A REAL-TIME RISK-INFORMED BOP RETRIEVAL DECISION TOOL

Luiz Fernando Oliveira[1], Joaquim D. Amaral Netto[1], and Gean Rocha[1]

[1] *DNV GL: Rua Sete de Setembro 111,12 andar, Rio de Janeiro, RJ, 20050-006,Brazil*
Email Address: Luiz.oliveira@dnvgl.com

In this paper we introduce the main functions of the Real-Time Risk-Informed BOP Retrieval Decision Tool. The main goal of this new tool is to contribute to better-informed decision-making regarding operational safety and reliability of BOPs, while its ultimate goal is to reduce BOP downtime thus reducing drilling costs while maintaining its safety margin. The BOP▪RDT incorporates both qualitative and quantitative methods to help guide the operator decision-making after detection of a BOP component or subsystem failure during drilling. Using deterministic criteria, the tool has a comprehensive qualitative method which is entirely based on the losses of redundancy resulting from the impact of detected failures on the reliability of each BOP critical safety function. The BOP condition states are reported to the user as a set of traffic light signals and block diagrams indicating the failed components and paths. Entirely new in this Tool is the use of quantitative probabilistic criteria, which makes it a fully quantitative risk-informed decision support system. The computational engine is based on an advanced time-dependent reliability analysis of each BOP safety function before (normal condition) and after one or more detected component or subsystem failures. The quantitative method allows the evaluation of the PFD of each safety function in real-time, providing a detailed graphic visualization of the impact of any detected component or subsystem failure on the values of the PFD for all BOP safety functions. The quantitative risk-informed criteria are based on the comparison of the PFD values of the safety functions with a range of Safety Integrity Levels (SIL) values as defined by IEC 61508. Results are presented for a real BOP operating in the North Sea.

I. INTRODUCTION

The Blowout Preventer (BOP) is the most critical of the safety systems involved in drilling operations. The recent Montara and Macondo (Refs. 1 and 2) accidents have made it entirely visible to the whole world the huge consequences that can result when the BOP fails to perform its assigned safety functions. In addition, recent studies have shown that BOP unreliability is responsible for 50-60% of drilling downtime, representing a cause of major losses to drilling contractors and oil operators.

The issue of the reliability of the BOP has long been discussed and despite important advances it continues to generate concerns among the offshore safety regulators. As for any typical safety equipment, it is difficult to know its operational status (working or not) during the process operation. The idea of devising means and methods to somehow monitor the condition of the BOP in real-time has always raised a lot of interest among those involved in offshore drilling. Already in 2010, just after the Macondo accident, a report from the Office of Inspector General of the U.S. Department of the Interior (Ref. 3) identified potential areas for improvements of the US offshore safety program and presented several recommendations. Of particular relevance is Recommendation 18, which reads like: “Analyze the benefits of obtaining electronic access to real-time data transmitted from offshore platforms/drilling rigs, such as operators’ surveillance cameras and BOP monitoring systems, and/or other automated control and monitoring systems to provide BOEMRE with additional oversight tools”. Additionally, the National Academy of Engineering (NAE) and National Research Council (NRC) committee that evaluated the causes of the Macondo accident (Ref. 4) made again a recommendation that addressed the issue of real-time monitoring (RTM) of BOPs: “Rec 3.4: The instrumentation on the BOP system should be improved so that the functionality and condition of the BOP can be monitored continuously”.

The recently published final version of the Well Control Regulation by BSEE (Ref. 5) dedicates a significant portion of its contents to spell out a series of requirements to be met by subsea BOPs, including RTM and increased maintenance to help ensure the functionality and operability of the BOP system that will help reduce the safety and environmental risks.

As can be seen from the above references, RTM of BOP safety functions is very much on the current agenda of both regulators and operators. But in our opinion, RTM alone does not solve the problem. It is certainly an essential enabler but it has to be coupled to good analytical tools which are themselves capable of analyzing the RTM data stream and providing concise results that can be readily understood by decision makers. One way to monitor the "functionality and condition of the BOP" is to monitor the reliability of its main safety function (typically of the order of five or six). As for any safety system, its main reliability indicator is the probability of failure on demand (PFD) which can be separately evaluated for each of the main safety functions of the BOP.

The BOP is actually a rather complex assembly of devices designed to shut in the well at varying stages and when circumstances dictate, close down the well completely. It is comprised of numerous subsystems and components with a highly complex logical control system. The PFD of each BOP safety function is a combination of the logical configuration of its subsystems and components, the intrinsic reliability of each of its components and the frequency and type of periodic proof tests that they are subjected to during the drilling process.

One important operational decision with direct impact on drilling downtime relates to what to do when a component or subsystem failure is detected during drilling: pull up the BOP for repair or continue drilling with a degraded BOP? Being able to know in real-time (or quasi-real-time) what are the effects of the detected failure on the reliability of the most important BOP safety functions is certainly a very desirable factor which can give an important contribution to this decision making process. Until now most drilling contractors have used tools or procedures which are based on qualitative arguments related to the loss of redundancy implied by the detected failure. But it is quite simple to show that not all redundancy losses have the same implications for the probability of failure on demand (PFD) of the BOP. Some redundancy losses bring about much bigger increases in the BOP PFD than others.

