Reliability Engineering and System Safety 196 (2020) 106779

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Optimization of maintenances following proof tests for the final element of a safety-instrumented system

Aibo Zhang[a], Tieling Zhang[b], Anne Barros[a,c], Yiliu Liu[a,*]

[a] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway
[b] School of Mechanical, Materials, Mechatronic and Biomedical Engineering, University of Wollongong, Wollongong, NSW 2522, Australia
[c] CentraleSupelec, Paris Saclay University, France

ARTICLE INFO

Keywords:
Safety-instrumented system
Final element
Degradation
Preventive maintenance
Maintenance strategy
PFD_{avg}

ABSTRACT

Safety-instrumented systems (SISs) have been widely installed to prevent accidental events and mitigate their consequences. Mechanical final elements of SISs often become vulnerable with time due to degradations, but the particulars in SIS operations and assessment impede the adaption of state-of-art research results on maintenances into this domain. This paper models the degradation of SIS final element as a stochastic process. Based on the observed information during a proof test, it is essential to determine an optimal maintenance strategy by choosing a preventive maintenance (PM) or corrective maintenance (CM), as well deciding what degree of mitigation of degradation is enough in case of a PM. When the reasonable initiation situation of a PM and the optimal maintenance degree are identified, lifetime cost of the final element can be minimized while keeping satisfying the integrity level requirement for the SIS. A numerical example is introduced to illustrate how the presenting methods are used to examine the effects of maintenance strategies on cost and the average probability of failure on demands (PFD_{avg}) of a SIS. Intervals of the upcoming tests thus can be updated to provide maintenance crews with more clues on cost-effective tests without weakening safety.

1. Introduction

Considering production safety and environment protection, many safety-instrumented systems (SISs) have been employed in different industries. For example, on an offshore oil and gas production platform, emergency shutdown (ESD) systems are installed to protect the facility in case of an undesired event. Normally, a SIS, like the ESD system, consists of sensor(s) (e.g. pressure transmitters), logic solver(s) and final element(s) (shutdown valves) [1]. The final element performs one or more safety-instrumented functions (SIFs), by closing itself down to stop the gas flow in a pipeline if an emergency occurs in production. The facility protected by the ESD system is called equipment under control (EUC) in this context.

An ESD system is a typical SIS operating in a low demand mode, where the activation frequency is less than once per year in general. The final elements of such a SIS are mainly in a dormant state unless there is a proof test or a real shock on the equipment being protected by the SIS, or equipment under control (EUC) [1]. Therefore, some failure modes of final elements will stay hidden until the time to be activated. These hidden failures are called dangerous undetected (DU) if they can result in serious accidents. The average probability of failures on demands (PFD_{avg}) is a common-used measure in the evaluation of unavailability of SISs in the low demand mode [2], and DU failures are the main contributors for PFD_{avg}. In IEC standards, the value of PFD_{avg} will be used to determine the safety integrity level (SIL) of a SIS.

Many researches have paid attention to the calculation of PFD_{avg}, using: simplified formulas [1,3], Markov methods [4–7] and Petri Nets [8–10]. Common for most of these methods is the assumption of constant failure rates of all elements in a SIS. In practices, such an assumption is always valid for electronic components, but its validity for mechanical components is in question.

Mechanical components, such as many final elements of SISs, including shutdown valves, are operated in harsh conditions, and they are rather vulnerable to creeping or other degradation processes [11]. Thus, their failure rates, namely the conditional probability of failure in the next short time period, always increase with time. Several authors have assessed unavailability of SISs in consideration of non-constant failure rate [11,12]. Meanwhile, several dynamic reliability method, e.g. multiphase Markov process, have been applied to SISs for reliability assessment [5,13–16]. Their findings show that PFD_{avg} is changing with time and becomes different from one proof test interval to the next. The changing PFD_{avg} makes the updating of proof test interval necessary

* Corresponding author.
E-mail address: yiliu.liu@ntnu.no (Y. Liu).

https://doi.org/10.1016/j.ress.2019.106779
Received 2 August 2019; Received in revised form 29 October 2019; Accepted 22 December 2019
Available online 23 December 2019

based on the requirement from SILs.

With the development of sensor technologies, more data about operation conditions and system degradation status can be collected in periodic proof tests. Information about degradation is helpful for the assessment of system performance [17]. Numerous parameters, such as lubricant ingredient, corrosion extent and so on, can be measured and utilized for failure prediction and diagnosis [18]. When any deviation from the normal, or early-phase signal of failure is identified, the upcoming tests and following maintenance actions need to be re-scheduled.

In terms of the final elements of an ESD, they can suffer several failure mechanisms, including erosion, corrosion, cracks etc., which can lead the capacity of performing safety functions to degrade with time [19]. For example, closing time on demand is an indicator of the performance of a shutdown valve. Once degradation of the valve reaches a certain level, the final element will be in a faulty/failed state. Such a DU failure will be hidden until a proof test identifies that closure of the valve needs too much time.

However, even though the shutdown valve is qualified in a proof test, the final element may be not as-good-as-new. Namely, the closing time is under the acceptable maximum value, but it is still longer than that when the SIS is just put into operation. As-good-as-new after each proof test is the extension of the constant failure rate assumption, meaning that PFD_{avg} remains a fixed value in each test interval [20]. Since, the unavoidable gradual degradation of mechanical components challenges the constant failure rate assumption, the unavailability of final element should be supposed to increase by time.

In the simple calculation of PFD_{avg}, more frequent proof tests are regarded to lower risks, but some practical issues can weaken such a conclusion. If a proof test of SISs fully stops the process, or complete a whole trip of shutdown, stoppage and restart of the process will cause production loss, especially in offshore engineering and facilities [1]. In addition, such a whole shutdown trip may damage the valve (e.g. wear of the valve seat area) in some degree due to high stress level [11,21]. Hence, it is reasonable to consider how to utilize given proof test information to schedule future tests more effectively (e.g. to avoid unnecessary tests), while keeping the SIS availability meeting in the required level.

With the observation in a proof test of a shutdown valve, three options of follow-ups are possible: (1) No action if the valve in test is working well; (2) preventive maintenance (PM) if a certain degradation has been identified; (3) repair or replacement of the valve if it is failed. Repair/replacement can be regarded as perfect, leading the SIS to work as-good-as-new. For a PM, degradation of the valve can be mitigated but not be eliminated, so that the probability of failure by the next test is reduced. The mitigation degree can be naturally assumed positively correlated with the resources and time spent in the PM, namely the cost of PM. However, it is challenging to decide what is the optimal degree of PM that can balance the cost and the SIS availability. In addition, questions exist in the level of degradation initiating a PM. In other words, when closing time of a valve is a bit longer than the design value, a decision needs to be made whether the degradation can be ignorable, or some actions should be taken immediately. Ignoring means to take more risks to EUC, but actions are costly especially when they are not needed.

It should be noticed that even though many studies on maintenance optimization with degradation have been conducted, they are not naturally suitable for SIS final elements. As aforementioned, failures and degradations of SISs are hidden and only can be observed periodically. Decision-making on maintenances is not based on instantaneous availability but should be based on the estimation of system performance in the next test interval. In addition, to comply with international standards, the effects of maintenances should be connected with the average unavailability of a SIS in a period (PFD_{avg}) and should always be a strict constraint when making any testing and maintenance strategies. Considering those maintenance models for renewal systems having some similarities with SISs, they assume perfect PM or CM [22–26] and focus on the average long-run cost rate [27–29]. However, for SISs, the total cost in the designed service time (e.g. 20 years) is more of interest, and perfect PMs are often not practical or necessary.

Therefore, the main objective of this paper is to deal with both the challenges by degradation to SIS assessment and the challenges by SISs to maintenance optimization, to identify the optimal PM strategies of a SIS. Specifically, the optimal combination of the two threshold values of a SIS final element is in search: the degree of degradation initiating a PM (ω_a), and the degree of degradation where completing of this PM (ω_b) can be acceptable.

