Reliability Engineering and System Safety 209 (2021) 107393

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state

Aibo Zhang [a], Himanshu Srivastav [a], Anne Barros [b], Yiliu Liu [a,*]

[a] Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway
[b] CentraleSupelec, Paris Saclay University, France

ARTICLE INFO

Keywords:
Safety-instrumented system
Degrading final element
Imperfect state revealing
Testing and maintenance strategy
performance analysis

ABSTRACT

Safety-instrumented systems (SISs) have been widely installed to lower risks of equipment/ process by performing the designed safety functions in cases of demands. Final elements remain dormant mostly in a low demand mode but become vulnerable due to degradation along with time. Tests and maintenances are key activities to prevent the SIS from any failures, including those thank to degradation, to activate upon demands. This paper models the degradation of SIS final elements by considering an intermediate degraded state between the working- and failed states. Sometimes, the actual system states are not distinguished perfectly during proof tests. Such imperfectness in state revealing, consequently, weakens the real performance of follow-up maintenances. The effects of imperfect degradation state revealing are quantified, together with three testing and maintenance strategies for 1-out-of-2 configured SISs. Time-dependent PFD of the system and cumulative life-cycle cost are then estimated in a finite service time. Numerical examples under proposed strategies are presented to provide clues in selection of optimal testing and maintenance strategies for 1oo2 final element in SISs.

1. Introduction

Safety-instrumented systems (SISs) are widely applied in different industries to detect the onset of hazardous event and/or to mitigate their consequences, such as emergency shutdown (ESD) systems on an oil & gas production platform, high pressure protection systems (HIPPSs) in the process industry. Normally, a SIS consists of sensor(s) (e.g. pressure transmitters), logic solver(s) and final element(s) (e.g. shutdown valves) [1,2].

Both ESD and HIPPS are typical SISs operating in a low demand mode, where the activation frequency is less than once per year in general. Some failure modes of final elements will stay hidden until a proof test is executed or an undesired event occurs on the equipment under control (EUC) by the SIS [2]. These hidden failures are called dangerous undetected (DU) failures if they can lead to dangerous events with severe consequences. Redundant structures are often used in SISs to improve the system availability and so to enhance safety. IEC 61508 [3] recommends the average probability of failure on demand (PFD_{avg}) as a measure in the performance evaluation of SISs in the low demand mode.

Some widely used methods have been developed for the calculation of PFD_{avg}, including simplified formulas [1,2,4], fault tree analysis [5–8], Markov methods [9–13], Bayesian methods [14–16], Petri Nets [17–19] and AltaRica modeling [20]. The common for most of these methods is assumed that all elements in a SIS are as-good-as-new after a repair in case a DU is revealed in a proof test. Such an assumption is valid for electronic components with exponentially distributed lifetime, but its validity for mechanical component is in question.

There exists literature in abundance for reliability assessment of units like safety valves under various maintenance strategies such as as-bad-as-old(ABAO) under corrective maintenance or imperfect maintenance under preventive maintenance. The important assumption with these methods is binary state model [21–24].

The final execution elements of SISs, mainly consisted of mechanical components, may not always fail at a constant failure rate. They are rather vulnerable to creeping or other degradation processes [25]. In general, the reliability of a mechanical system decreases as the degradation processes develop [26], which contribute to a time-dependent failure rate. Thus, several dynamic reliability methods with advantage of represent time- and age-dependent performance have been applied to address degradation mechanisms of such mechanical components, e.g. stochastic process [27–29], multi-phase Markov process [9,11,30–32].

For SIS final elements with degradation, Mechri et al. [9] have considered the imprecision on the failure rates of components in

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

https://doi.org/10.1016/j.ress.2020.107393
Received 6 May 2020; Received in revised form 9 October 2020; Accepted 2 December 2020
Available online 16 December 2020

performance evaluation of the SIS in low demand using fuzzy multi-phase Markov process. Innal et al. [31] have generalized PFD_{avg} formulas by including partial and full periodic tests. Wu et al. [11] have conducted the time dependent unavailability analysis of blind shear ram preventers (BSRPs) by incorporating testing strategies into multi-phase Markov process. Three states for 1oo1 configuration have been considered, including functioning, failed and waiting for repair. Zhang et al. [29] have performed the PFD_{avg} of a 1oo1 configuration subjected to continuous aging degradation process. Different follow-ups based on the system state in proof test are considered. Srivastav et al. [32] have considered the negative effects of proof tests on SIS by adding discrete degraded states between working and failed state.

On the other hand, with the development of sensor technologies, more data about operation conditions and system status can be collected. Numerous parameters such as the lubricant ingredients, vibration signal, thermography picture, corrosion extent and so on can be measured and analyzed for failure prediction and diagnosis [33]. For example, a series of studies have been conducted on choke valve erosion based on the flow coefficient obtained from process parameters [34–37]. The deviation between actual value and reference value is regarded as one useful indicator for choke valve erosion. When the deviation is beyond the acceptable level, the valve is regarded to be failed.

Health indicators are helpful to implement condition-based maintenance on SISs, namely corresponding maintenance actions are conducted based on the observed states. After a proof test on a SIS final element, different following-ups are possible based on the system state of working, degraded or failed. The presence of the degraded state is beyond the scope of binary-state system analysis, and several studies have been conducted on such multi-state systems reliability analysis and maintenance optimization [38–43]. However, the existing literature relies on an assumption that system degradation state revealing is perfect [39,44,45]. This is not always right for SISs because the degradation level of a SIS is not observed directly in many cases but is determined by the difference between a reference value and an estimate value of status, while the estimated value is calculated from some relevant process parameters [34,37]. When the collected data in a proof test, e.g. by sensors, process conditions and media in valve, is imprecise or different from working conditions, these inaccurate measurements will be passed into the physical condition estimation for valves. These unintended errors can be amplified or diminished in calculation of actual status of valves. Errors can also come from inaccurate setting of the threshold between working and degradation [29].

Secondly, existing studies on testing strategies for redundant SISs mainly focus on addressing uncertainty [46] and common cause failures (CCFs) [2,5,47], neglecting degrading units and preventive maintenance policies. In this context of imperfect degradation revealing, it is worth studying to analyze how the degradation of a single unit affects the whole redundant structure under different testing strategies. In addition, the life-cycle cost of an SIS in the designed service time (e.g. 20 years) is more of interest, compared to existing studies focusing on the average long-run cost rate [48,49].

As a response, this paper is aiming to take potential imperfect state revealing into account of state-based SIS assessment, to make a comparison among different testing and maintenance strategies. The specific objectives include:

- Modeling and quantifying the imperfectness of state revealing in proof tests and their effects on the performance of redundant final elements in SISs.
- Evaluating condition-based maintenance strategies in the contexts where different testing approaches are used.
- Incorporating and balancing system availability and life cycle costs in seeking testing and maintenance strategies and providing guidance to operational decision-makers of SISs.

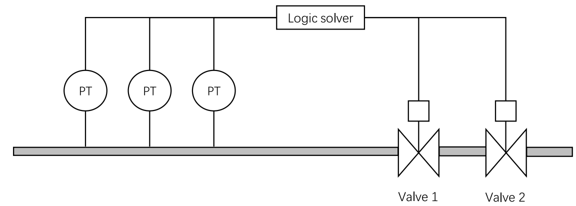


Fig. 1. Example of a HIPPS.

The remainder of this paper is organized as follows: Section 2 illustrates the characteristics of final elements in SIS, as well as the testing and maintenance strategies; Section 3 investigates the calculation of system PFD_{avg} and cumulative life-cycle cost given the certain assumptions; Section 4 conducts a numerical example to present the system performance and cumulative cost with state revealing coverage under different test and maintenance strategies and discusses the pros and cons of different strategies; Concluding remarks are given in Section 5.

2. System description

2.1. Structure and operations of a SIS

As mentioned, a typical SIS consists of sensor(s), logic solver(s) and final element(s). Without losing generality, a high pressure protection system (HIPPS) in oil & gas industry is used to study SIS operations and tests here, whose architecture is shown in Fig. 1. Two redundant shutdown valves (Valve 1 and 2), serving as the final elements in HIPPS, are installed on the same pipeline to stop the flow and relieve pressure in case the downstream pressure is too high. When one of two valves cannot be activated, the process, namely EUC, is still safe if the other valve works. Such kind of configuration is called as 1-out-of -2 (1oo2), which can improve system availability and so to enhance safety to some extent.

The performance measure of valves in HIPPS is expressed by an average probability that the item will not be able to perform its required safety function if the demand occurs, and it is denoted as Probability of Failure on Demand (PFD_{avg}) [2]. IEC 61508[3] specifies the requirement into four safety integrity levels (SILs), with SIL1 being the least reliable and SIL4 being the most reliable. To fulfill the requirements of a SIL, the SIS in low demand mode must have a PFD_{avg} in the corresponding interval.

Given the inevitable degradation mechanisms in valves, the actual performance of a mechanically final element always degrades along with time. Through the life-cycle of valves, at least three distinguishable states can be defined which are linked with the physical condition of system. (See Table 1.)

2.2. Proof test and maintenance strategies

Proof tests address the necessary functional safety requirements of SIS, including functions such as response time and leakage class of safety valves, with reflecting real conditions as accurately as possible. During a test it is possible to check the actual performance of valves, e.g. fully open/closed, the time to perform safety function and leakage rate in closed position. These kind of information can be employed as indirect indicators which provide us an opportunity to prognostics the valve condition [50].

In the designed phase of SISs, the final elements, such as valves, are allocated a target value with acceptable deviation to meet the specified performance requirement, e.g. leakage rate and closing time. When the leakage rate or closing time exceeds the acceptable deviation, as a safety barrier, the valve will not meet the performance requirements for risk mitigating of EUC. The corresponding failure modes are called 'leakage (through the valve) in a closed position (LCP)' and 'closing too

Table 1
System state definition.

State	Status	Notation	State description
1	Working	W	System is working as specified
2	Degraded	D	System has a degraded performance but still functioning
3	Failed	F	System has a fault and fails to function

slowly', respectively. In most cases, it is not possible to observe such kind of failure without activating the valve, so these failures are DU failures. When DU failure presents, the SIS will be into a fault state as losing the corresponding pre-designed safety function.

LCP failure mode is mainly caused by erosion on the gate or the seat [2]. Referring to the existing studies of erosion in valves, a series of work have been conducted on selection of performance indicator. A potential erosion indicator is the difference value between the calculated result from collected information and a reference value from vendor data sheet. Complied to the performance requirement of SIS, when the difference is too big, the valve is said to be failed (in a fault state).

Considering state classification and the updated status indicator after a proof test, the condition-based maintenance can be adopted to improve system performance: (1) no action if the difference value is quite small, it means the system is the working condition; (2) preventive maintenance (PM) is executed if the difference value is quite big but still within the required range, in this case, the performance is not satisfying even though is still kind of working; (3) corrective maintenance (CM) if the difference value exceeds the required range, namely, a DU is found (with respect to this particular function).

3. SIS modeling and performance analysis

This part firstly presents the relevant modeling assumptions. Markov chain is one approach quoted in IEC 61511 [51] for reliability assessment of SIS. When using Markov chains, it is possible to make a dynamic analysis of the system in each test interval. The state of the tested units are observed and known through periodic proof test, which implies the inapplicability of the classical Markov chain. Thus, the probability that the SIS sojourns in a certain state is known or partially known in each proof test. The proof test and its follow-up maintenance reallocate the distribution of system states from the modeling perspective, and create a new phase in the Markov chain for latter phase. Thus, a multi-phase Markov process is used to model the performance of SIS.