II. OBJECTIVES OF THIS WORK

Unreliability of Blowout Preventers (BOP) is among the major causes of downtime in drilling operations. The decision related to the retrieval of BOP after the detection of a failure during drilling can be one of the most costly decisions made in the drilling of a subsea oil well. Undoubtedly, any detected failure in a BOP stack during drilling is an important cause of concern, but not all component failures are of equal importance. While the impact of some failures may lead to the total loss of a critical safety function, other failures may barely change its probability of failure on demand (PFD). Retrieval of the BOP for repair is a must in the first scenario. In the second scenario retrieval could be unnecessary. Between these two extreme cases there is a wide variety of intermediate cases where the retrieval decision must be made.

In this paper we present the basis for the development of a BOP reliability management tool which can respond in real-time (or quasi-real-time) to the information of a detected failure of a BOP component or subsystem. The developed tool is a risk-informed decision support one and is named the BOP Retrieval Decision Tool or BOP▪RDT for short. The main goal of this new tool is to contribute to better-informed decision-making regarding operational safety and reliability of BOPs, while its ultimate goal is to reduce BOP downtime thus reducing drilling costs while maintaining its safety margin. Both qualitative and quantitative criteria can be used as the basis for support of the decision making process. The computational engine is based on a time-dependent reliability model which has been specially developed to calculate the PFD of each one of the various BOP safety functions at any moment in time. It properly takes into account multiple testing levels of components and the associated test coverage factors, and accepts different failure rate models suitable for each BOP component. Following the detection of any BOP component failure, this information is passed to the Tool either manually or automatically. The new information is then used to evaluate its impact on the PFD(t) of each safety function and to evaluate their new average (PFDavg) and maximum values (PFDmax) during the drilling campaign. Some examples are presented in the paper to demonstrate its applications to various practical situations faced by drilling contractors and operators.

III. BOP SAFETY FUNCTIONS

According to API Standard 53 (Ref. 6), a Blowout Preventer or BOP is an equipment installed on the wellhead or wellhead assemblies to contain wellbore fluids, either in the annular space between the casing and the tubulars, or in an open hole during well drilling, completion and testing operations.

The BOP functions during drilling operation are to close relevant BOP valves in order to prevent blowouts and/or well leaks. OLF Guideline 070 (Ref. 7) defines the following functions for the BOP:

1. Shear drill pipe and seal off well
2. Seal around drill pipe
3. Seal an open hole

For execution of safety function 1 the drill pipe has to be sheared before the well can be sealed off. Historically this has been an event where the well has blown out through the drill string and stabbing valve at the top drive and/or the Kelly valve on the drill floor have failed. It is not industry practice to test on a regular basis the function of shear ram with pipe in the BOP. It is considered a destructive test. Factory acceptance testing is performed for the BOP to shear a pipe. Safety function 2 is the most commonly used and is executed by annular preventers and pipe rams. There can be limitations to when the pipe rams work properly, such as closing on drill collars, tool joints, perforation guns, etc. Safety function 3 is executed by the blind shear ram in order to seal the well. If a leak should occur there will be a possibility to run pipe in the hole and close the annular around the pipe. The blind shear ram may then be opened and the pipe stripped further in so the pipe rams may also be used.

In the OLF guideline 070 (Ref. 7) the SIL function related to closing in the well has been restricted to closing of the valve(s) and do not include the actual shearing of the pipe. Functions 1 and 3 can thus be combined; i.e. closing of the blind shear ram. As a minimum the SIL for annulus isolation using the annular preventers or pipe rams should be SIL 2 and the minimum SIL for closing the well by the blind shear ram should also be SIL 2 according to Ref. 7 which is accepted by the Norwegian regulatory agency (PSA).

The BOP analyzed in this paper as an example of application is a real one that is currently being used in the North Sea. It is configured with five rams (BSR – Blind Shear Ram, CSR – Casing Shear Ram, and three pipe rams) and dual annular preventers. The *PFD(t)* for the following Safety Functions were implemented and can be monitored by the BOP▪RDT:

- Riser Stay Connected - Drill Pipe Through the BOP:
  SF1: Shear drill pipe and seal off well - Cutting by Blind or Casing Shear Rams and Closing and Locking by Blind Shear Ram.
  SF2: Seal around drill pipe - Closing the Annular Preventers or the Pipe Rams.
- Riser Stay Connected - Casing Through the BOP:
  SF3: Shear casing and seal off well - Cutting by Casing Shear Ram and Closing and Locking by Blind Shear Ram.
- Riser Stay Connected - Open Hole:
  SF4: Seal off open hole - Closing and Locking by Blind Shear Ram.
- Riser Stay Connected – All drilling rig conditions:
  SF5: BOP Safety Functions SF1, SF2, SF3 and SF4
- Emergency Disconnection:
  SF6: Emergency Disconnection - Disconnect the lower marine-riser package (LMRP) from BOP stack.

In the example presented in this paper, Safety Function SF5 is built as the logical union of all the previous four safety functions and its objective is to provide a global indicator for the condition of the BOP safety functions with the riser connected. These SFs are related to the decision of retrieving or not the BOP in case of failure detection of a BOP component or subsystem. The sixth safety function is related to the emergency disconnection of the LMRP from the BOP stack and illustrates the fact that any other BOP function can be put in the Tool.

IV. MODELLING OF THE BOP SAFETY FUNCTIONS

The first part of the modelling process is the construction of a detailed fault tree for each of the BOP safety functions. For the example being presented in this paper, a fault tree is built for each of the six safety functions indicated in the previous but there is actually no limit to the number of safety function fault trees that can be put in the Tool. The fault trees have between 300 and 450 basic events, depending on the complexity of the safety function.

