Reliability modeling of subsea SISs partial testing subject to delayed restoration

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

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

[b]Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Abstract:

Subsea oil and gas production has always involved the challenging task of determining the overall reliability of safeguarding systems, such as safety instrumented systems (SISs). Partial testing and delayed restoration of SISs are the main issues in operation and maintenance activities. This paper proposes a novel reliability-modeling methodology for subsea SISs subject to partial testing and delayed restoration. The proposed methodology incorporates an increasing failure rate in conjunction with dangerous undetected failures for the final elements. Approximation formulas for evaluating the average probability of failure on demand are derived for SISs in the low-demand operating mode. In addition, the effects of degradation are modeled by following Weibull rules in different subsequent partial testing intervals. In contrast to previous works, the present research accounts for delayed restoration after detecting failures and also considers the repair time for different scenarios. The proposed formulas are compared with the existing ones for partial verification. A case study on the shutdown valves of a subsea high-integrity pressure protection system is presented to illustrate the feasibility of the proposed methodology. It is also proven that the proposed approximation offers a robust opportunity for testing strategy optimization and performance improvement of SISs.

Key words: Safety-instrumented systems, Failure probability on demand, Partial testing, Delayed restoration, Approximation formulas

1. Introduction

Safety-instrumented systems (SISs) are increasingly applied in subsea oil and gas industries to detect the onset of hazardous events and/or to mitigate their consequences [1, 2]. The availability of SISs plays a critical role in capturing key characteristics for the design of safety-instrumented systems (SISs). The international standard IEC 61508 [3] has presented requirements for SIS availability and reliability analyses, with the aim to frame the design and operation of SISs. The ISO/TR 12489 standard [4] has described reliability modeling and probabilistic calculation methods of SIS performed in petroleum, petrochemical, and natural gas industries. Some frequently used techniques have also been developed for SIS reliability modeling and performance assessment, including generalized formulas [5], Fault Tree Analysis [6], Bayesian methods [7-9], Markov Analysis [10], Petri Nets [2, 11] and AltaRica modeling [12]. The average probability of failures on demand (PFD_{avg}) which is, in fact, the average unavailability over a given interval, is considered as the suggested reliability measure for safety instrumented function (SIF) implemented by SISs when the low-demand mode is assumed [3].

In current literature regarding availability and reliability assessment, the effects of some factors including k-out-of-n voting structures [13, 14], common cause failures[15-17], process demand [17-19], spurious failures [20, 21], human and organizational factors [22], uncertainty [23], and periodical proof tests where all hidden failures are assumed to be discovered (so-called full proof tests)[1, 2], have been well studied. Other key parameters also need to be taken into account to quantify the PFD_{avg} of SISs, including failure rates, testing strategies, and repair time under the assumption that a full renewal takes place at each fully proof test.

In many real-world SIS subsystems, the final elements may not always fail at a constant failure rate. It is well known that when the failures of components are time-dependent, the constant failure rate-based methods are not well suited for evaluating system reliability[10, 24-26]. Weibull distributions as a suitable choice have been adopted to model reliability for the mechanical equipment with an increasing failure rate [5]. Some case studies related to Weibull distributed components have been studied. One method is proposed for PFD calculation based on the ratio between cumulative Weibull distribution functions for MooN system in full proof testing [27] and such a method has been further developed by Rogova et al. [28] considering non-constant failure rates and common cause failures. Wu et al. have presented an approach for reliability assessment of SIS final elements with time-dependent failure rates in full and partial testing [29].

Many SISs are considered passive systems since they are only activated when a demand occurs, periodic full proof tests are therefore required to reveal failures for reliability assessment [3, 11]. However, for subsea exploration and production, frequent full proof tests will disturb the operations/production and finally result in an increase of production downtime and higher operational costs [30]. Taking shutdown valves of SISs for instance, such tests can thoroughly verify that the valves operate on demand, but they may also bring some negative impact to valves due to strong stresses. The overall risk level may also increase due to more abruption of normal operation. For such valves, partial testing has been therefore introduced as a supplement of full proof testing [30, 31]. Partial stroke testing means to partially operate a valve, which meets the requirement for valve movement without any extra production disturbances and can also detect the several types of dangerous failures related to sticking of valves or delayed operation. The safety may also be improved if such partial testing as an effective strategy in SISs is added with existing proof testing regime [30].

Some efforts have been made in the development of PFD_{avg} by integrating with the influence of FT and PT. The generalized PFD_{avg} formulas have been established using the multi-phase Markov models in consideration of partial tests and repair times [32]. Jin and Rausand [15] have developed approximate generalized expressions that can calculate the PFD_{avg} for general k-out-of-n systems subject to partial-testing and common-cause failures. A multi-objective genetic algorithm has been used by [33] to develop generalized expressions, which takes into account the common cause failure, diagnostic coverage, lifecycle cost and spurious trip rate to optimize testing strategies. Pascual et al. [34] have presented a model to find optimal inspection intervals by calculating availability, and subsystems decomposition, dependent and independent failures, and non-negligible inspection time are considered.

However, several issues need to be further investigated when they are applied to the subsea SIS system. The existing literatures [2, 15, 33, 35] focus to a large extent on the reliability assessment of SIS based on assumptions that are questionable in a subsea context, for example: 1) The failures of SISs are mostly assumed to be exponentially distributed with the constant failure rates in these studies [3, 5]. But in fact for many final elements working in a subsea environment, they are more likely to deteriorate with an increasing failure rate over time especially in the wear-out period [28, 29]. Such an assumption may be not suitable for equipment that is subject to degradation of time. 2) The repair time for the revealed dangerous failures has been always assumed to be negligible compared to proof and partial test intervals in the already existing formulas. The IEC 61508 and ISO/TR 12489 standards [3, 4] have presented repair time taxonomies and the effects of repair times on PFD_{avg} calculation have been discussed in [5, 32]. This assumption may not be always realistic for a subsea system since it is not easy to initialize maintenance in a short time.

In order to overcome these limitations as mentioned above, the objective of this paper is to develop new approximation formulations that take into account the effects of degradation and delayed repair under subsequent partial testing intervals. The potential contribution can be specified as:

- An increasing failure rate is introduced to model the effects of degradation when failures of SIS final actuators follow Weibull rules.

- Conditional probability is introduced to develop approximation formulas under different partial testing intervals, which is able to predict the PFD_{avg} given the previous partial testing period without failures.
- Restoration action will be taken into account and contributions from delayed repair are made to handle the issues of difficulties in accessing subsea equipment.

The remainder of this paper is organized as follows: Section 2 discusses the definition and assumptions. Section 3 develops PFD_{avg} approximation subject to partial testing and delayed repair. The time-dependent failure rate following Weibull rules is introduced to model the degradation behavior of the system. A case study for HIPPS valves is carried out to demonstrate the applications of proposed models in Section 4. In Section 5 reliability block diagram driven Petri net modeling is performed and compared with approximation formulas. Section 6 presents conclusions and research perspectives.

2. Definitions and assumptions

This section *firstly* presents some definition and *then* gives relative assumptions for developing PFD_{avg} approximation subject to partial testing and delayed restoration.

