Reliability assessment for final elements of SISs with time dependent failures

Shengnan Wu[a,b] Laibin Zhang[a] Mary Ann Lundteigen[b] Yiliu Liu[b] Wenpei Zheng[a]

[a]College of Mechanical and Transportation Engineering, China University of Petroleum-Beijing, Beijing, China

[b]Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Abstract:

Reliability assessment for safety-instrumented systems (SISs) plays a vital role in improving the design of SISs. Traditional methods for SIS reliability assessment that assume constant failure rates are, however, not realistic for many final elements of SISs, e.g. electro-mechanical and hydraulic/mechanical actuators that are subject to degradation. This paper presents an approach for the reliability assessment of SIS final elements with time dependent failure rates. Different operational issues, such as partial and full testing, are investigated for their effects on reliability of SISs. Approximation formulas for evaluation of average probability of failure on demand ($\mathrm{PFD}_{\mathrm{avg}}$) involving degradation are developed within different subsequent proof testing intervals, and Weibull distributions are adopted to model the degradation processes of the final elements. The corresponding numerical results of $\mathrm{PFD}_{\mathrm{avg}}$ from the set of the derived formulations are validated by Petri nets models that are developed for different scenarios. Shutdown valves installed as part of a high integrity pressure protection system are analyzed as the case, to illustrate the feasibility of the proposed approach, and also demonstrate that the approximation can provide possibilities for testing strategies design and optimization.

Key words: Final elements, Reliability assessment, Partial tests, Approximation formulas, Petri nets models

1. Introduction

Safety-instrumented systems (SISs) are installed in many industries to detect the onset of hazardous events, and automatically or manually manage such situations to avoid occurrence of accidents. A SIS generally consists of sensors (e.g. pressure transmitters), logic solver(s) (e.g. programmable logic controllers) and final elements (e.g. valves, breakers and switches). Final elements may be regarded as the most vital subsystems as they (upon events like process upsets) interact directly with the process, but due to the force and motion to be exerted when action is asked, these devices are rather vulnerable to creeping degradation processes. Therefore their preparedness to act when required has to be checked rather frequently. The final elements are normally passive during normal operation, and they may for this reason be subjected to failures that cannot be revealed unless a test is carried out (or a real demand for safety function occurs). Such failures are therefore regarded as hidden (or undetected) dangerous failure. Periodical tests are able to reveal these hidden failures, and the average probability of failures on demand ($\mathrm{PFD}_{\mathrm{avg}}$) is the suggested reliability measure for safety instrumented functions (SIFs) carried out by a SIS when low-demand mode is assumed [1]. In current literature regarding reliability assessment, the effects of periodical proof tests, where all hidden failures are assumed to be discovered (so called full proof tests), have been well studied [2-4].

However, for subsea exploration and production, frequent proof tests may be not realistic. Taking shutdown valves of SISs final elements for instance, full proof testing (FT) on these valves include regular full stroke operation and leakage testing. FT can fully verify that the valves close and keep tight on demand, but FT may also bring some negative impacts to valves (e.g. wear of the valve seat area) due to strong stresses [5]. In addition, the shutdown of the whole system needed in proof tests can lead to some other operational problems, e.g. during start-up [5, 6]. Therefore, partial testing (PT) has been introduced in recent years as a supplement to FT [5, 7, 8]. For the shutdown valve case, a partial test means to partially operate a valve, which meet the requirement for valve movement and can also detect the several types of dangerous failures such as the failure mode “fail to close on demand”. These partial tests can be performed without any extra production disturbances.

Some reliability assessment approaches have been developed to evaluate influence of PT. Innal et al. [9] have considered impacts of partial tests and established new generalized formulations for SIS unavailability using the multi-phase Markov models. Jin and Rausand [10] have developed approximate generalized expressions for general k-out-of-n (koon) systems subject to partial-tests. Brissaud et al. [11] have proposed formulas for koon systems subject to non-periodic partial-testing. In addition, Pascual et al. [12] have explored the optimal partial testing intervals by considering periodic and non-periodic tests, and Torrres-Echeverria et al. [2] have proposed a method to optimize proof testing intervals partial tests.

However, several issues need to be further investigated when these approaches are applied to the subsea final elements. For example, many simplified formulas for PFDavg in [1, 13, 14] assume the failures of SISs are exponentially distributed, . But in fact for many final elements, like actuated valves involving electro-mechanical and/or hydraulic-mechanical components working in a subsea environment, they are more likely to deteriorate with an increasing failure rates instead of constant failure rates over time especially in the wear-out period [14, 15]. Moreover, some other assumptions relied by the existing literatures [9, 16-18] are also questionable in a subsea context, e.g. the failure rates are generally assumed to be constant, which mean that all channels restored after a proof test are in an as-good-as-new state. This has been a generally accepted limitation for these methods, but it is not a very well suited assumption for equipment that is subject to degradation of time.

For the system with non-constant failure rates, Weibull distributions as a suitable choice are used to model the degradation behaviors and Weibull parameters for all the mechanical equipment make the reliability calculation more suitable. A few case studies related to Weibull distributed components have been investigated in a full proof test. Jigar [19] proposed an analytical formula for reliability assessment based on ratio between cumulative distribution functions for a full test. Rogova et al. [20] have extended Jigar model and developed an analytical method including non-constant failure rate and common cause failures (CCFs). The common limitation is that effects of partial testing mentioned above are excluded and the forecasting a system behavior in the rest subsequent proof testing intervals are not taken into account.

The objective of this paper will therefore develop new approximations of $\mathrm{PFD}_{\mathrm{avg}}$ based on the time-dependent failure rates. The potential contributions can be specified as:

- A new approach is proposed to assess the influences of time dependent failures on SISs final actuators.
- Changing of probability of failure on demand is identified and conditional probability is introduced to develop approximation formulas under subsequent proof testing intervals.
- The effects of partial tests are taken into consideration when evaluating degradations.

The rest of this paper is organized as follows: In Section 2, the definition and assumptions of SISs final elements will be discussed. Section 3 presents the approximation $\mathrm{PFD}_{\mathrm{avg}}$ formulas for partial testing considering time-dependent failure rates based on Weibull distribution; verifications are given through special cases. In Section 4, reliability assessment results based on Petri-net simulation will be compared with those by approximation formulas. A case study for HIPPS shutdown valves including 1oo1 and 1oo2 systems is introduced in Section 5, to demonstrate the applications of proposed models. Concluding remarks and direction of future work are given in Section 6.

2. Definitions and assumptions

This section introduces some selected key concepts associated with failure classification，the rationales for introducing partial tests, assumptions for approximation formulas and system description.

2.1 Classification of failures

Dangerous failures of a SIS, which are able to prevent the SIS from performing its safety function on demand, are only considered in this paper. Dangerous failures of a SIS may be classified into dangerous detected (DD) failures and dangerous undetected (DU) failures (hidden failures) [1, 14]. DD failures are those that can be detected by the diagnostics/self-testing immediately after they occur, while DU failures remain hidden until the safety function is carried out, either by FT, PT or a real demand. In this paper, DU failures are further split into two categories when involving PT: (a) failures detected by a PT, and (b) remaining failures only detected by FT, assuming that the FT can detect all DU failures.

2.2 Rationales and basic concepts of PT

PT of final elements, like actuated valves, has been introduced as a supplement to FT. A PT interval is the interval between two subsequent stroke tests which are designed to reveal one or more specific types of DU failures by small movements. Such valve movement is so small that the impact on the process flow or pressure is negligible and also does not cause disturbances that may lead to process shutdowns. In a subsea environment, it is of high importance to reduce the number of planned and unplanned stops. All means to avoid stops that are not in response to true safety demands are therefore of interest. One reason is the complications that may occur while starting up (e.g. from hydrate formation), and another reason is the economic loss from being down (due to not fulfilling contractual requirements for delivery)[5].

Only some specific failure modes are detected in a PT interval, meaning that PT cannot fully replace FT, but it is possible to imagine that the interval of FT can be longer while keeping the SIS at the same availability level. Except the benefit in avoiding production loss, partial tests could also reduce wear of the valve seat area due to the less stress caused by PT in a fully closed state. The probability of sticking seals is also reduced due to more movements of valves in PT [21]. However, it is noticed that the valves should be designed to tolerate partial movement, and the increased wear does not result in spurious activations.

2.3 Assumptions

In the following analysis of this paper, the common assumptions have been made:

- The failure rate of a final element is assumed to follow Weibull distribution (due to degradation effects of being in subsea environment with limited access to regular maintenance).
- A limited number of DU failure modes can be revealed during a PT interval, whereas FT may reveal all DU failures.
- If a DU failure is revealed by PT or FT, it is necessary to initiate a request for repair. The following assumptions apply to the repair action:
  - ✧ Any DU failure revealed during a PT or FT interval is subject to minimal repair only. This means that the valve is brought to a functioning state, but not to an as good as new state.
  - ✧ One could foresee that a replacement or more extensive overhaul is scheduled on regular intervals (e.g. every 5 years) based on the recommendations from manufacturer. The effects of such overhaul are not included in the proposed formulas, but would represent a return to be in an as good as new state.
- All actuated valves are initially (i.e. at first start-up of subsea facility) in a perfect/functioning state.
- All partial tests are performed simultaneously for all actuator valves.
- The time spent in both a full and partial test is negligible.
- Valves will normally have zero diagnostic coverage, which means that no effect of DD failures have been included.
- Common cause failures (CCFs) in a 1oo2 system are also excluded.

2.4 System description

The HIPPS is a type of SISs protecting a platform from pressure build-up that may cause pipeline rupture by shutting off the source before exceeding the maximum pressure [5, 7]. HIPPS valves as the last safety barriers are always operated in low demand mode [22], and they can quickly stop the flow to avoid that the high pressure enters pipeline sections which are designed for low pressure.

Consider HIPPS valves that are tested at regular intervals. An important issue is to determine what kinds of dangerous failure modes of the valves are. They are specified as follows:

- Fail to close: The valve is not able to close on command. Such failure mode can be detected by PT. Experiences have shown that if valves are not activated (at all or very seldom), they may stick in one position. In fact, sticking in open position accounts for large percentage of the failures recorded for shutdown valves. Delayed operation can also be related to sticking, but also other causes (e.g. capacity constraints from operation of multiple valves).
- Leakage in closed position (internal leakage): The valve is able to close on command, but there is a leakage through the closed valve that is higher than an accepted leakage. Such failures cannot normally be detected by PT but FT, but for subsea it may be possible to use other planned and unplanned stops to check if this failure is present.
- Other dangerous failures: Leakage to environment (external leakage) that may be detected by leakage detection and monitoring systems, and is not normally a type of failure that would be revealed independently of PT/FT.

These failure modes cannot be detected automatically unless we closed the valves, and these failures are therefore recognized DU-failures during normal operation. It is also noticeable that the first one which can be detected by PT is considered *first* type of failure and the latter two which are only detected by FT are considered as *second* type of failure.

3. Approximation formulas

This paper is limited to SISs operating in low demand modes defined by key standards, such as IEC 61508 and IEC 61511[1, 23]. Two sets of formulas will be presented in this section:

- Time-dependent failures,
- Modeling PFD_{avg} for full proof and partial testing.

3.1 Time-dependent failures

Weibull distribution is one of the most widely used life distribution in reliability analysis, and the distribution includes a scale parameter and shape parameter required to for modeling of failure rates that can be decreasing, constant and increasing [14]. The time-dependent failure rate function denoted $z(t)$ for a single actuated valve with DU-failures is introduced and defined as:

$$z(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1-F(t)} = \alpha\lambda^{\alpha}t^{\alpha-1} \quad (1)$$

where λ is a scale parameter, α is a shape parameter, $f(t)$ is the probability density function, $\mathrm{R(t)}$ and $\mathrm{F(t)}$ is survival and failure probability distribution respectively, and they may be found in e.g. [14].

