Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Optimization of periodic inspection time of sis subject to a regular proof testing

H. Srivastav, A.V. Guilherme, A. Barros & M.A. Lundteigen
Department of Mechanical and Industrial Engineering, NTNU, Norway

F.B. Pedersen & A. Hafver
Group Technology and Research, DNV GL, Høvik, Norway

F.L. Oliveira
R&D Center, DNV GL, Rio de Janeiro, Brazil

ABSTRACT: Periodic testing is a method to ascertain the availability of Safety Instrumented Systems (SIS). These systems are generally passive and are activated only on demand. Testing is then required to diagnose their current state and to take the corresponding maintenance action. However, the testing procedure can provoke damage on some units of the SIS (especially the mechanical parts) and the system as a whole becomes more prone to failures. This situation is currently not well covered by standards under the so-called umbrella of imperfect testing. The decision maker must in practice come across to an optimization problem where the objective is to determine the optimal compromise between an accurate diagnostic of the current system state (high tests frequency) and the possible failures or degradation provoked by the testing procedure itself. The commonly used criteria to assess the performance of SIS are all related to the mean downtime of the SIS between two tests. The IEC 61508 provides subsequent analysis for multi-unit SIS when all the units are supposed to follow exponential lifetime distributions. It cannot be applied in this case as some parts of the system have a time varying failure rate which can increase after every test. We propose the use a of Markov process to model the degradation of the mechanical parts upon test and possible preventive maintenance after testing. Since the degradation due to tests is experienced at deterministic dates, we use the modelling framework of multiphase Markov processes to calculate the mean downtime. The paper is focused on explaining the optimization problem between the frequency of testing versus PFD_{avg} and find out the optimum frequency through simulations

1 INTRODUCTION

A Safety Instrumented System (SIS) is often used to detect hazardous events and to mitigate their consequences at facilities and plants that produce or handle hazardous substances, like e.g. hydrocarbon fluids and gases. Due to their criticality, they must obey to regulatory requirements and international standards on safety. IEC 61508 (1998) and related standards (such as IEC 61511 (2002) for the process industry sector) are key in framing the design and operation of SIS. One important requirement mandated by these standards is the need to verify, by quantitative analysis, that the safety performance is adequate in light of risk acceptance criteria. Most safety functions implemented by a SIS, the so-called Safety Instrumented Functions (SIFs), are seldom demanded as the normal operation is managed by a dedicated control system. According to the mentioned IEC standards, the SIFs are classified as operating in the low demand mode.

This means that the SIFs are passive most of the time and are supposed to act only when needed ("on demand"). The reliability of low demand SIFs is measured by the average probability of failure on demand (PFD_{avg}). PFD_{avg} is calculated over a time interval between two proof tests and corresponds to the mean downtime per unit of time between proof tests. The same measure is also used to express the reliability requirement for the each SIF„ but then the associated required value is derived on the basis of a risk analysis (Jin et al. 2012). IEC 61508 suggests four levels of safety integrity levels (SIL), each giving a specified range of PFDavg. For example, a SIF with a SIL 2 requirement must demonstrate that the PFD_{avg} is within $10^{-3}$and 10^{-2}.

The PFD_{avg} can be quantified using different reliability models. These models are based on assumptions and simplifications and in some situations they can lead to different results, depending on the dominating contributing factors. Lowdemand

SIS are periodically tested (proof tests) in order to confirm that they are able to act on demand. Length of intervals between such tests is an important contributor to PFD_{avg}. Normally, it is assumed that the proof tests are perfect, and that the equipment is restored to an to as-good-as-new condition (Shao-Ming et al. 1994). These assumptions imply that the proof tests are carried out in a manner and under conditions which are similar to a real demand, so that all dangerous failure modes,- i.e. failure modes that result in a failure to carry out the SIF, are revealed.The assumptions also imply that no degradation is experienced by the SIS due to the test itself (a non-destructive test). However, in reality, proof tests may not beperfect, and the equipment may degrade from exposures that are applied during the tests. The latter example is also identified by Brissaud et al. (2010). Rausand (2014a) gives one practical example on how the proof test can degrade a Downhole Safety Valve (DHSV) installed in to protect against releases from oil and gas wells. The DHSV is exposed to harsh conditions when operated (due to high pressures drop and in some cases high temperature). A perfect proof test, would imply that the DHSV is closed with full flow from the well (which would be the real demand situation). However, this type of exposure is known to degrade the performance of the DHSV, and the proof test is therefore carried out under non-perfect/imperfect test condtions by closing DHSV with downstream valves already closed. Still, it is interesting to understand better the impact of perfect versus non-perfect/imperfect test conditions. One approach has been suggested by Oliveira et al. (2016), where an additive test-step varying (ATSV) model was elaborated to reflect the increment of the failure rate after each proof test in a blowout preventer (BOP) system. Yet, it is still not clear how to implement the full effect of degradation for the quantification of PFD_{avg}. A review of the modelling framework was performed by Rouvroye & Brombacher (1999) and Bukowski (2005) and both promoted the use of Markov processes when other states than functioning and failed are to be included.