2.1 SIS definitions

A typical subsea SIS consists of sensors (e.g. pressure transmitters), logic solver(s) (e.g. programmable logic controllers) and final elements (e.g. valves, breakers, and switches). The redundant sensor subsystem detects hazardous events by measuring physical parameters of the protected system. The logic solver subsystem makes appropriate decisions, by comparing the measurements with given thresholds. The final elements as vital subsystems of SISs are therefore designed to actually perform the intended corrective actions and maintain the process to be in a safe state. Specific subsystems are used to carry out specific safety instrumented functions (SIFs). In real-world SIS final element subsystems, taking shutdown valves for instance, such a subsystem includes one element or two parallel components which are defined as 1oo1 system and 1oo2 system, respectively. These elements may always suffer from dangerous hidden failures, dangerous undetected (DU) failures, that will be discovered by a test or a demand when they are only activated. This paper is limited to SISs final elements operating in low demand, and the frequency of such demands is assumed to be less than once per year [3].

2.2 Partial testing

Partial testing (PT) of final elements, like actuated valves, has been introduced as a supplement to full proof testing (FT). For the shutdown valve case, a partial test means to partially operate a valve, which meets the requirement for valve movement and can also reveal 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 that may lead to process shutdowns [30, 32]. In a subsea environment, it is of high importance to reduce the number of planned and unplanned stops. Only some specific failure modes are detected by PT, meaning that PT cannot fully replace FT. Except the benefit in avoiding production loss, because the valve movement in PT is so small that the impact on the process flow or pressure is negligible, partial tests could reduce wear of the valve seat area that may be caused by FT in a fully closed state with more stress. With PT, fewer full valve closures are expected, meaning that the number of potentially dangerous situations when reopening the valves is reduced. The probability of sticking seals may also be reduced due to more movements of valves in a FT. 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 Delayed restoration

Challenges from subsea context are not well handled with, for instance, the non-ignorable time to repair even for a revealed failure. For subsea equipment, repairs are always delayed since: Firstly, repairs imply the mobilization of a maintenance vessel (rig), which can last several days of weeks. In the same ways, the spare parts may need some time to be available. Then, it is quite difficult to access to subsea equipment, and finally, some potential risk may increase due to the unscheduled pulling for repair. The mean repair time (MRT) of DU-failures refers to the time required to repair a failure or make a replacement for a component when it has been detected by PT or FT. This part also includes time waiting for repairs if there are logistic delays. The safety function of the channel is regarded to be lost during the MRT.

2.4 Assumptions

PFD_{avg} formulas have been developed in this section for the SIS final element subsystem. When a DU-failure is detected with a partial test, a repair action can be initiated to restore the valves to a normal state. If such action is not carried out immediately, repair time is considered. In this case, the SISs continue in the degraded mode of operation, assuming that the risk is managed by some other risk compensating measures. For the formulas, the following common assumptions have been made:

- Failure rates of components (i.e. rate of occurrence of failures) are assumed to follow the Weibull distribution (due to degradation effects of being in the subsea environment with limited access to regular maintenance).
- MRT is regarded to be non-negligible due to delayed repair.
- All components are initially (i.e. at first start-up of the subsea facility) in a perfect/functioning state.
- All partial tests are performed simultaneously for the final elements.
- The time spent in a full and partial test is negligible for the final elements.
- After restoration action involving subsea intervention work (regardless of how types of failures are revealed) in a test, the subsystem is assumed an as-good-as-new condition.
- Same MRT is expected no matter how many valves that are being repaired.
- Valves will normally have zero diagnostic coverage, which means that no effect of DD failures has been included.
- Common cause failures are excluded, but they can be considered by introducing the β-factor model.
- All DU-failures are assumed to be independent for testing.

3. Proposed methodology

This paper is limited to SISs operating in low demand modes defined by key standards, such as IEC 61508 and IEC 61511. PFD_{avg} formulas are developed for SISs final elements in partial testing subject to delayed restoration. The effects of degradation of final elements with DU failures are modeled into the proposed formulas. Two types of PFD_{avg} [5] also need to be introduced to calculate the total PFD_{avg}:

- PFD_{avg} in partial testing,
- PFD_{avg} with delayed repairs.

3.1 Modeling PFD_{avg} for partial testing

One proof test interval is considered here to determine the PFD_{avg} if partial testing is involved. All components will still be in a functioning state after minor repair actions, but the degradation exists due to the incomplete replacement assumed. When DU failures are detected by proof/partial testing given the repair action initiated immediately, two types of approximate formulas are developed in this section:

- Formulas without partial testing
- Formulas with partial testing

3.1.1 Nonconstant failure rates

Based on the ISO/TR 12489 standard, the average failure rate is the average value of the time-dependent failure rate over a given time interval. In fact, the average failure rate is the mathematical expectation of the failure rate [4]. If an item has a nonconstant failure rate function, we will here approximate this failure rate function z(t) by an average failure rate. The average value of z(t) in the proof test interval (0, τ), denoted z_{avg} (0, τ), is:

$$z_{avg}(0,\tau)=\frac{1}{\tau}\int_0^{\tau} z(t)dt \quad (1)$$

The survivor function for the item is given as:

$$R(t)=P_r(T>t)=e^{-\int_0^t z(s)ds}=e^{z_{avg}(0,\tau)t} \quad (2)$$

The probability that the item will fail at t = τ is given by:

$$F(\tau)=1-R(\tau)=1-e^{z_{avg}(0,\tau)\tau}\approx z_{avg}(0,\tau)\tau \quad (3)$$

The average failure rate can therefore be approximated by:

$$z_{avg}(0,\tau)\approx F(\tau)/\tau \quad (4)$$

It is worth noting that this approximation is acceptable only for rather short intervals. However, for large values of τ, the average failure rate $z_{avg}(0,\tau)$, calculated by the above method, approaches zero, which is not realistic.

Compared to constant failure rates generally assumed by previous research work [3, 36], the non-constant failure rate can allow the components that are deteriorating with an increasing failure rate. Weibull distribution is one of the most widely used life distribution in reliability analysis, which may provide a wide range choice for parameters to model the various failure behaviors [5]. The time-dependent failure rate function [29] denoted $z(t)$ is defined as:

$$z(t)=\frac{f(t)}{R(t)}=\frac{f(t)}{1-F(t)}=\alpha\lambda^{\alpha}t^{\alpha-1} \quad (5)$$

where λ is a scale parameter, α is a shape parameter, f(t) is the probability density function, R(t) and F(t) are survival and failure probability distributions respectively, and they may be found in e.g. [5].

The average failure rate in the proof test interval (0, τ) is given by:

$$z_{avg}(0,\tau)=\frac{1}{\tau}\int_0^{\tau} z(t)dt=\frac{1}{\tau}\int_0^{\tau}\alpha\lambda^{\alpha}t^{\alpha-1}dt=\lambda^{\alpha}\tau^{\alpha-1} \quad (6)$$

Let α = 2, λ = 4.00E-06 per hours, and the proof testing interval τ =8760 hours, the average failure rate in (0, τ) is from Eq.(4), $z_{avg}(0,\tau)$≈1.4007E-07 per hour, and using the Eq.(6) yields $z_{avg}(0,\tau)$=1.4016E-07 per hour. The

difference between the exact value and the approximated value is approximately 0.064% of the exact value, and this approximation is able to generate conservative results.

