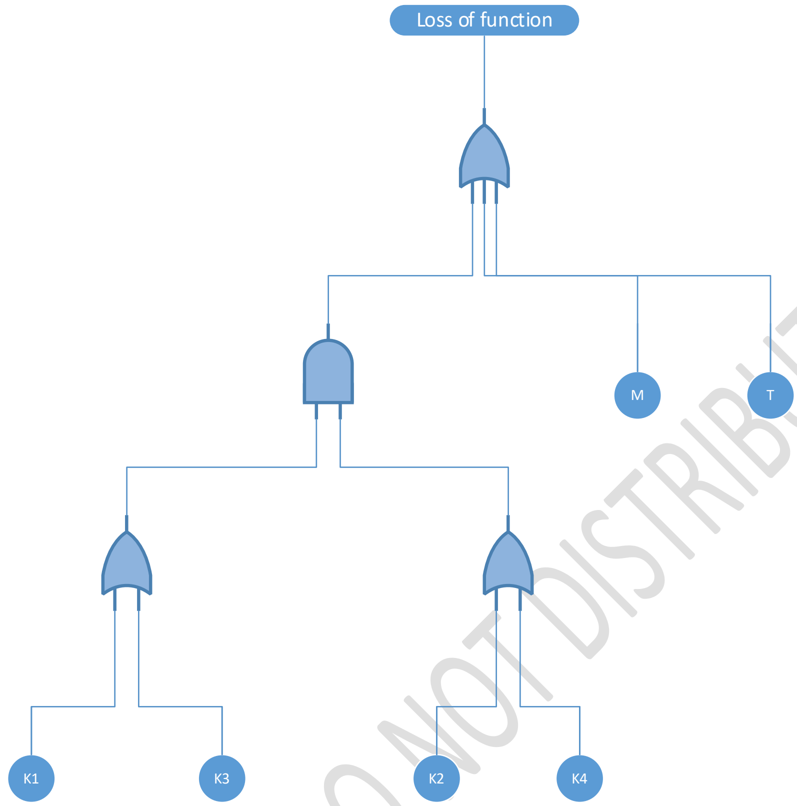


Figure 4. Fault Tree for the Simple Circuit

Figure 5 shows an illustrative example of a fault tree as it may apply to a BOP. To analyze this type of tree, a software package would typically be employed. The software would compute the probability of a failure at the TE, “BOP Fails to Seal and Secure the well”, as the product of the failure probabilities of the next two events, “Failure of Deadman Autoshear” and “Failure of Primary Control.” The “Failure of Primary Control” probability would be calculated according to Equation 4 (see 4.3.1). This process is done for all branches of the tree.

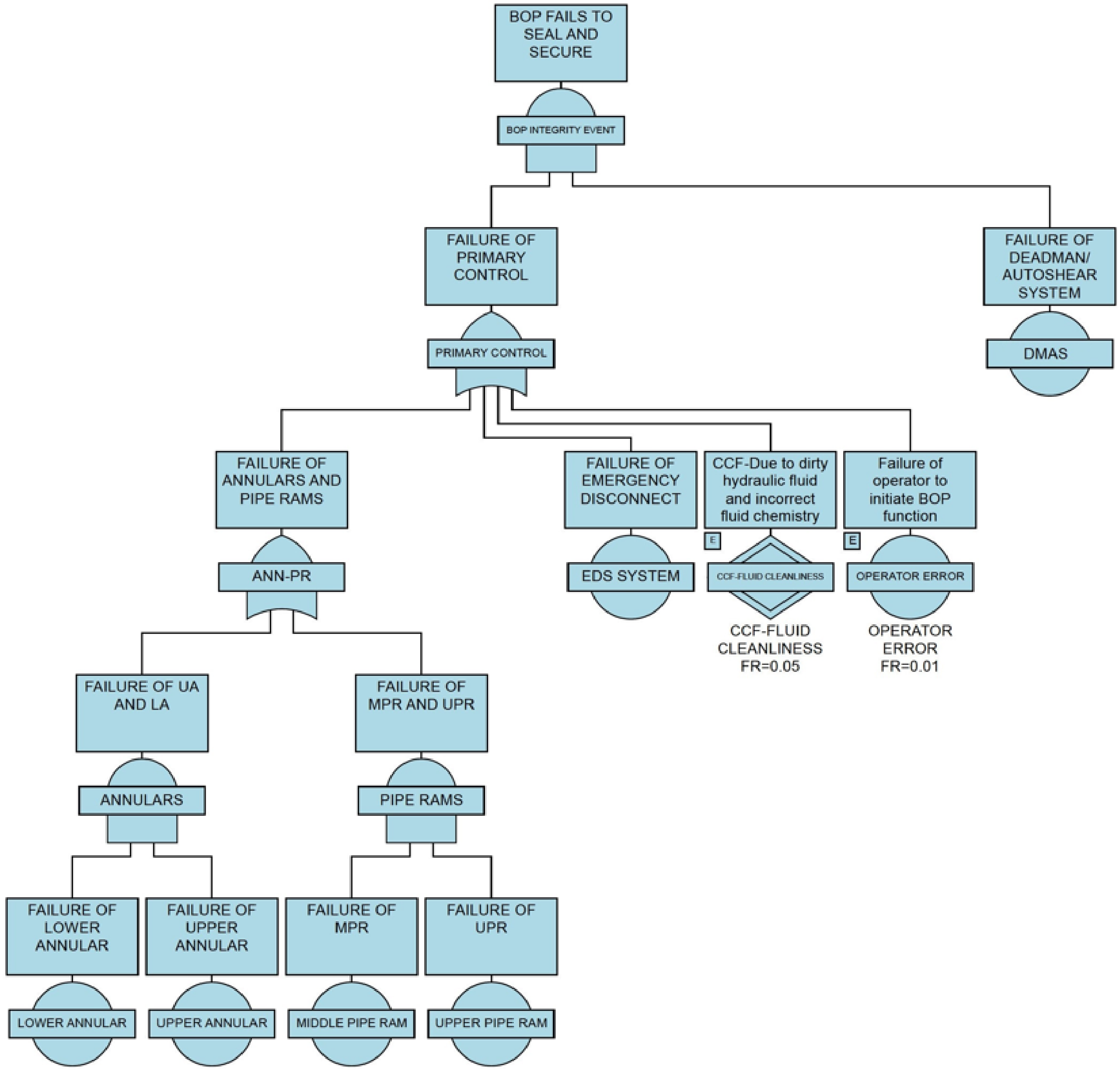


Figure 5. Small BOP Example Fault Tree

4.3.3 Common Cause and Single Point Failures

Common cause failures (CCF) can undermine the benefits of redundancy (IEC61508-7 c.6.3). The appearance of a CCF can drive failures in multiple parts of a system at the same time. Many of the critical functions of a BOP system (e.g. control pods, annluars) mitigate single point failures by using redundant solutions. Some failures, however, may occur due to environment, a common design flaw, common manufacturing, maintenance practices, etc.