The remainder of this paper is organized as follows: Section 2 explains how a SIS final element operates and what are the assumptions in the analysis; Section 3 investigates the calculation of instantaneous unavailability of SIS, PFD_{avg} and expected cumulative maintenance cost; Section 4 discusses the optimal values of two thresholds PMs based on the minimum expected cost and the SIL requirement respectively; Section 5 illustrates a method to update the test interval and conclusions are in Section 6.

2. Descriptions of safety-instrumented systems

2.1. System states and performance requirements

Without losing generality, we use an ESD system to study behaviors and operations of SISs. The ESD system is designed to maintain or achieve the EUC in a safe state, e.g. a normal pressure in process. One of main SIFs of an ESD valve is to cut off the flow when the high pressure occurs. To keep the risk of EUC within acceptable level, the valve is designed with a specific closing time, for example, 12 s. The actual performance requirement for this valve is, normally, the designed target value with acceptable deviations, e.g. 3 s. It means that the valve is considered to be functioning (with respect to this particular function) as long as the closing time is within the interval (9, 15) seconds.

If the valve closes too slowly, e.g. 18 s, it, as a safety barrier, will not meet the performance requirements for risk mitigating of EUC. A failure occurs on this valve since the required function is terminated. The corresponding failure mode is called ‘closing too slowly’, which is one of dangerous failure modes of ESD valve [1]. Degradation like corrosion or erosion due to the harsh environment is the reason of such a failure. Meanwhile, even the closing time is still within the acceptable interval, the criticality of the failure will obviously increase with the deviation from the target value (12 s) [20]. In most cases, it is not possible to observe such kind of failure without activating the valve, and so the failure mode ‘closing too slowly’ is a DU failure. Therefore, closing time checked in proof tests can be collected and reflect the valve status/degradation [30].

It is obvious that when the closing time is beyond 15 s, the valve is in a failed state. When the closing time is shorter than a certain value, e.g.14 s, we can regard the valve in a good condition. While if the closing time is between 14 and 15 s, we can consider the valve with a degraded performance but still functioning. Therefore, we can consider the valve with three different states: working, degraded and failed, as shown in Table 1. It should be noted that degradation still can exist in state 0, but it can be accepted without any maintenance action.

Because maintenance or replacement after each proof test is often

Table 1
System state definition.

state	status	State description
0	Working	The system is functioning as specified
1	Degraded	The system has a degraded performance but functioning
2	Failed	The system has a fault

expensive, no action is welcomed when the estimation based on the observed situation has shown that failure probability of the SIS by the next test is rather low. Specifically, when the valve is at the working state (state 0), no maintenance will be executed. When the valve in a degraded state, even it is still functioning, a PM with reasonable costs will be employed. The degradation is mitigated but is not eliminated considering a perfect maintenance is too costly. When the valve in a failed state, replacement is needed.

2.2. System operation and test

Possible causes of 'closing too slowly' failure mode may be because of the loss of stiffness of a spring [1,31,32]. According to [33,34], such kind of degradation could be described by stochastic process. Gamma process has been justified by practical applications for modeling degradations [35,36] due to its strongly monotone increasing property [37–39].

The final element of such a SIS is assumed to be subject to a homogeneous gamma degradation process, and a hidden failure occurs when the degradation level exceeds a predefined threshold L. The SIS is periodically tested at τ, 2τ, …, where τ is the test time interval, e.g. one year. In a proof test, degradation level is checked. As shown in Fig. 1, at 4τ, the degradation level is found beyond the failure threshold, L, then the failed system is replaced by a new one. When the degradation level is found beyond $\omega_a L$ in a proof test, PM is needed. For example, at 6τ or 8τ in Fig. 1, PM is executed and the degradation level goes back to a specific level ($\omega_b L$) rather than 0.

Consider a one-unit system that is subject to a continuous aging degradation process. The degradation process is modeled by a Gamma process with the initial state $X_0 = 0$. Then, the degradation $X(t)$ follows a gamma probability density function (PDF).

$$X(t) \sim \Gamma(\alpha t, \beta) = f_{X(t)}(x) = \frac{\beta^{\alpha t}}{\Gamma(\alpha t)} x^{\alpha t - 1} e^{-\beta x},\ \alpha, \beta > 0 \tag{1}$$

The cumulative density function (CDF) of $X(t)$ for $t > 0$ is

$$F_{X(t)}(x) = \Pr\{X(t) \le x\} = \int_0^x f_{X(t)}(z)dz \tag{2}$$

Then, the mean and variance of $X(t)$ are $\alpha t/\beta$ and $\alpha t/\beta^2$, respectively.

Periodic proof tests are executed. Proof tests are assumed perfect in this study and have no direct influence on the degradation process. In addition, we assume that the time spent in repair and test is negligible compared with the much longer test intervals.

3. Maintenance modeling and unavailability estimation

3.1. Maintenance modeling of a final element

The SIS is periodically tested with an interval τ and with cost C_{PT}. During each proof test, if the observed the degradation level $X(t)$ of the final element is less than the predefined $\omega_a L$, no action is carried out and total cost is only C_{PT}. If the degradation level is higher than $\omega_a L$ but less than L, a PM is performed with cost C_{PM} and $C_{PM} > C_{PT}$. However, if the system is found failed, it will be replaced by a new one with C_{CM}, where $C_{CM} > C_{PM}$. In addition, the cost (C_D) related with risks of EUC needs to be considered in the downtime of SIS, C_D is calculated by the product of demand rate λ_{de} and the possible loss in an EUC accident.

The long-run cost rate could be calculated with the renewal theorem [29].

$$C^{\infty} = \lim_{t\to\infty} \frac{C(t)}{t} = \frac{E[C(S_1)]}{E(S_1)} \tag{3}$$

where $C(t)$ is the cumulated maintenance cost by time t, and S_1 is the length of the first renewal cycle.

The designed service time of most SISs is not infinite, and thus the steady-state assumption may not be accepted. We estimate the cost rate over a SIS lifetime as

$$C_t^{(\omega_a,\omega_b)} = C_T N_i(t) + C_{CM} N_{CM}(t) + C_{PM} N_{PM}(t) + C_D T_d(t) \tag{4}$$

where N_i (t), N_{CM} (t), N_{PM} (t) and T_d (t) are, respectively, number of proof tests, number of CMs, PMs and the expected downtime in $[0, t]$.

It is not hard to understand that the $C_t^{(\omega_a,\omega_b)}$ is a function of maintenance parameters, including the degradation level L, PM coefficient (ω_a, ω_b) and test interval τ.

Here, minimization of cost over the designed life (e.g. 20τ) is the criterion of selecting a suitable maintenance strategy.

3.2. Unavailability calculation

We start from estimation availability ($A(t)$) of the maintained final element at time t, namely the conditional probability that the component is working at time t given $X_0 = x$, with $x \in [0, \omega_a L]$. $A(t)$ is the probability that the system performs its required function at time t, when the degradation level is less than the predefined failure threshold L.

$$A(x, t) = \Pr(X_t < L) \tag{5}$$

In the case $t \le \tau$, there is no maintenance action on $[0, t)$. So,

$$A(x, t) = F_{X(t)}(L - x), \quad \text{for } t \le \tau \tag{6}$$

From the second interval, the prior test result acts as the condition

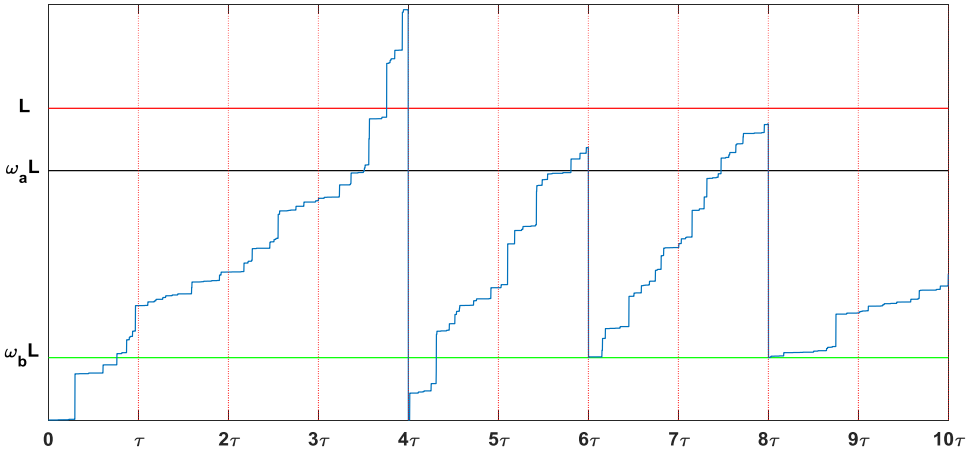


Fig. 1. Possible degradation path.