3.1.2 PFD_{avg} without partial testing

The failure probability of systems can be therefore approximately evaluated for final elements using the time-dependent failure rate. The time-dependent $PFD(t)$ for DU-failures occurrence in a proof testing interval [0, τ] is equal to the unavailability in this interval, which can be also expressed as:

$$PFD(t) = \Pr(T_{DU} \le t) = U(t) \quad (7)$$

where $\Pr(T_{DU} \le t)$ is the probability that a DU-failure of a single channel is revealed in a proof test and U(t) is the unavailability function of this channel at time t.

In a full proof testing interval [0,τ], the PFD_{avg} for 1oo1 system subject to FT without PT is expressed as [29]:

$$\begin{aligned} PFD_{avg} &= \frac{1}{\tau}\int_0^\tau PFD(t)dt = \frac{1}{\tau}\int_0^\tau \Pr(T_{DU} \le t)dt \\ &= \frac{1}{\tau}\int_0^\tau 1 - e^{-\frac{z(t)}{\alpha}t}dt \\ &\approx \frac{1}{\tau}\int_0^\tau \frac{z(t)}{\alpha}tdt = \frac{z_{avg}(0,\tau)\cdot\tau}{\alpha+1} \end{aligned} \quad (8)$$

PFD_{avg} refers to the average $PFD(t)$ for the DU-failure detected in a proof test interval. Note that this approximation will be applied when $z(t)\cdot t/\alpha$ takes low values.

Similarly, we also have PFD_{avg} without PT for 1oo2 system:

$$PFD_{avg} = \frac{1}{\tau}\int_0^\tau (1 - e^{-\frac{z(t)}{\alpha}t})^2 dt \approx \frac{1}{\tau}\int_0^\tau (\frac{z(t)}{\alpha}t)^2 dt = \frac{(z_{avg}(0,\tau)\cdot\tau)^2}{2\alpha+1} \quad (9)$$

3.1.3 PFD_{avg} with partial testing

Two types of failures are introduced when involving PT for PFD_{avg} evaluations: Failures detected by PT, and remaining failures only detected by FT, assuming that the FT can detect all DU failures. It means at full test intervals that both a PT and FT is carried out, so that all DU failures are identified. The assumptions that failures are either detected by PT or by FT is well accepted, e.g. in ISO TR 12489 [4] and IEC 61508-6 [3]. Two scenarios related to degradation analysis are presented as follows.

- Partial tests are performed to detect parts of failures, and so the components will not be in the as-good-as-new state due to remaining failures.
- Effects of degradations may exist if the full replacement will not be performed after the testing. If no DU-failure is revealed in a partial test, the component is still functioning after a test, but it is not as-good-as-new since other properties of the components have not been changed.

When all final elements are assumed to be independent, PFD_{avg} of having two types of failures involving PT in an FT interval is expressed by the sum of $PFD_{avg,FT}$ and $PFD_{avg,PT}$. $PFD_{avg\ FT}$ stands for the average probability for the remaining DU-failure detected by proof testing and $PFD_{avg\ PT}$ stands for the average probability for the DU-failure detected by partial testing. The total PFD_{avg} [15, 30, 37] for a general system is therefore approximated as: $PFD_{avg} \approx PFD_{avg,FT} + PFD_{avg,PT}$.

The $PFD_{avg\ FT}$ is illustrated as:

$$PFD_{avg,FT} = \frac{1}{\tau}\int_0^\tau PFD(t)dt \quad (10)$$

Several partial tests are normally carried out during an FT interval [0, τ], and *m* stands for the number of partial tests in [0, τ]. The occurrence of failures in the partial testing interval [0, τ/m] is regarded as a stochastic process, and the $PFD_{avg\,FT}$ is, therefore, an unknown unavailability since the system is protected by the SIF. Due to the effects of degradations, $PFD(t)$ in the current partial testing interval is different from that in the previous partial testing interval. PFD_{avg} should be calculated by introducing conditional probabilities for different periods.

If the failure is detected in the first partial testing interval $[0,\tau_1]$, the PFD_{avg} is expressed as:

$$PFD_{avg,1} = \frac{1}{\tau_1}\int_0^{\tau_1} PFD(t)dt = \frac{1}{\tau_1}\int_0^{\tau_1} \Pr(T_{DUP} \le t)dt \quad (11)$$

where $\Pr(T_{DUP} \le t)$ is the probability that a DU-failure of a single channel is revealed in the first partial test.

If the channel passes the first testing interval perfectly, the PFD_{avg} in the second testing interval $[\tau_1,\tau_2]$ is written by:

$$\begin{aligned} PFD_{avg,2} &= \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} PFD(t)dt \\ &= \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} \Pr(T_{DUP} \le t / T_{DUP} > \tau_1)dt \\ &= \frac{1}{\tau_2 - \tau_1}\int_{\tau_1}^{\tau_2} \frac{\Pr(T_{DUP} \le t) - \Pr(T_{DUP} \le \tau_1)}{\Pr(T_{DUP} > \tau_1)}dt \end{aligned} \quad (12)$$

If the channel passes the previous testing intervals perfectly, and in the testing interval $[\tau_{i-1},\tau_i]$, the PFD_{avg} is given by:

$$\begin{aligned} PFD_{avg,i} &= \frac{1}{\tau_i - \tau_{i\text{-}1}}\int_{\tau_{i-1}}^{\tau_i} \Pr(T_{DUP} \le t / T_{DUP} > \tau_{i-1})dt \\ &= \frac{1}{\tau_i - \tau_{i\text{-}1}}\int_{\tau_{i-1}}^{\tau_i} \frac{\Pr(T_{DUP} \le t) - \Pr(T_{DUP} \le \tau_{i-1})}{\Pr(T_{DUP} > \tau_{i-1})}dt \end{aligned} \quad (13)$$

So, we have the $PFD_{avg,PT}$ for partial testing

$$PFD_{avg,PT} = \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i} \frac{\Pr(T_{DUP} \le t) - \Pr(T_{DUP} \le \tau_{i\text{-}1})}{\Pr(T_{DUP} > \tau_{i\text{-}1})}dt \quad (14)$$

where $\tau_0 = 0$.

It should be noted that this model is based on the assumption that if a DU-failure is discovered in a test, the minimal repair is carried.

- In the partial testing interval $[\tau_{i-1}, \tau_i]$, assuming $\tau/m = \tau_i - \tau_{i-1}$, we have the PFD_{avg} for 1oo1 system in a proof test interval $[0,\tau]$ as follows.