The objective of this paper is to demonstrate the implementation of the Markov process to model the combined effects of degradation due to equipment wear out (aging) and the exposure from the proof test. A simple homogeneous Markov process cannot be used,since the transition rates will change after each proof test. Instead, a multiphase Markov approach is suggested. This method was applied in Strand and Lundteigen (2015) to assess the BOP reliability and also in Innal et al. (2016) to establish new generalized formulas with repair time. Compared to simple Markov processes, multiphase Markov processes allows one to take into account changes of the transition rates at deterministic time points (Wu et al. 2018). The paper is organized as follows: Section 2 provides the problem statement and assumptions. The model is discussed in section 3, within a multiphase Markov framework. Section 4 describes the model implementation in terms of discrete event simulation and Monte Carlo simulations. The last section is devoted to numerical results and the consequent optimization problem.

2 MODELLING FRAMEWORK AND MODEL ASSUMPTIONS

PFD_{avg} is defined as Rausand (2014b):

"..If a demand of safety function of the item occur at a random time in future, the PFD_{avg} is the average probability that the item is not able to react and perform its safety function in response to demand.."

Theoretically, PFD_{avg} value stems from the risk analysis. For practical purposes, it is estimated on the basis of the reliability model of the SIF. In general, an estimator for PFD_{avg} ($\widehat{PFD_{avg}}$) can be interpreted as long run average value of unavailability, it can be defined as:

$$\widehat{PFD_{avg}} = \frac{1}{n}\sum_{k=1}^{n}\int_{(k-1)\tau}^{k\tau}\frac{U(t)}{\tau}dt$$

where:

- PFD_{avg} Probability of failure on demand on average
- n = Total number of inspection performed
- τ= Duration between two consecutive inspection
- $U(t)$ = Unavailability of the system at t

Inspection is an integral part of the proof test which reveals about the state of the system at the time of proof test. For all calculations, frequency of inspection is equal to frequency of proof test performed. In this situation $\widehat{PFD_{avg}}$ is proportion of time on average that the multiphase Markov process spends in the failed state. It is the dangerous failure rate that is considered in the calculation of $\widehat{PFD_{avg}}$, i.e. the failures that can prevent the SIF from functioning on demand.

The modelling framework to model this problem is described hereafter.

2.1 *Modelling framework*

There are basically two different mindsets for modelling degradation due to equipment wear out (aging) and degradation due to proof test. One mindset is more inherited from Reliability theory: the main idea is to model the degraded unit by a binary random variable moving from working

state to failed state and to consider that the transition rate between these two states will increase with time or with the number of tests experienced by the unit. In other words, the unit has a lifetime law with an increasing failure rate which is a function of the number of tests. Another mindset is more applied for people working in the framework of maintenance optimization. The unit is modelled by a random variable with more than two states. The state space can be a discrete finite space, an infinite discrete one or a continuous one. The main idea is that there exists intermediate states between the new one and the failed one. All the intermediate states can be considered as working states but with possibly degraded performances and they are taken as a health indicator of the system. They often correspond to degradation phenomena or symptoms that can be monitored, diagnosed and used as a decision indicator to trigger preventive maintenance actions. The advantage of such models is that

- We can make correspondence between degradation phenomena and the performance of the system (here 1-PFD).
- We can use the intermediate states to optimize and define preventive condition-based maintenance

However, if expert judgments can be relevant enough to define the number and the nature of intermediate states, the law of the sojourn time in every single state may be difficult to estimate. A model relying only on lifetime law and a binary random variable may be then more reasonable.

Most of the existing models that are described in the introduction are inherited from Reliability theory. The calculation of the PFD for SIS is mainly based on binary random variables. In this paper, we want to explore the use of intermediate states in a specific context when the tests have a negative impact on the system condition. We want to investigate such a framework because

- The literature, guidelines and practices related to negative impact of testing should be linked at some point to the identification of some degradation mechanism.
- This seems to be a good way to go ahead and prepare the future for condition-based maintenance and optimal use of condition monitoring.