Consider a hypothetical design where two subsea electronics modules were packaged in a single one-atmosphere housing. The two modules could provide redundancy and failover increasing the overall reliability of the system. But, if the one atmosphere housing was flooded, both subsea electronic modules would fail. Another example may be a batch manufacturing issue of an elastomeric seal that is deployed on a specific model annular. If the same batch seals were used on two annulars in a single system, both annular seals may degrade at a common rate due to the manufacturing defect, causing both annular component failures upon the next deployment.

Methods to minimize CCF's do exist. Some of the methods used include quality control, design reviews, independent test teams, lessons learned from fielded systems, etc.

CCF's may also include common mode failures and cascade failures. For the purposes of this document all three types of failures are lumped into the CCF category. CCF's generally fall into two groups. One group is dependent failures due to deterministic root causes and the other group is residual potential multiple failure events (IEC61508-6 d.1.2). Deterministic failures can be analyzed and corrected using standard methods. However, residual multiple failure events need to be represented in an FTA to give a true picture of the probability of failure.

Generally, fault trees represent independent failures. A method of introducing common failures in the analysis is necessary. The first step is to determine the magnitude of the CCF probability. Consider the diagram in Figure 6. Several methods exist to quantify CCF. These methods include β factor, multiple Greek letters, α factor, etc.

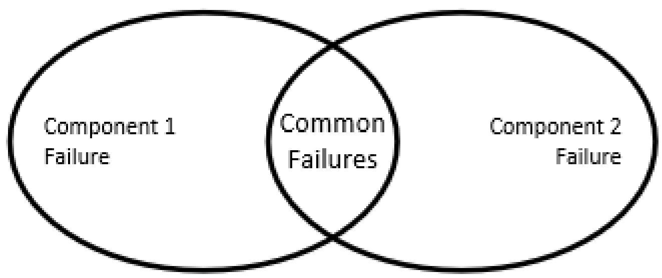


Figure 6. Relationship of Independent and Dependent Failures

The β factor method is well established. This method uses a multiplier to the failure rate to provide an estimate of the likely fraction of component failures that may occur due to common causes. Equation 12 shows how to calculate the failure rate (λ) for common cause based on the known component failure rate.

$$\lambda_{CCF} = \lambda_{Component} * \beta \qquad \text{Equation 12}$$

There are several methods to select β. IEC61508-6 Annex D suggests use of a detailed questionnaire to determine how much commonality exists in the components/assemblies. Other methods include estimating β using values between 1% and 10%. To maintain conservatism in BOP modelling, the models developed for this report estimated a β of 10%.

Once the value of β is established λ_{CCF} can be added to the FTA model. To model CCF's at the higher system level, a statistical equivalent is used. The left model of Figure 7 shows modelling of a CCF at the higher system level. The right model of Figure 7 shows CCF being modelled at the lower component level. These two models produce identical results in the probability calculation. The reason these are equivalent is that CCF is not independent, refer to Figure 6. Rather, Event 1 is the probability of the component failing minus the CCF value. This dependence between CCF and the events shown in the diagram allow modelling of CCF at various levels in the FTA. Modelling CCF at the higher level in the model creates some advantages in better coverage of system assembly, test, etc. Modelling at the higher level also creates advantages in model validation. This allows the model reviewer to be sure CCF is included at all the proper levels in the system.

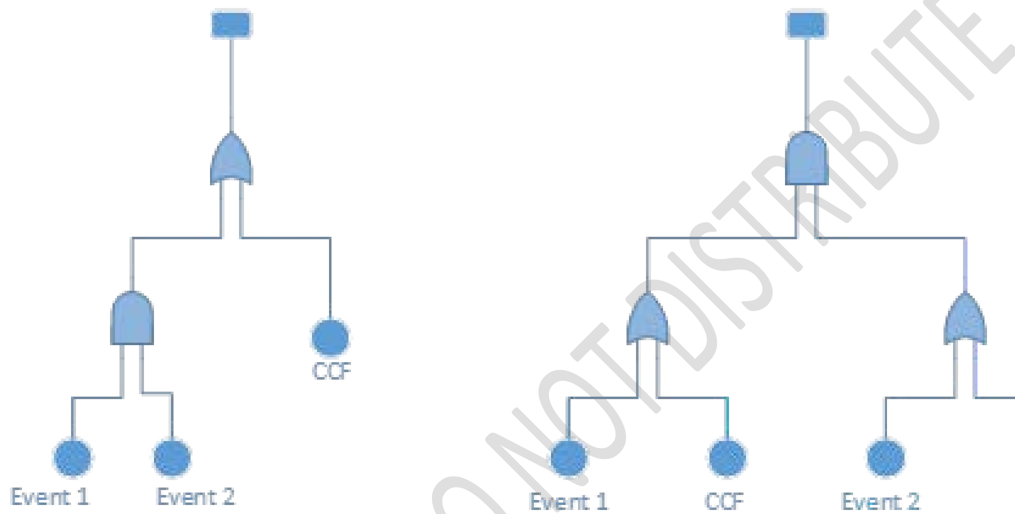


Figure 7. Common Cause Equivalent Models

4.3.4 Sensitivity Analysis

Sensitivity analysis is a study of how discrete changes in a model input affect the model output. Typically, by changing a value of one input parameter, and running the model, the change in the output value is observed. By repeating such a process, the model's input parameters with the largest impact on the model's results can be identified.

In our model, we mainly rely on sensitivity analysis to determine how different values of an independent variable (e.g. failure rate) change a particular dependent variable (e.g. TE safety integrity) under a given set of assumptions.