to estimate the instantaneous availability. For $i \geq 2$, we have the conditional knowledge given the degradation level μ at time τ, for $\tau < t \leq 2\tau$:

$$A(x, t) = \Pr(X(t) < L | X_\tau = \mu < L) = F_{X(t-\tau)}(L - x - \mu) \quad (7)$$

Similarly, we can get $A(x,t)$, for $(i\text{-}1)\tau < t \leq i\tau$ as,

$$A(x, t) = \Pr(X(t) < L | X_{(i-1)\tau}) = F_{X(t-(i-1)\tau)}(L - x - X_{(i-1)\tau}) \quad (8)$$

The valve will fail to function when the degradation level reaches or overpasses a predefined critical threshold L. PFD_{avg}, the widely measure of a low demand SIS, is not the long-term approximation here, but the average proportion of time where the system is not able to perform the required safety function within one test interval [1]. PFD_{avg} in the first test interval is

$$\text{PFD}^1_{\text{avg}} = \frac{\int_0^\tau \bar{A}(x, t)dt}{\tau} = \frac{\int_0^\tau 1 - A(x, t)dt}{\tau} = 1 - \frac{\int_0^\tau F_{X(t)}(L - x)dt}{\tau} \quad (9)$$

While PFD_{avg} in the second interval $(\tau, 2\tau)$ with known degradation level μ at time τ can be calculated as

$$\text{PFD}^2_{\text{avg}} = \frac{\int_\tau^{2\tau} \bar{A}(x, t)dt}{\tau} = 1 - \frac{\int_\tau^{2\tau} F_{X(t-\tau)}(L - x - \mu)dt}{\tau} \quad (10)$$

Similarly, PFD_{avg} in the i th interval can be calculated using Eq. (8).

$$\text{PFD}^i_{avg} = \frac{\int_{(i-1)\tau}^{i\tau} \bar{A}(x, t)dt}{\tau} = 1 - \frac{\int_{(i-1)\tau}^{i\tau} F_{X(t-(i-1)\tau)}(L - x - X_{(i-1)\tau})dt}{\tau} \quad (11)$$

Each SIF should comply with the specific SIL. IEC 61,508 [2] specifies four SILs, with SIL4 most strict in terms of safety. SILs and their associated values of PFD_{avg} are shown in Table 2.

To estimate degradation of the SIS element in each test interval, Monte Carlo simulation is implemented here by generating random events to obtain the probability distributions for the variables of the problem. A number of papers can be found using Monte Carlo methods in the domains of reliability, availability, maintainability and safety (RAMS) [40–43].

The main idea here is to randomly generate M degradation paths to simulate M possible components and use the average value in each test interval to estimate the performance.

4. Evaluation and optimization of maintenance strategies

4.1. Optimization criteria

As mentioned in Eq. (4), the cost is a function of several parameters, including failure threshold, L, test interval, τ, PM coefficient factors (ω_a, ω_b). It is difficult to obtain exact values of cost parameters [44], especially those related with production loss of shutdown process and the potential effects of hazardous event due to the failure of a SIS. Therefore, cost ratios, instead of absolute costs, are used here in optimization. Taking C_{PT} as the unit cost, C_D, C_{CM}, C_{PM}, can be expressed as k_1C_{PT}, k_2C_{PT}, and k_3C_{PT} respectively, where $k_1 > k_2 > k_3 \geq 1$.

For a SIS, the optimal (ω_a, ω_b) should find a trade-off between the minimum lifetime cost and the required SIL. For an ESD valve as an example, its required SIL is SIL3 (see Table 2), meaning that PFD_{avg} should be in the range of $(10^{-4}, 10^{-3})$.

Table 2
SILs for low demand SISs, from [2].

IL	PFD_{avg}
SIL4	10^{-5}~10^{-4}
SIL3	10^{-4}~10^{-3}
SIL2	10^{-3}~10^{-2}
SIL1	10^{-2}~10^{-1}

Table 3
Parameter values for system analysis.

Parameter	Value
L	1.25×10^{-3}
α	1.02×10^{-4}
β	1.2×10^{4}
τ	8760
λ_{de}	2.5×10^{-5}
N_i	20
C_T	1
k_1	1×10^{5}
k_2	10
k_3	5

4.2. Numerical example

To illustrate the proposed method for optimizing maintenance strategy, a numerical example is employed with the degradation and operation parameters listed in Table 3.

4.2.1. Instantaneous availability

The degradation level $X(t)$, availability $A(t)$ and PFD_{avg} of such an element can be plotted based on Eq. (1), Eqs. (6)–(8) and Eqs. (9)–(11) respectively, as depicted in Fig. 2.

At the starting point, $X_0 = 0$, and $A(0) = 1$. With time elapsing, the degradation level $X(t)$ is accumulating, meanwhile, $A(t)$ is decreasing and PFD_{avg} is increasing. Given the periodic proof tests, the system status will be updated after each proof test. $A(t)$ curve has a certain periodicity but $A(t)$ reduces faster due to the accumulation of degradation. PFD_{avg} curve indicates that even the valve is functioning at each proof test, PFD_{avg} is increasing with time. It implies that the final element is becoming more fragile compared to that at the beginning. Given that the accumulated degradation level, $X(t)$, exceeds PM threshold, $\omega_a L$, at 8τ, a PM is applied. After that, the degradation level is set back to $\omega_b L$, the correspondingly instantaneous availability is improved. In other words, the SIS goes back to a situation performing its SIF well. But due to the existing degradation, PFD_{avg} is still higher than that in the first test interval. At 12τ, the degradation level $X(t)$ goes beyond failure threshold L, and then replacement is executed. The system availability, $A(t)$, is improved while PFD_{avg} decreases as low as the first test interval. Another similar process is the execution of a PM at 18τ.

4.2.2. Scenarios with different maintenance strategies

With the parameters given in Table 3, the expected cumulative costs in 20τ under three scenarios are compared:

(1) Scenario 1: The valve is only be repaired as-good-as-new once the failure has occurred, $\omega_a = 1$, $\omega_b = 0$.
(2) Scenario 2: The initial state is $X_0 = \omega_b L$ ($\omega_b \neq 0$), the system is repaired to as-good-as-new $X_0 = \omega_b L$ ($\omega_b \neq 0$) for both PM and CM with $\omega_a = 0.8$, $\omega_b = 0.1$.
(3) Scenario 3: The initial state is $X_0 = 0$, under the proposed maintenance strategy with $\omega_a = 0.8$, $\omega_b = 0.1$.

Two maintenance strategies are considered: One is reflected by Scenario 1, without PM; the other is reflected by Scenarios 2 and 3, with PMs. For the latter two, they are indicating different initial degradations occurred in manufacturing or installation. More specially, Scenario 3 means higher manufacturing and installation quality.

With the parameters in Table 3, the cost curves of these 3 scenarios are obtained as shown in Fig. 3.