As a preliminary study, we propose a model with two intermediate states. This number is arbitrarily chosen and we do not investigate any preventive maintenance. We only aim at showing that there is a trade off between the negative effect of tests (pushingthe system randomly into more degraded states) and the added value performing more tests to detect failures earlier.

Equipment wear out is modelled by a finite number of intermediate degraded states between the new state and the failed one. Degradation due to proof test is modelled by an increase of the transition rates between two states at inspection time. In addition, direct transitions are possible from any functioning state to the failed one: they model sudden failures that are not due to wear. Since the unit is passive, all the failures are undetectable without testing, whatever the failure mode is. At last, in order to develop further analytical formulations, we chose a Markovian framework. Because the transition rates are changing at inspection times, we refer it as a Multiphase Markov process. The current paper is only devoted to Monte Carlo simulations in order to demonstrate the relevance of the problem statement and the possible trade off that arises due to the negative effect of testings. Analytical formulations seems to be tractable but are left for further work.

2.2 *Assumptions*

Modelling degradation using Multiphase Markov process, we have used following assumptions:

- In general, we can consider that a SIF equipment is exposed to two types of failures:
  - Dangerous detected (DD) failures, i.e. the dangerous failures revealed by online diagnostics.
  - Dangerous undetected (DU) failures, i.e. the dangerous failures that are not DD and which are to be revealed by regular proof tests.
- For the sake of simplicity to begin with the modelling, we only consider the effect of DU failures in our analysis, since the equipment focused in our study (valves) have no or very limited facilities for diagnostics. However, effect of DD failures,for modeling purposes beyond equipment type in our study, will be considered in the future paper. From now, when we use the term "detected" or "detectable" , it is used to denote DU failures that are revealed by the proof test, in light of the real (non-perfect/imperfect) test conditions.
- DU—failures are of two types: they can be sudden or they can be due to a progressive degradation process named hereafter aging. Sudden failures are modelled by a failure rate λ_u, and aging is modelled by several intermediate states (degradation levels) between new state and failed one, with associated transition rates. Whatever the failure mode is, the system will stay in failed state until the next inspection, and then the system is repaired as per the chosen maintenance policy.

- There are 4 degradation levels: A, B, C, D. These are the states of a Markov process. (A: System working with no degradation, B: System working with degradation of system of level 1, C: System working with degradation of level 2, D: Failed)
- In our model the following instantaneous transitions are possible:
  - System can always jump to next higher state of degradation due to effect of aging.
  - System can always jump to failed state due to sudden DU failures.
  - System can not go to lower degraded state until the maintenance is performed.
- Instantaneous transitions rate for the multiphase Markov process are represented in the Figure 1.
- In the Figures above represents the effect of aging on the system, which changes every time when a proof test is performed on the system. We consider that the proof test has a negative effect on the system condition (shock leading to extra stress) and this negative effect increases the aging transition rates. The modelling of impact of negative effect of testing is done through the following model.

$$\lambda_a(t_0^+) = \begin{cases} 1.01 * \lambda_a(t_0^-) & \text{Current State A} \\ 1.03 * \lambda_a(t_0^-) & \text{Current State B} \\ 1.05 * \lambda_a(t_0^-) & \text{Current State C} \end{cases} \quad (1)$$

We assume here that a proof test is performed at $t = t_0$ and the current state is the state of the system at $t = t_0$.

- The underlying idea behind this modelling is to show that the negative impact of the proof test increases with the degradation of the system

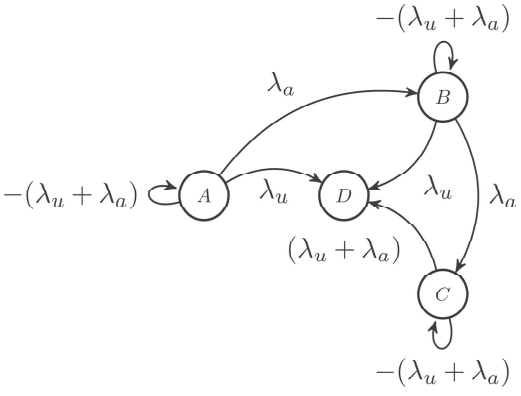

Figure 1. Instantaneous transition rates for the multiphase Markov process.