$$PFD_{avg} \approx PFD_{avg,FT} + PFD_{avg,PT}$$

$$= \frac{1}{\tau}\int_0^{\tau} 1 - e^{-\frac{z_{FT}(t)}{\alpha}t}dt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i} \frac{(1-e^{-\frac{z_{PT}(t)}{\alpha}t}) - (1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})}{e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}}dt$$

$$\approx \frac{1}{\tau}\int_0^{\tau} \frac{z_{FT}(t)}{\alpha}tdt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i} \frac{\frac{z_{PT}(t)}{\alpha}t - \frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}{1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}dt \quad (15)$$

$$= \frac{z_{avg,FT}(0,\tau)\cdot\tau}{\alpha+1} + \frac{1}{\tau}\sum_{i=1}^{m} \frac{\frac{z_{avg,PT}(0,\tau_i)\cdot\tau_i^{\,2} - z_{avg,PT}(0,\tau_{i-1})\cdot\tau_{i-1}^{\,2}}{\alpha+1} - \frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}(\tau_i-\tau_{i-1})}{1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}$$

where DU failure rate in this section is the sum of two rates: $z_{FT}(t) = \alpha\cdot\lambda_{FT}^{\alpha}\cdot\tau^{\alpha-1}$ is DU failure rate corresponding to failure modes revealed by FT, and here λ_{FT} is a parameter in a proof test with PT. $z_{PT}(t) = \alpha\cdot\lambda_{PT}^{\alpha}\cdot\tau^{\alpha-1}$ is DU failure rate with regard to failure modes revealed by PT, and λ_{PT} is a parameter in a partial test. $z_{avg,FT}(0,\tau) = \lambda_{FT}^{\alpha}\cdot\tau^{\alpha-1}$ and $z_{avg,PT}(0,\tau_i) = \lambda_{PT}^{\alpha}\cdot\tau_i^{\alpha-1}$stands for two types of average failure rates in a proof test and a partial test, respectively. And they agree $\lambda_{FT}^{\alpha} + \lambda_{PT}^{\alpha} = \lambda_{DU}^{\alpha}$ and here λ_{DU} is a parameter in a proof test without PT.

- Similarly, we also have PFD_{avg} with PT for 1oo2 system:

$$PFD_{avg} \approx PFD_{avg,FT} + PFD_{avg,PT}$$

$$\approx \frac{1}{\tau}\int_0^{\tau} (\frac{z_{FT}(t)}{\alpha}t)^2 dt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i} \frac{(\frac{z_{PT}(t)}{\alpha}t)^2 - (\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}{(1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}dt \quad (16)$$

$$= \frac{(z_{avg,FT}(0,\tau)\cdot\tau)^2}{2\alpha+1} + \frac{1}{\tau}\sum_{i=1}^{m} \frac{(z_{avg,PT}(0,\tau_i)\cdot\tau_i^{\,2})^2\tau_i - (z_{avg,PT}(0,\tau_{i-1})\cdot\tau_{i-1}^{\,2})\tau_{i-1}}{2\alpha+1} - \frac{(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2(\tau_i-\tau_{i-1})}{(1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}$$

3.2 Modeling PFD_{avg} for delayed restoration

The time required to restore a revealed failure is considered to be non-negligible, and this may sometimes be the case in subsea practice. The different MRT is assumed for FT with perfect repair and PT with minimal repair. $PFD_{avgFT,\,MRTF}$ refers to the average unavailability of delayed restoration for proof tests. During repairs, the system has no capability to perform its safety function, and this is, therefore, a known unavailability [5]. $PFD_{avgFT,\,MRTF}$ in the FT proof test interval $[0,\tau]$ is illustrated as

$$PFD_{avgFT,MRTF} = \frac{\Pr(T_{DU} \le \tau)\bullet MRTF}{\tau} \quad (17)$$

where $\Pr(T_{DU} \le \tau)$ is the probability of a single channel for DU failures revealed by a proof test.

$PFD_{avgPT,\,MRTP}$ refers to the average unavailability of delayed restoration for partial tests. Similarly, in the first PT interval $[0,\tau_1]$, we have

$$PFD_{avg1PT,MRT} = \frac{\Pr(T_{DUP} \le \tau_1) \bullet MRTP}{\tau_1} \quad (18)$$

where $\Pr(T_{DUP} \le \tau_1)$ is the probability of a single channel for DU failures revealed by the first partial test.

If restoration occurs in the second testing interval $[\tau_1,\tau_2]$, we also have

$$PFD_{avg2PT,MRTP} = \frac{\frac{\Pr(T_{DUP} \le \tau_2) - \Pr(T_{DUP} \le \tau_1)}{\Pr(T_{DUP} > \tau_1)} \bullet MRTP}{\tau_2 - \tau_1} \quad (19)$$

If the restoration occurs in the testing interval $[\tau_{i-1},\tau_i]$, the formula can be expressed by

$$PFD_{avgiPT,MRTP} = \frac{\frac{\Pr(T_{DUP} \le \tau_i) - \Pr(T_{DUP} \le \tau_{i-1})}{\Pr(T_{DUP} > \tau_{i-1})} \bullet MRTP}{\tau_i - \tau_{i-1}} \quad (20)$$

So, we have the $PFD_{avgPT,\ MRTP}$ for delayed repair:

$$PFD_{avgPT,MRTP} = \frac{\sum_{i=1}^{m} \frac{\Pr(T_{DUP} \le \tau_i) - \Pr(T_{DUP} \le \tau_{i-1})}{\Pr(T_{DUP} > \tau_{i-1})} \bullet MRTP}{\tau} \quad (21)$$

Based on the previous work, there are four scenarios for obtaining the total PFD_{avg} related to delayed restoration.

- Scenario 1 Consider FT only for 1oo1 system. It is assumed that the repair is delayed for a period of MRTF. The PFD_{avg} then becomes:

$$\begin{aligned} PFD_{avg} &= PFD_{avg,FT} + PFD_{avgFT,MRTF} \\ &= \frac{1}{\tau}\int_0^{\tau} 1 - e^{-\frac{z(t)}{\alpha}t} dt + \frac{(1 - e^{-\frac{z(\tau)}{\alpha}\tau}) * MRTF}{\tau} \\ &\approx \frac{1}{\tau}\int_0^{\tau} \frac{z(t)}{\alpha} t dt + \frac{z(\tau) * MRTF}{\alpha} \\ &= \frac{z_{avg}(0,\tau) \cdot \tau}{\alpha + 1} + \frac{z(\tau) * MRTF}{\alpha} \end{aligned} \quad (22)$$

- Scenario 2 Consider effects of FT and PT for 1oo1 system. It is assumed that repair is delayed both for FT (with time MRTF) and PT (with MRTP). In this case, PFD_{avg} is expressed as

$$PFD_{avg} \approx PFD_{avg,FT} + PFD_{avg,PT} + PFD_{avgFT,MRTF} + PFD_{avgPT,MRTP}$$

$$= \frac{1}{\tau}\int_0^{\tau} 1 - e^{-\frac{z_{FT}(t)}{\alpha}t}dt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i} \frac{(1-e^{-\frac{z_{PT}(t)}{\alpha}t}) - (1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})}{e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha_{PT}}\tau_{i-1}}}dt$$

$$+ \frac{(1-e^{-\frac{z_{FT}(\tau)}{\alpha}\tau})*MRTF}{\tau} + \frac{\sum_{i=1}^{m} \frac{(1-e^{-\frac{z_{PT}(\tau_i)}{\alpha}\tau_i}) - (1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})}{e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}} * MRTP}{\tau}$$

$$\approx \frac{1}{\tau}\int_0^{\tau} \frac{z_{FT}(t)}{\alpha}tdt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i} \frac{\frac{z_{PT}(t)}{\alpha}t - \frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}{1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}dt$$

$$+ \frac{z_{FT}(\tau)*MRTF}{\alpha} + \frac{\sum_{i=1}^{m} \frac{\frac{z_{PT}(\tau_i)}{\alpha}\tau_i - \frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}{(1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})} * MRTP}{\tau}$$

$$= \frac{z_{avg,FT}(0,\tau)\cdot\tau}{\alpha+1} + \frac{1}{\tau}\sum_{i=1}^{m} \frac{\frac{z_{avg,PT}(0,\tau_i)\cdot\tau_i^{\,2} - z_{avg,PT}(0,\tau_{i-1})\cdot\tau_{i-1}^{\,2}}{\alpha+1} - \frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}(\tau_i - \tau_{i-1})}{1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}} \quad (23)$$

$$+ \frac{z_{FT}(\tau)*MRTF}{\alpha} + \frac{\sum_{i=1}^{m} \frac{\frac{z_{PT}(\tau_i)}{\alpha}\tau_i - \frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}}{(1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})} * MRTP}{\tau}$$