3.1. Assumptions

For unavailability and maintenance analysis, the following assumptions are needed as most of the existing literature:

- DU failures of units follow the exponential distribution;
- All units are repairable and repair time is negligible;
- Proof tests are executed periodically to check system performance and independently for units.
- Both preventive and corrective maintenance once conducted are perfect to make the objective as-good-as-new (AGAN).
- Common cause failures (CCFs) are excluded, with the purpose to illustrate the effects of α_i in a single unit on the redundant structure apparently.

In this study, proof tests are imperfect in revealing degraded states with a revealing probability or testing coverage α_i for unit i. When identifying failed states, tests are perfect.

3.2. Performance analysis

Considering the discrete states assumption, a system can be in $r+1$ distinct states with a state space $\{1,\dots,r+1\}$. We define the stochastic process $\{X(t), t \geqslant 0\}$ to represent the system state at time t. Vector $\mathbf{P}(t) = [\mathbf{P}_1(t), \mathbf{P}_2(t), \dots, \mathbf{P}_{r+1}(t)]$ stands for the probabilities of the process in each state at time t. The system is always in one of states, so that the sum of state probabilities should be equal to 1 at any time. A generic mathematical notion of a Markov model is

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{QP}(t) \tag{1}$$

where $\mathbf{Q}$ is the Markov transition matrix containing all transition rates (assumed to be constant in each phase). Considering the periodic proof tests, the overall life cycle of system could be modeled by multi-phase Markov process, the i testing intervals are denoted as $[0, \mathrm{T}_1], [\mathrm{T}_1, \mathrm{T}_2], \dots, [\mathrm{T}_{(i-1)}, \mathrm{T}_i]$, accompanying with Markov transition matrix $\mathbf{Q}_i$ and $\mathbf{M}_i$ to represent the transition rates and probability matrix of different states after a testing/repair action in the ith test phase, respectively. To accompany the set of equations, a set of initial state probabilities $\mathbf{P}(t=0) = \mathbf{P}_0$ is also required. Then by solving Chapman–Kolmogorov's equation, we can calculate system state probabilities at time t in first test phase $[0, \mathrm{T}_1]$.

$$\mathbf{P}(t) = \mathbf{P}_0 \cdot exp(\mathbf{Q}_1 \cdot t) \tag{2}$$

If the time immediately before a test (pretest) at time T_1 is indicated as T_1^- and immediately after a test (post-test) as T_1^+, the effect of test and maintenance actions at time T_1 can be described as

$$\mathbf{P}(\mathrm{T}_1^+) = \mathbf{P}(\mathrm{T}_1^-) \cdot \mathbf{M}_1 \tag{3}$$

where $\mathbf{M}_1$ represents the probability matrix of different states after a testing and repair action. $\mathbf{P}(\mathrm{T}_1^+)$ stands for the state probabilities at time T_1. So, the system state probabilities at time t in second phase can be calculated as:

$$\begin{aligned}\mathbf{P}(t) &= \mathbf{P}(\mathrm{T}_1^+) \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{t} - \mathrm{T}_1)) \\ &= \mathbf{P}(\mathrm{T}_1^-) \cdot \mathbf{M}_1 \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{t} - \mathrm{T}_1)) \\ &= \mathbf{P}_0 \cdot exp(\mathbf{Q}_1 \cdot \mathrm{T}_1) \cdot \mathbf{M}_1 \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{t} - \mathrm{T}_1))\end{aligned} \tag{4}$$

Therefore, we can have $\mathbf{P}(\mathrm{T}_2^-)$

$$\begin{aligned}\mathbf{P}(\mathrm{T}_2^-) &= \mathbf{P}(\mathrm{T}_1^+) \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{T}_2 - \mathrm{T}_1)) \\ &= \mathbf{P}_0 \cdot exp(\mathbf{Q}_1 \cdot \mathrm{T}_1) \cdot \mathbf{M}_1 \cdot \exp(\mathbf{Q}_2 \cdot (\mathrm{T}_2 - \mathrm{T}_1))\end{aligned} \tag{5}$$

Similarly, $\mathbf{P}(\mathrm{T}_{(i-1)}^-)$ could be calculated as

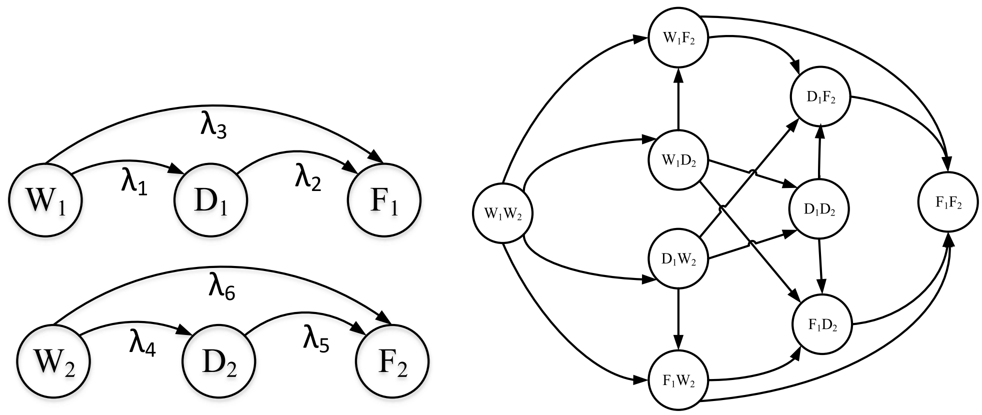
$$\begin{aligned}\mathbf{P}(\mathrm{T}_{(i-1)}^-) &= \mathbf{P}(\mathrm{T}_{i-2}^+) \cdot \exp(\mathbf{Q}_{i-1} \cdot (\mathrm{T}_{i-2} - \mathrm{T}_{i-1})) \\ &= \mathbf{P}_0 \prod_{n=1}^{i-2} (exp(\mathbf{Q}_n \cdot (\mathrm{T}_n - \mathrm{T}_{n-1})) \cdot \mathbf{M}_n) \cdot \exp(\mathbf{Q}_i \cdot (\mathrm{T}_{i-1} - \mathrm{T}_{i-2}))\end{aligned} \tag{6}$$

Then if t is in the i testing phase $[\mathrm{T}_{(i-1)}, \mathrm{T}_i]$, we can have $\mathbf{P}(t)$

$$\begin{aligned}\mathbf{P}(t) &= \mathbf{P}(\mathrm{T}_{i-1}^-) \cdot \mathbf{M}_{i-1} \cdot \exp(\mathbf{Q}_i \cdot (\mathrm{t} - \mathrm{T}_{i-1})) \\ &= \mathbf{P}_0 \prod_{n=1}^{i-1} (exp(\mathbf{Q}_n \cdot (\mathrm{T}_n - \mathrm{T}_{n-1})) \cdot \mathbf{M}_n) \cdot \exp(\mathbf{Q}_i \cdot (\mathrm{t} - \mathrm{T}_{i-1}))\end{aligned} \tag{7}$$

For a 1oo1 configuration, the system will not be functional in the failed state, and the instantaneous PFD(t) in each testing phase is given by

$$\mathrm{PFD}(t) = \Pr(X(t) = F) = \mathbf{P}(t) \cdot [0, 0, 1]^{\mathbf{T}} \tag{8}$$



(a) (b)

Fig. 2. State transition diagrams for (a) 1oo1 configuration and (b) 1oo2 configuration.

Meanwhile, for a 1oo2 configuration, the system will not be functional when both of two units are in the failed states, then the instantaneous PFD(t) is given by

$$\mathrm{PFD}(t) = \Pr(X(t) = \mathrm{FF}) = \mathbf{P}(t) \cdot [0, 0, 0, 0, 0, 0, 0, 0, 1]^{\mathbf{T}} \tag{9}$$

Then performance measure of system, $\mathrm{PFD}^{\mathrm{i}}_{\mathrm{avg}}$, in ith testing phase is given by

$$\mathrm{PFD_{avg}}^{i} = \frac{1}{T_i - T_{i-1}} \int_{T_{i-1}}^{T_i} \mathrm{PFD}(t)dt \tag{10}$$

3.3. Modeling for proof tests and maintenances

In this paper, each unit in a 1oo2 configuration is assumed to have three states, including working, degraded and failed. The transition diagram for 1oo1 and 1oo2 configuration is shown in Fig. 2, the corresponding transition matrix is $\mathbf{Q}$ as shown in Appendix B.

As assumptions in Section 3.1, proof tests are perfect in revealing failed states, but imperfect in revealing degraded states. To quantify such imperfectness, a coverage indicator α is defined as the conditional probability that a degraded state will be detected by the proof test, given that degradation has occurred when initiating the proof test.

$$\alpha = \Pr(\text{Degradation is detected in a proof test } | \text{Degradation has occurred}) \tag{11}$$

The parameter α does not affect the transition matrix and diagram as the unrevealed degraded state is physically in degraded. Since the maintenance actions are based on the detected state of system, the imperfectness in revealing of degraded state should be taken into matrix which upon testing and maintenance actions.

3.3.1. Testing strategies

Two different testing strategies for a redundant structure of SIS final element will be investigated here, include:

- Simultaneous testing: Two units are tested at (almost) same time with a fixed interval τ. The ith proof test is executed at time $t_i = i\tau, (i = 1, 2, \ldots)$, and independently for two units.
- Staggered testing: Two units are tested at different times with a constant test interval. Here, we assume that unit 1 is tested at time $t_{2j-1} = (2j-1)\times\tau/2$ and unit 2 at time $t_{2j} = (2j)\times\tau/2$, $(j = 1, 2, \ldots)$, since $\tau/2$ has been identified as the optimal interval [52].

3.4. Follow-up maintenance strategies

Considering the aforementioned testing strategies, several optional maintenance strategies are proposed for 1oo2 configuration:

- Strategy I: Under the simultaneous testing policy, the tests for two units are two separate processes. A PM or CM action will be executed if any unit is found in the degraded or failed state in test. Both PM and CM actions are perfect and make units as-good-as-new.
- Strategy II: Under the staggered testing policy, repair actions are only executed on the tested unit. A PM or CM will be executed when the tested unit is in degraded or failed state, respectively. Since no information of another unit is collected during the testing, then no repair is executed on the untested unit.
- Strategy III: Opportunistic maintenance with perfect action under the staggered testing policy. The maintenance policy is described as follows: 1. PM will be executed for tested degraded unit and perform CM if the tested unit fails. 2. At the moment of CM, this opportunity is taken to perform a replacement action on the other unit no matter the actual state is.

3.5. Life-cycle cost

Life-cycle cost for final elements in SISs mainly consists of purchase, installation, maintenance and disposal, while almost three-quarters of total cost goes for maintenance while one fifth goes for purchase [53]. The huge proportion for maintenance cost represents an opportunity for cost reduction.

The acknowledged maintenance criteria is to optimize certain parameter with renewal theorem. Differ from usual production systems, most SISs are designed with finite service time and thus the steady-state criteria is not applicable [29]. Therefore, the life-cycle cost of SISs could be estimated by the sum of expected cost after each proof test.