The time-dependent failure rate function for DU-failures is approximated by an average failure rate and the average failure rate in the proof test interval $(0, \tau)$ is denoted $z_{avg}\,(0, \tau)$. So we have:

$$z_{avg}\left(0,\tau\right) = \frac{1}{\tau}\int_0^\tau z(t)dt = \frac{1}{\tau}\int_0^\tau \alpha\lambda^\alpha t^{\alpha-1}dt = \lambda^\alpha\tau^{\alpha-1} \quad (2)$$

The average failure rate in any test interval (τ_{n-1}, τ_n) is denoted z_{avg} (τ_{n-1}, τ_n). So we have:

$$z_{avg}\left(\tau_{n-1},\tau_n\right) = \frac{1}{\tau_n-\tau_{n-1}}\int_{\tau_{i-1}}^{\tau_i} z(t)dt = \lambda^\alpha \frac{\tau_n^\alpha-\tau_{n-1}^\alpha}{\tau_n-\tau_{n-1}} \quad (3)$$

Generally, the time dependent $PFD(t)$ for DU-failures of any system occurring in a proof testing interval [0, τ] can be expressed as:

$$PFD\left(t\right) = \Pr(T_{DU} \leq t) = F(t) \quad (4)$$

where $Pr(T_{DU} \leqslant t)$ is the probability that a DU-failure is occurring in a proof test and T_{DU} is the time of failure occurrence.

Taking 1oo1 system for instance, based on the time-dependent failure rate *z(t)* and average time-dependent failure rate z_{avg} *(0, τ),* we have $PFD_1(t)$ in the first proof testing interval (0, *τ*):

$$PFD_1\left(t\right) = 1-e^{-(\lambda t)^\alpha} = 1-e^{-\frac{z(t)}{\alpha}t} \quad (5)$$

3.2 Modeling PFD_{avg} for full proof and partial testing

The assumption about time-dependent failures or regular testing that does not involve full renewal will result in a PFD_{avg} that will change (most likely increase) over time. Conditional probabilities are introduced to assess the changes. For comparisons, three sets of analytical formulas have been derived in the following sub-sections:

- Formulas excluding the effects of PT
- Formulas including the effects of PT
- Formulas considering the combination of PT and FT

Only formulas for 1oo1 and 1oo2 systems have been developed, under the arguments that they are the most common systems for actuated valves.

3.2.1 PFD_{avg} with FT only

Several full proof tests are normally carried out before overhaul, and *i* stands for the number of full proof tests. Due to the increasing failure rate actuated valves have, the PFD (t) in current FT interval is different from that in the previous FT interval. PFD_{avg} should be calculated for subsequent intervals excluding the effects of PT:

- For 1oo1 system that is subject to FT only, the PFD_{avg} in the first proof test (0, τ) becomes:

$$PFD_{avg} = \frac{1}{\tau}\int_0^\tau PFD\left(t\right)dt = \frac{1}{\tau}\int_0^\tau \Pr(T_{DU} \leq t)dt = \frac{1}{\tau}\int_0^\tau 1-e^{-\frac{z(t)}{\alpha}t}dt \quad (6)$$

$$PFD_{avg} \approx \frac{1}{\tau}\int_0^\tau \frac{z(t)}{\alpha}tdt = \frac{z_{avg}(0,\tau)\cdot\tau}{\alpha+1} \quad (7)$$

Note that the approximation $z(t)\cdot t/_{\alpha}$ in Eq. (7) takes low values, i.e. <0.01. The Eq. (7) is the approximation that is derived from the Eq. (6).

So we then have the PFD_{avg} in the second proof test (τ, 2τ):

$$PFD_{avg} = \frac{1}{\tau}\int_{\tau}^{2\tau} PFD\left(t\right)dt = \frac{1}{\tau}\int_{\tau}^{2\tau} \Pr(T_{DU} \le t / T_{DU} > \tau)dt$$

$$= \frac{1}{\tau}\int_{\tau}^{2\tau} \frac{\Pr(T_{DU} \le t) - \Pr(T_{DU} \le \tau)}{\Pr(T_{DU} > \tau)}dt = \frac{1}{\tau}\int_{\tau}^{2\tau} \frac{(1 - e^{-\frac{z(t)}{\alpha}t}) - (1 - e^{-\frac{z(\tau)}{\alpha}\tau})}{e^{-\frac{z(\tau)}{\alpha}\tau}}dt \quad (8)$$

$$PFD_{avg} \approx \frac{1}{\tau}\int_{\tau}^{2\tau} \frac{\frac{z(t)}{\alpha}t - \frac{z(\tau)}{\alpha}\tau}{1 - \frac{z(\tau)}{\alpha}\tau}dt = \frac{\frac{z_{avg}\left(\tau, 2\tau\right)}{\alpha + 1} \cdot \frac{(2\tau)^{\alpha+1} - \tau^{\alpha+1}}{(2\tau)^{\alpha} - \tau^{\alpha}} - \frac{z(\tau)}{\alpha}\tau}{1 - \frac{z(\tau)}{\alpha}\tau} \quad (9)$$

where $z_{avg}(\tau,\ 2\tau)$ is the average failure rate in second FT interval.
Similarly, in subsequent proof test $((i-1)\tau, i\tau)$, the $\mathrm{PFD}_{\mathrm{avg}}$ of 1oo1 system can be approximated as:

$$PFD_{avg} \approx \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{\frac{z(t)}{\alpha}t - \frac{z\left((i-1)\tau\right)}{\alpha} \cdot \left(i-1\right)\tau}{1 - \frac{z\left((i-1)\tau\right)}{\alpha} \cdot \left(i-1\right)\tau}dt = \frac{\frac{z_{avg}\left((i-1)\tau, i\tau\right)}{\alpha + 1} \cdot \frac{(i\tau)^{\alpha+1} - ((i-1)\tau)^{\alpha+1}}{(i\tau)^{\alpha} - ((i-1)\tau)^{\alpha}} - \frac{z\left((i-1)\tau\right)}{\alpha} \cdot \left(i-1\right)\tau}{1 - \frac{z\left((i-1)\tau\right)}{\alpha} \cdot \left(i-1\right)\tau}$$

(10)

where $z_{avg}((i-1)\tau, i\tau)$ is the average failure rate in subsequent FT interval.

- We may derive $\mathrm{PFD}_{\mathrm{avg}}$ for 1oo2 system using the same approach (but replacing failure function of single element with two elements). The $\mathrm{PFD}_{\mathrm{avg}}$ in the first proof test $(0, \tau)$ therefore becomes:

$$PFD_{avg} = \frac{1}{\tau}\int_{0}^{\tau} \Pr(T_{DU} \le t)dt = \frac{1}{\tau}\int_{0}^{\tau} (1 - e^{-\frac{z(t)}{\alpha}t})^{2}dt \quad (11)$$

$$PFD_{avg} \approx \frac{1}{\tau}\int_{0}^{\tau} (\frac{z(t)}{\alpha}t)^{2}dt = \frac{(z_{avg}(0, \tau) \cdot \tau)^{2}}{2\alpha + 1} \quad (12)$$

In the second proof test (τ, 2τ), we have:

$$PFD_{avg} = \frac{1}{\tau}\int_{0}^{\tau} PFD\left(t\right)dt = \frac{1}{\tau}\int_{\tau}^{2\tau} \Pr(T_{DU} \le t / T_{DU} > \tau)dt = \frac{1}{\tau}\int_{\tau}^{2\tau} \frac{(1 - e^{-\frac{z(t)}{\alpha}t})^{2} - (1 - e^{-\frac{z(t)}{\alpha}t})^{2}}{1 - (1 - e^{-\frac{z(t)}{\alpha}t})^{2}}dt \quad (13)$$

$$PFD_{avg} \approx \frac{1}{\tau}\int_{\tau}^{2\tau} \frac{(\frac{z(t)}{\alpha}t)^{2} - (\frac{z(\tau)}{\alpha}\tau)^{2}}{1 - (\frac{z(\tau)}{\alpha}\tau)^{2}}dt = \frac{\frac{\left(z_{avg}\left(\tau, 2\tau\right)\right)^{2}}{2\alpha + 1} \cdot \frac{(2\tau)^{2\alpha+1} - \tau^{2\alpha+1}}{\left((2\tau)^{\alpha} - \tau^{\alpha}\right)^{2}} \cdot \tau - (\frac{z(\tau)}{\alpha}\tau)^{2}}{1 - (\frac{z(\tau)}{\alpha}\tau)^{2}} \quad (14)$$

Similarly, in subsequent proof test$((i-1)\tau, i\tau)$, the formula can be expressed as :

$$PFD_{avg} \approx \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{\left(\frac{z(t)}{\alpha}t\right)^2 - \left(\frac{z\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2}{1-\left(\frac{z\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2}dt$$

$$= \frac{\frac{\left(z_{avg}\left((i-1)\tau, i\tau\right)\right)^2}{2\alpha+1}\cdot\frac{(i\tau)^{2\alpha+1}-((i-1)\tau)^{2\alpha+1}}{(i\tau)^{\alpha}-((i-1)\tau)^{\alpha}}\cdot\tau-\left(\frac{z\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2}{1-\left(\frac{z\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2} \qquad (15)$$

When $\alpha = 1$, for 1oo1 system, $\mathrm{PFD}_{\mathrm{avg}} = \lambda\tau/2$, and for 1oo2 system, $\mathrm{PFD}_{\mathrm{avg}} = (\lambda\tau)^2/3$, which are identical to $\mathrm{PFD}_{\mathrm{avg}}$ formulas in some work [14] for systems with constant failure rate in proof test interval [0, τ]. This is also the verification for the proposed formulas by comparing special cases with widely accepted formulas.

3.2.2 $\mathrm{PFD}_{\mathrm{avg}}$ of PT

DU failure rate in this section is the sum of two rates: DU failure rate corresponding to failure modes revealed by PT is expressed as, $z_{PT}(t) = \alpha \cdot \lambda_{PT}^{\alpha} \cdot \tau^{\alpha-1}$ where λ_{PT} is a parameter in a partial test; and DU failure rate with regard to failure modes revealed by a FT becomes, $z_{FT}(t) = \alpha \cdot \lambda_{FT}^{\alpha} \cdot \tau^{\alpha-1}$ where λ_{FT} is a parameter in a proof test, and they agree $\lambda_{PT}^{\alpha} + \lambda_{FT}^{\alpha} = \lambda^{\alpha}$. Note that there are two assumptions for not as good as new states in partial tests:

- The remaining DU failure modes not detected by PT will make the system in not as good as new state.
- Effects of degradations may exist if there is no DU-failure revealed in one partial test or minor repairs after a test. The actuated valve still performs function in the next PT interval, but it is not as-good-as-new since other properties of the actuated valve have not been changed.

Several partial tests are normally carried out during a FT interval, and *m* stands for the number of partial tests in a proof test interval τ. Due to the increasing failure rate actuated valves have, their $\mathrm{PFD}_{\mathrm{PT}}(t)$ in current PT interval is also different from that in the previous PT interval. $\mathrm{PFD}_{\mathrm{avg}}$ should be calculated by introducing conditional probabilities for different periods:

First PTinterval [0,τ₁]: Under the assumption that the state is as good as new at time zero, we get:

$$PFD_{avg,1} = \frac{1}{\tau_1}\int_0^{\tau_1} PFD_{PT}(t)dt = \frac{1}{\tau_1}\int_0^{\tau_1} \Pr(T_{DU,PT} \le t)dt \quad (16)$$

where $PFD_{PT}(\mathrm{t}) = Pr(T_{DU,PT} \leqslant t)$ is the probability that DU-failures are occurring in PT intervals and $T_{DU,PT}$ is the time for failure occurrence in a PT.