- Scenario 3 Consider FT only for 1oo2 system. It is assumed that the repair is delayed for a period of MRTF. Some additional assumptions are made:
  (1) When one DU failure of an actuated valve is discovered by PT, the other remaining component is still available. However, this remaining channel may get a DU failure during the repair time, and the associated mean downtime is introduced to calculate the $PFD_{avg,MRT1}$.
  (2) If DU failures for both components are discovered by PT, the 1oo2 system is out of function until both components are repaired. The average probability still follows the Eq.(24).

$$PFD_{avg,MRT1} = \frac{\int_0^{MRTF}(1-e^{-\frac{z_{DU}(t)}{\alpha}t})dt}{\tau} \quad (24)$$

The PFD_{avg} therefore becomes:

$$
\begin{aligned}
PFD_{avg} &= PFD_{avg,FT} + PFD_{avg,MRTF} \\
&= \frac{1}{\tau}\int_0^{\tau} \Pr(T_{DU} \le t)dt + \frac{\int_0^{MRT}(1-e^{-\frac{z(t)}{\alpha}t})dt}{\tau} + \frac{\Pr(T_{DU} \le t)\cdot MRTF}{\tau} \\
&= \frac{1}{\tau}\int_0^{\tau}(1-e^{-\frac{z(t)}{\alpha}t})^2 dt + \frac{\int_0^{MRT}(1-e^{-\frac{z(t)}{\alpha}t})dt}{\tau} + \frac{(1-e^{-\frac{z(\tau)}{\alpha}\tau})^2\cdot MRTF}{\tau} \\
&\approx \frac{1}{\tau}\int_0^{\tau}(\frac{z(t)}{\alpha}t)^2 dt + \frac{\int_0^{MRT}\frac{z(t)}{\alpha}tdt}{\tau} + \frac{(\frac{z(\tau)}{\alpha}\tau)^2\cdot MRTF}{\tau} \\
&= \frac{(z_{avg}(0,\tau)\cdot\tau)^2}{2\alpha+1} + \frac{(z_{avg}(0,MRTF)\cdot 2MRTF)}{(\alpha+1)\tau} + \frac{z^2(\tau)\cdot\tau}{\alpha}\cdot MRTF
\end{aligned}
\tag{25}
$$

where， $z_{avg}\left(0, MRTF\right)$ denotes the average failure rate of one DU failure occurs in remaining component given the repairing time interval [0, MRTF].

- Scenario 4 Similarly, considering effects of FT and PT for 1oo2 system, PFD_{avg} is therefore given by

$$
\begin{aligned}
PFD_{avg} &\approx PFD_{avg,FT} + PFD_{avg,PT} + PFD_{avgFT,MRTF} + PFD_{avgPT,MRTP} \\
&= \frac{1}{\tau}\int_0^{\tau}(1-e^{-\frac{z_{FT}(t)}{\alpha}t})^2 dt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i}\frac{(1-e^{-\frac{z_{PT}(t)}{\alpha}t})^2-(1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})^2}{1-(1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})^2}dt + \frac{\int_0^{MRTF}(1-e^{-\frac{z_{FT}(t)}{\alpha}t})dt}{\tau} \\
&+ \frac{(1-e^{-\frac{z_{FT}(\tau)}{\alpha}\tau})^2\cdot MRTF}{\tau} + \frac{\int_0^{MRTP}(1-e^{-\frac{z_{PT}(t)}{\alpha}t})dt}{\tau} + \frac{\sum_{i=1}^{m}\frac{(1-e^{-\frac{z_{PT}(\tau_i)}{\alpha}\tau_i})^2-(1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})^2}{1-(1-e^{-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1}})^2}\cdot MRTP}{\tau} \\
&\approx \frac{1}{\tau}\int_0^{\tau}(\frac{z_{FT}(t)}{\alpha}t)^2 dt + \frac{1}{\tau}\sum_{i=1}^{m}\int_{\tau_{i-1}}^{\tau_i}\frac{(\frac{z_{PT}(t)}{\alpha}t)^2-(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}{(1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}dt + \frac{\int_0^{MRTF}\frac{z_{FT}(t)}{\alpha}tdt}{\tau} \\
&+ \frac{(\frac{z_{FT}(\tau)}{\alpha}\tau)^2\cdot MRTF}{\tau} + \frac{\int_0^{MRTP}\frac{z_{PT}(t)}{\alpha}dt}{\tau} + \frac{\sum_{i=1}^{m}\frac{(\frac{z_{PT}(\tau_i)}{\alpha}\tau_i)^2-(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}{1-(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}\cdot MRTP}{\tau} \\
&= \frac{(z_{avg,FT}(0,\tau)\cdot\tau)^2}{2\alpha+1} + \frac{1}{\tau}\sum_{i=1}^{m}\frac{\frac{(z_{avg,PT}(0,\tau_i)\cdot\tau_i^{\,2})^2\tau_i-(z_{avg,PT}(0,\tau_{i-1})\cdot\tau_{i-1}^{\,2})^2\tau_{i-1}}{2\alpha+1}-(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2(\tau_i-\tau_{i-1})}{(1-\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2} \\
&+ \frac{(z_{avg,FT}(0,MRTF)\cdot 2MRTF)}{(\alpha+1)\tau} + \frac{z^2{}_{FT}(\tau)}{\alpha}\tau\cdot MRTF + \frac{(z_{avg,PT}(0,MRTP)\cdot 2MRTP)}{(\alpha+1)\tau} \\
&+ \frac{\sum_{i=1}^{m}\frac{(\frac{z_{PT}(\tau_i)}{\alpha}\tau_i)^2-(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}{1-(\frac{z_{PT}(\tau_{i-1})}{\alpha}\tau_{i-1})^2}\cdot MRTP}{\tau}
\end{aligned}
\tag{26}
$$

Considering a proof test only given α=1, for 1oo1 system, $PFD_{avg}=\lambda_{DU}\tau/2$, and for 1oo2 system, $PFD_{avg}=(\lambda_{DU}\tau)^2/3$, which is identical to PFD_{avg} formulas in some work [5] for systems with constant failure rates in proof test interval [0, τ]. It is worth noting that the failure rate in the simplified formulas considers DU failures only, and that

other types of failure modes (e,g,.DD failures) are omitted. Considering the non-negligible repair time (MRT) in a proof test interval [0, τ] given α=1, for 1oo1 system, there is $PFD_{avg}=\lambda_{DU}\tau/2+\lambda_{DU}\cdot MRT$, and for 1oo2 system, there is $PFD_{avg}=(\lambda_{DU}\tau)^2/3+MRT\cdot\lambda_{DU}^2\cdot\tau+(\lambda_{DU}\cdot MRT)^2/2$, which is identical to PFD_{avg} formulas in the work [5] for systems with constant failure rates in a proof test interval [0, τ]. These proposed formulas seem complicated, however, it can provide a method to straightforwardly calculate the unavailability considering partial testing and delayed repair.