Failure rate sensitivity determines the how a change in a specific component failure rate would affect the overall BOP system's ability to seal and secure the well bore. This is used to perform what-if analysis and anticipate overall BOP system performance upon a given component performance degradation

Test interval sensitivity analysis determines the effect of change in proof test intervals of BOP components on the overall BOP system's ability to seal and secure the well bore.

Redundancy sensitivity analysis helps to understand the BOP systems performance changes for an implied addition of redundant BOP functions (example blind shear ram (BSR) or deadman / autoshear function (DMAS))

Operators' sensitivity analysis is performed by varying operator's ability to initiate the BOP functions. The Operator's ability is the percentage that the Operator will successfully recognize a well control event or an equipment failure and initiate the BOP function.

The full-scope uncertainty analysis can be also conducted assuming that the failure rate uncertainty distributions are properly identified and implemented in the model.

4.4 Assumptions

The following are assumptions for creating a fault tree for a blowout preventer.

- Typical well depth for offshore wells – 25,000 feet measured depth
- Typical well depth for onshore wells – 20,000 feet measured depth and 10,000 feet true vertical depth
- Typical BOP stack configuration:

    1. moored subsea BOP – 15k, 1 shear ram (BSR), 2 pipe rams, 2 annulars;
    2. dynamically positioned (DP) mobile offshore drilling unit (MODU) subsea BOP – 15k; 2 shear rams (BSR and casing shear ram (CSR)), 2 pipe rams, 2 annulars;
    3. surface offshore – 15k, 1 BSR, 2 pipe rams, 1 annular;
    4. land BOP with BSR – 15k, 1 BSR, 2 pipe rams, 1 annular;
    5. land BOP with BR – 10k, 1 BR, 2 pipe rams, 1 annular.

- The rig utility systems (electrical, pneumatic, water) are not modeled in this FTA as they are assumed to be 100% available. But BOP controls including pneumatic and hydraulic valves are modelled to accurately depict control system options
- Surface electrical control systems failures are grouped together as a single failure event for which RAPID-S53 failure rates are available
- Component failure rates as defined in RAPID-S53 are used.
- Components are assumed to be within their useful life (systematic failures are eliminated prior to the introduction of hydrocarbons and are replaced prior to wear-out failure).
- Test frequency is assumed to be as defined in API S53.
- For surface control panels, programmable logic controllers and electrical systems, it is assumed that failures are only identified during weekly function tests
- Failure rates for subassemblies were used when RAPID-S53 lacked component level data.
- Confidence interval of +/- 10% margin of error is implied in the failure rates gathered from RAPID-S53
- A response time of 12 hours is assumed, considering the time taken to detect the failure and take subsequent well control actions to further risk assess and make decision(s) to returning the system to operation. Where integrity monitoring is available, it is assumed that 100% of dangerous failures are detected. To accurately model the effectiveness of the monitoring capabilities of each of the component's dangerous failure modes, a separate study needs to be conducted.
- CCF for redundant BOP functions is assumed to be 10% of the mean unavailability of the individual BOP function failure to operate.
- Lower pipe rams are not modeled because they are not required in S53.
- BOP operating lifetime (years used for drilling operation) is assumed to be 15 years.
    - The hydraulic fluid source from the surface accumulators is assumed to be available for BOP controls, hence hydraulic pumping units (HPU) that are only used to charge the surface accumulators are not modeled in this FT.
    - The time percentage of shearable and non-shearable tubulars across the BSR are assumed as follows:

1. Presence of a non-shearable tubular (e.g. casing, drill pipe tool joint) across a BSR – is 11.5% of the total lifetime of the operation.

2. Presence of a shearable tubular (e.g. drill pipe excluding tool joint, tubing) across BSR – is 88.5% of the total lifetime of the operation.

3. Presence of wireline or tubular that cannot seal by annular(s) and pipe ram(s) – is 5% of the total lifetime of the operation.

4. Presence of drill pipe across that can be sealed by annular(s) and pipe ram(s) – is 85% of the total lifetime of the operation.

5. Open hole duration across the stack is 10% of the total lifetime of the operation. For this purpose of analysis, we assume annulars cannot seal an open hole completely due to unknown mechanical wear that could compromise seal integrity.

6. Time duration where pipe ram or BSR/BR cannot seal due to an open hole or wireline or tubular is 15% of the total lifetime of the operation.

The operator's ability to recognize and respond to an event is assumed to be 100%. This is applicable for operator initiated BOP functions including swapping to the backup pod.

Software reliability is included in surface control units with a 10% CCF on redundant BOP function failures.

The sequence of BOP function operation for DP MODU is as follows:

a) annular to seal around tubulars (shut-in Stage I);
b) middle pipe ram or hangoff ram to hangoff and/or seal around the drill pipe (shut-in Stage III);
c) upper pipe ram (shut-in Stage IV);
d) shear ram (CSR followed by upper blind shear ram (UBSR)) (shut-in Stage V);
e) EDS (CSR followed by UBSR) (shut-in Stage VI);
f) emergency control system activation – DMAS System (CSR followed by UBSR).

The sequence of BOP function operation for moored DU is as follows:

a) annular to seal around tubulars (shut-in Stage I);
b) middle pipe ram or hangoff ram to hangoff and/or seal around the drill pipe (shut-in Stage III);
c) upper pipe ram (shut-in Stage IV);
d) shear ram (blind ram or BSR) (shut-in Stage V);
e) emergency control system activation – DM/AS system (BR/BSR).

The sequence of BOP function operation for Surface BOP (for onshore and offshore) is as follows

a) annular to seal around tubulars (shut-in Stage I);
b) upper pipe ram (shut-in Stage II);
c) lower pipe ram (LPR) to seal around the drill pipe (shut-in Stage III);
d) shear ram (blind ram or BSR) (shut-in Stage IV).

Dormant failure models are used for components without condition monitoring (e.g. hydraulic, mechanical). Fixed rate failure models are used for components with condition monitoring (e.g. electrical/electronic/communication).

Operational failures from RAPID-S53 are considered for failure-rate calculation.