Second PT interval [τ₁, τ₂]: The PFD_{avg} in the second testing interval is conditional based on the state of the system in the first interval where no failure is assumed to occur, and it may be written as

$$
\begin{aligned}
PFD_{avg,2} &= \frac{1}{\tau_2-\tau_1}\int_{\tau_1}^{\tau_2} PFD(t)dt \\
&= \frac{1}{\tau_2-\tau_1}\int_{\tau_1}^{\tau_2} \Pr(T_{DU,PT}\le t/T_{DU,PT}>\tau_1)dt \qquad (17)\\
&= \frac{1}{\tau_2-\tau_1}\int_{\tau_1}^{\tau_2} \frac{\Pr(T_{DU,PT}\le t)-\Pr(T_{DU,PT}\le\tau_1)}{\Pr(T_{DU,PT}>\tau_1)}dt
\end{aligned}
$$

Subsequent PT interval [τ$_{\mathbf{m-1}}$, τ$_{\mathbf{m}}$]: Similar to the approach shown for the second PT interval, we get:

$$
\begin{aligned}
PFD_{avg,i} &= \frac{1}{\tau_{j-1}-\tau_j}\int_{\tau_{j-1}}^{\tau_j} \Pr(T_{DU,PT}\le t/T_{DU,PT}>\tau_{j-1})dt \\
&= \frac{1}{\tau_{j-1}-\tau_j}\int_{\tau_{j-1}}^{\tau_j} \frac{\Pr(T_{DU,PT}\le t)-\Pr(T_{DU,PT}\le\tau_{j-1})}{\Pr(T_{DU,PT}>\tau_{j-1})}dt
\end{aligned}
\qquad (18)
$$

The resulting PFD$_{avg,PT}$ for PT therefore becomes:

$$
PFD_{avg,PT} = \frac{1}{\tau}\sum_{j=1}^{m}\int_{\tau_{j-1}}^{\tau_j} \frac{\Pr(T_{DU,PT}\le t)-\Pr(T_{DU,PT}\le\tau_j)}{\Pr(T_{DU,PT}>\tau_j)} \quad (19)
$$

where $PFD_{avg,PT}$ stands for the average probability for DU-failure detected by partial testing.

3.2.3 Combination FT with PT

When all actuate valves are assumed to be independent, PFD_{avg} of having two types of failures involving PT in a FT interval is expressed by $PFD_{avg,FT}$ and $PFD_{avg,PT}$. $PFD_{avg,FT}$ stands for the average probability for DU-failure detected by proof testing. So we therefore have the total PFD$_{avg}$ for a general system:

$$
PFD_{avg} = PFD_{avg,PT} + PFD_{avg,FT} \, (20)
$$

(1) PFD$_{avg}$ of 1oo1 system

For 1oo1 system that is subject to PT, PFD$_{avg}$ in the first FT interval [0, τ] becomes:

$$
\begin{aligned}
PFD_{avg} &\approx \frac{1}{\tau}\int_0^{\tau}\frac{z_{FT}(t)}{\alpha}tdt + \frac{1}{\tau}\sum_{j=1}^{m}\int_{\tau_{j-1}}^{\tau_j}\frac{\frac{z_{PT}(t)}{\alpha}t-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}}{1-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}} \\
&= \frac{z_{avg,FT}(0,\tau)\cdot\tau}{\alpha+1} + \frac{1}{\tau}\sum_{j=1}^{m}\frac{\frac{z_{avg,PT}(\tau_j,\tau_{j-1})\cdot(\tau_j-\tau_{j-1})}{\alpha+1}\cdot\frac{\tau_j^{\alpha+1}-\tau_{j-1}^{\alpha+1}}{\tau_j^{\alpha}-\tau_{i-1}^{\alpha}}-\frac{z_{PT}(\tau_{j-1})}{\alpha}\cdot\tau_{j-1}\cdot(\tau_j-\tau_{j-1})}{1-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}}
\end{aligned}
\qquad (21)
$$

PFD$_{avg}$ in subsequent FT interval $((i-1)\tau, i\tau)$ can be expressed as:

$$PFD_{avg} \approx \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{\frac{z_{FT}(t)}{\alpha}t - \frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}{1-\frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}dt + \frac{1}{\tau}\sum_{j=m}^{im}\int_{\tau_{j-1}}^{\tau_j} \frac{\frac{z_{PT}(t)}{\alpha}t - \frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}}{1-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}}$$

$$= \frac{\frac{z_{avg,FT}\left((i-1)\tau, i\tau\right)}{\alpha+1}\cdot\frac{(i\tau)^{\alpha+1}-((i-1)\tau)^{\alpha+1}}{(i\tau)^{\alpha}-((i-1)\tau)^{\alpha}} - \frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}{1-\frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}$$

$$+\frac{1}{\tau}\sum_{j=m}^{im}\frac{\frac{z_{avg,PT}(\tau_j,\tau_{j-1})\cdot(\tau_j-\tau_{j-1})}{\alpha+1}\cdot\frac{\tau_j^{\alpha+1}-\tau_{j-1}^{\alpha+1}}{\tau_j^{\alpha}-\tau_{i-1}^{\alpha}} - \frac{z_{PT}(\tau_{j-1})}{\alpha}\cdot\tau_{j-1}\cdot(\tau_j-\tau_{j-1})}{1-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}}$$

(22)

(2) PFD$_{avg}$ of 1oo2 system

Similarly, we also have PFD$_{avg}$ with PT for 1oo2 system:

$$PFD_{avg} \approx \frac{1}{\tau}\int_0^{\tau}(\frac{z_{FT}(t)}{\alpha}t)^2 dt + \frac{1}{\tau}\sum_{j=1}^{m}\int_{\tau_{j-1}}^{\tau_j}\frac{(\frac{z_{PT}(t)}{\alpha}t)^2-(\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1})^2}{(1-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1})^2}dt$$

$$= \frac{(z_{avg,FT}(0,\tau)\cdot\tau)^2}{2\alpha+1} + \frac{1}{\tau}\sum_{j=1}^{m}\frac{\frac{\left(z_{avg,PT}(\tau_{j-1},\tau_j)\cdot(\tau_j-\tau_{j-1})\right)^2}{2\alpha+1}\cdot\frac{\tau_j^{2\alpha+1}-\tau_{j-1}^{2\alpha+1}}{\left(\tau_j^{\alpha}-\tau_{j-1}^{\alpha}\right)^2} - \left(\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}\right)^2\cdot(\tau_j-\tau_{j-1})}{\left(1-\left(\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}\right)^2\right)} \tag{23}$$

PFD$_{avg}$ in subsequent FT interval $((i-1)\tau, i\tau)$ for 1oo2 system becomes:

$$PFD_{avg} \approx \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau}\frac{\left(\frac{z_{FT}(t)}{\alpha}t\right)^2-\left(\frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2}{1-\left(\frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2}dt + \frac{1}{\tau}\sum_{j=m}^{im}\int_{\tau_{j-1}}^{\tau_j}\frac{(\frac{z_{PT}(t)}{\alpha}t)^2-(\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1})^2}{(1-\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1})^2}dt$$

$$= \frac{\frac{\left(z_{avg,FT}\left((i-1)\tau,i\tau\right)\right)^2}{2\alpha+1}\cdot\frac{(i\tau)^{2\alpha+1}-((i-1)\tau)^{2\alpha+1}}{(i\tau)^{\alpha}-((i-1)\tau)^{\alpha}}\cdot\tau - \left(\frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2}{1-\left(\frac{z_{FT}\left((i-1)\tau\right)}{\alpha}\left(i-1\right)\tau\right)^2} \tag{24}$$

$$+\frac{1}{\tau}\sum_{j=m}^{im}\frac{\frac{\left(z_{avg,PT}(\tau_{j-1},\tau_j)\cdot(\tau_j-\tau_{j-1})\right)^2}{2\alpha+1}\cdot\frac{\tau_j^{2\alpha+1}-\tau_{j-1}^{2\alpha+1}}{\left(\tau_j^{\alpha}-\tau_{j-1}^{\alpha}\right)^2} - \left(\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}\right)^2\cdot(\tau_j-\tau_{j-1})}{\left(1-\left(\frac{z_{PT}(\tau_{j-1})}{\alpha}\tau_{j-1}\right)^2\right)}$$

4 Verification with reliability block diagram driven Petri net

In this section, Petri-net approach is used to check SIS reliability and verify the proposed formulas. Petri net is suggested in IEC61508 [1] as a suitable approach to model reliability especially for testing strategies of SISs [3, 24]. The stochastic Petri net with Predicates and Assertions (SPNPA) [25], a form of Petri net, is adopted in this study to model reliability of the HIPPS valves system.

4.1 Stochastic Petri net with Predicates and Assertions (SPNPA)

A SPNPA is a bipartite graph that easily gives the formalism an intuitive graphic interpretation, and it is also used to validate the model derived from the analytic theory. A SPNPA consists of places drawn as circles, transitions drawn as bars, directed arcs connecting places and transitions, drawn as arrows, and tokens illustrated as black bullets and assigned to places as well as all types of mathematical variables and available logic operators (or, and, if-then, etc.) , as shown in Fig. 1. These variables represent indicators and act on the validation of transitions (Predicates) and can also be modified when firing transition (Assertions).

The primitives of the notation are the following. Places are used to represent conditions or local system states, e.g. a place may relate to one phase in the behavior of a particular component. Transitions are used to describe local events that occur in the system; these will usually result in a modification to the system state. Tokens are dynamic elements that reside in places. The distribution of a token in a place can be used to reflect the corresponding condition or a system state. Arcs specify the relationships between local states or conditions (places) and events (transitions). An arc from a place to a transition is termed an input arc. This indicates the local state in which an event can occur. An arc to a place from a transition is termed an output arc. More details about Petri net can be found in IEC62551 [26].

The Petri net module in the GRIF software [25] serves to model the behavior of complex dynamic systems for performance evaluation based on SPNPA. It enables users to obtain both standard dependability values (availability, reliability, etc.). The great properties of SPNPA are capable of describing the dysfunctional states of an installation (components failures) and the working states. Strong dependences among components can be modeled with reconfigurations over time, using deterministic or stochastic transitions: Exponential, Weibull, Uniform or any other law programmed. Priorities among different actions (such as working, testing), intervention times, etc. can be easily included in such SPNPA. The numerical simulation results can be produced, including evaluation on mean over the calculation period, mean per time interval, variation frequency, etc. basis of any indicator created.

The reliability block diagram (RBD) driven SPNPA is adopted here and suggested in IEC 61508 [1]. As shown in Fig. 1(a), a bar with gradient color refers to a transition with Weibull firing time, a thick bar with black color is for the transition with constant firing time and a thin bar with black color is used to represent an immediate transition. In such kind of models, predicates denoted as “?” are introduced to represent the enabling condition of a transition, and assertions denoted as “! ” represents the formulas to update one variable when the transition is fired [16].