4. Case study

The typical subsea high integrity pressure protection system (HIPPS) is a type of SISs protecting a subsea production system from pressure build-up that may cause pipeline rupture by shutting off the source before exceeding the maximum pressure [30, 31]. Such a HIPPS consists of pressure sensors, logic solvers, and shutdown valves, which is shown in Fig.1. In the case study, HIPPS valves are installed as the final elements, and they as the last safety barriers are always operated in low demand mode [35], which actually perform the corrective action in the subsea system to maintain the process to be in a safe state. The safety function of valves is to stop the flow sufficiently fast to avoid that high pressures enter pipeline sections which are designed for low pressure.

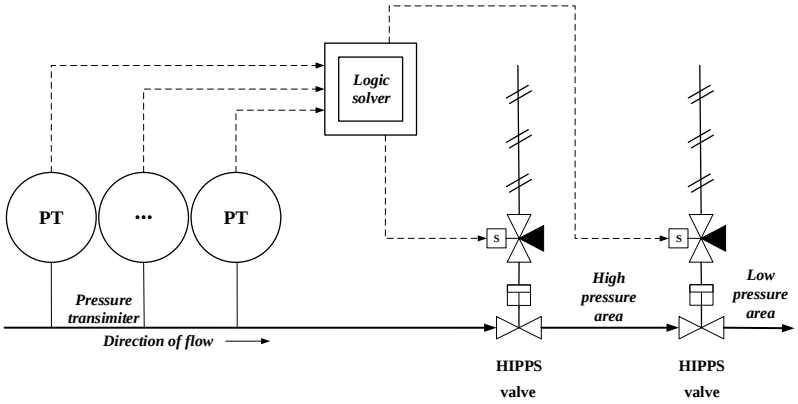


Fig. 1 A typical HIPPS system

Consider HIPPS valves that are tested at regular intervals. An important issue is to determine what kinds of dangerous failure modes of the valves have. Field experience has shown that if valves are not operated (at all or very seldom), they can stick in the position. In fact, sticking in open position accounts for large percentage of the failures recorded for shutdown valves. A delayed operation can also be related to sticking, but also other causes (e.g. capacity constraints from operations of multiple valves). These failure modes cannot be detected automatically unless we close or partially close the valves, and these failures are therefore recognized DU failures during operation. DU failure modes are specified as follows. DU1 failure is that can be detected by PT, e.g., the valve is not able to close on command. DU2 failure is that cannot normally be detected by PT but FT, e.g., the valve is able to close on command, but there is a leakage through the closed position that is higher than accepted levels. For such failures may also be possible to use other planned and unplanned stops to check if this failure is present [29]. HIPPS valves for both 1oo1 system and 1oo2 system with two types of DU failures are shown in Fig. 2.

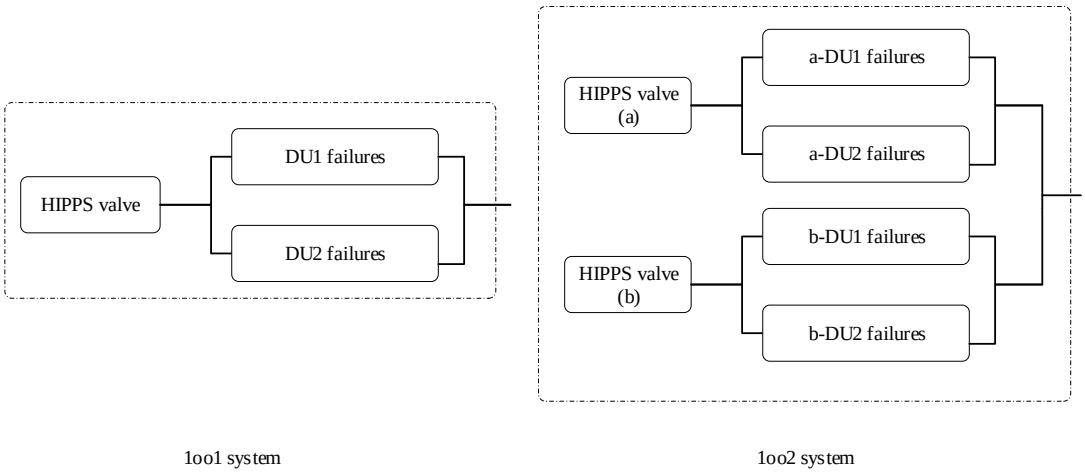


Fig. 2 HIPPS valves for 1oo1 system and 1oo2 system with two types of DU failures

These two mentioned DU failures will be discussed in this section, PFD_{avg} are analyzed for 1oo1 and 1oo2 systems under different scenarios:

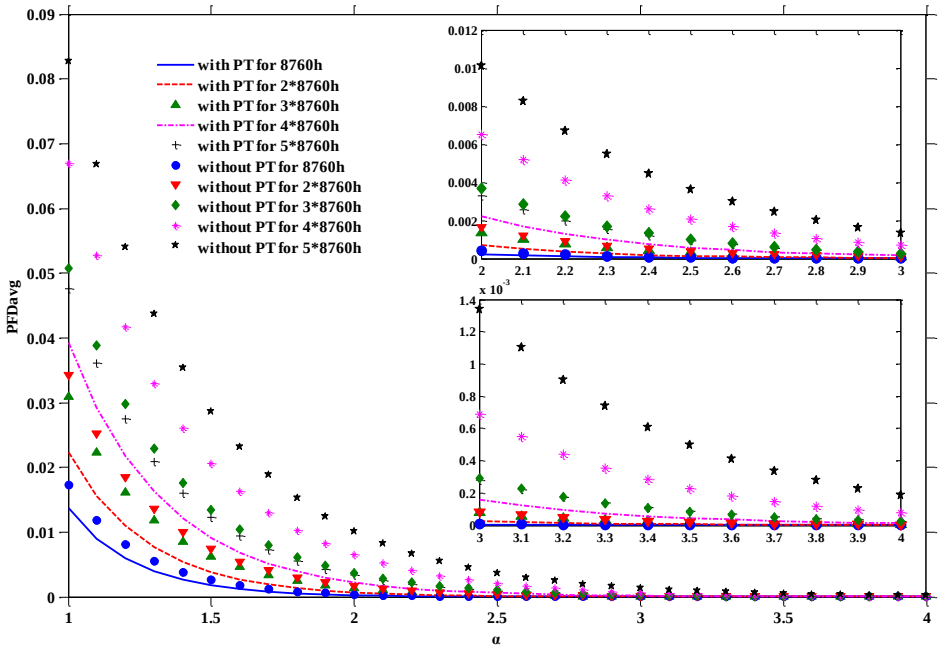
- The effects of shape parameter on PFD_{avg} will be modeled under different proof testing strategies.
- The effects of partial tests on PFD_{avg} will be modeled with different partial testing intervals.
- The effects of delayed repairs on PFD_{avg} will be modeled with different MRT.