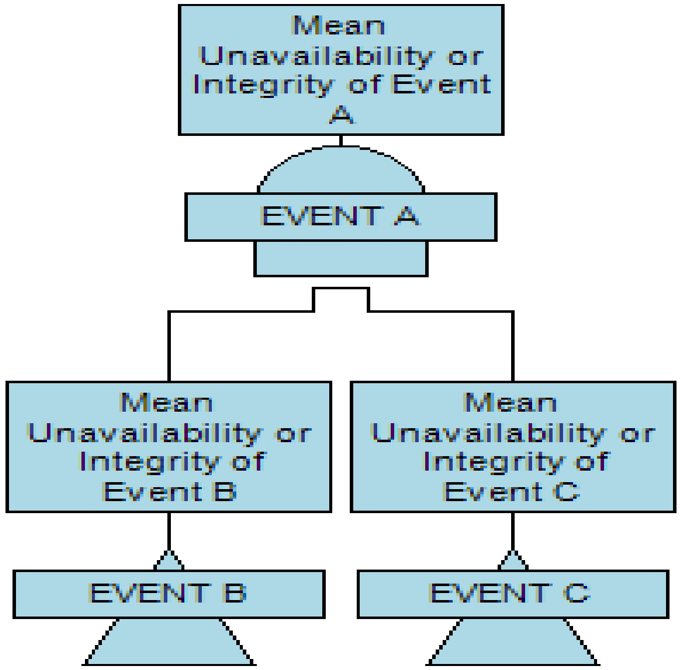
4.5 Methodology

This Fault Tree is developed using the following methodology:

a) A modelling naming convention should be established at the beginning of a modelling project. For an example naming convention see PRA Procedures Guide for Offshore Applications (DRAFT) - JSC-BSEE-NA-24402-02 Appendix A
b) The failures that are continuously monitored via control panels are considered dangerous detected revealed" failure modes. For revealed component failure modes, "rate- mean time to repair" failure model is used to quantify the failure contribution to the TE.
c) The dangerous undetected failures that are only revealed during testing or inspection are considered "dormant" failure modes. For dormant component failures, "dormant" failure model is used to quantify the failure contribution to the TE.
d) The mean unavailability calculated from average probability of failure on demand of the gate represents the individual component's or system's contribution to the TE.
e) The importance of BOP components is sorted based on the Boolean reduction representing the minimal cut set.
f) CCF's are modelled at the higher system or subsystem level to consider common design, manufacturing, and operating condition failures. These are combined as a separate gate for redundant BOP functional failure to operate (i.e. both annulars, both pipe rams).
g) As needed, alternate percentage contribution of different shut-in stages to TE is calculated using Equations 13 & 14:

The percentage contribution % of event C to event A = $100 \times \frac{(C-A)}{(C-A)+(B-A)}$ Equation 13

The percentage contribution % of event B to event A = $100 \times \frac{(B-A)}{(C-A)+(B-A)}$ Equation 14



A - The resultant top level mean unavailability value

B - Event B mean unavailability value

C - Event C mean unavailability value

Figure 8. Percentage Contribution of Different Shut-in Stages

4.6 Operational Risk Analysis Use of Reliability Models

When a defect affects the availability of a critical BOP component, the decision to stop operations, bring the well to a safe state, and retrieve the BOP is often clear. However, when a non-critical component is defective or multiple defects are present, the fault tree can be utilized to inform the decision to continue operations or not. The fault tree can enable timely and quick failure analysis using pre-defined fault propagation logic, modeled to the BOP system's lowest maintainable components. This method allows for -risk analysis with a singular defect as well as providing cumulative risk analysis should there be more than one defect on the BOP system, subsystem, or components. The below methodology provides an example for how this can be accomplished.

The effect of a defect(s) is modeled to calculate the probability of failure on demand (PFD), of the entire system and to determine the relative capability of the system to inhibit the TE. The TE generally modelled for BOP systems is "failure to seal and secure the well". First, a model is run for a completely healthy system and a quantity for the overall PFD is established. Then, several model's configurations are run to demonstrate the percentage of degradation of the system's PFD, due to the unavailability of industry or regulatory required components. This percentage of degradation then becomes the established baseline for a system's unacceptable

PFD limit. Hence, when a component is not required by regulation or industry standard, or there are multiple defects to consider, a model can be run again, and that value is compared to the unacceptable PFD value for critical components/system as discussed above. This information can be used as a quantitative risk evaluation input to the decision maker to continue operations or not.

Minimal cut sets provide additional insights for the equipment owner to understand the critical components or single point failures to BOP system. Due to dependency of multiple common components to perform one or more BOP functions, this minimal cut set analysis also provides insights on those components required to operate multiple BOP functions during primary well control and emergency operations. Using fault tree, the equipment owner could also simulate the failure of these critical components to understand the PFD change before and after the failure. For example, failure of a pod, BSR or manifold regulator, typically considered a part of minimal cut sets, would help calculate the % PFD degradation before and after the failure to inform risk. This can provide the operations team insight for making an informed decision knowing the criticality of these components within minimal cut sets for its related BOP functions. An example of using minimal cut sets can be found in Annex A.

4.7 Data Sources

The data for this BOP system safety integrity analysis, was sourced from Gulf of Mexico Rig BOP failures reported to RAPID-S53 (Reliability and Performance Information Database for the Well Control Equipment (WCE) covered under API S53) as of 10 May 2019. RAPID-S53 is the industry recognized reliability database. The inputs listed below were used as inputs to the model.

- system schematics: Piping & Instrumentation Diagrams, electrical single line drawings;
- FMECA of BOP WCE;
- calculated component failure rate (expressed as failure count per annum per rig);
- component failure events model categorized by event-type:
    - dormant: fixed;
    - basic: rate;
    - *time at risk* for presence of non-shearable tubular in well-bore.
- API S53 function test and pressure test intervals;
- calculated fraction of shearable/non-shearable length of a 30-foot drill-string;
- average response time (failure detection to resumption of operation) of 12 hours;
- CCF factor of 10% applied to redundant BOP functions.

5 Model Results and Examples

The following are examples from the generic fault tree models for DP and moored MODU systems, plus onshore and offshore surface systems. They demonstrate the type of analysis that the 16G model can provide. Specific rig scenarios using actual rig equipment configurations may generate different results.

The TE for the model examples below is: failure to shear and seal the wellbore.

5.1 Pressure and Function Test Frequency Analysis

The following figures depict the impact of test frequency changes on the TE integrity. This is calculated by varying individual component's testing frequency from the standard testing frequency and assessing the % change on the TE integrity. The component's testing frequency is denoted as "0%" in Figures 9, 10, and 11, and defined in API S53 Table C.3 and/or regulatory requirements.