To quantify the life-cycle cost, several cost items related maintenance and testing actions are defined as: C_0, C_{PT}, C_{PM}, C_{CM} represents one-time installation cost per unit, proof test cost per unit, preventive maintenance cost and corrective maintenance cost (purchase) per unit, respectively.

The expected maintenance cost after ith test (EC_i) should equal to the sum of proof test cost (EC_{PT}), expected PM cost (EC_{PM}) and CM cost (EC_{CM}) in ith test interval, where expected cost depends on the system state probability and corresponding maintenance actions.

$$EC_i = EC_{PT} + EC_{\mathrm{PM}} + EC_{\mathrm{CM}} \tag{12}$$

Considering the imperfectness of revealing degraded state, the expected maintenance cost should be linked with parameter α, for 1oo1 configuration after the first test,

$$\begin{aligned} EC_{\mathrm{PM}} &= \mathbf{P}_2(\tau^-)\cdot \mathrm{C_{PM}} = \mathbf{P}_2(\tau^+)\cdot\alpha\cdot \mathrm{C_{PM}} \\ EC_{\mathrm{CM}} &= \mathbf{P}_3(\tau^-)\cdot \mathrm{C_{CM}} = \mathbf{P}_3(\tau^+)\cdot \mathrm{C_{CM}} \end{aligned} \tag{13}$$

Then the expected maintenance cost EC_1 for 1oo1 configuration SIS after first test can be expressed as following,

$$EC_1 = C_{PT} + \mathbf{P}((\tau)^+)\cdot\begin{pmatrix} 0 \\ \alpha\cdot C_{\mathrm{PM}} \\ C_{\mathrm{CM}} \end{pmatrix} \tag{14}$$

Afterwards, the total expected life-cycle cost (LCC) for 1oo1 configured SIS in n test intervals can be estimated as

$$\mathrm{LCC} = C_0 + \sum_{i=1}^{n} EC_i \tag{15}$$

Similarly, the expected maintenance cost for 1oo2 configuration after single proof test with Strategy I can be estimated as Eq. (16),

$$EC_i = 2C_{PT} + \mathbf{P}((i\tau)^+) \cdot\begin{pmatrix} 0 \\ \alpha_2\cdot C_{\mathrm{PM}} \\ C_{\mathrm{CM}} \\ \alpha_1\cdot C_{\mathrm{PM}} \\ \alpha_1\cdot(1-\alpha_2)\cdot C_{\mathrm{PM}} + \alpha_1\cdot(1-\alpha_2)\cdot C_{\mathrm{PM}} + 2\cdot\alpha_1\cdot\alpha_2\cdot C_{\mathrm{PM}} \\ \alpha_1\cdot(C_{\mathrm{PM}}+C_{\mathrm{CM}}) + (1-\alpha_1)\cdot C_{\mathrm{CM}} \\ C_{\mathrm{CM}} \\ \alpha_2\cdot(C_{\mathrm{PM}}+C_{\mathrm{CM}}) + (1-\alpha_2)\cdot C_{\mathrm{CM}} \\ 2C_{\mathrm{CM}} \end{pmatrix} \tag{16}$$

the total expected life-cycle cost (LCC) for 1oo2 configured SIS with Strategy I in n test intervals can be estimated as

$$\mathrm{LCC} = 2\cdot C_0 + \sum_{i=1}^{n} EC_i \tag{17}$$

For Strategy II, unit 1 is tested at time $t_{2j-1} = (2j-1)\times\tau/2$ and unit 2 at time $t_{2j} = (2j)\times\tau/2$, $(j = 1,2,\ldots)$, the expected cost after single test can be estimated by Eq. (18).

$$\begin{aligned} EC_{2j-1} = C_{PT} &+ \mathbf{P}(((2j-1)\cdot\tau/2)^+) \\ &\cdot\left(0,0,0,\alpha_1\cdot C_{\mathrm{PM}},\alpha_1\cdot C_{\mathrm{PM}},\alpha_1\cdot C_{\mathrm{PM}},C_{\mathrm{CM}},C_{\mathrm{CM}},C_{\mathrm{CM}}\right)^{\mathbf{T}} \\ EC_{2j} = C_{PT} &+ \mathbf{P}(((2j)\cdot\tau/2)^+) \\ &\cdot\left(0,\alpha_2\cdot C_{\mathrm{PM}},C_{\mathrm{CM}},0,\alpha_2\cdot C_{\mathrm{PM}},C_{\mathrm{CM}},0,\alpha_2\cdot C_{\mathrm{PM}},C_{\mathrm{CM}}\right)^{\mathbf{T}} \end{aligned} \tag{18}$$

Similarly, for Strategy III, the expected cost after each test can be estimated by Eq. (19).

$$\begin{aligned} EC_{2j-1} = C_{PT} &+ \mathbf{P}(((2j-1)\cdot\tau/2)^+) \\ &\cdot\left(0,0,0,\alpha_1\cdot C_{\mathrm{PM}},\alpha_1\cdot C_{\mathrm{PM}},\alpha_1\cdot C_{\mathrm{PM}},2C_{\mathrm{CM}},2C_{\mathrm{CM}},2C_{\mathrm{CM}}\right)^{\mathbf{T}} \\ EC_{2j} = C_{PT} &+ \mathbf{P}(((2j)\cdot\tau/2)^+) \\ &\cdot\left(0,\alpha_2\cdot C_{\mathrm{PM}},2\cdot C_{\mathrm{CM}},0,\alpha_2\cdot C_{\mathrm{PM}},2\cdot C_{\mathrm{CM}},0,\alpha_2\cdot C_{\mathrm{PM}},2\cdot C_{\mathrm{CM}}\right)^{\mathbf{T}} \end{aligned} \tag{19}$$

Using Eq. (17), the total expected LCC for 1oo2 configuration under Strategy I in a finite lifetime can be estimated by summing up the expected cost from Eq. (16). Similar equations could be conducted for Strategy II and Strategy III by summing up results from Eqs. (18) and (19), respectively.

Table 2
Parameter value.

Parameter	value
λ_1	8E−6
λ_2	2E−5
λ_3	4E−6
λ_4	8E−6
λ_5	2E−5
λ_6	4E−6
τ	8760

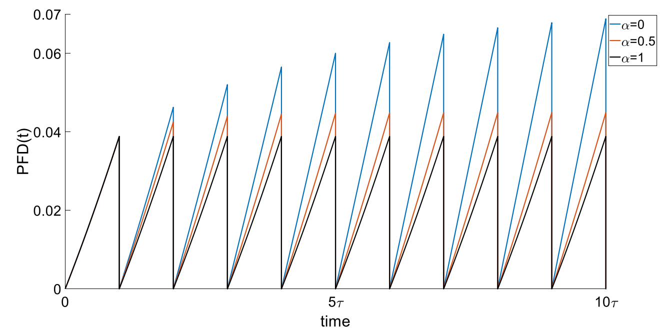


Fig. 3. PFD(t) of 1oo1 configuration.

4. Numerical example

To illustrate the proposed model and maintenance strategies, a numerical example is conducted here. Assumed parameters for transition rates in the example are listed in Table 2.

4.1. Effect of α on the performance of a 1oo1 configuration

To investigate the effect of imperfectness in revealing degraded state α on the 1oo1 configuration, a perfect PM or CM will be executed if the system is manifested in degraded or failed state in proof tests. The effect of coverage α of proof test in revealing degraded state is shown in Fig. 3.

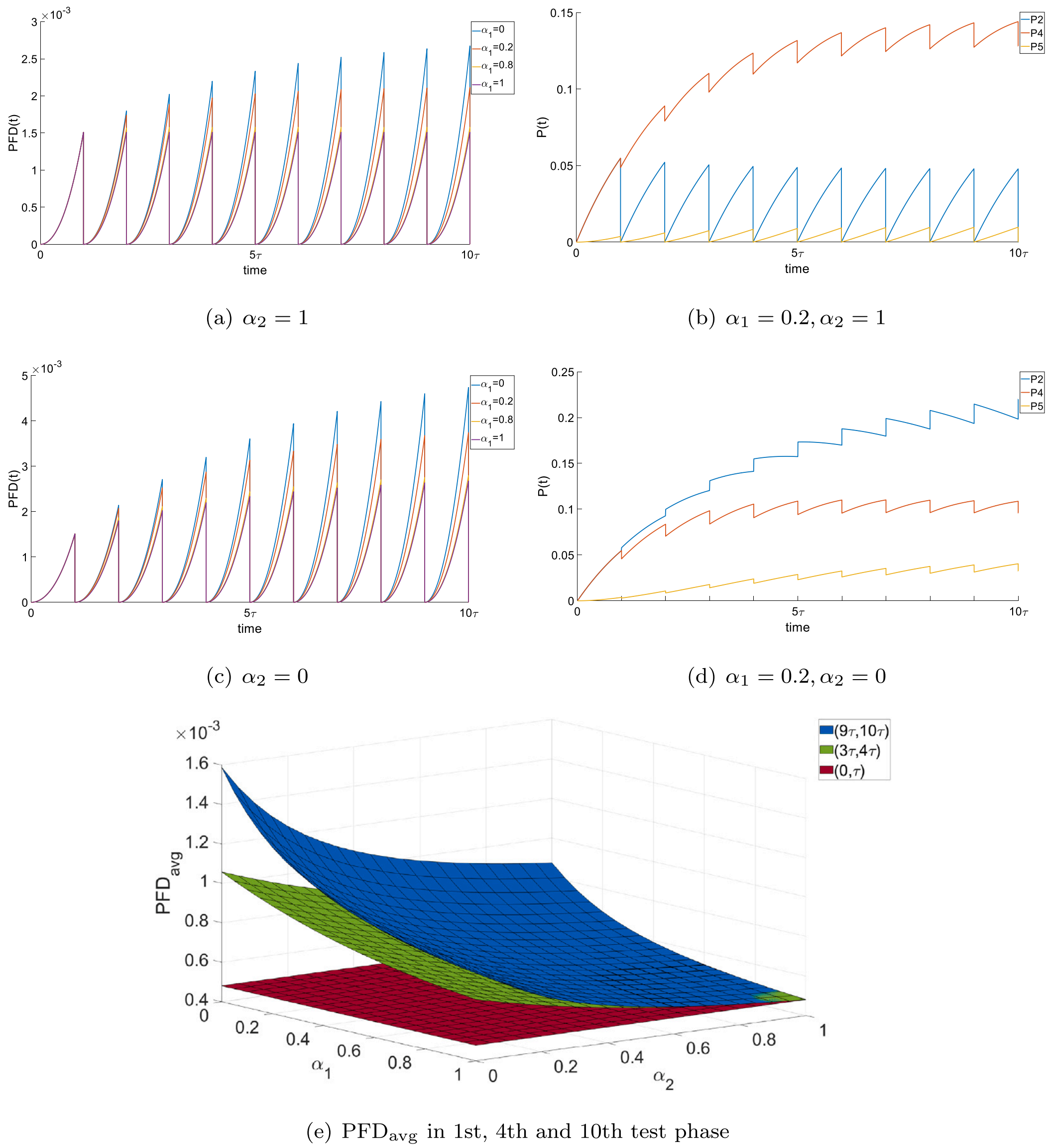
It is easy to notice that the testing coverage α has an obvious effect on system PFD(t). In the first test phase $(0,\tau)$, system PFD(t) is overlapped when $\alpha = 0, 0.5, 1$, thanks to the same initial state probability $\mathrm{P}(t) = [1,0,0]$ at $t = 0$. When $\alpha = 1$, the proof testings are perfect in revealing degraded states and failed state, the element will reach a stable and lowest tendency since the initial state is $\mathrm{P}(t) = [1,0,0]$ in each test phase. When $\alpha < 1$, the system is still possible in the degraded state after perfect PM or CM, and then the initial state of the system in each phase is $\mathrm{P}(t) = [1-\alpha\mathrm{P}_2(t^-), \alpha\mathrm{P}_2(t^-), 0]$. Consequently, system PFD(t) is increasing with time under imperfect testing as $\alpha = 0$ and $\alpha = 0.5$ in each test phase as shown in Fig. 3. When $\alpha = 0$, the system PFD(t) reaches the highest value in same test phase.