In order to choose the optimized testing strategies considering partial testing and delayed repair, a safety instrumented function (SIF) in low-demand mode is used. A SIF is a function that has been intentionally designed to protect an equipment under control against a specific demand. IEC61508 uses safety integrity as a performance measure for a SIF and divides the requirements into four safety integrity levels (SILs)[3]. The SIL requirement is specified for the whole SIF of SISs (including sensors, logic solver, and valves). The SIL budget is therefore introduced and it defines the percentage of the requirement that can be consumed by each subsystem [5]. Considering a SIF implemented by the HIPPS that is required to fulfill $PFD_{avg} \leq$1.0E-3, this study assumes that the final element subsystem: consumes can only consume 50% of the maximum allowed PFD_{avg}, namely, $PFD_{FE,avg} \leq$ 5.0E-4. This maximum allowed $PFD_{FE,avg}$ of 5.0E-4 is assigned to the subsystem of HIPPS valves as the basis for comparisons.

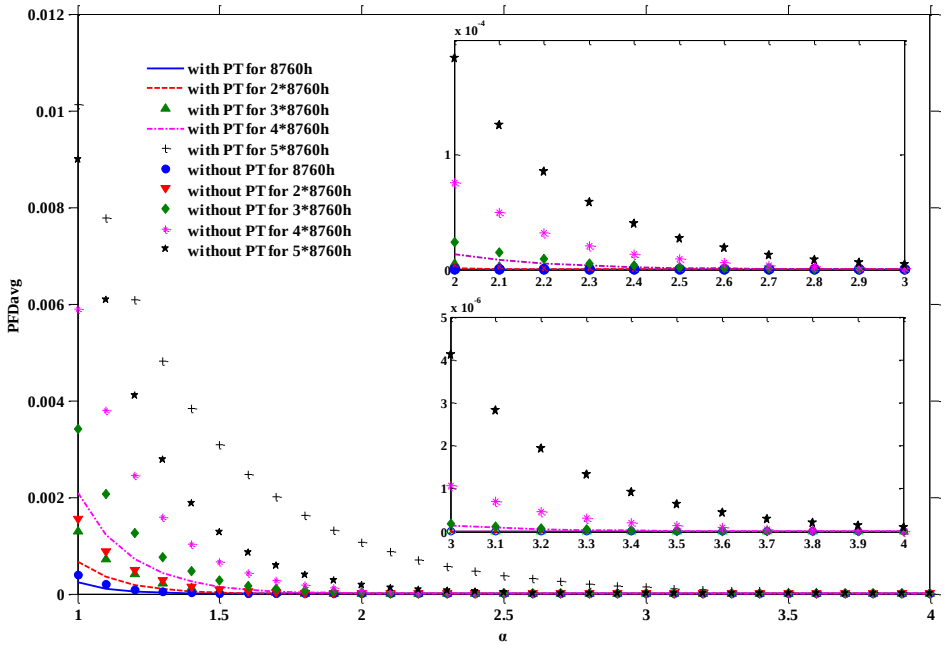
4.1 Proof testing strategy analysis

In accordance with HIPPS valves following the increasing failure rate, the shape parameter α may influence the contribution of PFD_{avg} under different proof testing strategies: FT without PT and FT with PT. In order to examine such effects on PFD_{avg}, different values are assigned to α that changes from 1 to 4, while keeping the λ_{DU} = 4.00E-06 for FT without PT and λ_{FT} = 2.00E-06, λ_{PT} = 3.464E-06 for FT with PT. Comparisons of PFD_{avg} and $Log_{10}(PFD_{avg})$ are made given different FT intervals of 8760h, 2*8760h, 3*8760h, 4*8760h and 5*8760h with PT interval of 2920h. As can be observed from Fig.3 (a) and (b), the values of PFD_{avg} for 1oo1 or 1oo2 systems increase as FT interval increases. And they under FT with PT are almost less than those without PT in the different FT intervals except for 1oo2 system with FT interval of 5*8760h in which the PT of 2920h is not suitable for improving the reliability of HIPPS valves. It is seen from Fig.3 (c) and (d) that the values of $Log_{10}(PFD_{avg})$ of such a valve, marked by the dot-dash line, are less than or equal to -3.3, meaning that the particular SIF of such a valve can meet the maximum allowed $PFD_{FE,avg}$ when α is approximately more than 1.8 for 1oo1 system and 1.0 for 1oo2 system under different testing strategies, respectively. Taking 1oo2 system for example, if α is approximately less than 2.4 in the FT interval

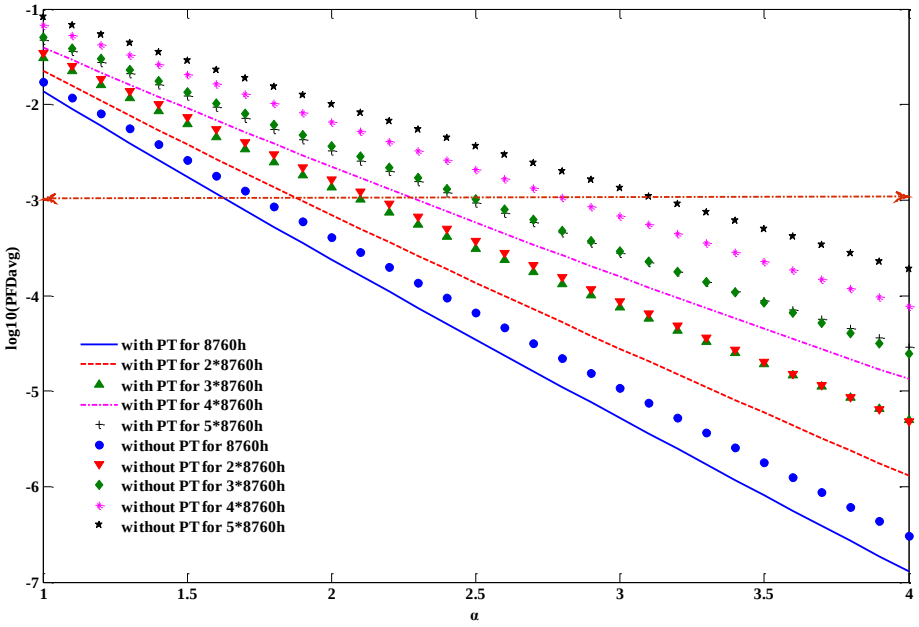
of 5*8760h considering PT, the value of $Log_{10}(PFD_{avg})$ is more than -3.3, meaning that the particular SIF of such valves cannot meet the maximum allowed $PFD_{FE,avg}$. Noting that the valves related to parameter α for meeting the maximum allowed $PFD_{FE,avg}$ can be found given different FT strategies.