For example, in Figure 9: the change in function testing of DMAS System from 6 months interval to 3 months interval leads to 34.4% improvement in our ability to detect DMAS safety integrity performance. While increasing the frequency to 1 month only increases the benefit by an additional 4.3% from the 3-month frequency.

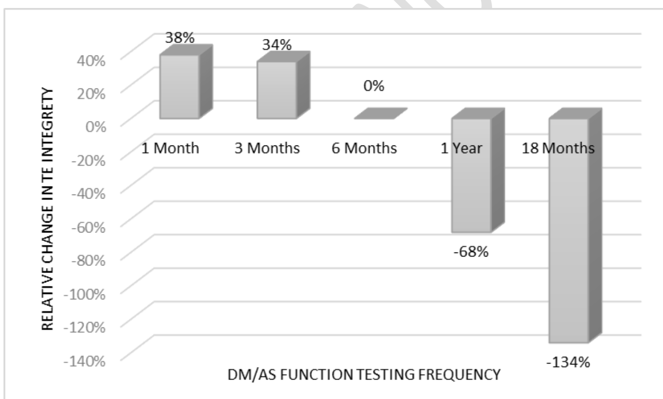


Figure 9. DP MODU BOP - Impact of Test Frequency on TE Integrity (Deadman/Autoshear)

Function testing of annulars, pipe rams and shear ram should proof-test all components of the BOP system and sub-systems except the BOP sealing capability. While pressure testing proves the functional capabilities of BOP system and sub-systems including the BOP mechanical, shear hardware and sealing element. Hence pressure testing brings only incremental value through proof-testing BOP shear and seal capabilities, while the majority of the BOP system and sub-systems are functionally validated through functional testing. These results are shown in Figures 10 and 11.

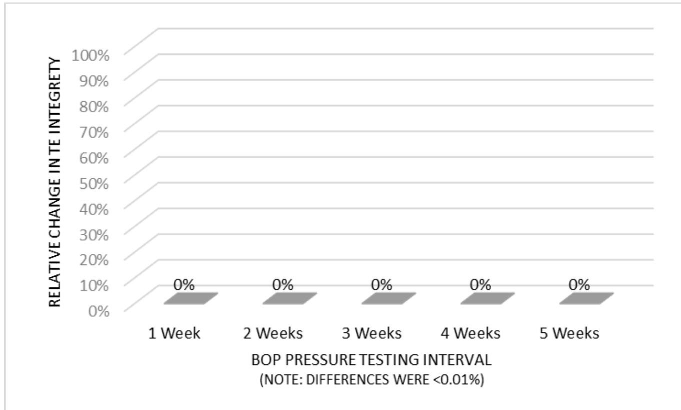


Figure 10. DP MODU BOP - Impact of Pressure Test Frequency on TE Integrity

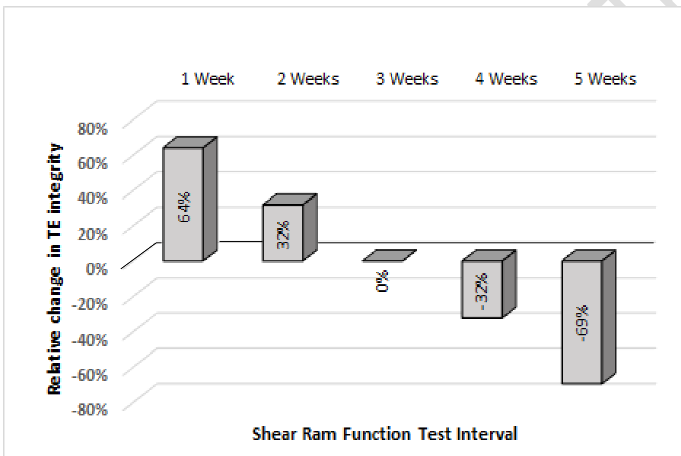


Figure 11. DP MODU BOP - Impact of Function Test Frequency on TE Integrity (Shear Rams)

5.2 Operator's Ability Sensitivity Analysis

The primary control system functionality requires an operator to successfully recognize a well control event or an equipment failure and initiate the BOP function, as required. The primary control system's integrity deteriorates with the individual's inability to recognize an event and respond accordingly. For example, on a DP MODU with a subsea BOP system: a decrease in an individual's ability to respond correctly by 0.5% may reduce the integrity of the primary control system by 118% or 1.18 times. Figure 12 below shows the trends associated for the three evaluated systems. The trends show that the complex systems require greater attention to human factors.

The operator's ability to identify, assess and execute timely actions involves numerous factors as outlined in ISO11064 and ABS Human Factor and Ergonomics standards and guidelines. The contributing factors include human-machine interfaces, training, procedures, risk perception, stress, fatigue, and situational awareness. In Figure 12, the percentage of "successful actions upon demand" is quantified and tested for various BOP control functions that warrant human or operator's interaction to recognize an event and respond.