- Between two consecutive proof tests λ_a and λ_u remains constant.
- When a failure is detected after the proof test, we assume that the mean time to repair the system is negligible.

3 METHODOLOGY

The multiphase Markov process was analyzed using discrete event simulation and exponential distribution for the time spent in each state. System starts in state, degradation time (T_d) and failure time (T_f) are sampled from the exponential distribution of the respective parameters $\lambda_a(t)$ and $\lambda_u(t)$. Then based on the minimum of (T_d, T_f, τ) the next state of the process was chosen. Some specific decisions were made for the modeling:

- If system goes to a failed state (state D), the unavailability is calculated by measuring the time spent in the state D by the system. On inspection the maintenance action is taken and process is re-initiated.
- If the minimum is τ, then the system stays in the same state for the duration between two consecutive proof tests. Then the inspection is performed and we repeat the process with the increased $\lambda_a(t)$.
- If system goes to more degraded state, then the T_d', T_f', are again sampled from the corresponding exponential distributions. Now, the minimum is compared between ($T_d', T_f', \tau - T_a$). And the process repeats itself until system goes to failed state. Once the system fails, the unavailability is calculated,the maintenance action is taken and process is re-initiated.

The following maintenance policies were proposed when the system was found to be in the failed state on inspection:

- As-good-as-new (AGAN): System is reset to new state (A) and the failure rate of the system is reset to $\lambda_a[i + 1] = \lambda_a[1]$, ie we consider that system is as-good-as-new when we take away the effect of aging after maintenance of the system
- As-bad-as-old (ABAO): On maintenance, the new state of the system is set to C and the failure rate of the system is reset to $\lambda_a[i + 1] = \lambda_a[i]$

4 RESULTS AND DISCUSSION

Recall that the PFD_{avg} is the performance measure. Simulations were performed to estimate PFD_{avg} by calculating the average unavailability of the system. The proof test interval (τ) is varied from 3 days to 1 year, where represents the time

between two consecutive inspections/proof tests. We considered following values τ of for simulations: τ = (3 days, 6 days, 15 days, 21 days, 1 month, 2 month, 3 month, 4 month, 5 month, 6 month, 7 month, 8 month, 9 month, 10 month, 11 month, 12 month).

Values of parameters like λ_a, λ_u, and mission time are chosen based on industry guidelines on the performance measure. The mission time of the system for the purpose of simulation is chosen to be 5 years. Based on industrial guideline, the impact factor of the proof test is considered as per equation 1. For each value of τ, 500 random realizations were simulated to obtain average unavailability of the system.

Figure 2, shows the estimated value of PFDavg of the system for different values of τ. The borderlines of SIL 1 and SIL 2, showing that the .01 < PFD_{avg} < 0.1 for being within the range of SIL 1 and PFD_{avg} < 0.01 for being in the range of SIL 2. Left side plot in Figure 2 shows that when both λ_a and λ_u are of the order of 10^{-6} per hour, the PFD_{avg} remains within SIL 2 for both AGAN and ABAO maintenance policies for 15 days $\leq \tau \leq$ 1 year. Right side plot in Figure 2 shows that when λ_a and λ_u are increased to the order of 10^{-5} per hour, the PFD_{avg} increases for both maintenance policies. For AGAN maintenance policy, PFD_{avg} leaves the range of SIL 2 and enters SIL 1 at τ = 15 days and leaves the range of SIL 1 at τ = 6 months. For ABAO maintenance policy the PFD_{avg} leaves range of SIL 1 for $\tau \geq 4$ months and $\tau \leq 15$ days and stays within the range of SIL 1 for an optimal proof test interval (15 days < $\tau \leq$ 3 months).

In Figure 2, when the plots pertaining to AGAN maintenance policy are observed, it is found that the information gain through inspection is more significant over the negative effect of testing. This is because with AGAN maintenance policythe system did not carry the history of past tests experienced by the system.

The important conclusion that can be derived from Figure 2 is that when the maintenance policy ABAO is chosen, PFD_{avg} of the system shows a trade off between the negative effect of performing a proof test versus the gain of information by performing the proof test on the system. In other words, when the system undergoes through high frequency of proof tests, the unavailability represented by the PFD_{avg} increases instead of decreasing as it did for AGAN policy. At the same time, when the frequency of proof tests is reduced, the user does not get enough information about the state of the system. Therefore, there exists an optimum frequency of testing which minimizes the value of PFD_{avg} in the Figure 2.