It can be found that maintenance costs of the three scenarios are

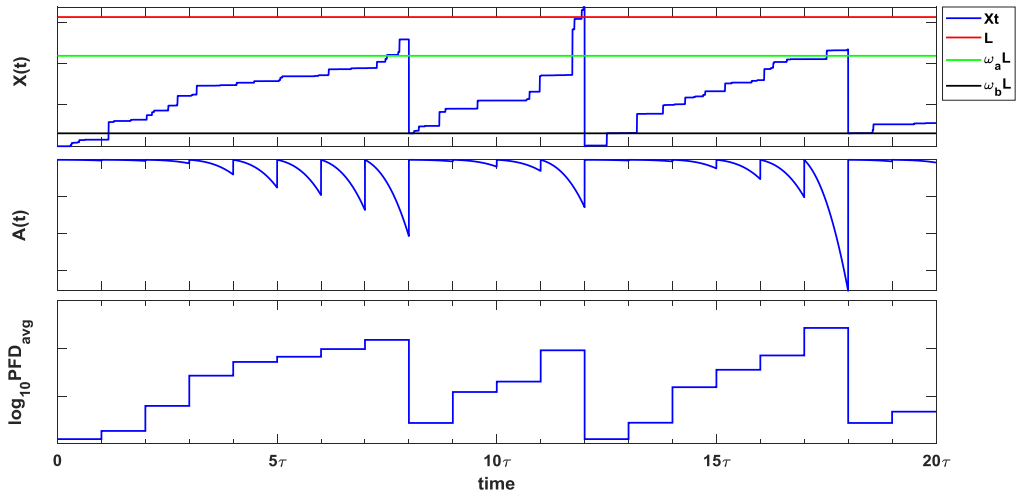


Fig. 2. A possible degradation path $X(t)$and the corresponding$A(t)$ and PFDavg.

almost same until around 10τ. By this time, PM or CM is seldom carried out. Then the cost of Scenario 1 increases significantly mainly due to the potential downtime cost. For Scenarios 2 and 3, their cost curves are very similar, with that of Scenario 2 a bit higher. By comparing the cumulative costs of Scenario 1 and Scenarios 2&3 in the total 20 test intervals, it can be found that PMs reduce the total lifetime cost dramatically, but the cost difference between Scenario 2 and Scenario 3 is quite small.

The PFD_{avg} values of the SIS in different scenarios are shown in Fig. 4. At beginning, PFD_{avg} increases with time (app. by 10τ) because of the continuous degrading process. For Scenario 1, PFD_{avg} still increases after 10τ without PM and the SIS is within SIL1 most time, while for Scenarios 2 and 3, PFD_{avg} is always lower, no worse than SIL2. Obviously, PMs improve SIS availability effectively, especially after the half of designed service time.

In practices, due to materials or mis-operation in the manufacturing or installation process, zero degradation is too ideal for a valve even it is new. In comparison of Scenarios 2 and 3, initial degradation is only found a slight negative effect on performance during the overall cycle. When rescheduling proof tests, it is not necessary to prioritize the considering of initial degradation.

4.2.3. Effect of PM strategies on lifetime costs

With the parameters in Table 3, the expected maintenance cost of the final element is calculated based on Eq. (4). The expected lifetime cost is a function of (ω_a,ω_b) with different (k_2, k_3) as shown in Fig. 5.

The CM cost is fixed as $k_2 = 10$, and Fig. 5 illustrates the impact of k_3 on the lifetime cost, i.e., the expensiveness of PMs. In general, when k_3 is larger, a PM is more costly, and the lifetime cost in 20 test intervals increases as well.

In Fig. 5(a), $k_3 = 1$ means that PM cost is very low, same as the test cost. Given a fixed ω_a, the total lifetime cost slightly increases with respect to ω_b. Even the higher ω_b can lead to more PMs, but due to the quite low PM cost in each time, the expected lifetime cost almost keeps unchanged under the same ω_a. However, given a fixed ω_b, the expected lifetime cost increases significantly with ω_a. When ω_a closes to 1, it means that the PM threshold $\omega_a L$ is near the failure threshold L, namely PMs are being avoided. CM cost is thus dominant for the increasement of lifetime cost.

In Fig. 5(b), compared to CM cost, PM cost is still quite low, so the overall tendency of lifetime cost is similar to that shown in Fig. 5(a). Within this assumed range of k_3 and (ω_a,ω_b), it can be obtained that the optimal value of (ω_a,ω_b) is (0.70,0).

In Fig. 5(c) and Fig. 5(d), PMs are more expensive. The lifetime cost increases with respect to ω_b, while decreases firstly and then increases with respect to ω_a. There is a trade-off between PM cost and the potential downtime cost. Because a smaller ω_a increases the PM expenses, but it results in a higher failure possibility that can increase CM and downtime costs. This phenomenon becomes more obvious in Fig. 5(d) when PM cost is equivalent to 80% CM cost.

For both Fig. 5(c) and Fig. 5(d), it is necessary to find an optimal (ω_a, ω_b) under the certain parameters. With calculation, the optimal

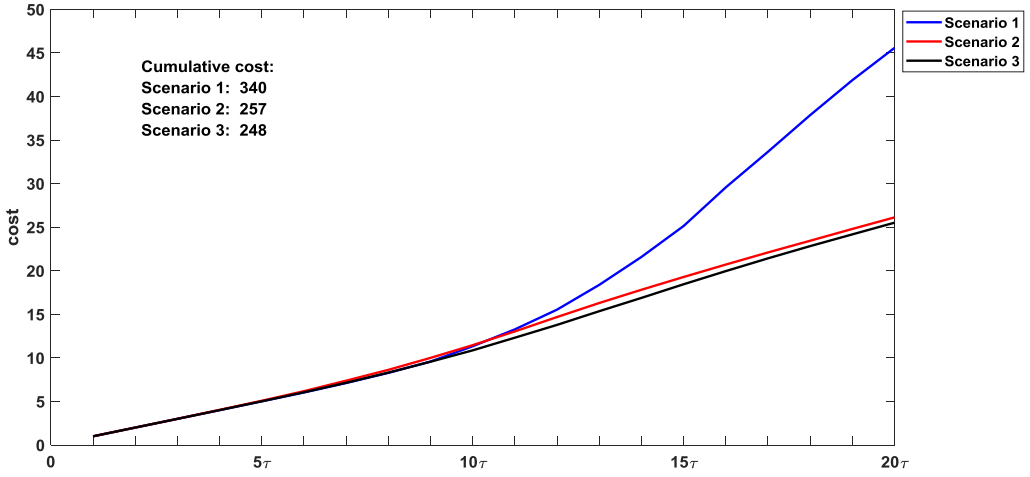


Fig. 3. Cumulative cost under different scenarios.

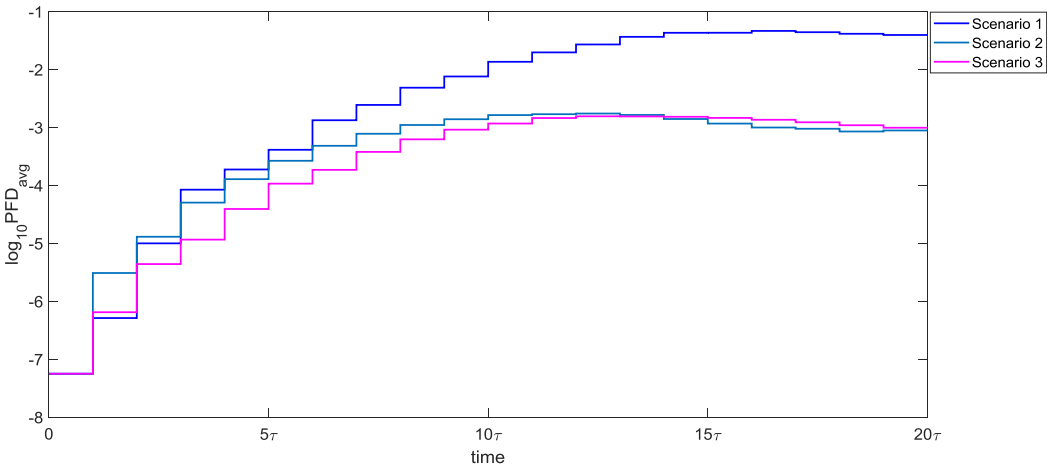


Fig. 4. PFD_{avg} under different scenarios.