The next part is to obtain the minimal cut sets for each safety function. These two parts are done outside the Tool using any of the available fault tree programs in the market. In the example of this paper, we have operated with min cut sets up to order four. It is unlikely that a BOP is going to be allowed to continue operating with more than two detected failures. Therefore, retaining up to order four min cut sets gives very good results. If needed, higher order cut sets may be included but that increases a little the computational time used by the Tool. With six safety functions and around 2500 to 3000 min cut sets (up to order four) the computational time varies from two to five minutes depending on the number of detected failures and the speed of the computer. This is a very fast response for the problem at hand and it means that there is room for increasing the complexity of the problem if that is really needed.

The lists of min cut sets for each safety function are then fed as input to the Tool and from this point on, everything else is done inside of it. When a failure is detected either by diagnostic during the drilling operation or by any of the various proof tests that are periodically performed, this information is passed to the Tool (either manually or automatically). Procedures are built-in to perform Boolean reduction operations to find the new cut set structures for each safety function. From this point on, the assessment procedure is divided in two different alternative ways: a qualitative assessment and a quantitative assessment, which are explained in the next two sections.

The novelty of the BOP▪RDT is the fully quantitative time-dependent reliability model which is applied to the minimal cut set structure derived from the fault trees of each BOP safety functions. Nevertheless, because in some areas of the world regulators and companies may not yet be using probabilistic criteria for decisions regarding safety issues, a qualitative model has also been added to the Tool as explained in the next section.

V. QUALITATIVE ASSESSMENT MODEL AND RESULTS

V.A. Qualitative Assessment Method

The qualitative assessment model is based on deterministic criteria which are solely based on the losses of redundancy resulting from the information regarding the detected failure. As explained in the preceding section, upon receiving the information about the occurrence of a certain component or subsystem failure, the Tool produces the new cut set structure for each safety function.

A comparison is then done to determine how the minimal cut sets before the failure changed into those after the failures. The comparative procedure consists of checking how the order of each min cut set changed from before the failure to after the failure. A table is produced which indicates how many min cut sets of changed from order n to order n-1, n-2, and so on. Considering that a change from order n to order n-1 represents a weakening of the redundancy built into the safety function reliability structure, this information is used to build management rules which can be applied to support the decision making related to the pull up or not of the BOP.

V.B. Qualitative Assessment Management Decision Rules

The condition status of each safety function is classified in four states: GREEN, YELLOW, ORANGE and RED. In the qualitative assessment model, the state of the safety function depends on the loss of redundancy resulting from the change of the order of the min cut sets of the function. The following rules are used in this example to specify the condition states of the safety function at any point in time:

GREEN state – no detected failure; the reliability structure function is the same as it was at time t=0; there is no change of order of any min cut set since there is not any detected failure.

YELLOW state – as a result of one or more detected failures, at least one min cut set of third order changed to second order and there was no change in the min cut sets of order smaller than three.

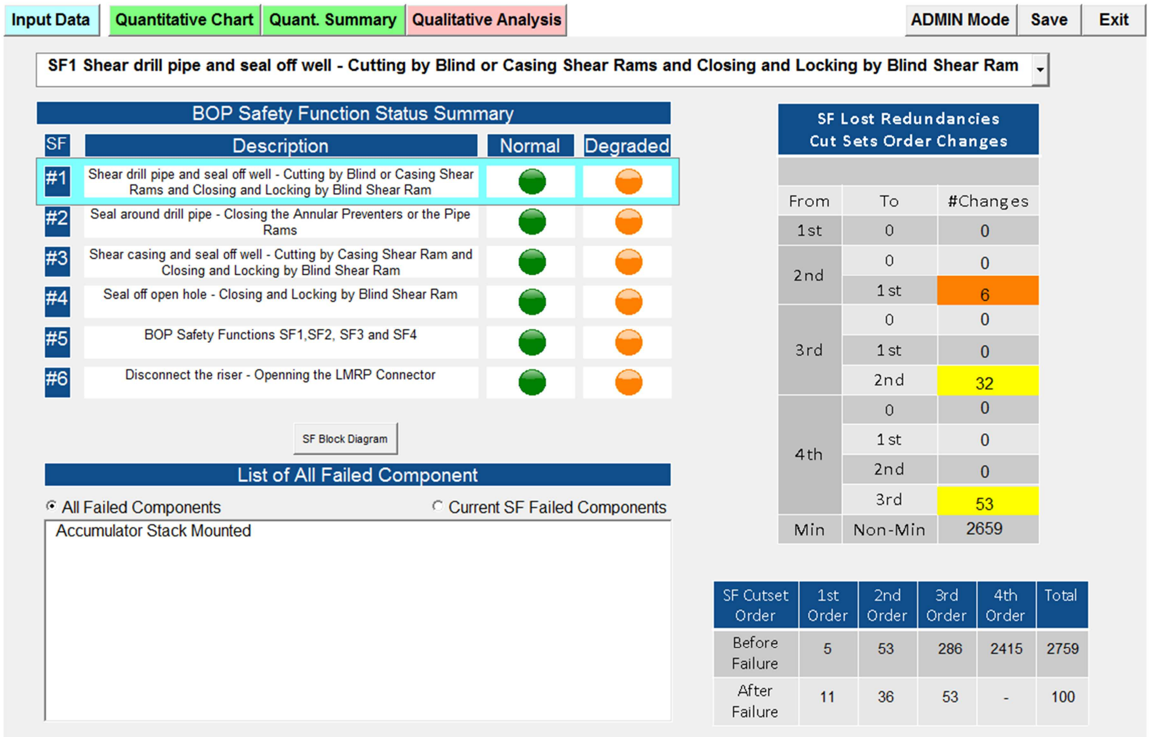
ORANGE state - as a result of one or more detected failures, at least one min cut set of second order changed to first order and there was no change in the min cut sets of order smaller than two.