The confidence intervals [27, 28] are intended to provide a more practical explanation as well as to better assess the failure distribution of the system. It is assumed that the true value of PFD_{avg} of a system could be estimated by PFD_{avge}. If the number of simulations N is large enough, the confidence intervals can be obtained through the s-normal approximation of PFD_{avg} with mean PFD_{avge} and standard deviation $\sigma(PFD_{avge})$. Note that PFD_{avge} and $\sigma(PFD_{avge})$ are obtained via the SPNPA approach. The approximation of the confidence intervals under a given confidence level 100(1-α)% is generated [29, 30]:

100(1-α)% confidence lower bound

$$\mathrm{PFD_{avgL}} \geqslant \mathrm{PFD_{avge}} - z_{\alpha/2}\sqrt{\frac{\sigma^2(\mathrm{PFD_{avge}})}{N}}$$

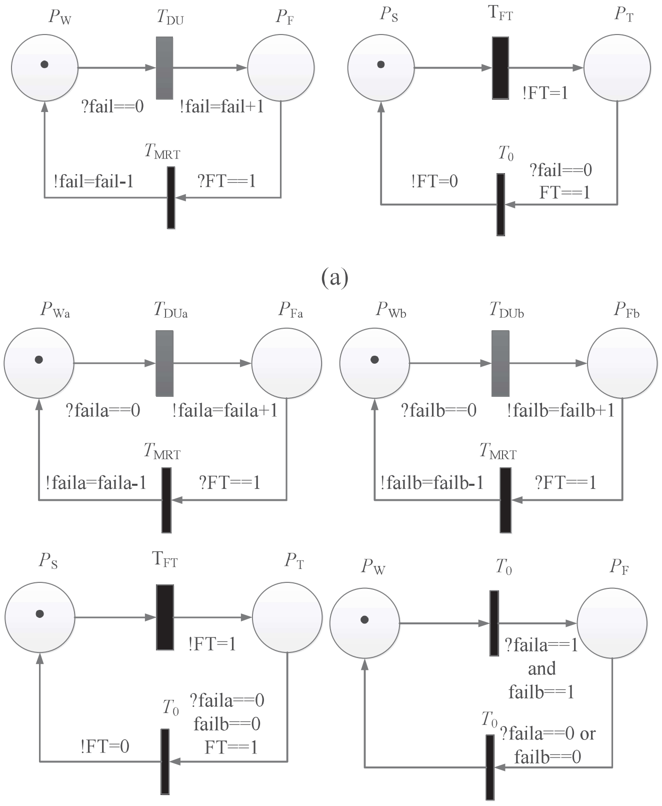
100(1-α)% confidence lower bound

$$\mathrm{PFD_{avgU}} \leqslant \mathrm{PFD_{avge}} + z_{\alpha/2}\sqrt{\frac{\sigma^2(\mathrm{PFD_{avge}})}{N}}$$

where $z_{\alpha/2}$ indicates the 100(1- α)th percentile of the standard normal density and $z_{\alpha/2}$ is normally equal to 1.96.

4.2 Proof tests verification

A RBD driven SPNAP model is established for 1oo1 system as presented in Fig. 1 (a). On the left part of the Fig. 1(a), we model the process of failure occurrence. A DU-failure will occur when the token in P_W is removed to P_F. We can set a variable of 'fail' to denote the number of DU failures, and the description "fail = fail+1" means a DU failure occurs. Similarly, the assertion of "!fail = fail-1" means a DU failure is repaired after the transition T_{MRT} is fired. On the right part of the Fig. 1(a), we model the testing process. When the token in Ps is removed, a test occurs, and the value of the variable 'FT' is set as 1. The transition T_0 is only enabled when there is no DU failure existing, and after it is fired, FT becomes to 0, meaning that the test is finished.



(a)

(b)

Fig. 1 SPNPA modeling during full proof tests for (a) 1oo1 system and (b) 1oo2 system, with Places P_W, P_F, P_S, and P_T that denote the working state, failure state, state of ready to start FT and full proof testing state of systems, and with

Transition T_{DU}, T_{FT}, T_0, and T_{MRT} that denote DU failure occurring, testing performed, testing finished and repair finished, and especially for 1oo2 system with component *a* and component *b,* the corresponding symbols are followed by *a* and *b.*

In Fig.1 (b), the values of "faila" and "failb" stand for whether there are DU failures in the two components respectively. The predicate of "?faila==1 and failb==1" means that the system in a complete failing state, and the predicate of "?faila==0 or failb==0" represents that at least one channel of the system is restored.

The input data for Fig. 1(a) are λ = 4.00E-06, τ = 8760h, keeping α in different values as listed in Table 1, and for α = 2 given different values of λ as listed in Table 2. Results are obtained by using the GRIF software and simulating given T_{MRT} = 0 in, with setting the number of iterations for 1oo1 system with 10 million times and for 1oo2 system with 100 million times. Such simulation times are also used for Section 4.3 for PT. Simulation results are compared with those obtained from proposed formulas based on Eq. (7) and Eq. (12) as shown in Tables 1 and 2 where 95% confidence intervals of a probability sample for the proof testing are calculated. Taking 1oo1 system with the $\alpha = 1.5$, PFD_{avg} lies in the interval from 2.60E-03 to 2.70E-03 with the best estimate being 2.63E-03 that is nearly close to the real values of 2.62E-03. Approximation formulas developed for FT are verified by the closeness of the results from the SPNAP simulation.

Table 1 Comparisons of proposed formulas and Petri-net model at different α

α	1oo1 system				1oo2 system			
	PFD_{avg} from Eq.(7)	PFD_{avge} from SPNAP	$\sigma(PFD_{avge})$	$[PFD_{avgL}, PFD_{avgU}]$	PFD_{avg} from Eq.(12)	PFD_{avge} from SPNAP	$\sigma(PFD_{avge})$	$[PFD_{avgL}, PFD_{avgU}]$
1	1.75E-02	1.73E-02	1.06E-01	[1.72E-02, 1.74E-02]	4.09E-04	3.98E-04	1.41E-02	[3.95E-04, 4.01E-04]
1.3	5.57E-03	5.57E-03	5.79E-02	[5.50E-03, 5.60E-03]	4.57E-05	4.46E-05	4.41E-03	[4.37E-05, 4.55E-05]
1.5	2.62E-03	2.63E-03	3.87E-02	[2.60E-03, 2.70E-03]	1.08E-05	1.09E-05	2.09E-03	[1.05E-05, 1.13E-05]
1.8	8.57E-04	8.60E-04	2.12E-02	[8.47E-04, 8.73E-04]	1.25E-06	1.27E-06	6.55E-04	[1.14E-06, 1.40E-06]
2	4.09E-04	4.12E-04	1.43E-02	[4.03E-04, 4.21E-04]	3.01E-07	2.60E-07	3.00E-04	[2.20E-07, 3.19E-07]
2.5	6.57E-05	6.62E-05	5.43E-03	[6.28E-05, 6.96E-05]	8.80E-09	7.74E-09	3.70E-05	[4.88E-10, 1.50E-08]

Table 2 Comparisons of proposed formulas and Petri-net model at different λ

λ	1oo1				1oo2			
	PFD_{avg} from Eq.(7)	PFD_{avge} from SPNAP	$\sigma(PFD_{avge})$	$[PFD_{avgL}, PFD_{avgU}]$	PFD_{avg} from Eq.(12)	PFD_{avge} from SPNAP	$\sigma(PFD_{avge}$	$[PFD_{avgL}, PFD_{avgU}]$
2.00E-6	1.02E-04	1.03E-04	7.18E-03	[9.86E-05, 1.07E-04]	1.88E-08	1.71E-08	2.68E-05	[1.18E-08, 2.23E-08]
4.00E-6	4.09E-04	4.12E-04	1.43E-02	[4.03E-04, 4.21E-04]	3.01E-07	2.60E-07	3.00E-04	[2.07E-07, 3.19E-07]

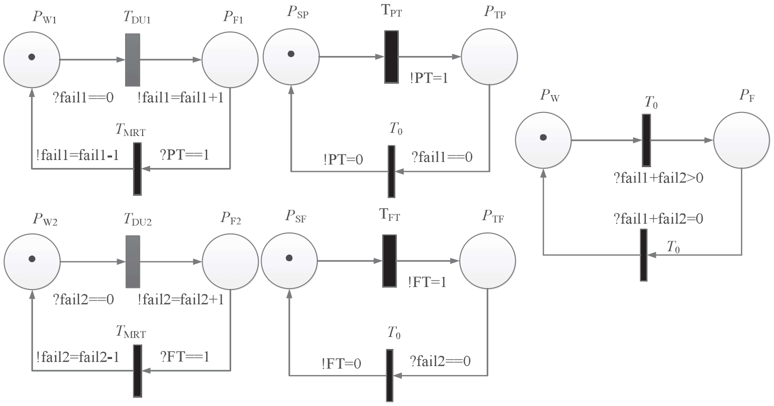
6.00E-6	9.21E-04	9.19E-04	2.14E-02	[9.06E-04, 9.32E-04]	1.52E-06	1.48E-06	6.82E-04	[1.35E-06, 1.61E-06]
8.00E-6	1.64E-03	1.64E-03	2.86E-02	[1.6E-03, 1.7E-03]	4.82E-06	4.83E-06	1.27E-03	[4.58E-06, 5.08E-06]
1.00E-5	2.56E-03	2.56E-03	3.57E-02	[2.5E-03, 2.6E-03]	1.18E-05	1.16E-05	1.95E-03	[1.12E-06, 1.20E-06]
2.00E-5	1.02E-02	1.02E-02	7.07E-02	[1.02E-02, 1.02E-02]	1.88E-04	1.84E-04	7.84E-03	[1.82E-04, 1.86E-04]

4.3 Partial tests verification

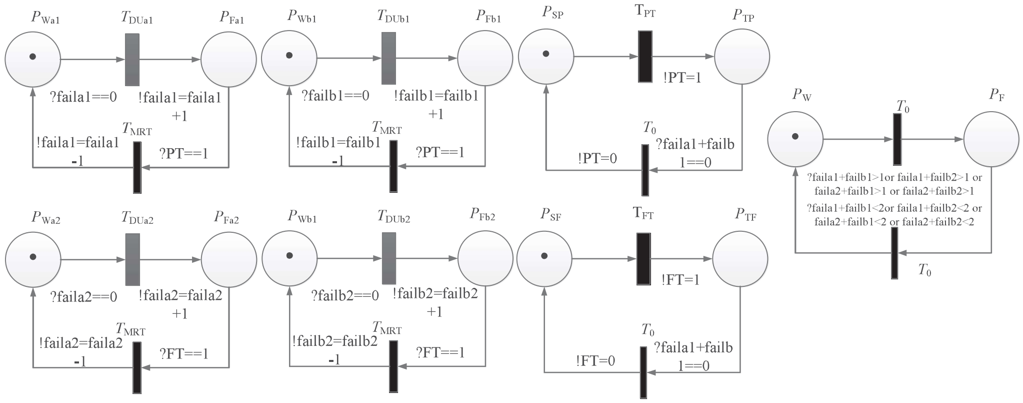
Fig.1 (a), the values of “fail1” and “fail2” stand for whether DU failures are detected by PT or FT respectively. In this model, a DU-failure will occur when the token in P_{W1}/ P_{W2} is removed to P_{F1}/ P_{F2} during PT/FT. On the intermediate part of the Fig. 2(a), we model the proof and partial testing processes. When the token in P_{SP} is removed, a partial test occurs, and the value of the variable ‘PT’ is set as 1. The same method is used for P_{SF} modeling. The predicate of “?fail1 + fail2 > 0” means that at least the system is in a complete failing state in FT or PT, and the predicate of “? fail1 + fail2 = 0” represents that the system is restored in both FT and PT.

In Fig.1 (b), the values of “faila1”, “faila2”, “failb1” and “failb2” stand for whether there are DU failures in the two components for both PT and FT respectively. The predicate of “? faila1+failb1>1or faila1+failb2>1 or faila2+failb1>1 or faila2+failb2>1” means that the system in a complete failing state in FT or PT, and the predicate of “?faila1+failb1<2or faila1+failb2<2 or faila2+failb1<2 or faila2+failb2<2” represents that at least one channel of the system is restored in FT or PT.

The input data for Fig. 2 are $\alpha = 2$, $\lambda = 4.00\text{E-}06$, $\lambda_{FT} = 2.00\text{E-}06$, $\lambda_{PT} = 3.464\text{E-}06$, and $\tau = 8760\text{h}$, given different partial testing intervals as listed in Table 3. PFD_{avg} results obtained both from the proposed formulas based on Eq. (21) and Eq. (22) and the Petri-net simulation are given in Table 3 where the 95% confidence intervals of a probability sample for PT are calculated. Take 1oo1 system with the PT interval of 2920h, PFD_{avg} lies in the 95% confidence interval from 2.34E-04 to 2.46E-04 with the best estimate being 2.40E-04 that is nearly close to the real values of 2.39E-04.