4.2. Effect of α on the performance of a 1oo2 configuration

Performance of a 1oo2 configuration is analyzed according to the proposed testing and maintenance strategies respectively.

4.2.1. Simultaneous testing with maintenance strategy I

For strategy I, given the imperfect revealing coverage on degraded state for two units, undoubtedly, the observed state probabilities will not be equal to the actual physical ones when $\alpha_i < 1$. According to assumptions in Section 3.1, test and repair time is assumed to be negligible. The instantaneous state transition process at time $i\tau, i = 1,2,\ldots$ with revealing coverage α_1 and α_2 on degraded state for selected states are shown in Table 3. The whole matrix regarding test and repair is shown as $\mathbf{M}$ in Appendix B.



(a) $\alpha_2 = 1$

(b) $\alpha_1 = 0.2, \alpha_2 = 1$

(c) $\alpha_2 = 0$

(d) $\alpha_1 = 0.2, \alpha_2 = 0$

(e) $\mathrm{PFD_{avg}}$ in 1st, 4th and 10th test phase

Fig. 4. PFD(t) and selected state probabilities of 1oo2 configuration under strategy I.

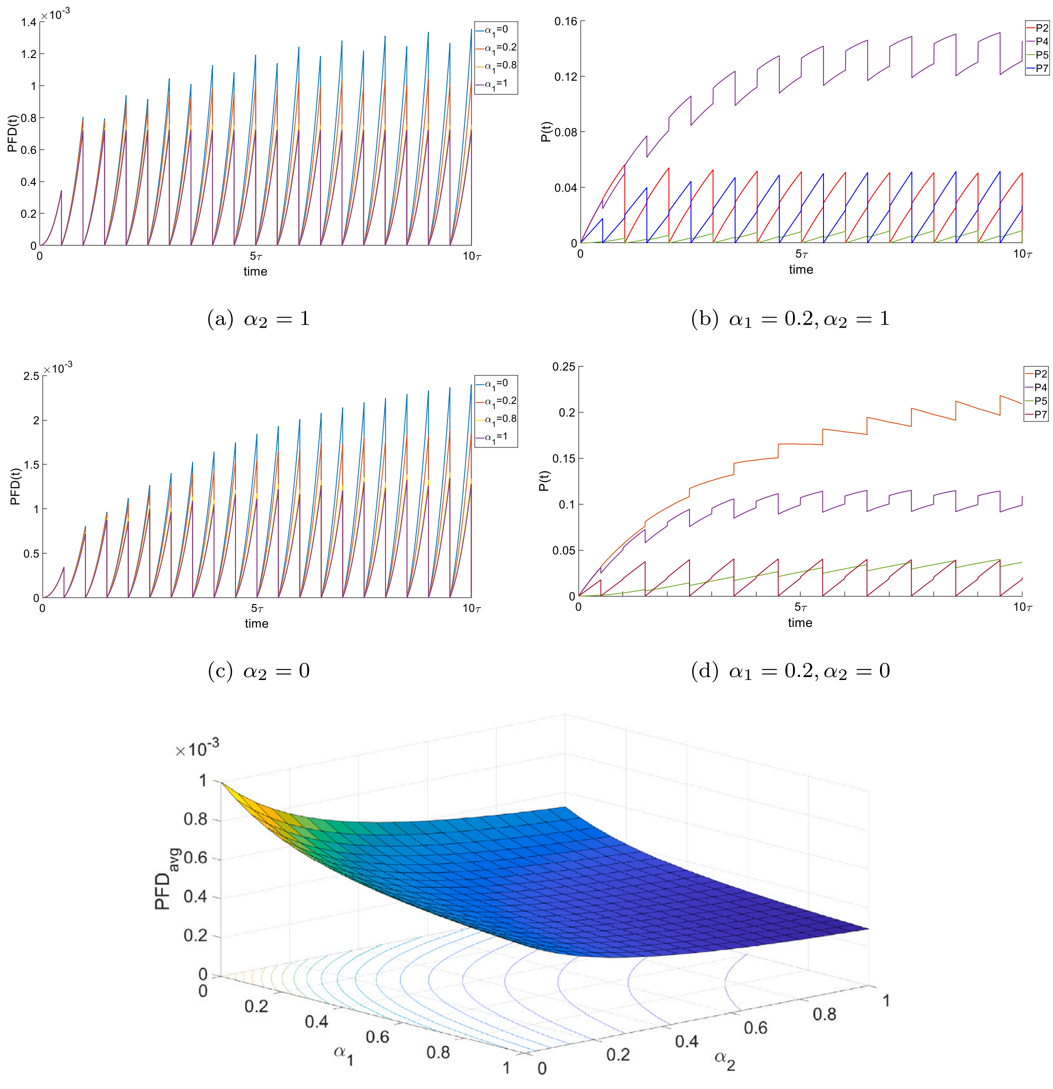
Table 3
Instantaneous state transition at test time $i\tau$ with strategy I.

Physical at $i\tau^-$	After test	After repair	Physical at $i\tau^+$
F_1D_2	α_2 F_1D_2 $1-\alpha_2$ F_1W_2	α_2 W_1W_2 $1-\alpha_2$ W_1W_2	α_2 W_1W_2 $1-\alpha_2 W_1D_2$
D_1D_2	$\alpha_1\alpha_2$ D_1D_2 $\alpha_1(1-\alpha_2)$ D_1W_2 $(1-\alpha_1)\alpha_2$ W_1D_2 $(1-\alpha_1)(1-\alpha_2)$ W_1W_2	$\alpha_1\alpha_2$ W_1W_2 $\alpha_1(1-\alpha_2)$ W_1W_2 $(1-\alpha_1)\alpha_2$ W_1W_2 –	$\alpha_1\alpha_2$ W_1W_2 $\alpha_1(1-\alpha_2)W_1D_2$ $(1-\alpha_1)\alpha_2D_1W_2$ $(1-\alpha_1)(1-\alpha_2)$ D_1D_2
D_1F_2	α_1 D_1F_2 $1-\alpha_1$ W_1F_2	α_1 W_1W_2 $1-\alpha_1$ W_1W_2	α_1 W_1W_2 $1-\alpha_1D_1W_2$

System PFD(t) and selected state probabilities of 1oo2 configuration with strategy I are shown in Fig. 4.

System PFD(t) is increasing under strategy I with the set parameters in Table 2 when $\alpha_i < 1$, meaning that system unavailability is increasing in each testing phase. In Fig. 4(a), the test coverage of revealing degraded state α_1 for unit 1 has a more evident effect on PFD(t) with time when $\alpha_2 = 1$. When α_1 closes to 1, PFD(t) has a slowing decrease with α_1 in each test interval. System PFD(t) with $\alpha_1 = 0.8$ is almost overlapping with that of $\alpha_1 = 1$. Selected state probabilities with $\alpha_1 = 0.2, \alpha_2 = 1$ is shown are 4(b). When $\alpha_2 = 1$, the degraded state of unit 2 will be revealed perfectly after each test. Then the state probabilities for state 2 (W_1D_2) and 5 (D_1D_2) will decrease to 0 at the beginning of each test phase. Meanwhile, the state probability of state 4 (D_1W_2) should theoretically equal to 0. But, given the imperfect revealing coverage for unit 1, the state probability $P_4(i\tau^-)$ decreases at each test point ($P_4(i\tau^-) < P_4(i\tau^+)$) with overall increases ($P_4(i\tau^-) < P_4((i+1)\tau^-)$) instead, which comes from the partly imperfect repair of state 5 (D_1D_2) and 6 (D_1F_2) as shown in Table 3.

Similar as system PFD(t) tendency in Fig. 4(a), PFD(t) in Fig. 4(c) is also increasing along with time. In each test phase, PFD(t) monotonically increases in each test phase and reaches a maximum at $i\tau^+, i = 1, 2, \ldots$. PFD($t$) decreases slowly with a higher α_1. State probabilities $P_2(t), P_4(t)$ and $P_5(t)$ in Fig. 4(d) show different tendencies compared to Fig. 4(b). Since $\alpha_2 = 0$, no degraded state for unit 2 is revealed in proof tests. For state 2 (W_1D_2), $P_2(i\tau^+) > P_2(i\tau^-)$, the increment comes from the partly repair of state 5 (D_1D_2) and 6 (D_1F_2) as described in Table 3. $P_5(i\tau^-)$ will be divided into four possible states 5(D_1D_2), 4(D_1W_2), 2(W_1D_2)and 1(W_1W_2) with portions 0,0.2,0,0.8, respectively. When the system is in $P_5(i\tau^-)$, it has 20% of probability to be repaired, and the probability of being skipped is 80%.



(a) $\alpha_2 = 1$ (b) $\alpha_1 = 0.2, \alpha_2 = 1$

(c) $\alpha_2 = 0$ (d) $\alpha_1 = 0.2, \alpha_2 = 0$

(e) $\mathrm{PFD_{avg}}$ in $(9.5\tau, 10\tau)$

Fig. 5. PFD(t) and selected state probabilities of 1oo2 configuration under strategy II.

System $\mathrm{PFD_{avg}}$ with α_1 and α_2 in selected test phases is shown in Fig. 4(e). In first test phase (0, τ), $\mathrm{PFD_{avg}}$ shows a flat surface with the value of 4.81×10^{-4} for independent on α_1 and α_2. It means that the system performance in first phase is only depending on the initial state vector and the length of test. It is reasonable to conclude that system $\mathrm{PFD_{avg}}$ is increasing with time, since showing a highest value for 10th with an intermediate and lowest value for 4th and 1st test phase in Fig. 4(e), respectively. Meanwhile, it is not difficult to notice that $\mathrm{PFD_{avg}}$ reaches a minimum value when $\alpha_1 = \alpha_2 = 1$ and a maximum value when $\alpha_1 = \alpha_2 = 0$ with up to 1.59×10^{-3} for 10th and 1.06×10^{-3} in 4th test phase. This finding also provide clues to take system $\mathrm{PFD_{avg}}$ in final test phase as a reference in the whole life-cycle in the further discussions.

4.2.2. Staggered testing with maintenance strategy II

The point of testing for unit 1 is shifted with a time $\tau/2$ compared to the unit 2. And unit 1 is tested at $t_{2j-1} = (2j-1) \times \tau/2$ and unit 2 at time $t_{2j} = (2j) \times \tau/2$, $(j = 1, 2, \ldots)$. System PFD(t) of 1oo2 configuration with strategy II is shown in Fig. 5. In the first testing phase, system PFD(t) has no relation with either α_1 or α_2 thanks to the same initial state probability $\mathbf{P}_0$.