(ω_a, ω_b) is (0.75, 0) in Fig. 5(c), while the optimal (ω_a, ω_b) is (0.80, 0) in Fig. 5(d).

The findings can help the decision-making of maintenance crew of SISs. If PM costs are much lower than those led by a SIS failure, it is reasonable to take more PMs to keep the system safe. Otherwise, if PM costs are close to CM costs, many PMs are not essential.

However, we have an assumption so far that PM cost is same no matter what the value of ω_b is. In practices, when a system is aging, the PM cost often increases as well. The PM factor ω_b should link with system installation time and actual healthy status.

Meanwhile, the effects of failure threshold, L, and PM parameter, ω_a, on the lifetime cost are analyzed. The values of L are set as $[1.05,1.15,1.25,1.35,1.45] \times 10^{-3}$ respectively, and then lifetime cost of the final element is calculated with the result shown in Fig. 6.

When $L = 1.45 \times 10^{-3}$, the lifetime cost has minor increase from $\omega_a = 0.7$ to $\omega_a = 0.9$. This is because such a threshold is so high that

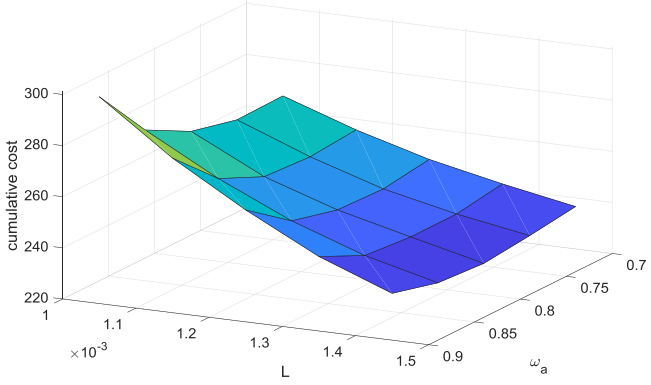
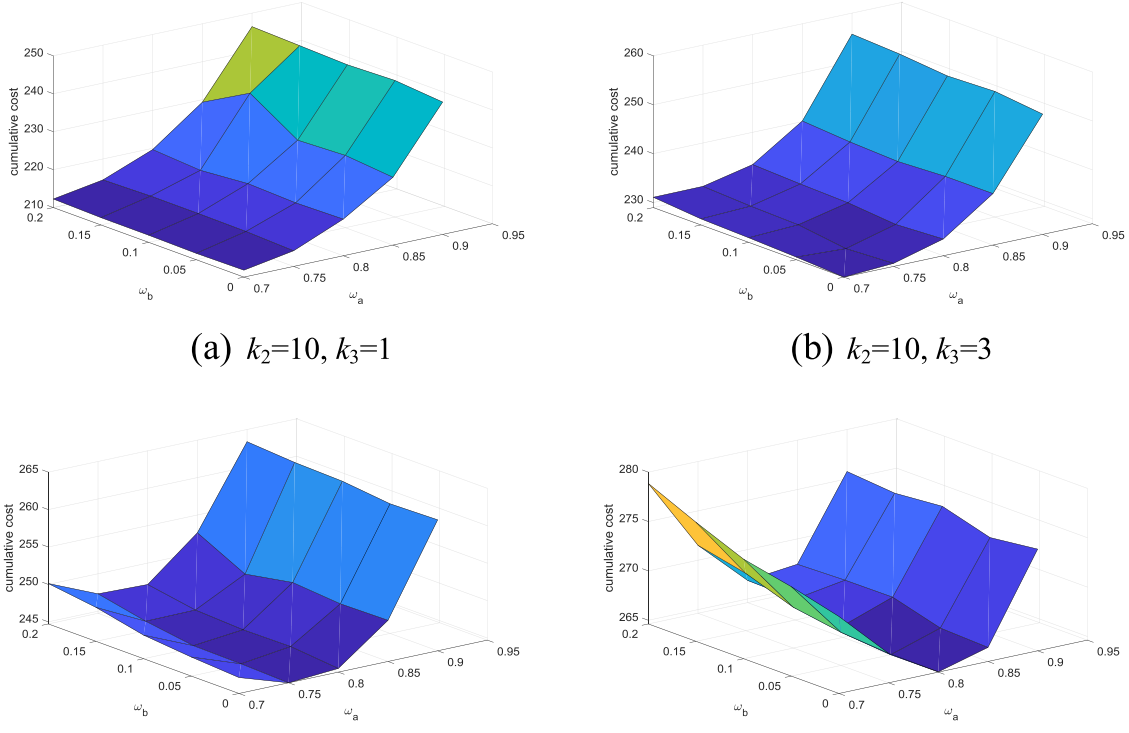


Fig. 6. Expected maintenance cost.



(a) k_2=10, k_3=1 (b) k_2=10, k_3=3

(c) k_2=10, k_3=5 (d) k_2=10, k_3=8

Fig. 5. Mesh plot the expected total maintenance cost on (k_2, k_3).

the chance of a failure event is very low. When the value of L is lower, e.g. 1.05×10^{-3}, the lifetime cost differences between the solutions of $\omega_a = 0.7$ and $\omega_a = 0.9$ is more apparent. For lower failure threshold with higher value of ω_a, the degradation level can exceed the failure threshold with higher possibility.

Given a fixed ω_a, the lifetime cost decreases with a higher threshold L, because a smaller threshold L will increase downtime.

The failure threshold L can be affected by manufacturing process and risk acceptance criteria. In manufacturing, high-quality material could lead to higher degradation-tolerant threshold. In operations, when it is acceptable to tolerate more risks to the EUC, the failure threshold also could be set higher.

In determining the optimal value of ω_a, failure threshold should also be considered. When the failure threshold is quite high, from the perspective of maintenance cost, ω_a could be set a higher value as of the low failure probability.

4.2.4. Effects of PM strategies on PFDavg

Here we study how PM strategies with different (ω_a, ω_b) influence PFD_{avg}.

The PFD_{avg} of such a SIS can be obtained using simulation based on Eqs. (9)–(11). PFD_{avg} in each test interval is illustrated in Fig. 7.

It is obvious that the PFD_{avg} has a strong correlation with parameters, (ω_a, ω_b).

The effect of ω_a on PFD_{avg} in Fig. 7(a) is analyzed with setting with $\omega_b = 0.1$. At early stage, for example, t is around $t = 8\tau$, PFD_{avg} increases over time but still remains within SIL3. After 8τ, PFD_{avg} falls into SIL2 for $\omega_a = 0.9$. PFD_{avg} starts to keep stable in each interval and just fluctuates in a small range (same SIL). These curves show that the value of PFD_{avg} in each test interval decreases with ω_a. With the lower ω_a, the earlier PM will be taken. After a PM, the degradation is mitigated so that the probability of failure is reduced.

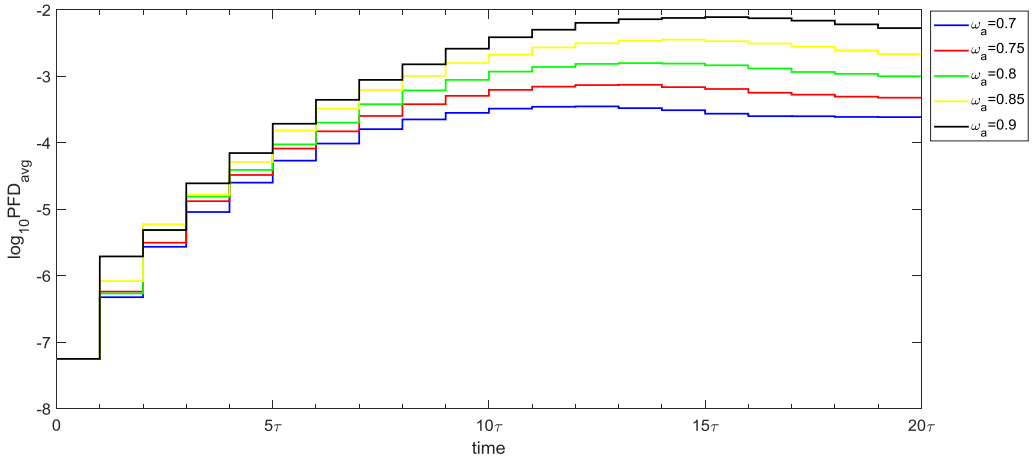
The effect of parameter ω_b on PFD_{avg} in Fig. 7(b) is evaluated with $\omega_a = 0.75$. Compared to ω_a, parameter ω_b has slight impact on system PFD_{avg}.