(a)



(b)

Fig. 2 SPNPA modeling during partial tests for (a) 1oo1 system and (b) 1oo2 system, with Places P_{W1}, P_{F1}, P_{W2}, P_{F2} P_{SP}, P_{TP}, P_{SF} and P_{TF} that denote the working state for PT, state of failure detected by PT, working state for FT, state of failure detected by FT, state of ready to start PT, PT state of systems, state of ready to start FT and FT state of systems, and with Transition T_{DU1}, T_{PT}, T_{DU2}, T_{FT}, T_0, and T_{MRT} that denote DU1 failure occurring, PT performed, DU2 failure occurring, FT performed, testing finished and repair finished, and especially for 1oo2 system with component *a* and component *b,* the corresponding symbols are followed by *a* and *b.*

Table 3 PFD_{avg} verification for partial test

PT strategies	1oo1 systems				1oo2 systems			
	PFD_{avg} from Eq.(21)	PFD_{avge} from SPNAP	$\sigma(PFD_{avge})$	$[PFD_{avgL}, PFD_{avgU}]$	PFD_{avg} from Eq.(23)	PFD_{avge} from SPNAP	$\sigma(PFD_{avge})$	$[PFD_{avgL}, PFD_{avgU}]$
1460h	1.75E-04	1.76E-04	7.75E-03	[1.71E-04, 1.81E-04]	8.16E-08	6.75E-08	1.25E-04	[4.3E-08, 9.0E-08]
2190h	2.07E-04	2.09E-04	8.31E-03	[2.04E-04, 2.14E-04]	1.07E-07	9.35E-08	1.42E-04	[6.56E-08, 1.21E-07]
2920h	2.39E-04	2.40E-04	8.99E-03	[2.34E-04, 2.46E-04]	1.29E-07	1.23E-07	1.67E-04	[6.56E-08, 1.21E-07]
4380h	2.94E-04	2.97E-04	1.05E-02	[2.96E-04, 2.98E-04]	1.62E-07	1.99E-07	2.36E-04	[1.53E-07, 2.45E-07]

It can be seen that the two methods give rather close results. Approximation formulas developed for PT are verified by the closeness of the results from the SPNAP simulation. It should also be noted that such simulation models ignore the effects that the failure doesn't occur in the previous testing period.

5. Case studies

In the case study, we consider high integrity pressure protection systems (HIPPS) valves that are installed as the final elements in a subsea system. The safety instrumented function (SIF) of HIPPS valves in low-demand mode needs to fulfill the requirements for a safety integrity level (SIL) that is related to PFD_{avg}, and more information will be found in [14]. SIL3 is used here for reliability assessment of HIPPS valves to choose the optimal testing strategies.

In this section, given that failures are time dependent, the effects of the following variables will be evaluated:

- Proof testing intervals;

- Parameters (such as λ and α) in the Weibull distribution;
- Partial testing intervals.

5.1 Contribution from testing intervals

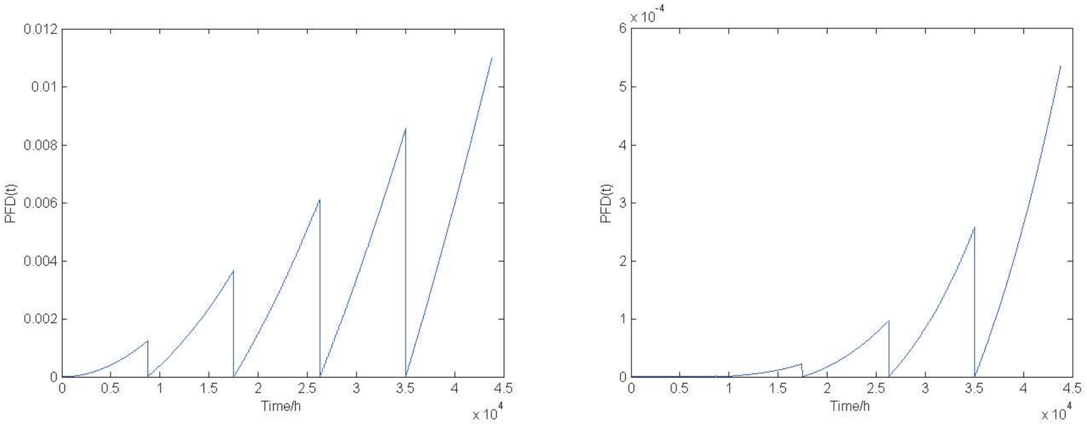
Due to the HIPPS valves taking time-dependent failure rates, their failures are assumed to increase over time and PFD(t)/PFD_{avg} in one testing interval will be different from that in the next interval. In order to examine such effects, a series of FT and PT intervals are considered here, with the relevant parameters in Table 4.

Table 4 Parameters for HIPPS valves

Property	Parameters	Value
Scale parameter	λ	4×10^{-6}
Shape parameter	α	2
FT interval	τ	8760h
Number of FT	i	5
PT interval	τ_m	2190h
Number of PT	m	4

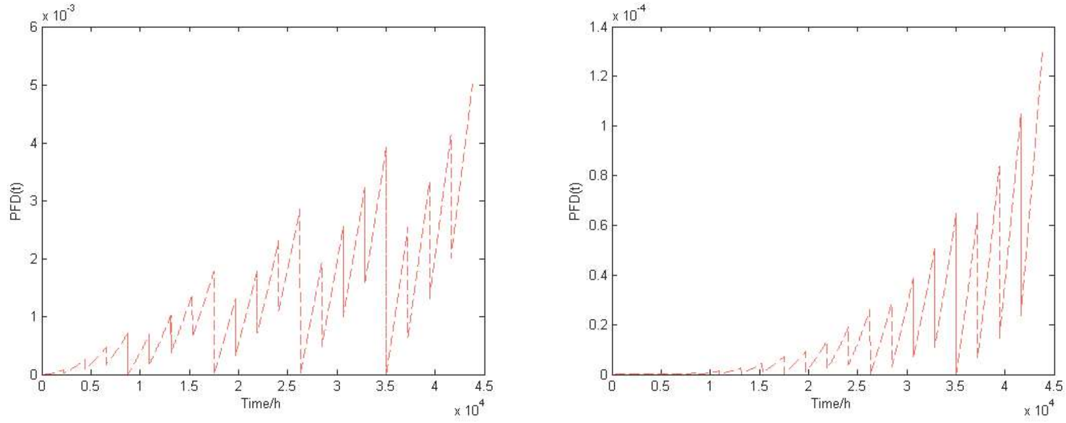
5.1.1 Tendency of PFD(t)

In order to evaluate the effects of a series of FT intervals on the time-dependent PFD(t), 5 periodic FT intervals excluding PT as inputs are chosen. The relevant PFD(t) over time is calculated for two types of HIPPS valves, and their trends of PFD(t) during FT intervals are predicted as shown in Fig. 3 (a) and (b) respectively. It can be seen that there is a trend of sharp increases over time in one interval and it can reach the as-good-as new state at the end of testing. We also find that the increase in PFD(t) is different in subsequent FT intervals, namely, PFD($t = i\tau$)<PFD($t = (i+1)\tau$). It can be explained that the degradation in different FT intervals makes such contributions. The 4 periodic PT intervals are modeled in 5 FT intervals as shown in Fig. 4 (a) and (b) given λ_{FT} =2 and λ_{PT} =3.464. It is obvious that the PFD(t) under FT including PT increases rapidly over time in different PT intervals and the values of PFD(t) also agree PFD($t = i\tau$)<PFD($t = (i+1)\tau$) in every FT interval. It is also found that the values of PFD cannot go back to 0 after PT because of some failures only revealed by FT. Fig. 5 (a) and (b) shows that a comparison of PFD(t) under FT without PT and that with PT for 1oo1 and 1oo2 systems respectively. Note that the maximum value of PFD(t) at the end of every subsequent FT interval can be reduced by introducing a series of PT compared to that under FT without PT, namely PFD_{PT} (t = $i\tau$)<PFD(t = $i\tau$). The implementation of PT can decrease PFD of the system in order to improve system reliability.



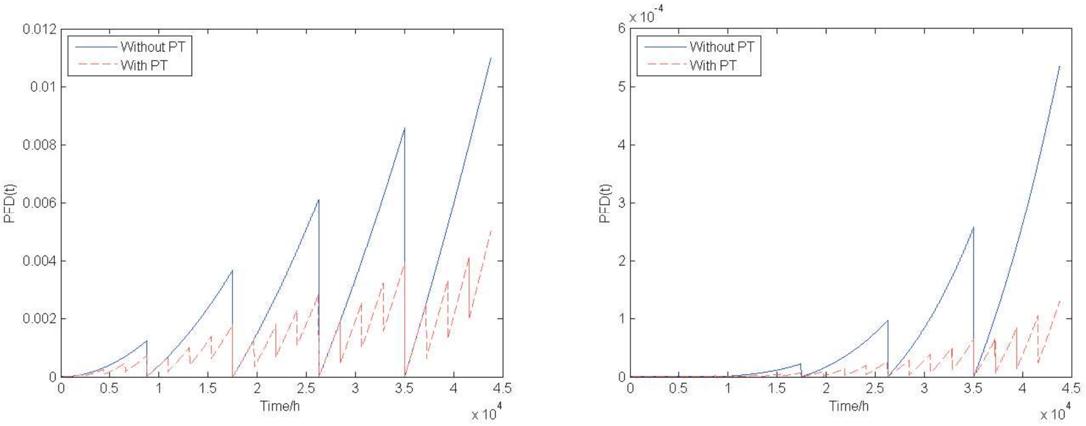
(a) (b)

Fig. 3 PFD(t) under FT without PT for (a) 1oo1 system and (b) 1oo2 system



(a) (b)

Fig. 4 PFD(t) under FT with PT for (a) 1oo1 system and (b) 1oo2 system

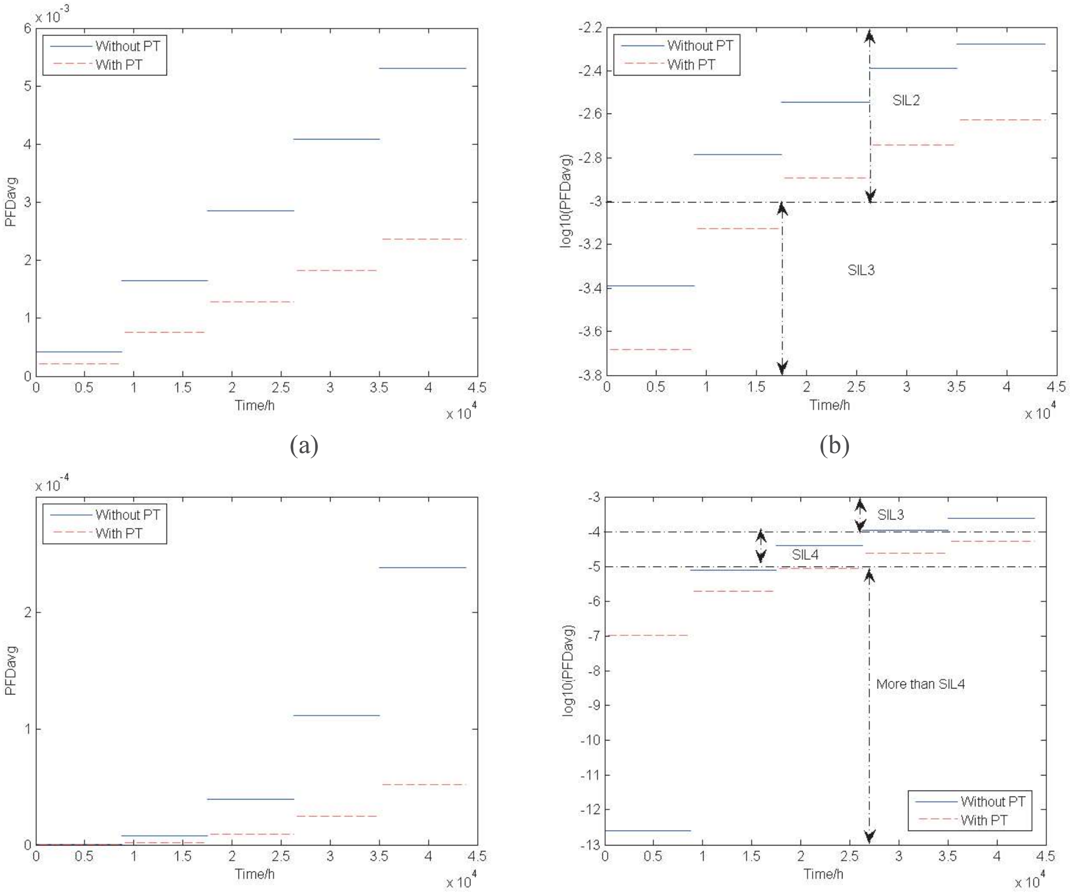


(a) (b)