As mentioned in Section 3.4, the staggered testing procedure introduces two separate matrices, which are shown in Appendix B, $\mathbf{M}_{U_1}$ is valid after a test of unit 1 and $\mathbf{M}_{U_2}$ is valid after a test of unit 2. When $\alpha_2 = 1$, in Fig. 5(a), system PFD(t) increases with a lower value of α_1 in each testing phase. Several system states, e.g. state 4($\mathrm{D_1W_2}$), state 5($\mathrm{D_1D_2}$) and state 6($\mathrm{D_1F_2}$) will still be hidden and not be repaired during the testing of unit 1 when $\alpha_1 \neq 0$. Because of the alternation and imperfect coverage, these hidden states after testing of unit 1 contribute to a fluctuating PFD(t) in the consecutive testing phase of unit 2. Similar tendencies are demonstrated in Fig. 5(c) with $\alpha_2 = 0$.

Selected state probabilities with $\alpha_1 = 0.2, \alpha_2 = 1$ are shown in Fig. 5(b). For example, state probability $\mathrm{P_4}(t)$ for state 4 ($\mathrm{D_1W_2}$) decreases instantly after testing of unit 1 because of the imperfect coverage α_1 but jumps to a higher value given the repair of state 5 ($\mathrm{D_1D_2}$) and state 6 ($\mathrm{D_1F_2}$) after testing of unit 2. Similarly, compared to Fig. 5(b), the lower increment magnitude of $\mathrm{P_4}(t)$ in Fig. 5(d) comes from the repair of state 6 ($\mathrm{D_1F_2}$) since no state 5 ($\mathrm{D_1D_2}$) is revealed with $\alpha_2 = 0$ in tests of unit 2.

It is worth noting that there are two specific cases: (1) $\alpha_1 = 0, \alpha_2 = 0$ (2) $\alpha_1 = 1, \alpha_2 = 1$.
(1) When $\alpha_1 = 0, \alpha_2 = 0$, it means that even the physical state of unit has shifted from working to degraded state, but no degraded states for either unit 1 or unit 2 are revealed in tests. Consequently, no PM will be executed. Therefore, system PFD(t) reaches a maximum value in each

Table 4
Different transition rates for unit 2.

Parameter	Value			
	Unit 21	Unit 22	Unit 23	Unit 24
λ_4	0.5 × 8E−6	8E−6	2 × 8E−6	3 × 8E−6
λ_5	0.5 × 2E−5	2E−5	2 × 2E−5	3 × 2E−5
λ_6	0.5 × 4E−6	4E−6	2 × 4E−6	3 × 4E-6

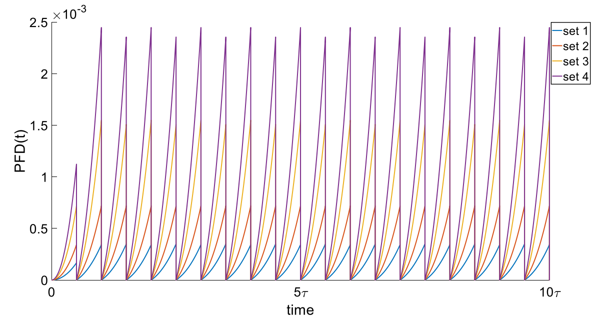


Fig. 6. PFD(t) of 1oo2 configuration under strategy II.

test phase, as shown in Fig. 5(c). This finding is also demonstrated by the maximum value of system $\mathrm{PFD_{avg}}$ in $(9.5\tau, 10\tau)$ after test of unit 1 at time 9.5τ in Fig. 5(e). Meanwhile, $\mathrm{PFD_{avg}}$ increases with a higher magnitude when either α_1 or α_2 is closing to 0.

(2) When $\alpha_1 = 1, \alpha_2 = 1$, it means that degraded state of unit 1 and unit 2 will be perfectly revealed in the tests. Corresponding repair actions are taken, system PFD(t) reaches a stable tendency and minimum value after few phases since two units are assumed identical with same transition rates.

To demonstrate the effect of transition rates, a brief study is conducted here. The transition rates for unit 1 keep the same values as in Table 2. Four optional unit 2 for 1oo2 configuration, which marked as Unit 21, 22, 23 and 24, are listed in Table 4 with different transition rates. For the simplification in the following, symbol 'set i' is employed to stand for the 1oo2 configuration with unit 1 and unit 2i.

The calculation result of PFD(t) for the 1oo2 configuration under strategy II with nonidentical units are shown in Fig. 6. It is obvious that system PFD(t) increases with higher values of transition rates for unit 2. Given the unequal transition rates for two units, system PFD(t) fluctuates when $\alpha_1 = \alpha_2 = 1$ with the test of unit 1 and 2 except a stable tendency for set 2.

4.2.3. *Staggered testing with maintenance strategy III*

The main difference between strategy II and strategy III is an additional replace action on the untested unit. It is easy to infer that system $\mathrm{PFD_{avg}}$ will be to some extent lower with strategy III compared to strategy II. Similarly as strategy II, the staggered testing procedure introduces two separate matrices, which are shown in Appendix B, $\mathbf{M}_{U_1}$ is valid after a test of unit 1 and $\mathbf{M}_{U_2}$ is valid after a test of unit 2.

System $\mathrm{PFD_{avg}}$ results with parameters from Table 2 under two strategies are shown in Fig. 7.

When $\alpha_1 = \alpha_2 = 1$, in Fig. 7(a), system $\mathrm{PFD_{avg}}$ reaches a constant value 2.91×10^{-4} with strategy II and a lower value with strategy III, at 2.84×10^{-4}, representing 2.45% decrease.

When $\mathrm{PFD_{avg}}$ if $\alpha_1 = \alpha_2 = 0$, only failed unit will be restored to working state. In Fig. 7(b), it is obvious that system $\mathrm{PFD_{avg}}$ keeps increasing with time with strategy II and III. Strategy III has a more evident advantage along with time on $\mathrm{PFD_{avg}}$.

The main shortcoming of strategy III is the abuse of restoring the untested unit, which consequently will contribute to a increasing maintenance cost. Therefore, the upcoming consideration is how to balance the decreased $\mathrm{PFD_{avg}}$ and economic loss.

Table 5
Parameter value regarding maintenance and test items.

Parameter	Item	value
C_0	One-time installation cost per unit	600
C_{PT}	test cost per unit	60
C_{PM}	preventive maintenance cost per unit	240
C_{CM}	corrective maintenance (purchase) cost per unit	6940

4.2.4. $\mathrm{PFD_{avg}}$ *Comparisons among proposed strategies*

For strategy I with $\alpha_1 = \alpha_2 = 1$, either degraded or failed state will be repaired. The system state probabilities will be same as initial vector $\mathbf{P}_0$, which leads to a stable performance of system in each test phase. As proved in previous sections, system will have a lower $\mathrm{PFD_{avg}}$ with $\alpha_1 = \alpha_2 = 1$ in same strategy. When α_1 and α_2 take same values, staggered test (strategy II and III) can lead to a better system performance than simultaneous test (strategy I).

For $\alpha_1 = \alpha_2 = 1$, in Fig. 8(a), system $\mathrm{PFD_{avg}}$ under strategy II and III is up to 60.6% and 59.2% of that under strategy I, respectively. In $(9.5\tau, 10\tau)$, the corresponding value is 63.1% and 54.4% for $\alpha_1 = \alpha_2 = 0$. It is worth mentioning that, in Fig. 8(b), system performance meet SIL 3 with $\alpha_1 = \alpha_2 = 0.5$ under any of proposed maintenance strategy.

To quantify the differences for $\mathrm{PFD_{avg}}$ under proposed strategies, an indicator k_{ji} is proposed here as following,

$$k_{ji} = \frac{\mathrm{PFD_{avg}}\ \text{with strategy } j}{\mathrm{PFD_{avg}}\ \text{with strategy } i} \tag{20}$$

In Figs. 8(c) and 8(d), indicator k_{21} and k_{31} fluctuates with time thanks to the unstable performance for 1oo2 configuration in the early stage when $\alpha_1 = \alpha_2 = 0$, meanwhile, fluctuations of k_{21} and k_{31} decreases gradually along with time.

From Fig. 8(c), the indicator k_{21} gradually reaches a constant value under the specified value of α_1 and α_2 after around 10τ. The overall of effects of strategy II can be approximated estimated in the range of $(0.6, 0.65)$ of strategy I. To infer from these findings that indicator k_{21} has quite weak relation with the value of α_1 and α_2 when the service time is quite long.

However, the indicator k_{31} shows a non-identical tendency in Fig. 8(d). $\mathrm{PFD_{avg}}$ of strategy III mainly located in the range of $(0.5, 0.6)$ with that of strategy I. Imprecision of revealing coverage in tests shows a more obvious effect on $\mathrm{PFD_{avg}}$ when α_1 and α_2 is less than 0.5. For example, k_{31} equals to 0.513 for $\alpha_1 = \alpha_2 = 0$ at 20τ, while 0.589 and 0.592 for $\alpha_1 = \alpha_2 = 0.5$ and $\alpha_1 = \alpha_2 = 1$, respectively.

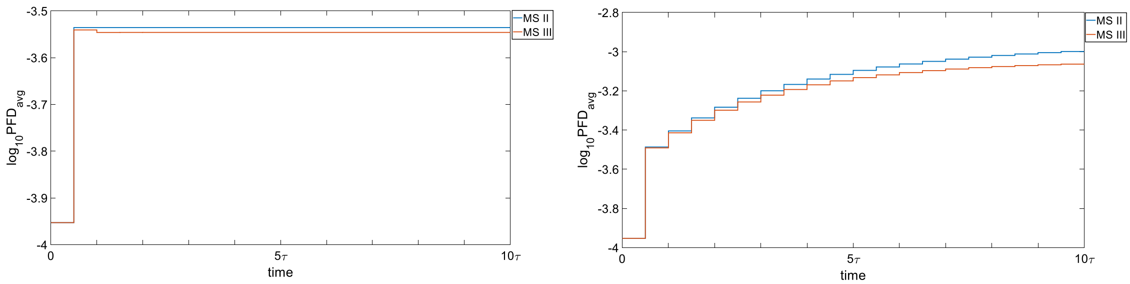
Fig. 8(e) depicts the differences between strategy II and III regarding imprecision revealing coverage α_1 and α_2 in tests. It demonstrates that system has a better performance under strategy III than strategy II as the indicator $k_{32} < 1$, which complies to the findings in Fig. 8(a) and Fig. 8(b). Similar as k_{31} in Fig. 8(d), indicator k_{32} shifts from 0.817 to 0.962 when α_1 and α_2 from 0 to 0.5 at 20τ, while only from 0.962 to 0.976 when α_1 and α_2 from 0.5 to 1. In the long run, strategy III results in an optimistic system performance compared to strategy I and II when the test coverage is quite low.

To conclude, for system $\mathrm{PFD_{avg}}$, staggered test could lead to a better system performance that simultaneous test when the state revealing coverage α_i takes same value. Meanwhile, strategy III is ahead of strategy II to some extent, which is strongly linked with parameter α_i.