The combined effect of (ω_a, ω_b) on system PFD_{avg} in several intervals are then depicted in Fig. 8.

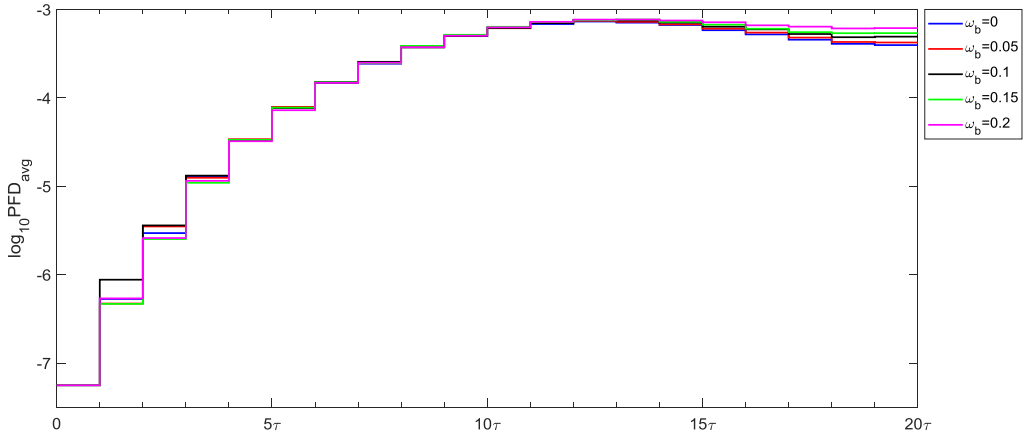
The overall tendency of PFD_{avg} in each test interval is almost same. Meanwhile, PFD_{avg} in each test interval is limited mainly in SIL3 and SIL2. Give a fixed ω_b, PFD_{avg} increases with ω_a. However, given a fixed ω_a, PFD_{avg} keeps almost the same value for different ω_b.

The values of failure threshold L are set $[1.05,1.15,1.25,1.35,1.45] \times 10^{-3}$, respectively, to observe the effect of threshold on PFD_{avg}. The mesh plot is shown in Fig. 9.

Given a same threshold L, PFD_{avg} is going down with lower ω_a. This finding can be regarded as a guideline for maintenance management. For the same SIS, the earlier the PM is executed, the more liable the system is. Without considering the PM cost, ω_a should be as small as



(a) Parameter ω_a effect on PFDavg



(b) Parameter ω_b effect on PFDavg

Fig. 7. (ω_a, ω_b) effect on PFDavg of the system in every test interval.

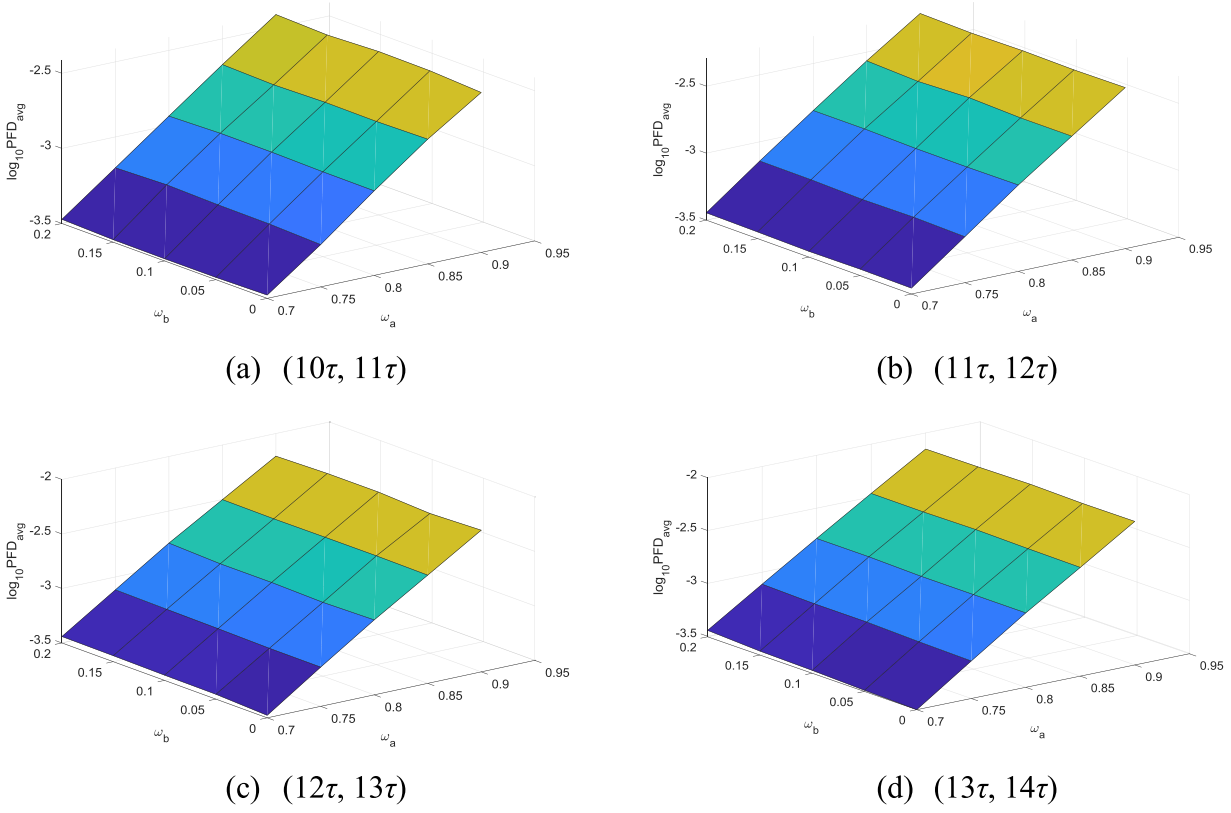


Fig. 8. Mesh plot PFD_{avg} in several intervals.

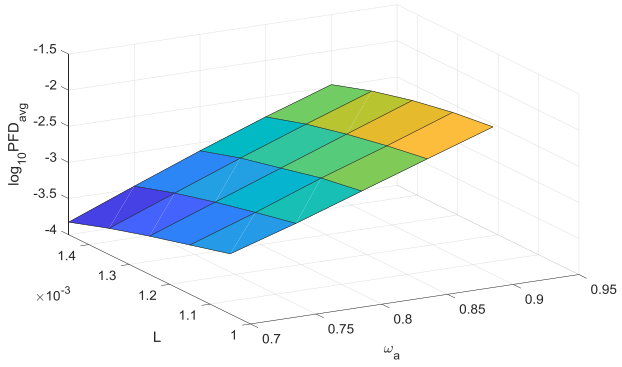


Fig. 9. Mesh plot PFD_{avg} on failure threshold $L$and ω_a.

possible.

Meanwhile, for a fixed ω_a, PFD_{avg} is going up with lower threshold L. For threshold $L = 1.45 \times 10^{-3}$, $\omega_a = 0.8$ is enough for the system to be limited within SIL3, whereas, $\omega_a = 0.7$ should be taken for $L = 1.05 \times 10^{-3}$.