Fig. 5 Comparisons of PFD(t) under FT without PT and that with PT for (a) 1oo1 system and (b) 1oo2 system

5.1.2 Tendency of PFD_{avg}

In this section, PFD_{avg} is calculated for every FT interval $((i-1)\tau, i\tau)$ based on the proposed formulas such as Eq. (10), Eq.(15), Eq.(22) and Eq.(24) and $Log_{10}(PFD_{avg})$ is used to assess the SILs of the system, using the parameters listed in Table 4. A numerical comparison of PFD_{avg} under FT without PT and that with PT is made as shown in Fig. 6. It can be seen from Fig. 6 (a) and (b) that the function of 1oo1 system can meet the requirement of SIL3 in first FT interval under both of them and in second FT interval for FT with PT only, while the requirement of SIL3 can’t been satisfied in the rest of FT intervals for both of them. Note that, the function of 1oo2 system among 5 FT intervals always can meet the requirement of SIL3 under both of them. It also reminds the decision makers how to choose the PT strategies and to provide the repair recommendations when the system subjects to the increasing failure rate.



(a) (b)

(c) (d)

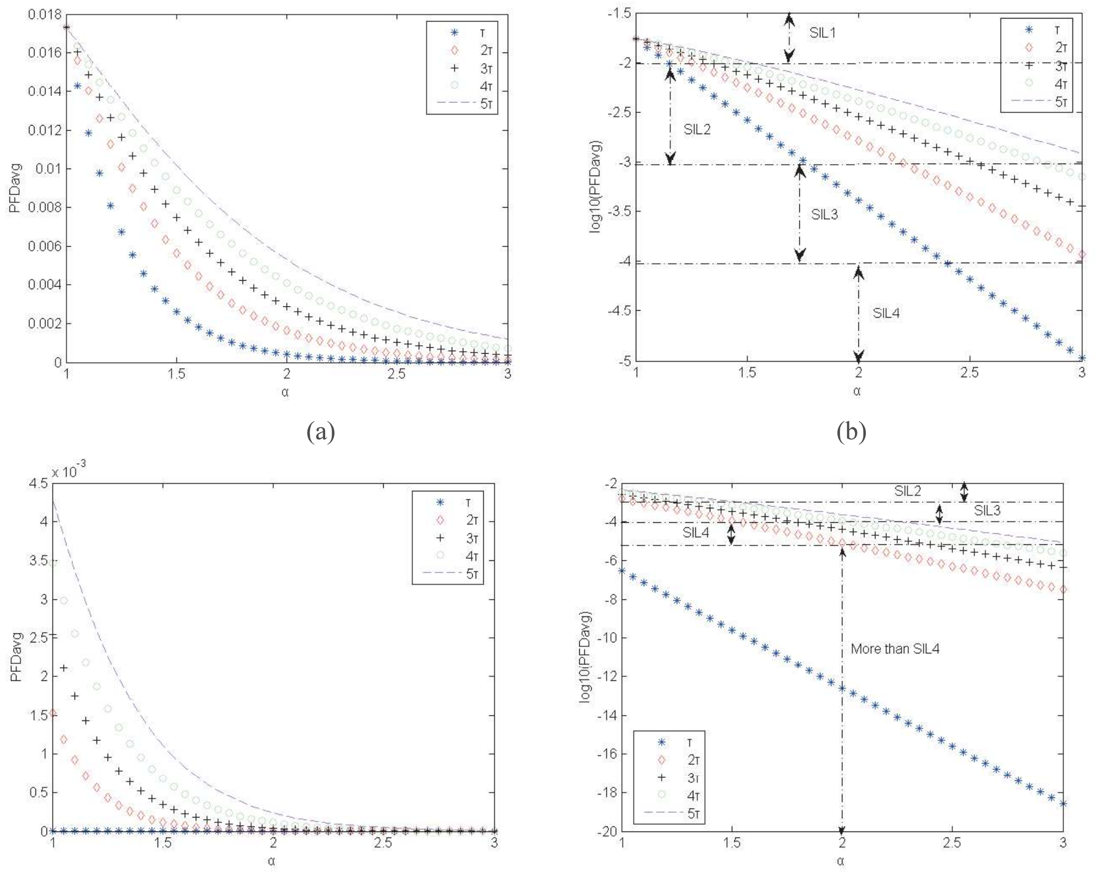
Fig. 6 Comparisons of PFD_{avg} under FT without PT and that with PT for (a) PFD_{avg} for 1oo1 system, (b) $Log_{10}(PFD_{avg})$ for 1oo1 system, (c) PFD_{avg} for 1oo2 system and (d) $Log_{10}(PFD_{avg})$ for 1oo2 system

5.2 Contribution from parameters

In accordance with HIPPS valves following the time-dependent failure rate, the scale parameter λ and shape parameter α, may influence the contribution of PFD_{avg} under a series of sequential FT intervals and the length of a FT interval.

5.2.1 Effects of parameters under sequential FT intervals

In the case study, different values are assigned to α, while keeping λ = 4.00E-06. Comparisons of PFD_{avg} and $Log_{10}(PFD_{avg})$ among a series of sequential FT intervals from τ to 5τ have been made given α changing from 1 to 3, as shown in Fig.7. As observed from Fig.7 (a) and (c), the values of PFD_{avg} for 1oo1 or 1oo2 systems decrease with the growth of α in any FT interval, while they increase in turn from τ to 5τ given the same α. As can be observed from Fig.7 (b) and (d), for 1oo1 system, when α of a valve is chosen for 2, the SIF of such a valve can only meet the requirement of SIL3 in the area marked by the dot dash line in the first FT interval. When α of a valve is 3, SIL3 can be met from 2τ to 4τ except for the last FT interval of 5τ. For the 1oo2 system, if the value of α lies in (1,1.5), the system function can not meet the requirement of SIL3 from 3τ to 5τ, while the others can meet SIL3. Similarly, the type of valves related to parameter α for meeting SIL3 can be found given a fixed FT interval. For example, supposing 1oo1 system needs to meet SIL3 in the third FT interval, the range of the parameter α (α>2.5) can be found.

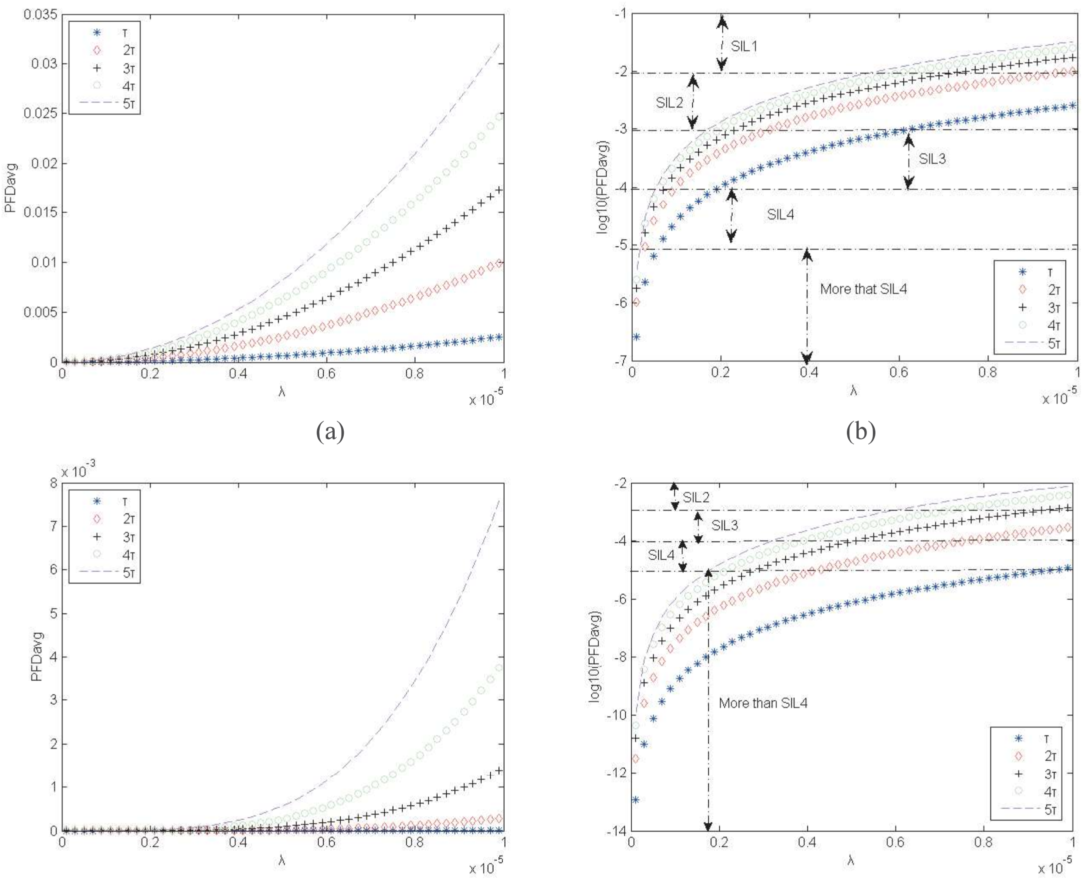


(a) (b)

(c) (d)

Fig. 7 Contributions from parameter α under 5-FT intervals on (a) PFD_{avg} of 1oo1 system, (b) $\text{Log}_{10}(\text{PFD}_{\text{avg}})$ of 1oo1 system, (c) PFD_{avg} of 1oo2 system, and (d) $\text{Log}_{10}(\text{PFD}_{\text{avg}})$ of 1oo2 system

In order to examine these effects of λ under subsequent FT intervals, comparisons have been made over λ in Fig. 8. Fig. 8 (a) and (c) has presented the contribution of PFD_{avg} from different λ under subsequent FT intervals for 1oo1 and 1oo2 systems. It is clear that the values of PFD_{avg} increase with the growth of the value of λ and also increase among a series of FT intervals from τ to 5τ give the same λ. As shown in Fig.8 (b) and (d), the area marked by the dot dash line with SIL3 can be found for both systems. It is found that the SIF of 1oo1 system can't satisfy the requirement of SIL3 when λ∈(6.00E-06，1.00E-05) and it can only meet the SIL3 in the first FT interval given that λ is chosen for 4.00E-06. The SIL3 of 1oo2 system cannot be met in the fourth and fifth FT interval when λ is more than 6.00E-06 and 7.00E-06, respectively. Similarly, the type of valves related to parameter λ for meeting SIL3 can be found given a FT interval. For example, assuming that 1oo1 system needs to meet SIL3 in the third FT interval, the selected λ should be more than 2.00E-06.