4.2.5. *Life-cycle cost*

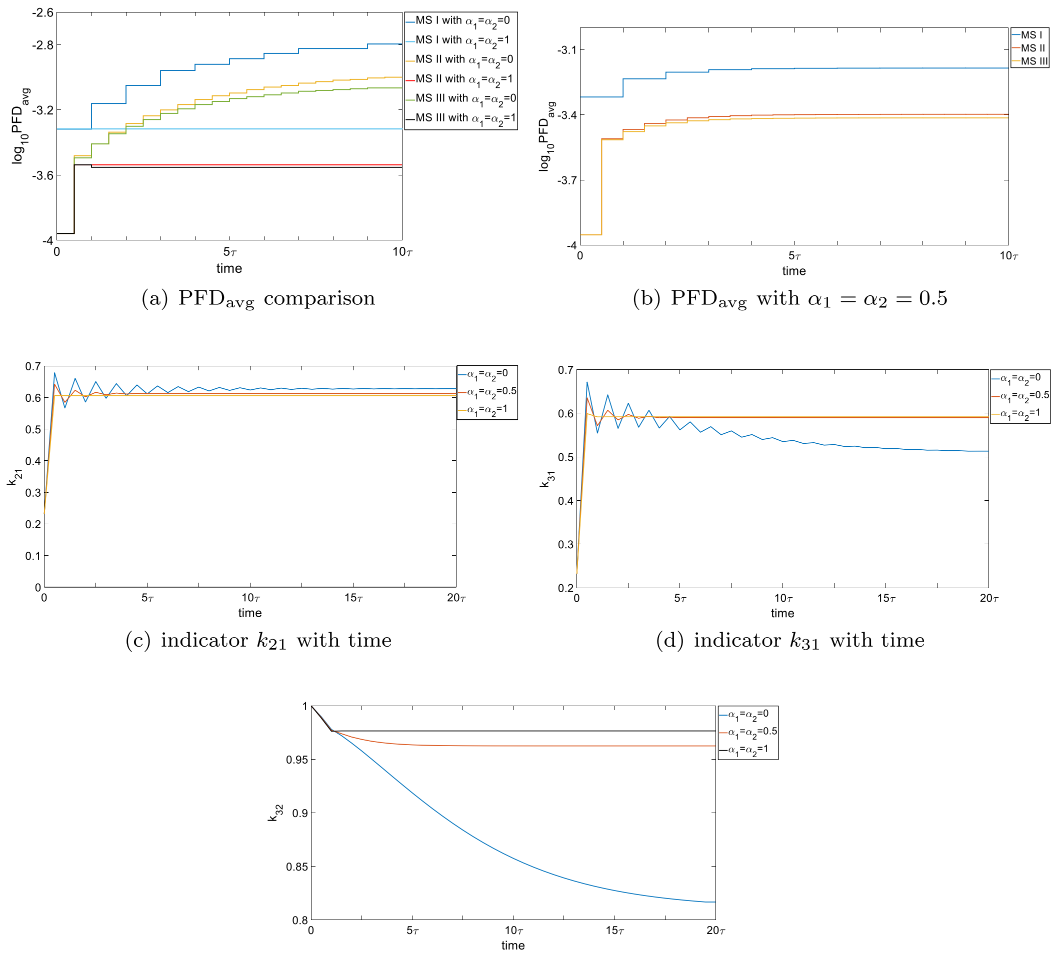
Life-cycle cost items and corresponding values are partly adopted from [47]. Maintenance cost parameters and values are presented in the following Table 5. Based on the finding in Section 4.2, system $\mathrm{PFD_{avg}}$ in final test phase is used as a reference of system performance in the whole life-cycle.

Cumulative maintenance cost for 1oo2 configuration in 20τ with different strategies are depicted in Fig. 9.



(a) $\alpha_1 = \alpha_2 = 1$ (b) $\alpha_1 = \alpha_2 = 0$

Fig. 7. System $\mathrm{PFD}_{\mathrm{avg}}$ comparison between strategy II and strategy III.



(a) $\mathrm{PFD}_{\mathrm{avg}}$ comparison (b) $\mathrm{PFD}_{\mathrm{avg}}$ with $\alpha_1 = \alpha_2 = 0.5$

(c) indicator k_{21} with time (d) indicator k_{31} with time

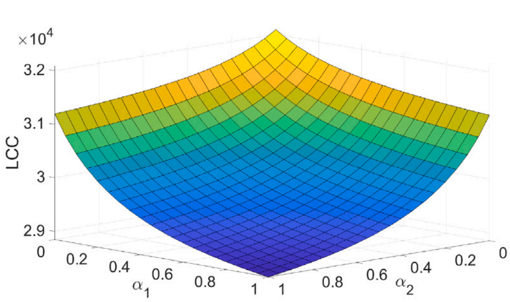
(e) indicator k_{32} with time

Fig. 8. Summary of system $\mathrm{PFD}_{\mathrm{avg}}$ based on proposed strategies.

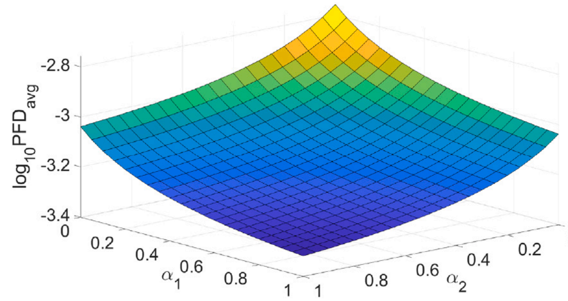
In Fig. 9(a), it is obvious that cumulative maintenance cost reaches a maximum value with $\alpha_1 = \alpha_2 = 0$ and a minimum value when $\alpha_1 = \alpha_2 = 1$. Cumulative maintenance cost decreases universally with a higher state revealing probability α_i. When the revealing probability is quite low, the SIS will be remained at the degraded state after proof test. The hidden degraded state will gradually develop to failed state, which will contribute an expensive CM cost compared to PM. This finding is demonstrated by the tendency of $\mathrm{PFD}_{\mathrm{avg}}$ in $(19\tau, 20\tau)$ in Fig. 9(b). System performance in $(19\tau, 20\tau)$ locates in SIL2 with quite low revealing test coverage, while in SIL3 with a better revealing coverage.

LCC with coverage α_i under strategy II in Fig. 9(c) shows a similar tendency but a lower value than that under strategy I in Fig. 9(a). Considering different test sequences of units 1 and 2, $\mathbf{P}(i\tau^+)$ will redistribute after the prior test and maintenance. The redistribution of state probabilities contributes to the phenomena that LCC is asymmetry about $\alpha_1 = \alpha_2$ given the certain testing sequences of unit 1 and 2, similar result also can be drawn for strategy III in Fig. 9(e).

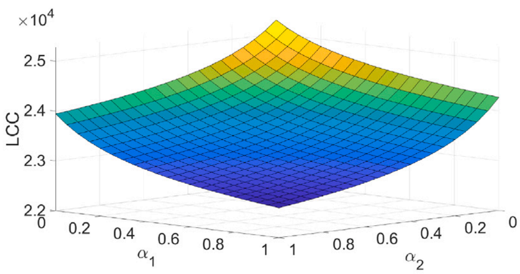
Distinguished from those by strategies I and II, LCC under strategy III reaches a minimum value when $\alpha_1 = \alpha_2 = 0$, namely, CM would only be executed when an item fails. When $\alpha_i \neq 0$, an additional CM on untested unit will be executed along with the PM for tested unit. Consequently, this maintenance action contributes to a higher life-cycle cost. Given $\mathbf{P}(i\tau^+)$ is time-dependent and α_i-dependent, the whole LCC in 20τ is not a monotonic with α_i. In fact LCC increases with α_i and reaches a peak, subsequently, decreases slightly. When revealing



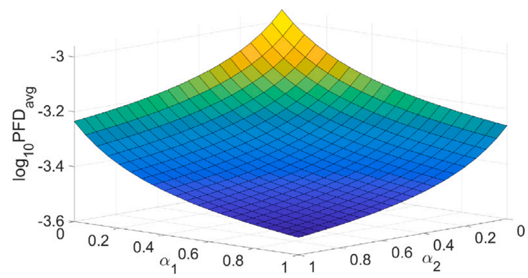
(a) Cumulative cost with strategy I



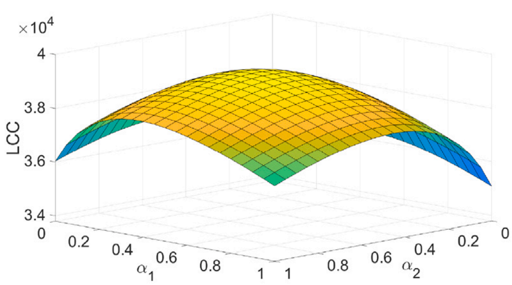
(b) $\mathrm{PFD_{avg}}$ in $(19\tau, 20\tau)$ with strategy I



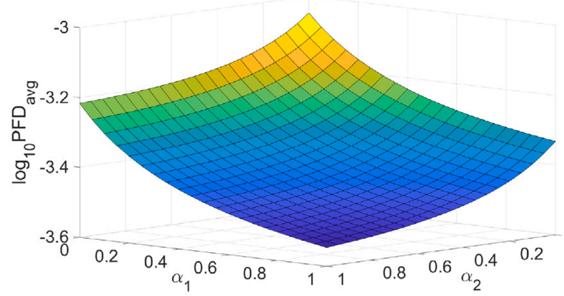
(c) Cumulative cost with strategy II



(d) $\mathrm{PFD_{avg}}$ in $(19.5\tau, 20\tau)$ with strategy II



(e) Cumulative cost with strategy III



(f) $\mathrm{PFD_{avg}}$ in $(19.5\tau, 20\tau)$ with strategyIII

Fig. 9. Cumulative maintenance cost in 20τ.

coverage α_i is quite low, less PMs will be taken, but which could lead to higher possibility of CM. PM cost contributes to an increment in accumulation with coverage α_i at first. When the efficiency of proof tests on degraded state is higher, PM increases and potential CM cost decreases as well. Decrement of potential CM contributes to a decline accumulative cost with higher coverage α_i.

Another potential doubt here is that PM cost is far less than CM (purchase) with values in Table 5. Therefore, a further calculation is conducted here with $C_{\mathrm{PM}} = 2400$. $\mathrm{PFD_{avg}}$ should be independent with the value of C_{PM}. The accumulative LCC in 20 years with different strategies is shown in Fig. 10.

It is obvious that each strategy has a higher cost with an expensive PM cost than previous results in Fig. 9. Inconsistent with the result in Fig. 9(a), LCC under strategy I has a minimum value when $\alpha_1 = \alpha_2 = 0$ and a maximum value when $\alpha_1 = \alpha_2 = 1$. It implies that the cumulative PM cost takes a higher proportion in life-cycle. For strategy II, LCC increases with α_i and reaches a peak, subsequently, decreases slightly, which is similar as the result with strategy III in Fig. 9(e). When it comes to strategy III, thanks to the opportunistic replacement of untested unit when maintenance action is executed on tested unit, the tendency of accumulative cost should be consistent with Fig. 9(e).