RED state - as a result of one or more detected failures, at least one min cut set of first order occurred, this actually means that the safety function entered a failed state upon the occurrence of the detected failure.

The green state indicates that no detected failure is registered at that moment and therefore the safety function reliability function has the same redundancies as at time zero. The yellow condition indicates that at least one triple redundancy has been changed to a double redundancy. It is also possible that many third order min cut sets have changed to second order and that many min cut sets of higher order have changed to a lower order but there was no change in the min cut sets of order lower than three. The orange condition indicates that at least one double redundancy has been changed to a single redundancy. As before, many second order min cut sets may have changed to second order and many of higher order have changed to a lower order but no changes occurred with the min cut sets of first order. This means it is possible that the reliability structure function before the failure may already contain one or more first order min cut sets but those were not changed by the input of the detected failure. It is the change caused by the detected failure that matters because it implies a reduction of the original accepted redundancy level of the safety function.

V.C. Example of Qualitative Assessment Results

An example of the results of the qualitative assessment method is shown in Figure 1 for the case of a failure of the stack mounted accumulator for the BOP configuration indicated in Section III. As can be seen this failure caused all safety functions to be in an ORANGE condition. The reason for that can be seen on the table of “SF Lost Redundancies – Cut Sets Order Changes” where it is shown that six min cut sets of this SF changed from second to first order and this is indicative of an ORANGE condition according to the management decision rules in Section V.B. About 32 min cut sets of third order changed from third to second order and 53 changed from fourth to third, but the BOP condition is dictated by the change from second to first which represent a more significant structural loss of redundancy (no credit is given to the probabilities in the qualitative method).



SF1 Shear drill pipe and seal off well - Cutting by Blind or Casing Shear Rams and Closing and Locking by Blind Shear Ram

BOP Safety Function Status Summary

SF	Description	Normal	Degraded
#1	Shear drill pipe and seal off well - Cutting by Blind or Casing Shear Rams and Closing and Locking by Blind Shear Ram	●	●
#2	Seal around drill pipe - Closing the Annular Preventers or the Pipe Rams	●	●
#3	Shear casing and seal off well - Cutting by Casing Shear Ram and Closing and Locking by Blind Shear Ram	●	●
#4	Seal off open hole - Closing and Locking by Blind Shear Ram	●	●
#5	BOP Safety Functions SF1,SF2, SF3 and SF4	●	●
#6	Disconnect the riser - Openning the LMRP Connector	●	●

List of All Failed Component

● All Failed Components ○ Current SF Failed Components

Accumulator Stack Mounted

SF Lost Redundancies
Cut Sets Order Changes

From	To	#Changes
1st	0	0
2nd	0	0
	1st	6
3rd	0	0
	1st	0
	2nd	32
4th	0	0
	1st	0
	2nd	0
	3rd	53
Min	Non-Min	2659

SF Cutset Order	1st Order	2nd Order	3rd Order	4th Order	Total
Before Failure	5	53	286	2415	2759
After Failure	11	36	53	-	100

Figure 1 - Example of Results of the Qualitative Assessment

VI. QUANTITATIVE ASSESSMENT AND RESULTS

VI.A. Quantitative Assessment Method

The quantitative assessment model is based on probabilistic criteria which take into account the magnitude of the increase of the PFD of each safety function as a result of the occurrence of one or more detected failures. As explained in the preceding section, upon receiving the information about the occurrence of a certain component or subsystem failure, the Tool produces the new cut set structure for each safety function and recalculates the new PFDs for each safety function.

In the example used in this paper, the base case for the PFD is the indication in OLF 070 (Ref. 7) that the two most important BOP safety functions should comply with SIL 2 ($10^{-3} < \text{PFD} < 10^{-2}$) but the Tool can be customized to consider any other range of values. In the BOP▪RDT the PFD value can be the average value or the maximum value within the drilling campaign. The corresponding management decision rules are presented in Section VI.B.

The general time-dependent equation for the evaluation of the *PFD(t)* is given by Equation (1) where $\lambda(t)$ is the dangerous undetected failure rate:

$$\boldsymbol{PFD(t+dt) = PFD(t) + [1 - PFD(t)] * \lambda(t)dt} \qquad (1)$$

Within the interval between two consecutive tests, the general solution to Equation (1) can be shown to be (Ref. 8):

$$\boldsymbol{PFD(t) = 1 - [1 - PFD(T_i^+)]e^{-\int_{T_i^+}^{t} \lambda(t)dt}} \qquad (2)$$

where $PFD(T_i^+)$ is the value of the *PFD(t)* at the beginning of the integration interval (initial condition set at a time just immediately after the conclusion of the test at the beginning of the ith interval between tests). Here we are assuming that both test and repair are perfect and we are neglecting their durations.