5. Updating test intervals with the information from tests

For low demand SISs, it might not be always worthwhile running proof tests periodically, especially if the shutdown and restart of process is costly. In this case, the date of the next proof test can be determined based on degradation state observed in the current test. Interval to the next test can be longer if the SIS element is very healthy, and the interval should be shorter as the element deteriorates. When the degradation level is closing to PM threshold, more tests are expected.

Having considered degradation and diverse maintenance strategies, it is interesting to introduce non-periodic proof tests. According to the study of [45], to keep system safety, 3 years is roughly set as the maximum length of a proof test interval.

In consideration of degradations, PM parameters are set as $\omega_a = 0.75$ and $\omega_b = 0.05$. The general expected test interval length is generated by Monte Carlo simulation.

The main steps of simulation algorithm for the expected test intervals are shown here.

- Step 1: Set $X_t = 0$ and $N = 1$. If $N \leq N_{\max}$ the process goes to steps.
- Step 2: Generate n degradation paths. Then the arrival time of the first reach failure threshold L can be obtained.
- Step 3: Get the 5-th percentile value as potential arrival time τ_1. Compare τ_1 and 3 years. If $\tau_1 < 3$ years, then take τ_1 as the new test interval of the system; if $\tau_1 \geq 3$ years, then 3 years are used as the new test interval.
- Step 4: Use the mean value and variance of Gamma process in Section 2.2 to estimate the increment $X_{0\sim\tau 1}$ between (0, τ_1). At the same time, safety margin is also considered. The 97.5-th percentile ($\rho = 0.975$) is used as the potential increment in (0, τ_1).
- Step 5: Compare the potential degradation level at time τ_1, $X_{\tau 1}$, with PM threshold or CM threshold to decide whether a maintenance strategy is required here. The $X_{\tau 1}$ after comparison is the new starting point.
- Step 6: Repeat Step 2∼ Step 5 and set $N = N + 1$.

The time to failure threshold L from $X_t = 0$ is verified to follow normal distribution. Different increment percentiles are investigated as the result shown in Table 4.

The updated general lengths of each test interval are listed in Table 4. We can see that with different percentile values, test interval length becomes different from the third updated test. With $\rho = 0.975$, a PM is executed after the second interval and the degradation is mitigated. When ρ is set as 0.90 or 0.825, the third test interval is shorter with the length of 0.5τ and 1.2τ, respectively.

It is worth mentioning that the degradation parameters (α, β) affect

Table 4
Updated test intervals under different increment percentiles.

	1st	2nd	3rd	4th	5th	6th	7th	8th
$P = 0.975$	$(0, 3\tau)$	$(3\tau, 6\tau)$	$(6\tau, 9\tau)$	$(9\tau, 11.5\tau)$	$(11.5\tau, 14.5\tau)$	$(14.5\tau, 17\tau)$	$(17\tau, 20\tau)$	$(20\tau, 22.5\tau)$
$P = 0.90$	$(0, 3\tau)$	$(3\tau, 6\tau)$	$(6\tau, 6.5\tau)$	$(6.5\tau, 9.5\tau)$	$(9.5\tau, 12.5\tau)$	$(12.5\tau, 15.5\tau)$	$(15.5\tau, 18.5\tau)$	$(18.5\tau, 21.5\tau)$
$P = 0.825$	$(0, 3\tau)$	$(3\tau, 6\tau)$	$(6\tau, 7.2\tau)$	$(7.2\tau, 10.2\tau)$	$(10.2\tau, 13.2\tau)$	$(13.2\tau, 14.2\tau)$	$(14.2\tau, 17.2\tau)$	$(17.2\tau, 20.2\tau)$

*$\tau = 8760\ h = 1\ year$.

the degradation rate directly. The simulation results in Table 4 are based on assumed (α, β) in Table 3. It only acts as a reference method for updating test intervals.

If the exact degradation level μ can be observed in each proof test. When updating the test lengths, the main constraint is the required SIL. Considering the degradation process, the first interval τ_1 can be calculated based on Eq. (12) with the given limit values of $\mathrm{PFD}_{\mathrm{avg}}$.

$$\mathrm{PFD}_{\mathrm{avg}}^{1} = \frac{1}{\tau_1}\int_0^{\tau_1} \bar{A}(t)dt = \frac{1}{\tau_1}\int_0^{\tau_1} \Pr(X(t) > L)dt \tag{12}$$

For calculating the second interval, the degradation level μ_1 at τ_1 is taken into consideration.

$$\mathrm{PFD}_{\mathrm{avg}}^{2} = \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} \bar{A}(t)dt = \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} \Pr(X(t) > L | X_{\tau_1} = \mu_1)dt \tag{13}$$

Using Eq. (13), the value of τ_2 can also be updated. By following the similar solution process for the latter intervals, the flexible test interval can be calculated and updated.

6. Conclusion

A stochastic process-based availability analysis for the final element of a SIS is carried out, and three states of the element are considered. This forms the basis for determining the maintenance strategies following proof tests. The algorithms of instantaneous availability of the SIS element and expected lifetime cost in the SIS operation are developed. $\mathrm{PFD}_{\mathrm{avg}}$ of the SIS element is calculated based on the homogeneous gamma process.

The findings in the case studies have shown that PM strategies, i.e. the optimal values of (ω_a, ω_b), and the expensiveness of PMs to CMs, are influential factors of the lifetime cost and SIL of a SIS.

$\mathrm{PFD}_{\mathrm{avg}}$ of the SIS is affected by the PM threshold ω_a significantly, especially after half of the service lifetime, but not too much affected by ω_b. Effects of ω_a on $\mathrm{PFD}_{\mathrm{avg}}$ are becoming more obvious with lower threshold L. When the failure threshold L is quite high, the value of ω_a has slight effects on $\mathrm{PFD}_{\mathrm{avg}}$ given the low possibility of failure.

Based on the above findings, suggestions on updating test intervals are given. Maintenance crews can be beneficiary of these suggestions, by saving maintenance costs through reducing frequency of proof tests.

For further studies, it would be interesting to consider the availability and maintenance cost on k-out-of-n architectures.

Declaration of Competing Interest

The authors declared that they have no conflicts of interest to this work. We declare that we do not have any commercial or associate interest that represents a conflict of interest in connection with the submitted manuscript, which entitled, 'Optimization of maintenances following proof tests for the final element of a safety-instrumented system'.

Acknowledgement

The authors acknowledge the financial support provided by China Scholarship Council (201706440015), and the secondment opportunities for joint research provided by the RISEN project (No 691135) under EU Marie Curie RISE program.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ress.2019.106779.