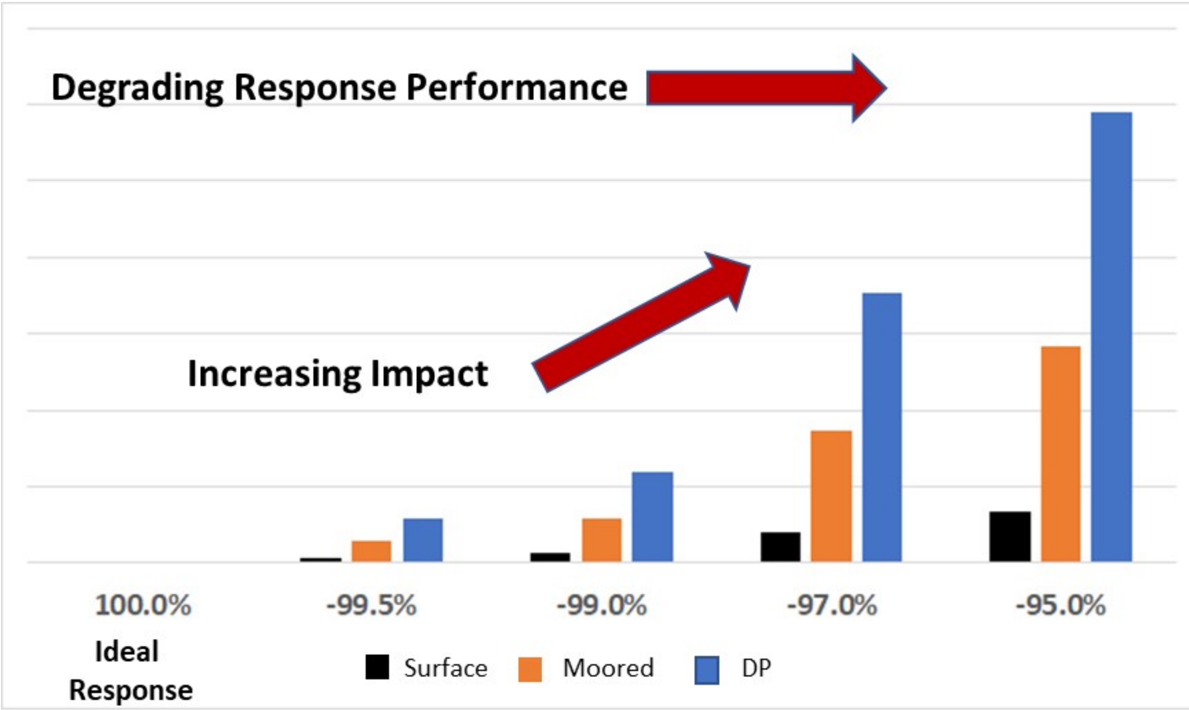


Figure 12. "Operator's Ability" Sensitivity Analysis

5.3 Failure Rate Sensitivity Analysis

A failure rate sensitivity analysis evaluates the TE failure rate after individually varying component failure rate percentage. Varying the individual component failure rate will have differing impact on the TE's integrity. The results of this analysis reveal the order of importance and effectiveness of component design upgrades and may indicate areas where maintenance quality is critical. Figure 13 is an example showing the critical items identified for a DP MODU's subsea stack.

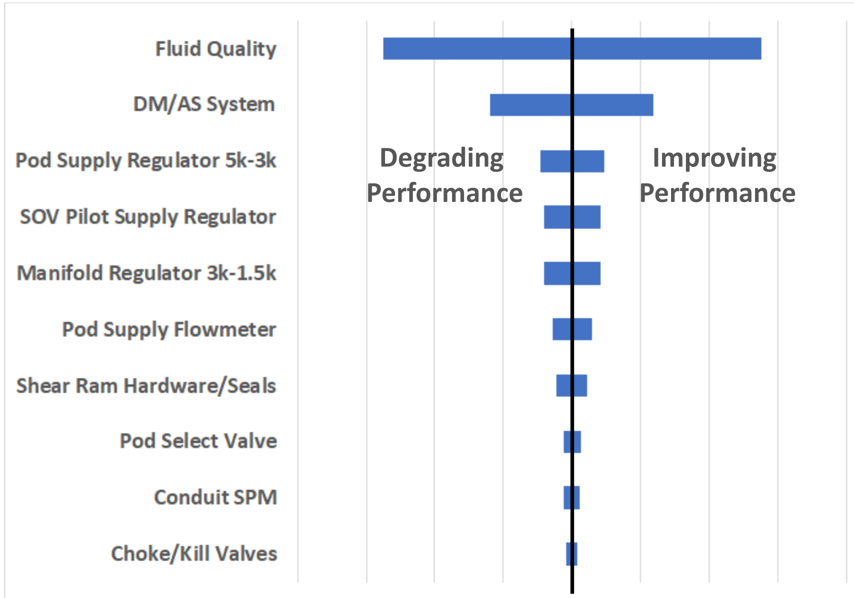


Figure 13. DP MODU BOP - TE Failure Rate Sensitivity Analysis

Figure 14 is an example showing the critical items identified for a DP Deadman Autoshear system (DMAS).

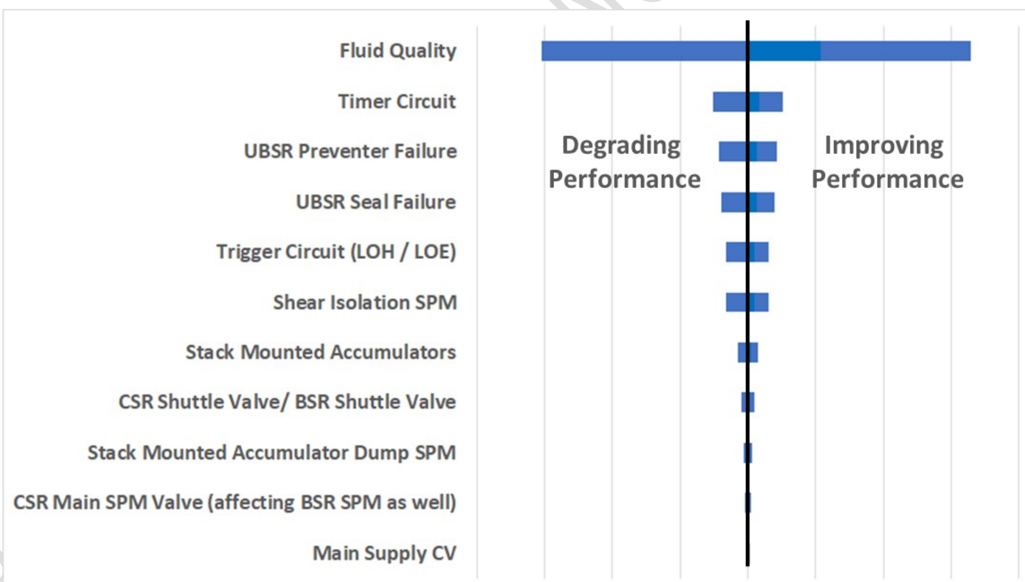


Figure 14. DP Deadman Autoshear (DMAS) - TE Failure Rate Sensitivity Analysis

5.4 Fluid Quality Sensitivity Analysis

Fluid quality is a significant common cause failure contributor of the primary BOP control system and the emergency control system due to the fact it is present in all systems. Any small improvement in fluid quality will considerably improve the TE integrity and change the results of the analyses conducted below. Table 2 and 3 show the Failure Rate Sensitivity analysis evaluating the control fluid quality. They show BOP control system's dependency to fluid quality and the need for preventive mitigations and filtering for drilling / completion fluids, metal, elastomer, or biologic debris.