(a)

(b)

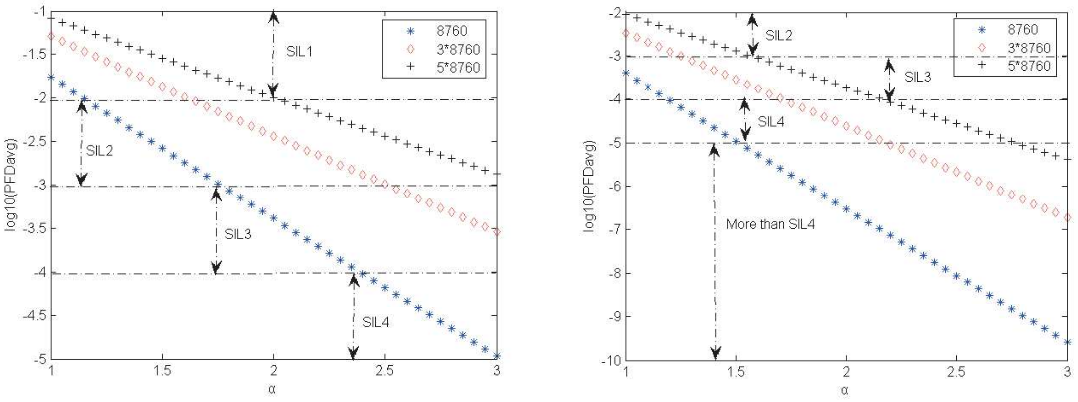
(c)

(d)

Fig. 8 Contributions from parameter λ under 5-FT intervals on (a) PFD_{avg} of 1oo1 system, (b) $Log_{10}(PFD_{avg})$ of 1oo1 system, (c) PFD_{avg} of 1oo2 system, and (d) $Log_{10}(PFD_{avg})$ of 1oo2 system

5.2.2 Effects of parameters under the different length of a FT interval

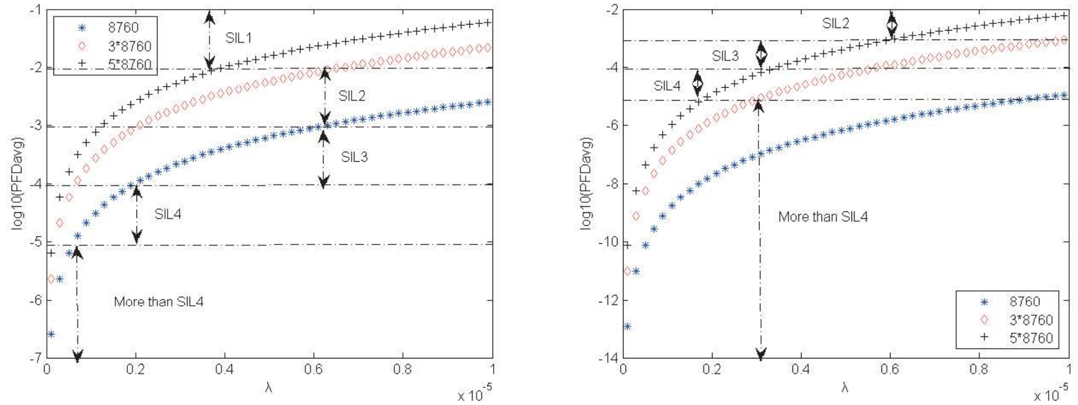
In order to examine the effects of parameter α under the different length of a FT interval, different values are assigned to α, while keeping λ = 4.00E-06. Comparisons of effects of a FT interval with 8760h, 3*8760h, and 5*8760h are carried out, given α from 1 to 3. As shown in Fig. 9 (a) and (b), the values of $Log_{10}(PFD_{avg})$ for 1oo1 or 1oo2 systems decrease with the growth of α given the constant FT period. It is found that the value of α for valves choosing is different under different FT strategies. Taking 1oo1 system for instance, if the SIF of such a valve needs to meet the SIL3 with the area marked by the dot dash line, a FT interval will be decided for 8760h, or 3*8760h, and the corresponding α value of a valve can be chosen approximately from 1.75 to 2.4 or from 2.5 to 3. Note that a FT interval of 5*8760h cannot meet SIL3. But for 1oo2 system, the FT interval of 5*8760h will meet the requirement of SIL3.



(a) (b)

Fig. 9 Contributions from parameter α under different FT strategies on $\mathrm{Log}_{10}(\mathrm{PFD}_{\mathrm{avg}})$ of (a) 1oo1 system, (b) 1oo1 system

In order to examine effects of the different length of a FT interval under different values of λ, keeping α = 2, Fig. 10 (a) and (b) has presented the contribution of $\mathrm{Log}_{10}(\mathrm{PFD}_{\mathrm{avg}})$ for 1oo1 and 1oo2 systems. It is clear that the values of $\mathrm{Log}_{10}(\mathrm{PFD}_{\mathrm{avg}})$ increase with the growth of the value of λ. The testing strategies can be used for choosing different λ range. Taking 1oo1 system for example, when a FT interval is determined for 8760h in the SIL3 area marked by the dot dash line, the corresponding λ range can be approximately chosen from 1.90E-06 to 6.00E-06. While a FT interval is 5*8760h, the range of λ will be shortened from 1.300E-06 to 1.60E-06. Note that for 1oo2 system, a FT interval of 8760h or 3*8760h can meet SIL3 except for 5*8760h given that λ is approximately chosen for 6.00E-06.



(a) (b)

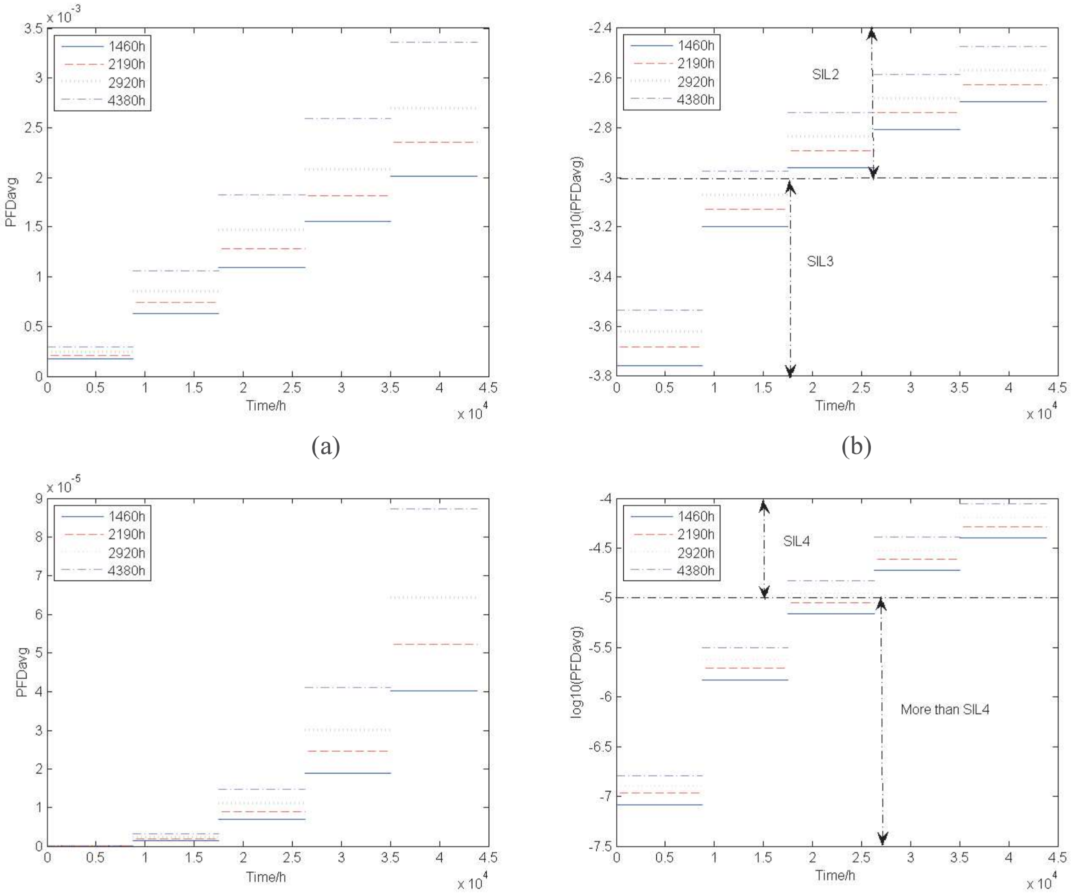
Fig. 10 Contributions from parameter λ under different FT strategies on $\mathrm{Log}_{10}(\mathrm{PFD}_{\mathrm{avg}})$ of (a) 1oo1 system, (b) 1oo2 system

5.3 Contribution of partial tests

In this section, numerical results for 1oo1 and 1oo2 HIPPS valves have been obtained using the following input data: $\alpha = 2$, $\lambda = 4.00\mathrm{E}\text{-}06$, $\lambda_{FT} = 2.00\mathrm{E}\text{-}06$, $\lambda_{PT} = 3.464\mathrm{E}\text{-}06$, $\tau = 8760\mathrm{h}$ and 5 sequential FT intervals. The contributions of sequential FT intervals, the FT interval in length and parameters have been made as follows.

5.3.1 Effects of sequential FT intervals for PT strategies

Fig. 11 (a) and (c) have presented the effects of subsequent FT intervals for PT strategies. It is clear that the values of PFD_{avg} increase in a series of subsequent FT intervals for same PT strategies, while they increase with PT strategies from 1460h to 4380h for every PT interval given the same FT interval. As shown in Fig.11 (b) and (d), for 1oo1 system, only the first and second FT intervals excluding the PT strategy of 4380h can be chosen for decision making since they can meet the requirement of SIL3, meaning that if the PT strategy of 4380h is determined, SIL3 cannot be met starting from the second FT interval. Similarly, for 1oo2 system, different PT strategies under 5 FT intervals are able to meet the requirements of SIL3.



(a) (b)

(c) (d)

Fig. 11 Contributions from 5-FT intervals for PT strategies on (a) PFD_{avg} of 1oo1 system, (b) $\text{Log}_{10}(\text{PFD}_{\text{avg}})$ of 1oo1 system, (c) PFD_{avg} of 1oo2 system, and (d) $\text{Log}_{10}(\text{PFD}_{\text{avg}})$ of 1oo2 system

5.3.2 Effects of the different FT interval length for PT strategies

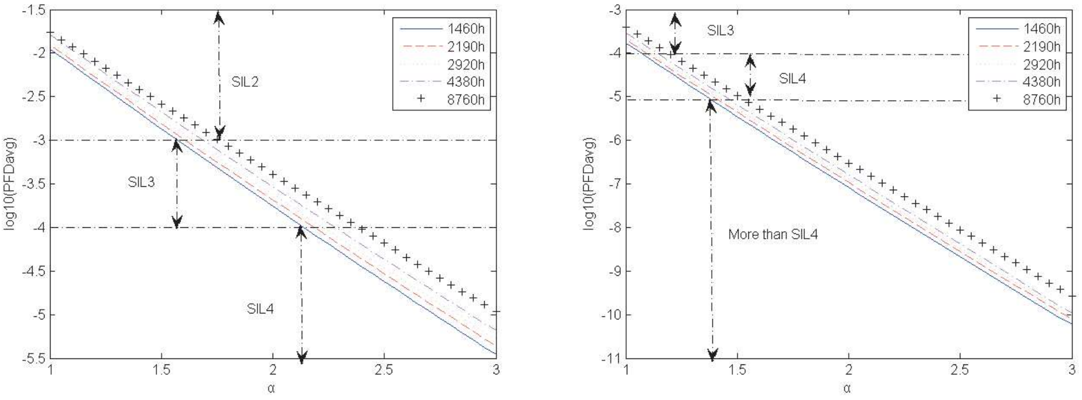
PFD_{avg} of HIPPS valves in a FT interval in the different length subject to different PT strategies are calculated. Table 5 presents results in FT intervals of 8760h and 3* 8760h for 1oo1 and 1oo2 systems. It is observed that the values of PFD_{avg} increase with PT strategies from 1460h to 4380h for every PT interval and the contributions of PFD_{avg} from 8760h is smaller than those from 3*8760h . Taking a PT strategy of 1460h for instance, the PFD_{avg} of 1oo1 system in a FT interval of 8760h is 1.75E-04 which is less than the value of 1.15E-04 from a 3*8760h length. This contribution can also provide the basis for choosing the optimized PT strategies in the different FT interval length.