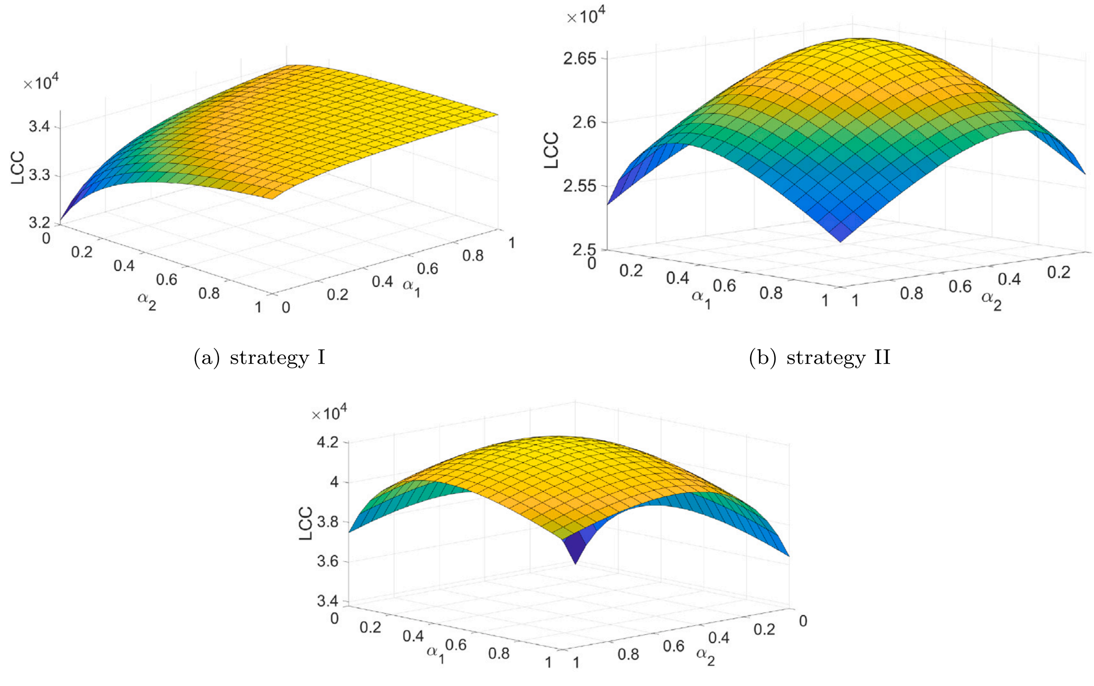
Combined the results from Figs. 9 and 10, generally, from the aspect of LCC, it is easy to conclude that strategy III > strategy I >strategy II in 20τ. But when the PM cost is quite high, the LCC in 20τ have an obvious increment, namely, the maintenance actions also need to be considered carefully. As for $\mathrm{PFD_{avg}}$, from the result in Figs. 9(b), 9(d) and 9(f), system performance with staggered test is universally better than simultaneous test. System with simultaneous test in $(19\tau, 20\tau)$ is within SIL2 and SIL3. For strategy II, except the extreme low revealing coverage of degraded state ($\alpha_1 < 0.2$ and $\alpha_2 < 0.2$), system performance mainly in SIL3. Namely, strategy II contributes to a better system performance than strategy I. Compared to strategy II, system $\mathrm{PFD_{avg}}$ in $(19.5\tau, 20\tau)$ complies to SIL3 totally with strategy III.

Table 6
Comparisons among proposed maintenance strategies.

Strategy	$\mathrm{PFD_{avg}}$	LCC
Strategy I	Poor	Medium
Strategy II	Medium	Low
Strategy III	Good	High

The universal pros and cons of proposed maintenance strategies without taking the values of revealing coverage α_i into consideration are listed in Table 6.

In reality, following the previous findings, if the α_i quite high ($\alpha_i > 0.5$), from Fig. 9, $\mathrm{PFD_{avg}}$ under each maintenance strategy is within SIL3. Therefore, LCC should be prioritized to reduce unnecessary economic loss. That is, the proposed strategy II is the optimal option.



(a) strategy I (b) strategy II

(c) strategy III

Fig. 10. Cumulative maintenance cost in 20τ with an expensive PM cost.

On the contrary, if the α_i quite low ($\alpha_i < 0.5$), not all system SIL complies to SIL3, PFD_{avg} is in the higher priority when it comes to select optimal test and maintenance strategy.

Meanwhile, it is obvious to conclude from Figs. 8 and 9 that the proposed strategy III can lead to the highest LCC and optimum PFD_{avg} regardless of the value of α_i. Nevertheless, in terms of PFD_{avg}, it has slight improvement compared to strategy II especially when α_i quite high ($\alpha_i > 0.5$). The high LCC is the definite disadvantage of the proposed strategy III.

Given that the inevitable degradation phenomena in mechanical elements, it is needed to study how dynamic monitoring can be better utilized. An indicator reflecting the working condition and system status could provide clues for maintenance actions. When a PM is implemented (parameter $\alpha_i > 0$ in this paper), the system performance is better, but LCC is higher. A systematic testing and maintenance policy for the SIS with coordinating the trade-off between PFD_{avg} and LCC should be carefully considered in the designed phase.

5. Concluding remarks

This paper has presented a state-based approach for performance analysis of redundant final elements in SIS subject to imperfect degradation state revealing. The system performance is calculated based on a multi-phase Markov process. Estimation methods for maintenance cost in a finite time regarding imperfect state revealing have been proposed.

A numerical example is given to illustrate the usefulness of the proposed strategies. Based on the assumption, for a 1oo2 configuration, we found that staggered tests can contribute to a better system performance compared to simultaneous tests. From the aspect of LCC, strategy III > strategy I > strategy II in 20τ. Through the proposed method and discussions, a systematic consideration in incorporating system availability and life cycle cost need to be conducted, for reliability practitioners of SISs, when choose testing and maintenance strategy in the overall life-cycle for redundant final element.

This paper focuses on the comparisons among three proposed testing and maintenance strategies for 1oo2 SIS subject to imperfect state revealing. However, several limitations have been remained here in terms of testing and maintenance for SISs, e.g. partial test, common cause failures (CCFs), time-dependent degradation state revealing probability and imperfect maintenance etc. Another point here is about the estimation of potential economic loss of EUC due to the testing and maintenance of SISs.

For further studies, it would be interesting to extend and apply this model to realistic issues of SISs with risk-based EUC cost involved.

CRediT authorship contribution statement

Aibo Zhang: Visualization, Methodology, Software, Investigation. **Himanshu Srivastav:** Visualization, Methodology. **Anne Barros:** Methodology, Writing - review & editing, Supervision. **Yiliu Liu:** Conceptualization, Validation, Writing - review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

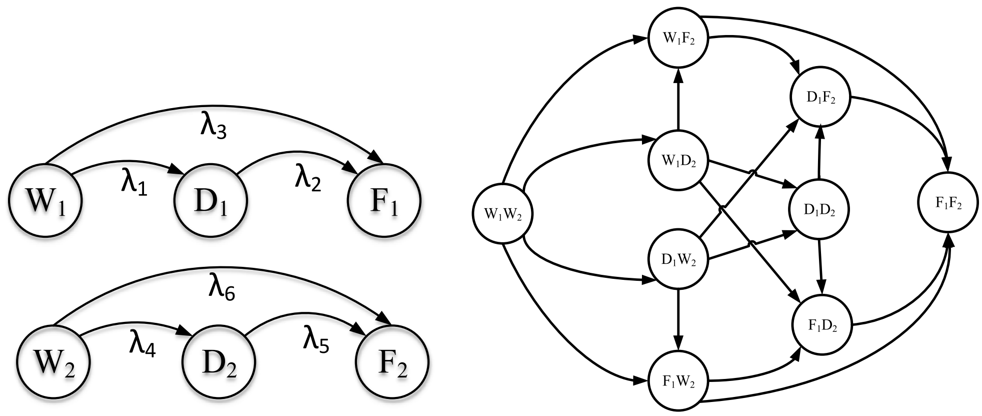
Acknowledgment

The research is supported by Norwegian Research Council under Grant No. 309628.

The authors are grateful to three anonymous reviewers for their useful comments and suggestions to the original version of this paper.

Appendix A. Possible states for 1oo2 configuration

See Table A.1 and Fig. A.1.



(a) (b)

Fig. A.1. State transition diagrams for (a) 1oo1 configuration and (b) 1oo2 configuration.

Table A.1
Possible states for 1oo2 configuration.

State	Notation
1	W_1W_2
2	W_1D_2
3	W_1F_2
4	D_1W_2
5	D_1D_2
6	D_1F_2
7	F_1W_2
8	F_1D_2
9	F_1F_2

Appendix B. Matrices mentioned in this paper

There are 3 possible states for each single unit under study. They are denoted by State W (working), State D (degraded) and State F (failed).

Transition rate matrix $\mathbf{Q}_{U_1}$ and $\mathbf{Q}_{U_2}$ for unit 1 and 2:

$$\mathbf{Q}_{U_1} = \begin{array}{cc} & \begin{array}{ccc} W_1 & D_1 & F_1 \end{array} \\ \begin{array}{c} W_1 \\ D_1 \\ F_1 \end{array} & \begin{pmatrix} -(\lambda_1+\lambda_3) & \lambda_1 & \lambda_3 \\ & -\lambda_2 & \lambda_2 \\ & & \end{pmatrix} \end{array} \quad \mathbf{Q}_{U_2} = \begin{array}{cc} & \begin{array}{ccc} W_2 & D_2 & F_2 \end{array} \\ \begin{array}{c} W_2 \\ D_2 \\ F_2 \end{array} & \begin{pmatrix} -(\lambda_4+\lambda_6) & \lambda_4 & \lambda_6 \\ & -\lambda_5 & \lambda_5 \\ & & \end{pmatrix} \end{array}$$

Transition rate matrix $\mathbf{Q}$ for 1oo2 configuration

$$\mathbf{Q} = \begin{array}{cc} & \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{array} & \begin{pmatrix} -\Sigma & \lambda_4 & \lambda_6 & \lambda_1 & & & \lambda_3 & & \\ & -\Sigma & \lambda_5 & & \lambda_1 & & & \lambda_3 & \\ & & -\Sigma & & & \lambda_1 & & & \lambda_3 \\ & & & -\Sigma & \lambda_4 & \lambda_6 & \lambda_2 & & \\ & & & & -\Sigma & \lambda_5 & & \lambda_2 & \\ & & & & & -\Sigma & & & \lambda_2 \\ & & & & & & -\Sigma & \lambda_4 & \lambda_6 \\ & & & & & & & -\Sigma & \lambda_5 \\ & & & & & & & & -\Sigma \end{pmatrix} \end{array}$$

The coverage indicator α_i is defined as the conditional probability that a degraded state will be detected by the proof test of unit i, given that degradation has occurred when initiating the proof test.

α_i = Pr(Degradation is detected in a proof test |Degradation has occurred)

$\mathbf{M}$ represents the probability matrix of different states after a testing and repair action.

$\mathbf{M}_{U_1}$ represents the probability matrix of different states after a testing and repair action of unit 1.

$\mathbf{M}_{U_2}$ represents the probability matrix of different states after a testing and repair action of unit 2.