Figure 3 shows the effect, of changing the values of λ_a while keeping the value of λ_u as constant 5×10^{-6} per hour, on the PFD_{avg}. Note that the tradeoff between multiplicative negative effect of testing by high frequency of testing versus loss of information by low frequency of testing, is an attribute of ABAO maintenance policy only. Hence, the maintenance policy considered in Figure 3 is ABAO. It is observed from the Figure 3 that the PFD_{avg} remains within the range SIL 2 when the value of $\lambda_a \leq 5 \times 10^{-6}$ per hour for $\tau \in$ [15 days, 5 months]. Plots show that for each value of λ_a, there exists an optimum value of τ for which PFD_{avg} attains a minimum value. It is also observed that the value of PFD_{avg} increases with increasing values of λ_a.

Figure 4 shows the effect, of changing the values of the failure rate λ_u, while keeping the value of λ_a constant 5×10^{-6} per hour, on the PFD_{avg}. ABAO maintenance policy is considered for obtaining these plots, using the same arguments as for plots in Figure 3. It is observed from the left side plot in Figure 4 that when λ_u is increased from 10^{-7} per

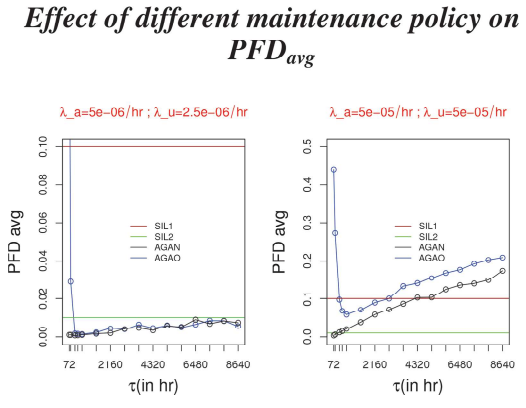

Figure 2. Effect of different maintenance policy on PFD_{avg}.

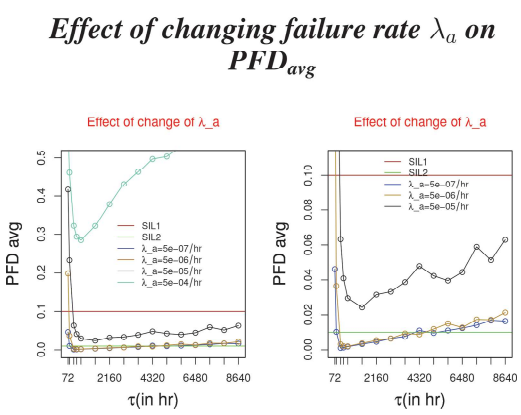

Figure 3. Effect of changing failure rate on PFD_{avg}.

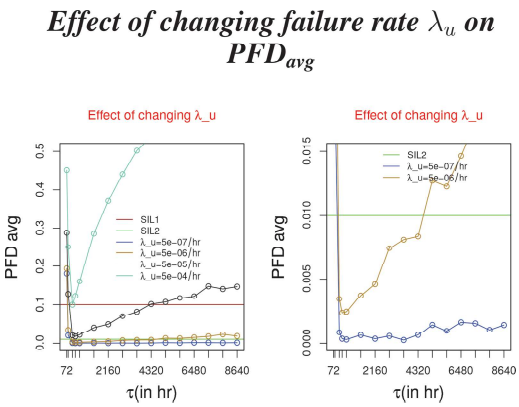

Figure 4. Effect of changing failure rate λ_u on PFD_{avg}.

hour to 10^{-4} per hour the shape of plot of PFD_{avg} changes from a flat convex to a steep convex indicating that PFD_{avg} increases with increase in λ_u.

The optimum time-interval (for performing proof test) which minimizes PFD_{avg} is significantly visible in Figure 4 for higher values of λ_u whereas for lower values of λ_u the curve needs to be zoomed up to observe the optimum time-interval (for performing proof test) as shown in the right side plot of Figure 4.

5 CONCLUSIONS AND IDEAS FOR FUTURE WORK

In AGAN maintenance policy, the technical state of the system is maintained to "as-good-as-new" after regular proof test meaning the system will not aggregate the negative effect of the regular proof test after maintenance. Hence, with AGAN we canmake PFD_{avg} as small as required by increasing the frequency of performing the proof test on the system. But using AGAN maintenance policy may not be economical in most of the practical situations, hence we focus on ABAO maintenance policy in this section.