Assuming an exponential model for the component failure rate, namely *λ(t)=λ =constant* and using the assumptions of perfect test and repair, Equation (2) becomes:

$$\boldsymbol{PFD(t) = 1 - e^{-\lambda.(t-T_i)}} \qquad T_i < t < T_{i+1} \qquad (3)$$

For a component subject to periodical tests with interval between tests equal to T_1, a more compact analytical representation of Equation (3) is given by:

$$PFD(t) = 1 - \exp[-\lambda . Mod(t,T_1)] \qquad 0 < t \leq n.T_1 \qquad (4)$$

where

$$Mod(t,T_1) = t - Int(t/T_1).T_1]. \qquad (5)$$

where Int(t/T) is the Integer Function (a function that returns the integer part of the quotient between *t* and T_1).

In addition to the above exponential failure rate model, two other failure rate models are implemented in the Tool: an increasing failure rate Weibull model and a "additive-test-step-varying" (ATSV) model. The former is well-known among reliability practitioners and it is used to represent the wear out degradation mechanism typical of that suffered by mechanical components (such as pumps and valves). We introduced the latter model to account for the shock degradation mechanism caused by tests (in particular the pressure tests of some BOP components).

For the Weibull model, the expression for the *PFD(t)* is given by:

$$\boldsymbol{PFD(t) = 1 - e^{-\lambda^{\beta}\left\{t^{\beta} - \left[Int(\frac{t}{T_1})T_1\right]^{\beta}\right\}}} \qquad (6)$$

where $\boldsymbol{\lambda}$ and $\boldsymbol{\beta}$ are the scale and the form parameters of the Weibull distribution, respectively.

The proposed ATSV model considers that any test causes the same percentage increase of the failure rate. The hazard rate of the ATSV model is given by:

$$\boldsymbol{\lambda(t) = \lambda_0 * (1 + f * i) \quad for\ i = 1, 2, \ldots, n} \qquad (7)$$

In Equation (7), $\boldsymbol{\lambda_0}$ is the failure rate of the system as new (before any test is performed), but it is here considered that prior to the start of operation, at t=0, a test is performed which results in a first increase of the failure rate. The failure rate is then constant during each time interval between tests but varies by a fixed fraction of the initial value, given by *f*, at each test, starting from the value $\lambda_0 * (1 + \mathrm{f})$ in the first interval. If *f* is positive, then the failure rate increases at each test, and if *f* is negative the failure rate decreases at each time step. We are here interested in the increasing effect (*f >0*) rather than in a possible reduction one. In Equation (7), *i* denotes the interval between *(i-1)th* and the *ith* tests. Using Equation (7) one can obtain the following equation for the *PFD(t)* in *ith* interval between tests:

$$PFD_i(t) = 1 - e^{-\lambda_0(1+i.f)[t-(i-1)T_1]} \qquad \text{(i-1)}T_1 < t \leqslant \text{i.}T_1 \ ; \quad 0 \leqslant i \leqslant n \qquad (8)$$

In practice some BOP components can be submitted to multiple testing levels (up to four, being three incomplete and the last a full test). In the BOP▪RDT, the above three failure rate models are implemented following the multiple testing level method initially derived by Eisinger et al (Ref. 9) for the exponential failure rate model for up to four testing levels (incomplete testing levels). As an example, the analytical equations are shown in the next section for the case of two testing levels for the Weibull failure rate model.

IV.A.1. Weibull Model with Three Test Levels

For this case it is considered that the first two test levels are incomplete ones (with coverage factors c_1 and c_2, respectively) and that a complete test is performed at the third testing level. Similarly as for the two testing levels, the component hazard rate can now be split in the three parts indicated below:

$$\lambda_1(t) = c_1.\lambda(t) = c_1\beta\lambda^\beta t^{\beta-1} \tag{9}$$

$$\lambda_2(t) = c_2(1-c_1).\lambda(t) = c_2(1-c_1)\beta\lambda^\beta t^{\beta-1} \tag{10}$$

$$\lambda_3(t) = (1-c_2)(1-c_1).\lambda(t) = (1-c_2)(1-c_1)\beta\lambda^\beta t^{\beta-1} \tag{11}$$

For this case it is considered that the test intervals for the three levels are, respectively, T_1, T_2 and T_3. Furthermore, it is assumed that:

- each interval T_3 contains n intervals of T_1, and
- each interval T_3 contains m intervals of T_2.

Therefore: $T_3=n.T_1=m.T_2$, which implies that $T_2=(n/m)T_1$.

Substituting Equations (9), (10), and (11) in (2) one obtains for each of the three testing levels:

a. First testing level (i^{th} T_1 interval)

$$P_{1i}(t) = 1 - e^{-c_1\lambda^\beta[t^\beta-((i-1)T_1)^\beta]} \qquad (i-1)T_1 < t \leqslant i.T_1\,; \quad 0 \leqslant i \leqslant n \tag{12}$$

b. Second testing level (j^{th} T_2 interval)

$$P_{2j}(t) = 1 - e^{-c_2(1-c_1)\lambda^\beta[t^\beta-((j-1)T_2)^\beta]} \qquad (j-1)T_2 < t \leqslant j.T_2\,; \quad 0 \leqslant j \leqslant m \tag{13}$$

c. Third testing level

$$P_3(t) = 1 - e^{-(1-c_2)(1-c_1)\lambda^\beta t^\beta} \qquad 0 < t \leqslant T_3 \tag{14}$$

The time-dependent unavailability, *PFD(t)*, of the component (encompassing the three testing levels) can be obtaining by the following equation:

$$PFD(t) = 1 - [1 - PFD_1(t)][1 - PFD_2(t)][1 - PFD_3(t)] \tag{15}$$

The value of PFD_{avg} can be obtained by integrating *PFD(t)* from 0 to T_3 and dividing it by T_3. In the BOP▪RDT this is numerically done.