Table 2. DP MODU BOP - Fluid Quality Sensitivity Analysis

Fluid Quality Sensitivity Analysis					
Fluid Quality	**100%**	**99%**	**98%**	**95%**	**90%**
TE	**Baseline 0%**	-208%	-411%	-988%	-1855%
DM/AS	**Baseline 0%**	-17%	-33%	-80%	-152%

Notes: 100% fluid quality was used as the baseline data during the Fault Tree Analysis.
Fluid quality degradation is a percentage of failed tests to meet fluid concentrate manufacturer's criteria.
Negative % indicates integrity degradation).

Table 3. Surface Systems - Fluid Quality Sensitivity Analysis

Fluid Quality Sensitivity Analysis					
Fluid Quality	**100%**	**99%**	**98%**	**95%**	**90%**
TE	**Baseline 0%**	-95%	-188%	-460%	-892%

Notes: 100% fluid quality was used as the baseline data during the Fault Tree Analysis.
Fluid quality degradation is a percentage of failed tests to meet fluid concentrate manufacturer's criteria
Note: negative % indicates integrity degradation)

5.5 Common Cause Sensitivity Analysis

A common cause sensitivity analysis models multiple failure of components installed that are identical. CCF's can be introduced due to:

a) common design deficiencies;

b) common manufacturing quality issue;
c) common incorrect maintenance activity or procedure.

Valid testing and inspection activities can reduce the CCFs.

The CCF rate for the base fault trees was set at 10% for identical common components. For this sensitivity analysis, the CCF rate was varied to 3%, 5%, 8%, 10%,12%, 15%, and 20% on the following components:

- annulars
- pipe rams

The results in Table 4, indicated very minor change (-5.58% to 3.87%) as measured to the primary control system. The percentage change is expressed to the Primary Control System failure as it did not indicate a measurable change to the TE failure rate.

Table 4. CCF - Sensitivity Analysis

CCF – Annulars + PR	**20% CCF**	**15% CCF**	**12% CCF**	**Baseline 10% CCF**	**8% CCF**	**5% CCF**	**3% CCF**
%TE Change	-5.58%	-2.77%	-1.12%	**Baseline 0%**	1.12%	2.77%	3.87%

Annex A

A.1 Use of minimal cut sets in Reliability Estimation

In analysis of complex system configurations, minimal sets approach is utilized to arrive at bounds and estimates of system reliability. A minimal cut set is any subset of system components, all of which must fail for the system to fail. A minimal path set is any subset of system components, all of which must function for the system to function.

While most reliable minimal path set forms the lower bound of system reliability, least reliable of minimal cut set determines the upper bound. System reliability estimate can be further refined by following either of the minimal set approaches. The accuracy of the estimate increases with the number of minimal sets included in FTA or RBD model (see Figure A.1).

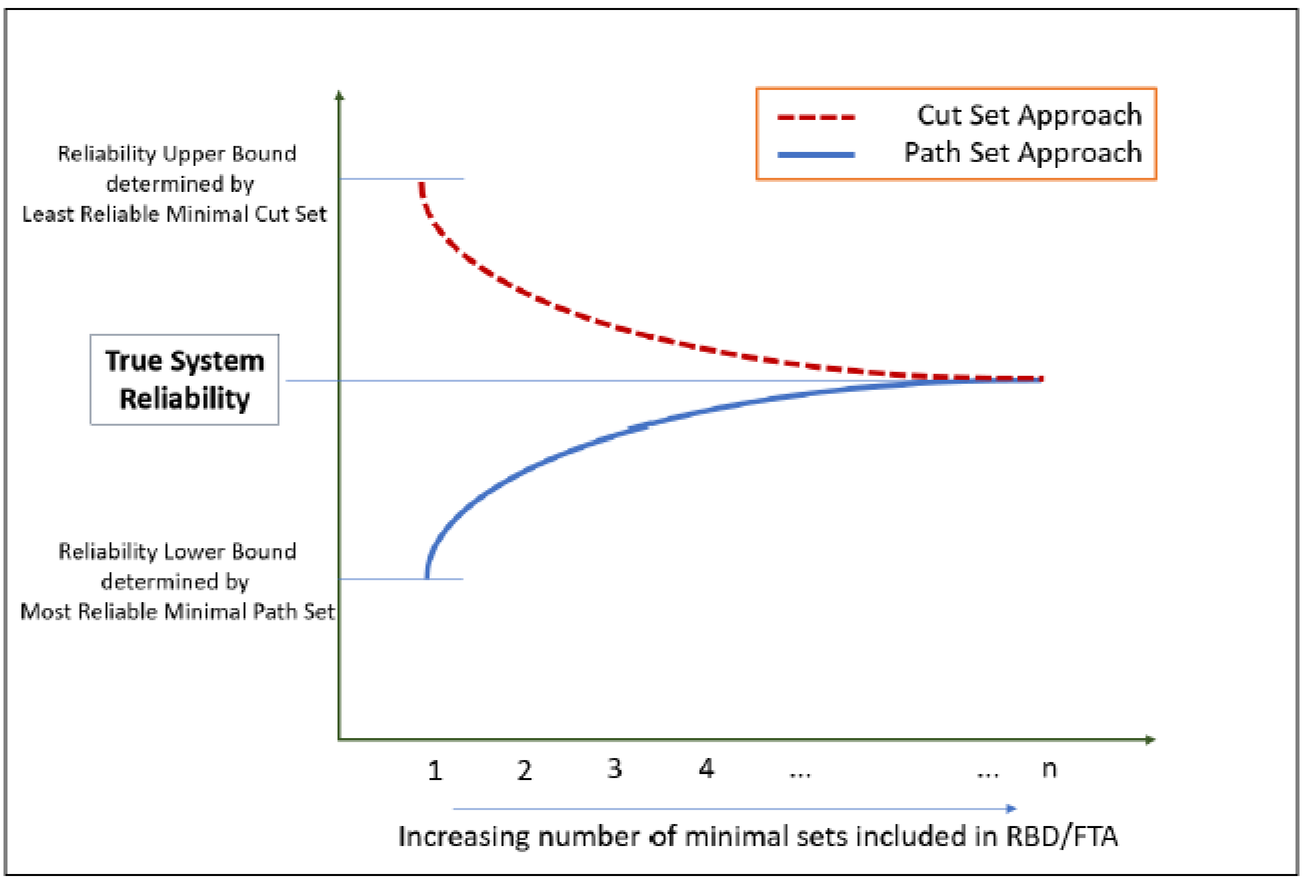


Figure A.1 Effect of minimal number of cut sets

For typical engineered system consisting of non-redundant and redundant components, minimal cut set method is simpler and more efficient of the two approaches. Non-redundant components (single points of failure) and assemblies with low levels of redundancy (100% or less) constitute lower Reliability minimal cut sets, which in turn allow for quick modeling turnaround time using FTA/RBD methods. The inherent need to order the minimal cut sets in increasing order of the Reliability allows engineering teams to focus on components or assemblies that need immediate attention.