Matrix $\mathbf{M}$ for simultaneous testing with testing coverage α_i and maintenance strategy I

$$\mathbf{M} = \begin{array}{cc} & \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{array} & \begin{pmatrix} 1 & & & & & & & & \\ \alpha_2 & 1-\alpha_2 & & & & & & & \\ 1 & & & & & & & & \\ \alpha_1 & & & 1-\alpha_1 & & & & & \\ \alpha_1\alpha_2 & (1-\alpha_2)\alpha_1 & & (1-\alpha_1)\alpha_2 & (1-\alpha_1)(1-\alpha_2) & & & & \\ \alpha_1 & & & 1-\alpha_1 & & & & & \\ 1 & & & & & & & & \\ \alpha_2 & 1-\alpha_2 & & & & & & & \\ 1 & & & & & & & & \end{pmatrix} \end{array}$$

Matrix $\mathbf{M}$ for staggered testing with testing coverage α_i and maintenance strategy II

$$\mathbf{M}_{U_1} = \begin{array}{cc} & \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{array} & \begin{pmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & 1 & & & & & & \\ \alpha_1 & & & 1-\alpha_1 & & & & & \\ & \alpha_1 & & & 1-\alpha_1 & & & & \\ & & \alpha_1 & & & 1-\alpha_1 & & & \\ 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & 1 & & & & & & \end{pmatrix} \end{array}$$

$$\mathbf{M}_{U_2} = \begin{array}{cc} & \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{array} & \begin{pmatrix} 1 & & & & & & & & \\ \alpha_2 & 1-\alpha_2 & & & & & & & \\ 1 & & & & & & & & \\ & & & 1 & & & & & \\ & & & \alpha_2 & 1-\alpha_2 & & & & \\ & & & 1 & & & & & \\ & & & & & & 1 & & \\ & & & & & & \alpha_2 & 1-\alpha_2 & \\ & & & & & & 1 & & \end{pmatrix} \end{array}$$

Matrix $\mathbf{M}$ for staggered testing with testing coverage α_i and maintenance strategy III

$$\mathbf{M}_{U_1} = \begin{array}{c} \\ 1\\2\\3\\4\\5\\6\\7\\8\\9 \end{array} \begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \left(\begin{array}{ccccccccc} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & 1 & & & & & & \\ \alpha_1 & & & 1-\alpha_1 & & & & & \\ & \alpha_1 & & & 1-\alpha_1 & & & & \\ & & \alpha_1 & & & 1-\alpha_1 & & & \\ 1 & & & & & & & & \\ 1 & & & & & & & & \\ 1 & & & & & & & & \end{array}\right) \end{array}$$

$$\mathbf{M}_{U_2} = \begin{array}{c} \\ 1\\2\\3\\4\\5\\6\\7\\8\\9 \end{array} \begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \left(\begin{array}{ccccccccc} 1 & & & & & & & & \\ \alpha_2 & 1-\alpha_2 & & & & & & & \\ 1 & & & & & & & & \\ & & & 1 & & & & & \\ & & & \alpha_2 & 1-\alpha_2 & & & & \\ 1 & & & & & & & & \\ & & & & & & 1 & & \\ & & & & & & \alpha_2 & 1-\alpha_2 & \\ 1 & & & & & & & & \end{array}\right) \end{array}$$

References

[1] Rausand M, Høyland A. System reliability theory: Models, statistical methods, and applications, Vol. 396. John Wiley & Sons; 2003.

[2] Rausand M. Reliability of safety-critical systems: Theory and applications. John Wiley&Sons; 2014.

[3] IEC 61508 functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.

[4] Hauge S, Lundteigen MA, Hokstad P, Håbrekke S. Reliability prediction method for safety instrumented systems–PDS method handbook, 2010 edition. SINTEF report STF50 A 6031, 2010.

[5] Longhi AEB, Pessoa AA, de Almada Garcia PA. Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. Reliab Eng Syst Saf 2015;142:525–38.

[6] Summers AE. Viewpoint on ISA TR84. 0.02-simplified methods and fault tree analysis. ISA Trans 2000;39:125–31.

[7] Chiremsel Z, Said RN, Chiremsel R. Probabilistic fault diagnosis of safety instrumented systems based on fault tree analysis and Bayesian network. J Fail Anal Prev 2016;16(5):747–60.

[8] Dutuit Y, Innal F, Rauzy A, Signoret J-P. Probabilistic assessments in relationship with safety integrity levels by using fault trees. Reliab Eng Syst Saf 2008;93(12):1867–76.

[9] 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(4):594–604.

[10] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab Eng Syst Saf 2015;133:212–22.

[11] 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.

[12] Azizpour H, Lundteigen MA. Analysis of simplification in Markov-based models for performance assessment of Safety Instrumented System. Reliab Eng Syst Saf 2019;183:252–60.

[13] Torres ES, Sriramula S, Celeita D, Ramos G. Reliability model and sensitivity analysis for electrical/electronic/programmable electronic safety-related systems. IEEE Trans Ind Appl 2020;56(4):3422–30.

[14] Cai B, Huang L, Xie M. Bayesian networks in fault diagnosis. IEEE Trans Ind Inf 2017;13(5):2227–40.

[15] Cai B, Xie M, Liu Y, Liu Y, Feng Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab Eng Syst Saf 2018;172:216–24.

[16] Cai B, Kong X, Liu Y, Lin J, Yuan X, Xu H, et al. Application of Bayesian networks in reliability evaluation. IEEE Trans Ind Inf 2018;15(4):2146–57.

[17] Liu Y, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prev Process Ind 2011;24(1):49–56.

[18] 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 O 2014;228(4):409–18.

[19] Liu Y, Rausand M. Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems. Reliab Eng Syst Saf 2016;145:366–72.

[20] Meng H, Kloul L, Rauzy A. Modeling patterns for reliability assessment of safety instrumented systems. Reliab Eng Syst Saf 2018;180:111–23.

[21] Čepin M, Mavko B. Probabilistic safety assessment improves surveillance requirements in technical specifications. Reliab Eng Syst Saf 1997;56(1):69–77.

[22] Martorell S, Sanchez A, Serradell V. Age-dependent reliability model considering effects of maintenance and working conditions. Reliab Eng Syst Saf 1999;64(1):19–31.

[23] Vaurio J. On time-dependent availability and maintenance optimization of standby units under various maintenance policies. Reliab Eng Syst Saf 1997;56(1):79–89.

[24] Martorell P, Martón I, Sánchez A, Martorell S. Unavailability model for demand-caused failures of safety components addressing degradation by demand-induced stress, maintenance effectiveness and test efficiency. Reliab Eng Syst Saf 2017;168:18–27.

[25] 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.

[26] Zio E. Some challenges and opportunities in reliability engineering. IEEE Trans Reliab 2016;65(4):1769–82.

[27] Zhang A, Barros A, Liu Y. Performance analysis of redundant safety-instrumented systems subject to degradation and external demands. J Loss Prev Process Ind 2019;62:103946.

[28] Zhang A, Liu Y, Barros A, Kassa E. A degrading element of safety-instrumented systems with combined maintenance strategy. In: Proceedings of the 29th European safety and reliability conference. Hannover, Germany: Research Publishing Services; 2019.

[29] Zhang A, Zhang T, Barros A, Liu Y. Optimization of maintenances following proof tests for the final element of a safety-instrumented system. Reliab Eng Syst Saf 2020;196:106779.

[30] 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(4):437–49.

[31] 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.

[32] Srivastav H, Barros A, Lundteigen MA. Modelling framework for performance analysis of SIS subject to degradation due to proof tests. Reliab Eng Syst Saf 2020;195:106702.

[33] Qingfeng W, Wenbin L, Xin Z, Jianfeng Y, Qingbin Y. Development and application of equipment maintenance and safety integrity management system. J Loss Prev Process Ind 2011;24(4):321–32.

[34] Nystad BH, Gola G, Hulsund JE, Roverso D. Technical condition assessment and remaining useful life estimation of choke valves subject to erosion. In: Annual conference of the prognostics and health management society. 2010. p. 11–13.

[35] Nystad BH, Gola G, Hulsund JE. Lifetime models for remaining useful life estimation with randomly distributed failure thresholds. In: First European conference of the prognostics and health management society, vol. 3, 2012.

[36] Gola G, Nystad BH. Prognostics and health management of choke valves subject to erosion: A diagnostic-prognostic frame for optimal maintenance scheduling. In: Diagnostics and prognostics of engineering systems: Methods and techniques. IGI Global; 2013, p. 313–31.

[37] Zhang Y, Barros A, Rauzy A. Assessment of a condition-based maintenance policy for Subsea systems: A preliminary study. In: Risk, reliability and safety: Innovating theory and practice: Proceedings of ESREL 2016. Glasgow, Scotland: CRC Press; 2017.

[38] Levitin G, Lisnianski A. Optimization of imperfect preventive maintenance for multi-state systems. Reliab Eng Syst Saf 2000;67(2):193–203.

[39] Soro IW, Nourelfath M, Aït-Kadi D. Performance evaluation of multi-state degraded systems with minimal repairs and imperfect preventive maintenance. Reliab Eng Syst Saf 2010;95(2):65–9.

[40] Liu Y, Huang H-Z. Optimal replacement policy for multi-state system under imperfect maintenance. IEEE Trans Reliab 2010;59(3):483–95.

[41] Nourelfath M, Châtelet E, Nahas N. Joint redundancy and imperfect preventive maintenance optimization for series–parallel multi-state degraded systems. Reliab Eng Syst Saf 2012;103:51–60.

[42] Sheu S-H, Chang C-C, Chen Y-L, Zhang ZG. Optimal preventive maintenance and repair policies for multi-state systems. Reliab Eng Syst Saf 2015;140:78–87.

[43] Ossai CI. Remaining useful life estimation for repairable multi-state components subjected to multiple maintenance actions. Reliab Eng Syst Saf 2019;182:142–51.

[44] Liu Y, Huang H-Z, Wang Z, Li Y, Yang Y. A joint redundancy and imperfect maintenance strategy optimization for multi-state systems. IEEE Trans Reliab 2013;62(2):368–78.

[45] Alaswad S, Xiang Y. A review on condition-based maintenance optimization models for stochastically deteriorating system. Reliab Eng Syst Saf 2017;157:54–63.
[46] Sal R, Nait-Said R, Bourareche M. Dealing with uncertainty in effect analysis of test strategies on safety instrumented system performance. Int J Syst Assur Eng Manag 2017;8(2):1945–58.
[47] Torres-Echeverria A, Martorell S, Thompson H. Modelling and optimization of proof testing policies for safety instrumented systems. Reliab Eng Syst Saf 2009;94(4):838–54.
[48] Castro IT, Barros A, Grall A. Age-based preventive maintenance for passive components submitted to stress corrosion cracking. Math Comput Modelling 2011;54(1–2):598–609.
[49] Huynh KT, Castro IT, Barros A, Bérenguer C. On the use of mean residual life as a condition index for condition-based maintenance decision-making. IEEE Trans Syst Man Cybern A 2013;44(7):877–93.
[50] Laskowska EM, Vatn J. State modelling and prognostics of safety valves used in the oil and gas industry. In: Proceedings of the 29th European safety and reliability conference. 2019.
[51] IEC 61511 functional safety – Safety instrumented systems for the process industry sector. 2016.
[52] Liu Y. Optimal staggered testing strategies for heterogeneously redundant safety systems. Reliab Eng Syst Saf 2014;126:65–71.
[53] Williams M. Lower your operating costs with regular valve maintenance. Tech. rep., PlantServices; 2004, https://www.plantservices.com/articles/2004/212/.