A variation of this model is also implemented in the BOP▪RDT where a maximum number of testing cycles is considered after which the component must be replaced by a new one. This is also implemented in the BOP▪RDT.

In Ref. 10 analytical equations are explicitly derived for the assessment of the time-dependent PFD function for all three failure rate models (exponential, Weibull and ATSV) for up to three testing levels. In the BOP▪RDT, equations are implemented for the three referred failure rate for up to four testing levels. In addition the consideration of a direct probability value is also given as an option to allow the consideration of human errors. Common-cause failures of redundant BOP components are implemented in the BOP▪RDT using the traditional beta-factor model.

VI.B. Quantitative Assessment Management Decision Rules

The condition status of each safety function is classified in four states: GREEN, YELLOW, ORANGE and RED. In the quantitative assessment model, the state of the safety function depends on the magnitude of the increase of the PFD of each safety function caused by the occurrence of one or more detected component failures. The corresponding management decision rules for the quantitative method are the following:

- GREEN – no failure detected;
- YELLOW – one or more failures detected but their effects do not increase the PFD beyond the acceptable range (SIL 2, for instance);
- ORANGE - one or more failures detected and their effects do increase the PFD above the acceptable range (to SIL 1 level, for instance);
- RED – the effects of the detected increase the PFD to a clearly unacceptable range (to SIL 0, for instance).

Based on the above rules, if a detected failure causes only a YELLOW condition in a safety function, this means that the effect of the failure is not big enough to drive the PFD of the function outside the compliance rule and therefore that the BOP could continue to be operated without the need to pull it up for repair of the failure.

An ORANGE condition is one that requires further thinking on the part of the operators. In this case, it is necessary to look at other factors, such as the conditions of the well and the DP system, how much time until the end of the drilling campaign, and others, before a decision is made to pull the BOP up or continue the drilling operation.

A RED condition is a clear “no-go” situation because the safety margin assured by the BOP is very deteriorated, meaning that the BOP has to be pulled up immediately for repair of the failed components.

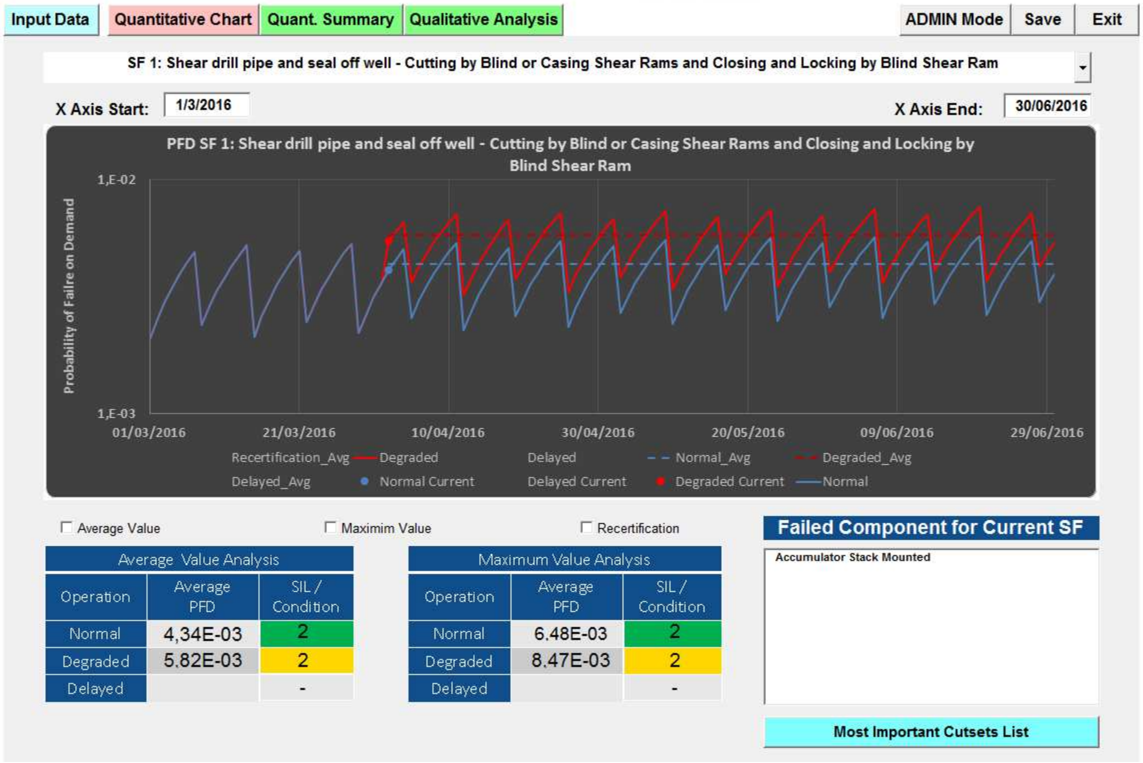
VI.C. Example of Quantitative Assessment Results

Some illustrative results of the application of the quantitative time-dependent model to the BOP configuration indicated in Section III are presented in this section. Firstly, the effect of the detection of a failure of the stack mounted accumulator is shown in Figure 2 for the same BOP configuration described in Section III. In the graph, the blue curve represents the normal PFD(t) without any detected failure.