5.1 *Conclusions*

Our case study showed that in case of ABAO maintenance policy, there are two competitive forces that can increase the PFD_{avg}. The first is the multiplicative negative effect of frequent proof tests, despite the maintenance that is carried out as part of the tests. This force becomes more dominant when the frequency of performing proof test is high. The second is the information obtained about the status of the system by carrying out the proof test. While the second force would like to increase the frequency of performing the proof test to lower PFD_{avg}. The first force would like to decrease the frequency of performing the proof test to obtain the same effect on the PFD_{avg}.

An optimum can be obtained for a regular proof test interval that can be verified against the constraints of the SIL requirement. It is therefore suggested that there exists an optimum frequency for performing the proof test that minimizes the PFD_{avg} of system whenever the following is true:

- The regular proof tests, that involves the inspection of technical state of the system, have some negative effect on the performance of the system due to test conditions and exposures.
- Some dangerous failure modes of the system can only be revealed by the regular proof tests, and not by other means (like e.g. diagnostic testing).
- System is maintained with the ABAO maintenance policy, meaning that the technical state is not "as-good-as-new" after a regular proof test. The ABAO maintenance policy will aggregate the negative effects of regular proof test.

5.2 *Ideas for future work*

The above studies were performed assuming no DD failures and mean time to repair as negligible. It would be an interesting proposition to see the effect of adding DD failures and mean time to repair to the above study. Analytical solutions need to be developed to find out the exact solution of the stochastic differential equation involved in the above situation. Two degraded states were chosen randomly in the above study, the connection between the physical phenomena of the degradation and quantification the degraded states needs to explored. Effect of the predictive maintenance and redundancies on the PFD_{avg} in this situation needs to be studied.

ACKNOWLEDGEMENTS

This paper has been written under the Norwegian Centre for Research based Innovation on Subsea Pro-duction and Processing (SUBPRO). The authors would like to thank the Research Council of Norway, as well to the industrial partners involved in this project.

REFERENCES

Bond, K. (2002). Iec 61511-functional safety: Safety instrumented systems for the process industry sector. In *Annual Symposium on Instrumentation for the Process Industries*, Volume 57, pp. 33–40. Instrument Society of America.

Brissaud, F., A. Barros, & C. B´erenguer (2010). Probability of failure of safety-critical systems subject to partial tests. In *Reliability and Maintainability Symposium (RAMS), 2010 Proceedings-Annual*, pp. 1–6. IEEE.

Bukowski, J.V. (2005). A comparison of techniques for computing pfd average. In Reliability and *Maintainability Symposium, 2005. Proceedings. Annual*, pp. 590–595. IEEE.

IEC, I. (1998). 61508 functional safety of electrical/- electronic/programmable electronic safety-related systems. *International electrotechnical commission*.

Innal, F., M.A. Lundteigen, Y. Liu, & A. Barros (2016). Pfdavg generalized formulas for sis subject to partial and full periodic tests based on multiphase markov models. *Reliability Engineering & System Safety 150*, 160–170.

Jin, H., M.A. Lundteigen, & M. Rausand (2012). Uncertainty assessment of reliability estimates for safety-instrumented systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of risk and reliability 226*(6), 646–655.

Oliveira, F., J. Domingues, A. Hafver, D.V. Lindberg, & F.B. Pedersen (2016). Evaluation of pfd of safety systems with time-dependent and test-step varying failure rates. *ESREL, Glasgow, UK* -, 413.

Rausand, M. (2014a). *Reliability of Safety-Critical Systems: Theory and Applications*, Volume -. Hoboken, Wiley.

Rausand, M. (2014b). *Reliability of safety-critical systems: theory and applications*. JohnWiley & Sons.

Rouvroye, J. & A. Brombacher (1999). New quantitative safety standards: different techniques, different results? *Reliability Engineering & System Safety 66*(2), 121–125.

Shao-Ming, W., H. Ren, & W. De-Jun (1994). Reliability analysis of a repairable system without being repaired "as good as new". *Microelectronics Reliability 34*(2), 357–360.

Strand, G.O. &M.A. Lundteigen (2015). Risk control in the well drilling phase: Bop system reliability assessment.

Wu, S., L. Zhang, A. Barros, W. Zheng, & Y. Liu (2018). Performance analysis for subsea blind shear ram preventers subject to testing strategies. *Reliability Engineering & System Safety 169*, 281–298.


Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com