The following example of an HPU in Figure 16, demonstrates minimal cut set approach to reliability estimation. Consider an HPU consisting of a fluid reservoir, 2x100% pumps (of different makes), 2x100% motors, 2x100% discharge filters, and a discharge relief valve.

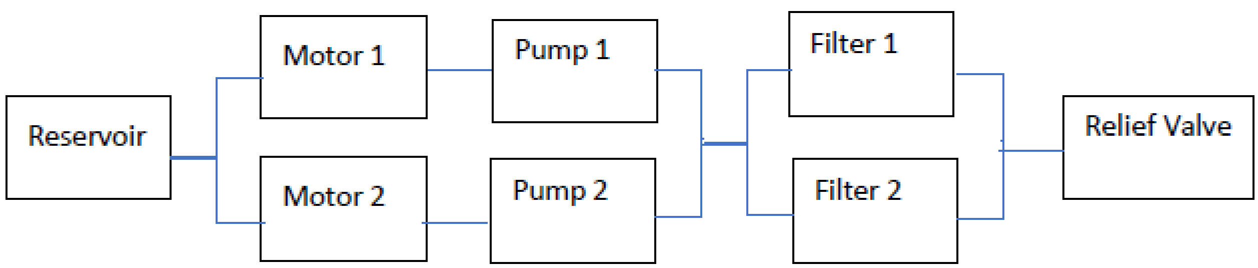


Figure A.2. HPU analysis using cut sets

Minimal cut sets for the system of Figure A.2 are as follows:

1. {Fluid Reservoir};
2. {Relief Valve};
3. {Motor1, Pump2};
4. {Motor2, Pump1);
5. {Filter1, Filter2}.

Minimal cut sets of Figure A.2 when ordered in increasing order of reliability **at end of design life** are as follows:

1. R{Filter1, Filter2} = 0.70
2. R{Relief Valve} = 0.80
3. R{Motor1, Pump2} = 0.90
4. R{Motor2, Pump1} = 0.95
5. R{Fluid Reservoir} = 0.99

The HPU system reliability upper bound is therefore 0.70 driven by the least reliable minimal cut set consisting of 2x100% discharge filters. Reliability estimate of the system can be gradually refined by iteratively factoring in additional ordered minimal cut sets. A reasonable system reliability estimate (0.50) was arrived at by factoring in three least reliable of the five minimal cut-sets.

1. System Reliability [{Filter1, Filter2}] = 0.70
2. System Reliability [{Filter1, Filter2}, {Relief Valve}] = 0.70*0.80 = 0.56
3. System Reliability [{Filter1, Filter2}, {Relief Valve}, {Motor1, Pump2}] = 0.70*0.80*0.90 = **0.50**

4. System Reliability [{Filter1, Filter2}, {Relief Valve}, {Motor1, Pump2}, {Motor2, Pump1}] = 0.70*0.80*0.90*0.95 = 0.48

5. System Reliability [{Filter1, Filter2}, {Relief Valve}, {Motor1, Pump2}, {Motor2, Pump1}, {Fluid Reservoir}] = 0.70*0.80*0.90*0.95*0.99 = 0.47

Annex C

DP MODU Fault Tree

The DP MODU fault tree can be accessed at the following link:

https://mycommittees.api.org/standards/ecs/sc16/Committee%20Documents/Ballot%205791%20for%20TR16G%2C%201st%20Edition/API%2016%20SC%20BOP%20Fault%20Tree%20Analysis%20-%20DP%20MODU.pdf

Annex D

Moored DU Fault Tree

The Moored DU fault tree can be accessed at the following link:

https://mycommittees.api.org/standards/ecs/sc16/Committee%20Documents/Ballot%205791%20for%20TR16G%2C%201st%20Edition/API%2016%20SC%20BOP%20Fault%20Tree%20Analysis%20-%20MOORED%20DU.pdf

Annex E

Surface DU Fault Tree

The Surface DU fault tree can be accessed at the following link:

https://mycommittees.api.org/standards/ecs/sc16/Committee%20Documents/Ballot%205791%20for%20TR16G%2C%201st%20Edition/API%2016%20SC%20BOP%20Fault%20Tree%20Analysis%20-%20Surface%20DU.pdf

Bibliography

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies (including any addenda/errata).

API Specification 16D, Control Systems for Drilling Well Control Equipment and Control Systems for Diverter Equipment, 3rd ed. November 2018.

API Standard 53, Blowout Prevention Equipment Systems for Drilling Wells, 5th ed. December 2018.

BSEE, Probabilistic Risk Assessment (PRA) Procedures Guide for Offshore Applications (DRAFT) - JSC-BSEE-NA-24402-02, Revision 1.

IADC, *RAPID-S53 - Reliability and Performance Information Database for the Well Control Equipment (WCE) covered under API S53.* RAPID-S53 (rapid4s53.com)

IEC 61025, Fault Tree Analysis (FTA). 2nd ed. December 2006.

IEC 61508-6, Guidelines on the application of IEC 61508-2 and IEC 61508-3. 2nd ed. April 2010.

IEC 61508-7, Overview of techniques and measures. 2nd ed. April 2010.

ISO 14224, Petroleum, petrochemical, and natural gas industries —Collection and exchange of reliability and maintenance data for equipment. 3rd ed. October 2016.

OLF GL 070 – Guidelines for the application of IEC 61508 and IEC 61511 in the Petroleum activities on the Norwegian continental shelf. (Recommended SIL Requirements).