Table 5 Contributions from different FT interval lengths for PT strategies

PT strategies	1oo1 system		1oo2 system	
	FT=8760h	FT=3*8760h	FT=8760h	FT=3*8760h
1460h	1.75E-04	1.15E-03	8.16E-08	3.35E-06
2190h	2.07E-04	1.26E-03	1.07E-07	4.20E-06
2920h	2.39E-04	1.36E-03	1.29E-07	5.03E-06
4380h	2.94E-04	1.57E-03	1.62E-07	6.57E-06
Without PT	4.09E-04	3.67E-03	3.01E-07	2.40E-05

5.3.3 Effects of parameters for PT strategies

We also observe from Fig. 12 (a) and (b) where the values of $\mathrm{Log}_{10}(\mathrm{PFD}_{avg})$ during every PT interval also follow the same trend with those during a FT interval. It should be noted that further increased PT frequency will decrease the values of PFD_{avg} on demand. This contribution can also provide the basis for choosing the optimized PT strategies according to the reliability analysis. For instance, if 1oo1 system with α is approximately changing from 1.6 to 2.3, the relevant PT intervals can be chosen to meet the requirement of SIL3.



(a) (b)

Fig. 12 Contributions from parameter α f parameters for PT strategies on $\mathrm{Log}_{10}(\mathrm{PFD}_{avg})$ of (a) 1oo1 system, (b) 1oo2 system

Based on the realistic parameters from the real-world system, the proposed method can provide a guide to choose the optimized testing strategies to guarantee safety with acceptable costs.

6. Concluding remarks

In order to consider the effects of degradation of final elements in SISs on decision making about design and operation, this paper has presented a time-dependent failure based approach, which can be used to study different operational issues, such as proof tests and partial tests. Approximation formulas for PFD_{avg} involving degradations have been developed, and Weibull distributions are adopted for modeling the increasing failure rates. The RBD driven SPNPA models incorporating partial testing have been developed for verification for the proposed formulas. The comparisons have shown that the values of PFD_{avg} from simulations are very close to those from the analytical formulas.

In the case study, a focus is given to 1oo1 and 1oo2 HIPPS valves. The most difficult challenge in relation to the approximations is to handle the degradation effects in a series of subsequent proof testing intervals. The experiments have shown that PFD(t) and $\mathrm{PFD_{avg}}$ are changing and different from the previous proof testing intervals. Decision should be made based on the requirements of SILs, so as to choose appropriate proof testing intervals with given measures. Investigations of Weibull Parameters have indicated that maintenance strategies can be made under predicating the $\mathrm{PFD_{avg}}$ within several testing intervals, which also provide a method for determining the suitable types of valves under limitation of testing. The contribution of $\mathrm{PFD_{avg}}$ from partial tests has been demonstrated in improving the performance of valves. The results provide the clues in choosing the optimized partial testing strategies given the requirements of SILs and the corresponding proof testing intervals.

The current paper is restricted to SISs with simple configurations. An extension of the current work is to develop the analytical formulas for more complex systems. Another issue to be considered is the common cause failure for the dependent components because the failures of components are assumed to be independent. Studies of more complex SISs considering non-negligible repair time will be reported in the future.

Acknowledgment

Authors thankfully acknowledge the financial support provided by China University of Petroleum (Beijing) (YSKY-2015-ZY-12) and China Scholarship Council(201506440028).

Appendix

Calculation on the PFD_{avg} in the subsequent testing interval $((i-1)\tau, i\tau)$: Here we will derive the $\mathrm{PFD_{avg}}$ given in Eq. (10) based on the time-dependent failure rate in Eq. (3) and the details will be shown in Eq. (25). The Eq. (15), and Eq. (21) - Eq. (24) also have been developed by following the same rules.

$$
\begin{aligned}
PFD_{avg} &= \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} PFD\left(t\right)dt = \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \Pr(T_{DU} \le t / T_{DU} > (i-1)\tau)dt \\
&= \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{\Pr(T_{DU} \le t) - \Pr(T_{DU} \le (i-1)\tau)}{\Pr(T_{DU} > (i-1)\tau)}dt \\
&= \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{(1-e^{-\frac{z(t)}{\alpha}t}) - (1-e^{-\frac{z((i-1)\tau)}{\alpha}\cdot(i-1)\tau})}{e^{-\frac{z((i-1)\tau)}{\alpha}\cdot(i-1)\tau}}dt \\
&\approx \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{\frac{z(t)}{\alpha}t - \frac{z\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}{1-\frac{z\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}dt \\
&= \frac{1}{\tau}\int_{(i-1)\tau}^{i\tau} \frac{(\lambda t)^{\alpha} - \frac{z\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}{1-\frac{z\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}dt \\
&= \frac{1}{\tau}\cdot\frac{\lambda^{\alpha}\cdot\left((i\tau)^{\alpha+1} - ((i-1)\tau)^{\alpha+1}\right) - \frac{z((i-1)\tau)}{\alpha}\cdot(i-1)\tau\cdot\tau}{\left(\alpha+1\right)\cdot\left(1-\frac{z((i-1)\tau)}{\alpha}\cdot(i-1)\tau\right)} \\
&= \frac{\frac{z_{avg}\left((i-1)\tau, i\tau\right)}{\alpha+1}\cdot\frac{(i\tau)^{\alpha+1}-((i-1)\tau)^{\alpha+1}}{(i\tau)^{\alpha}-((i-1)\tau)^{\alpha}} - \frac{z\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}{1-\frac{z\left((i-1)\tau\right)}{\alpha}\cdot\left(i-1\right)\tau}
\end{aligned}
\tag{25}
$$

where $z_{avg}\left((i-1)\tau, i\tau\right)$ is the average failure rate in the subsequent testing interval $((i-1)\tau, i\tau)$ and

$$
z_{avg}\left((i-1)\tau, i\tau\right) = \lambda^{\alpha}\frac{\left(i\tau\right)^{\alpha} - \left(\left(i-1\right)\tau\right)^{\alpha}}{\tau}.
$$

References

[1] IEC61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, Geneva, 2010.

[2] A. Torres-Echeverria, S. Martorell, H. Thompson, Modelling and optimization of proof testing policies for safety instrumented systems, Reliability Engineering & System Safety, 94 (2009) 838-854.

[3] Y. Liu, M. Rausand, Reliability effects of test strategies on safety-instrumented systems in different demand modes, Reliability Engineering & System Safety, 119 (2013) 235-243.

[4] H. Jin, M.A. Lundteigen, M. Rausand, New PFH-formulas for k-out-of-n: F-systems, Reliability Engineering & System Safety, 111 (2013) 112-118.

[5] M.A. Lundteigen, M. Rausand, Partial stroke testing of process shutdown valves: How to determine the test coverage, Journal of Loss Prevention in the Process Industries, 21 (2008) 579-588.

[6] M.A. Lundteigen, M. Rausand, The effect of partial stroke testing on the reliability of safety valves, ESREL’07, (2007).

[7] A. Summers, B. Zachary, Variable function voting solenoid-operated valve apparatus and testing method therefor, in, Google Patents, 2004.

[8] Y. Sato, Introduction to partial stroke testing, in: SICE Annual Conference, 2008, IEEE, 2008, pp. 2754-2758.

[9] F. Innal, M.A. Lundteigen, Y. Liu, A. Barros, PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models, Reliability Engineering & System Safety, 150 (2016) 160-170.

[10] H. Jin, M. Rausand, Reliability of safety-instrumented systems subject to partial testing and common-cause failures, Reliability Engineering & System Safety, 121 (2014) 146-151.

[11] F. Brissaud, A. Barros, C. Bérenguer, Probability of failure on demand of safety systems: impact of partial test distribution, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, (2012) 1748006X12448142.

[12] R. Pascual, D. Louit, A.K. Jardine, Optimal inspection intervals for safety systems with partial inspections, Journal of the Operational Research Society, 62 (2011) 2051-2062.

[13] S. Hauge, M.A. Lundteigen, P. Hokstad, S. Håbrekke, Reliability prediction method for safety instrumented systems–pds method handbook, 2010 edition, SINTEF report STF50 A, 6031 (2010).

[14] M. Rausand, Reliability of safety-critical systems: theory and applications, John Wiley & Sons, 2014.

[15] E. Rogova, G. Lodewijks, M. Lundteigen, Safety and Reliability of Complex Engineered Systems ESREL 2015.

[16] Y. Liu, M. Rausand, Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems, Reliability Engineering & System Safety, 145 (2016) 366-372.

[17] A. Torres-Echeverría, S. Martorell, H. Thompson, Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm, Reliability Engineering & System Safety, 106 (2012) 45-60.

[18] S. Wu, L. Zhang, S. Liu, Y. liu, A. Barros, M.A. Lundteigen, Reliability assessment for subsea HIPPS valves with partial stroke testing, ESREL 2016 (Glasgow, Scotland, 25-29 September 2016), 2016.

[19] A.A. Jigar, Quantification of reliability performance: Analysis methods for safety instrumented system, (2013).

[20] M. Abimbola, F. Khan, N. Khakzad, Dynamic safety risk analysis of offshore drilling, Journal of Loss Prevention in the Process Industries, 30 (2014) 74-85.

[21] A. Summers, B. Zachary, Partial-stroke testing of safety block valves, Control Engineering, 47 (2000) 87-89.

[22] K. Bond, IEC 61511-Functional Safety: Safety Instrumented Systems for the Process Industry Sector, in: ANNUAL SYMPOSIUM ON INSTRUMENTATION FOR THE PROCESS INDUSTRIES, INSTRUMENT SOCIETY OF AMERICA, 2002, pp. 33-40.

[23] IEC61511, Functional safety—Safety instrumented systems for the process industry sector, International Electrotechnical Commission Std, (2003).

[24] Y. Liu, M. Rausand, Reliability assessment of safety instrumented systems subject to different demand modes, Journal of Loss Prevention in the Process Industries, 24 (2011) 49-56.

[25] GRIF, Version 2017, http://grif-workshop.com, (2017).

[26] IEC62551, Analysis techniques for dependability Petri net techniques, 2013.

[27] D. Grabaskas, M.K. Nakayama, R. Denning, T. Aldemir, Advantages of variance reduction techniques in establishing confidence intervals for quantiles, Reliability Engineering & System Safety, 149 (2016) 187-203.

[28] J. Zhang, H.K.T. Ng, N. Balakrishnan, Statistical inference of component lifetimes with location-scale distributions from censored system failure data with known signature, IEEE Transactions on Reliability, 64 (2015) 613-626.

[29] J.E. Ramirez-Marquez, G. Levitin, Algorithm for estimating reliability confidence bounds of multi-state systems, Reliability Engineering & System Safety, 93 (2008) 1231-1243.

[30] A. Alban, H.A. Darji, A. Imamura, M.K. Nakayama, Efficient Monte Carlo methods for estimating failure probabilities, Reliability Engineering & System Safety, 165 (2017) 376-394.