The red curve is the degraded PFD(t) after the occurrence of the referred failure. The dotted blue and red lines are the PFDavg values before and after the failure. As can be seen both values are within the SIL 2 range and this is numerically confirmed by the values on the first table on the lower part of the figure with the average value analysis. The second table is the same analysis but now for the maximum values of the two functions. Given that the degraded PFD values are within the SIL 2 range, the SF1 is then in a YELLOW condition according to the management decision rules stated in Section VI.B. It is worth saying that the decision maker must decide in advance which criterion is going to be used, average or maximum values, to avoid confusion during a real situation (a button exists that can turn off one or the other according to which criterion is chosen).

The second illustrative example is that of the failure of both communication channels. Figure 3 shows the effect of such failure on the same SF1 for the same BOP configuration as before. Now it can be seen that the failure causes SF1 to jump to the SIL 1 range, thus characterizing an ORANGE condition.

Before a decision can be made (to pull or not) the decision maker needs to examine the effect of the failure on the condition of the other safety functions. A screen like the one above for SF 1 is available for all the other SFs but summary screen is also available where an overview of the quantitative results of the impact of the failure are shown for all safety functions. This is shown in Figure 4 for the case of the same failure of both communication channels. As can be seen, this failure has a huge impact on SF 2, showing that its PFDavg value changed from a SIL 3 range (prior to the failure) to a SIL 0 range after the failure. This is indicative of a RED condition for this safety function. The same failure also causes SF 6 to jump to the SIL 0 range, indicating a RED condition also for this function. These two RED conditions and the ORANGE conditions of all the other safety functions is a clear indication that the drilling operation should not continue and that the BOP needs to be pulled up for repair of the communication channels. Block diagrams are built in the Tool to help the operators to analyze the effect of the failed components on the system.



SF 1: Shear drill pipe and seal off well - Cutting by Blind or Casing Shear Rams and Closing and Locking by Blind Shear Ram

X Axis Start: 1/3/2016

X Axis End: 30/06/2016

☐ Average Value ☐ Maximim Value ☐ Recertification

Average Value Analysis

Operation	Average PFD	SIL / Condition
Normal	4,34E-03	2
Degraded	5,82E-03	2
Delayed		-

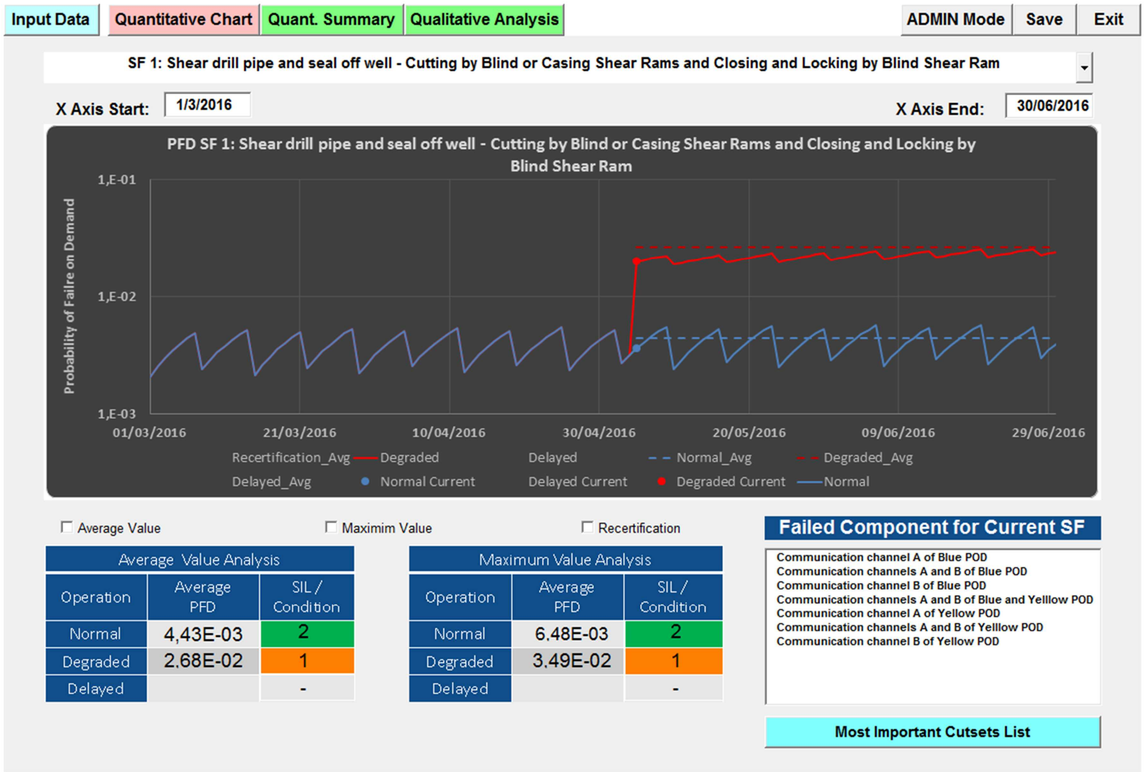
Maximum Value Analysis

Operation	Average PFD	SIL / Condition
Normal	6,48E-03	2
Degraded	8,47E-03	2
Delayed		-

Failed Component for Current SF

Accumulator Stack Mounted

Figure 2 - Example illustrating the effect of the failure of the stack mounted accumulator on Safety Function 1