References

[1] Rausand M. Reliability of safety-critical systems: theory and applications. John Wiley & Sons; 2014.
[2] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.
[3] Hauge S, Kråknes T, Håbrekke S, Jin H. Reliability prediction method for safety instrumented systems - PDS Method handbook 2013 edition. 2013.
[4] Bukowski JV. A comparison of techniques for computing PFD average. Annu Reliab Maintainab Symp 2005:590–5.
[5] Mechri W, Simon C, Bicking F, Othman KB. Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment. J Loss Prev Process Ind 2013;26:594–604. https://doi.org/10.1016/j.jlp.2012.12.002.
[6] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab Eng Syst Saf 2015;133:212–22. https://doi.org/10.1016/j.ress.2014.09.005.
[7] Zhang N, Fouladirad M, Barros A. Optimal imperfect maintenance cost analysis of a two-component system with failure interactions. Reliab Eng Syst Saf 2018. https://doi.org/10.1016/j.ress.2018.04.019.
[8] Liu Y, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prev Process Ind 2011;24:49–56.
[9] Liu Y, Rausand M. Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems. Reliab Eng Syst Saf 2016;145:366–72. https://doi.org/10.1016/j.ress.2015.06.016.
[10] Liu Y. Discrimination of low-and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability. Proc Inst Mech Eng Part O J Risk Reliab 2014;228(4):409–18.
[11] Wu S, Zhang L, Lundteigen MA, Liu Y, Zheng W. Reliability assessment for final elements of SISs with time dependent failures. J Loss Prev Process Ind 2018;51:186–99. https://doi.org/10.1016/j.jlp.2017.12.007.
[12] Rogova E, Lodewijks G, Lundteigen MA. Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates. Proc Inst Mech Eng Part O J Risk Reliab 2017;231:373–82. https://doi.org/10.1177/1748006x17694999.
[13] Wu S, Zhang L, Barros A, Zheng W, Liu Y. Performance analysis for subsea blind shear ram preventers subject to testing strategies. Reliab Eng Syst Saf 2018;169:281–98. https://doi.org/10.1016/J.RESS.2017.08.022.
[14] Innal F, Lundteigen MA, Liu Y, Barros A. PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models. Reliab Eng Syst Saf 2016;150:160–70. https://doi.org/10.1016/J.RESS.2016.01.022.
[15] Langeron Y, Barros A, Grall A, Bérenguer C. Combination of safety integrity levels (SILs): a study of IEC61508 merging rules. J Loss Prev Process Ind 2008;21:437–49. https://doi.org/10.1016/J.JLP.2008.02.003.
[16] Srivastav H, Guilherme AV, Barros A, Lundteigen MA, Pedersen FB, Hafver A, et al. Optimization of periodic inspection time of SIS subject to a regular proof testing. Safety and reliability–safe societies in a changing world–proceeding of the 28th International. European. safety and reliability conference ESREL 2018. 2018.
[17] Zhou Y, Ma L, Mathew J. A non-gaussian continuous state space model for asset degradation. Proceeding 3rd world congress on engineering asset management intelligence maintaince system conference 1(1). 1. 2008. p. 1981–92.
[18] Wang Q, Liu W, Zhong X, Yang J, Yuan Q. Development and application of equipment maintenance and safety integrity management system. J Loss Prev Process Ind 2011;24:321–32. https://doi.org/10.1016/j.jlp.2011.01.008.
[19] Zio E. Some challenges and opportunities in reliability engineering. IEEE Trans Reliab 2016;65:1769–82. https://doi.org/10.1109/TR.2016.2591504.
[20] Rausand M, Høyland A. System reliability theory: models, statistical methods, and applications. John Wiley & Sons; 2004.
[21] Lundteigen MA, Rausand M. Partial stroke testing of process shutdown valves: how to determine the test coverage. J Loss Prev Process Ind 2008. https://doi.org/10.1016/j.jlp.2008.04.007.
[22] Fouladirad M, Grall A. Condition-based maintenance for a system subject to a non-homogeneous wear process with a wear rate transition. Reliab Eng Syst Saf 2011;96:611–8. https://doi.org/10.1016/J.RESS.2010.12.008.

[23] Mercier S, Pham HH. A preventive maintenance policy for a continuously monitored system with correlated wear indicators. Eur J Oper Res 2012;222:263–72. https://doi.org/10.1016/J.EJOR.2012.05.011.
[24] Deloux E, Castanier B, Bérenguer C. Predictive maintenance policy for a gradually deteriorating system subject to stress. Reliab Eng Syst Saf 2009;94:418–31. https://doi.org/10.1016/J.RESS.2008.04.002.
[25] Zhu W, Fouladirad M, Bérenguer C. Condition-based maintenance policies for a combined wear and shock deterioration model with covariates. Comput Ind Eng 2015;85:268–83. https://doi.org/10.1016/J.CIE.2015.04.005.
[26] Huynh KT, Grall A, Bérenguer C. A parametric predictive maintenance decision-making framework considering improved system health prognosis precision. IEEE Trans Reliab 2019;68:375–96. https://doi.org/10.1109/TR.2018.2829771.
[27] Castro I, Barros A, Grall A. Age-based preventive maintenance for passive components submitted to stress corrosion cracking. Math Comput Model 2011. https://doi.org/10.1016/j.mcm.2011.03.003.
[28] Huynh KT, Castro IT, Barros A, Berenguer C. On the use of mean residual life as a condition index for condition-based maintenance decision-making. IEEE Trans Syst Man, Cybern Syst 2014. https://doi.org/10.1109/TSMC.2013.2290772.
[29] Huynh K, Barros A, Bérenguer C, Castro I. A periodic inspection and replacement policy for systems subject to competing failure modes due to degradation and traumatic events. Reliab Eng Syst Saf 2011;96:497–508. https://doi.org/10.1016/j.ress.2010.12.018.
[30] Hosktad P., Håbrekke S., Johnsen R., Sangesland S. Ageing and life extension for offshore facilities in general and for specific systems. 2010.
[31] Medjaher K, Skima H, Zerhouni N. Condition assessment and fault prognostics of microelectromechanical systems. Microelectron Reliab 2014. https://doi.org/10.1016/j.microrel.2013.09.013.
[32] Travé-Massuyès, L., Pons, R., Ribot, P., Pencolé, Y., & Jauberthie C.Condition-based monitoring and prognosis in an error-bounded framework. DX@ Safeprocess, 2015, p. 83–90.
[33] Singpurwalla ND. Survival in dynamic environments. Stat Sci 2007. https://doi.org/10.1214/ss/1177010132.
[34] Huynh KT, Langeron Y, Grall A. Degradation modeling and RUL estimation of deteriorating systems in S-Plane. IFAC-PapersOnLine 2017. https://doi.org/10.1016/j.ifacol.2017.08.2036.
[35] van Noortwijk JM. A survey of the application of gamma processes in maintenance. Reliab Eng Syst Saf 2009. https://doi.org/10.1016/j.ress.2007.03.019.
[36] Blain C, Barros A, Grall A, Lefebvre Y. Modelling of stress corrosion cracking with stochastic processes - Application to steam generators. Proceeding of the European safety reliability conference. 2007, ESREL 2007 - risk, reliability society and safety. 2007.
[37] Grall A, Bérenguer C, Dieulle L. A condition-based maintenance policy for stochastically deteriorating systems. Reliab Eng Syst Saf 2002;76:167–80. https://doi.org/10.1016/S0951-8320(01)00148-X.
[38] Van P D, Bérenguer C. Condition-based maintenance with imperfect preventive repairs for a deteriorating production system. Qual Reliab Eng Int 2012;28:624–33. https://doi.org/10.1002/qre.1431.
[39] Mercier S, Pham HH. A condition-based imperfect replacement policy for a periodically inspected system with two dependent wear indicators. Appl Stoch Model Bus Ind 2014;30:766–82. https://doi.org/10.1002/asmb.2011.
[40] Barata J, Soares CG, Marseguerra M, Zio E. Simulation modelling of repairable multi-component deteriorating systems for “on condition” maintenance optimisation. Reliab Eng Syst Saf 2002. https://doi.org/10.1016/S0951-8320(02)00017-0.
[41] Lin Y, Li Y, Zio E. A comparison between Monte Carlo simulation and finite-volume scheme for reliability assessment of multi-state physics systems. Reliab Eng Syst Saf 2018. https://doi.org/10.1016/j.ress.2018.01.008.
[42] Malefaki S, Koutras VP, Platis AN. Multi-state deteriorating system dependability with maintenance using Monte Carlo simulation. Proceeding. - 2nd international symposium on stochastic models in reliability engineering life sciences operations management SMRLO 2016 2016. https://doi.org/10.1109/SMRLO.2016.21.
[43] Nadjafi M, Farsi MA, Jabbari H. Reliability analysis of multi-state emergency detection system using simulation approach based on fuzzy failure rate. Int J Syst Assur Eng Manag 2017. https://doi.org/10.1007/s13198-016-0563-7.
[44] Alaswad S, Xiang Y. A review on condition-based maintenance optimization models for stochastically deteriorating system. Reliab Eng Syst Saf 2017;157:54–63. https://doi.org/10.1016/j.ress.2016.08.009.
[45] Hauge S., Lundteigen M.A., Onshus T., Bodsberg L. Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase PDS -multiclient safety sikkerhet operation drift. 2008.