SF 1: Shear drill pipe and seal off well - Cutting by Blind or Casing Shear Rams and Closing and Locking by Blind Shear Ram

X Axis Start: 1/3/2016

X Axis End: 30/06/2016

☐ Average Value ☐ Maximim Value ☐ Recertification

Average Value Analysis

Operation	Average PFD	SIL / Condition
Normal	4,43E-03	2
Degraded	2,68E-02	1
Delayed		-

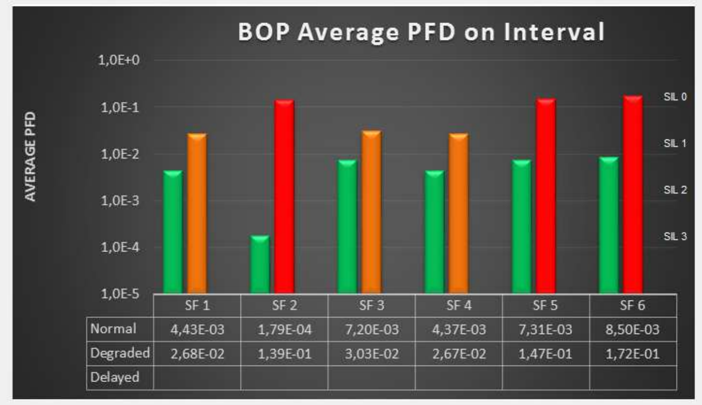
Maximum Value Analysis

Operation	Average PFD	SIL / Condition
Normal	6,48E-03	2
Degraded	3,49E-02	1
Delayed		-

Failed Component for Current SF

Communication channel A of Blue POD
Communication channels A and B of Blue POD
Communication channel B of Blue POD
Communication channels A and B of Blue and Yellow POD
Communication channel A of Yellow POD
Communication channels A and B of Yelllow POD
Communication channel B of Yellow POD

Figure 3 - Example illustrating the effect of the failure of both communication channels on Safety Function 1



	SF 1	SF 2	SF 3	SF 4	SF 5	SF 6
Normal	4,43E-03	1,79E-04	7,20E-03	4,37E-03	7,31E-03	8,50E-03
Degraded	2,68E-02	1,39E-01	3,03E-02	2,67E-02	1,47E-01	1,72E-01
Delayed						

Figure 4 - Overview of the effects of the failure of both communication channels on all six safety functions

VIII. FINAL COMMENTS

In this paper a fully quantitative time-dependent model for the probability of failure on demand (PFD) of safety functions is presented. It is shown that the model can be used to represent real-time values of the PFD of any BOP safety function before and after the detection of a failure of any of its components or subsystems. It has been designed to give a comprehensive response to the operational decision making problem related to what to do when a BOP component failure is detected during drilling. It can give both a full quantitative probabilistic response based on the effect of the failure on the PFD and a qualitative deterministic answer based on the losses of redundancy of each safety function. It incorporates both constant and time-varying failure rate models (exponential and Weibull) and also a new failure rate model (ATSV) that takes into account component shock degradation caused by pressure tests. The various types of tests and repair schemes used in subsea BOP testing and maintenance are incorporated in the model. Several other features are available in the Tool but were not shown here for lack of space.

Our model has undergone extensive verification and validation (V&V) cycles according to DNV GL V&V rules. It can be deployed either in manual or online versions or in a combination of these two alternatives. We are fully convinced that the presented model gives a clear contribution in the direction of the intensification of real-time monitoring application in the offshore oil and gas area, and in particular for the improvement of operational decision making regarding the retrieval or not of the BOP after the detection of a failure of one of its components or subsystems. Its application contributes to a reduction of drilling downtime caused by BOP failures, maintaining an adequate safety margin at the same time.

REFERENCES

1. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, “Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling”, Report to the President (2011).
2. Australian Government, “Final Government Response to the Report of the Montara Commission of Inquiry” (2011).
3. US Office of Inspector General, “A New Horizon: Looking to the Future of the Bureau of Ocean Energy Management, Regulation and Enforcement”, CR-EV-MMS-0015-2010. U.S. Department of the Interior, Washington, D.C. (2010).
4. US National Academy of Sciences, “Macondo Well Deepwater Horizon Blowout: Lessons for Improving Offshore Drilling Safety” (2012).
5. US Bureau of Safety and Environmental Enforcement (BSEE), Final Rule “Oil and Gas and Sulfur Operations in the Outer Continental Shelf-Blowout Preventer Systems and Well Control”, 30 CFR Part 250, (April 29, 2016).
6. American Petroleum Institute, “Blowout Prevention Equipment for Drilling Wells”, API Standard 53, 4th Ed. (2016).
7. Norwegian Oil and Gas Industry, “Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf”, OLF 070 Rev.2 (2004).
8. M. Rausand, “Reliability of Safety Critical Systems: Theory and Applications”, Wiley (2014)
9. S. Eisinger, L. F. Oliveira, L. Chame, and J. Domingues, “Reliability Analysis of Safety Systems Subject to Multiple Testing Levels”, ESREL 2015, Zurich, Switzerland, (Sept. 2015).
10. L. Oliveira, J. Domingues, A. Hafver, D. Lindberg, F. B. Pedersen, “Evaluation of PFD of Safety Systems with Time-Dependent and Test Step-Varying Failure Rates”, ESREL 2016 (accepted for presentation), Glasgow, Scotland, (2016).