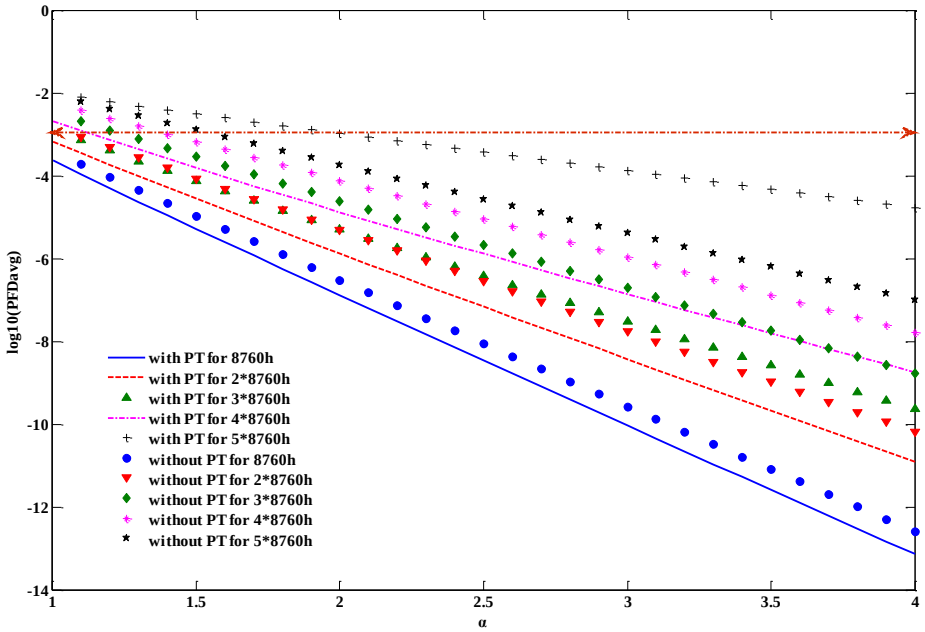
(a)



(b)



(c)



(d)

Fig. 3 Effects of parameter α on (a) PFDavg of 1oo1 system, (b) PFDavg of 1oo2 system, (c) log10(PFDavg) of 1oo1 system, and (d) log10(PFDavg) of 1oo2 system under different testing strategies with two scenarios: FT without PT and FT with PT

4.2 Contribution from partial testing strategies

In this section, numerical results for 1oo1 and 1oo2 HIPPS valves have been obtained during a full test interval of 2*8760h with the constant partial testing interval of 2190h. The input data is divided into two cases based on the assumption in Section 3.1.3. Case 1: $\alpha = 1$, $\lambda_{FT} = 2.00E\text{-}06$, $\lambda_{PT} = 2.00E\text{-}06$, and case 2: $\alpha = 2$, $\lambda_{FT} = 2.00E\text{-}06$, $\lambda_{PT} =$

3.464E-06. For FT without PT, the data is λ_{DU}= 4.00E-06. PFD_{avg} of 1oo1 and 1oo2 systems subject to a series of subsequent PT intervals is calculated by using Eqs. (15) and (16), as listed in Table 1. It can be seen that the values of PFD_{avg} have a gradual increase from one partial testing phase to another partial testing phase because of the degradation. It is worth noting that the values of PFD_{avg} for 1oo1 system with α = 1 keep the same due to the simple system without degradation. Moreover, the values of $Log_{10}(PFD_{avg})$ are more than -3.3 for 1oo1 system with case1 and case 2 under the last PT interval, meaning that the particular SIF of such a valve cannot meet the maximum allowed $PFD_{FE,avg}$. However, for 1oo2 system, those of $Log_{10}(PFD_{avg})$ are less than -3.3, meaning that if the PT interval of 2920h is determined, 1oo2 system will be as a safe choice in the early service time.

Table 1 PFD_{avg} under partial testing interval

PT interval/ h	1oo1 system				1oo2 system			
	α=1		α=2		α=1		α=2	
	PFD_{avg}	$Log_{10}(PFD_{avg})$	PFD_{avg}	$Log_{10}(PFD_{avg})$	PFD_{avg}	$Log_{10}(PFD_{avg})$	PFD_{avg}	$Log_{10}(PFD_{avg})$
[0, 2920]	2.91E-3	-2.54	3.41E-5	-4.47	1.13E-5	-4.95	2.09E-9	-8.68
[2920, 5840]	2.91E-3	-2.54	1.36E-4	-3.87	4.49E-5	-4.35	5.44E-8	-7.26
[5840, 8760]	2.91E-3	-2.54	2.39E-4	-3.62	7.80E-5	-4.11	2.74E-7	-6.56
[8760, 11680]	2.91E-3	-2.54	3.41E-4	-3.47	1.04E-4	-3.98	7.86E-7	-6.10
[11680, 14600]	2.91E-3	-2.54	4.43E-4	-3.35	1.42E-4	-3.85	1.71E-6	-5.77
[14600, 2*8760]	2.91E-3	-2.54	5.45E-4	-3.26	1.73E-4	-3.76	3.18E-6	-5.50

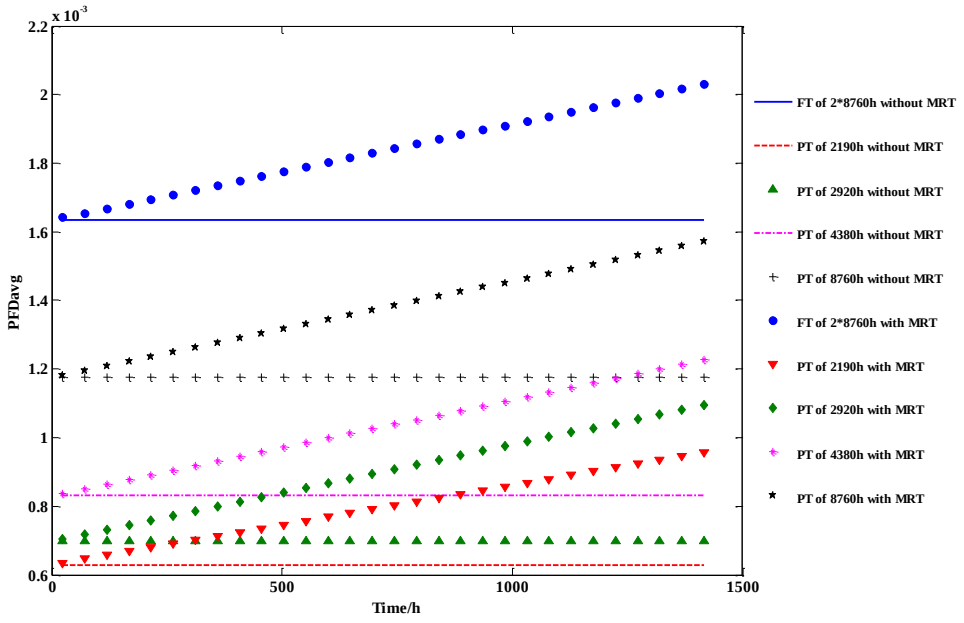
The effects in a full proof test interval of 2*8760h subject to different PT strategies have been presented in Table 2. It is seen that the values of PFD_{avg} of HIPPS valves are reduced by considering different PT strategies of 1460h, 2190h, 2920h and 4380h, compared with those without PT. Taking a partial test interval of 1490h with α = 2 for instance, they are equal to 5.58E-04 for 1oo1 system and 8.33E-07 for 1oo2 system respectively, while being less than those (1.63E-03 and 4.81E-06). By comparing different PT strategies, (e.g. 4380h and 1460h), the results are slightly increased. It should be noted that further increased PT frequency will improve the availability on demand but make the costs of testing growing. The contributions of two cases for 1oo1 system indicate that the particular SIF of such a valve the values cannot meet the maximum allowed $PFD_{FE,avg}$ under different PT strategies while those for1oo2 system can meet the maximum allowed $PFD_{FE,avg}$ except PT strategies of 4380h and FT without PT with α = 1. This contribution can also provide the basis for choosing the optimized partial testing strategies.

Table 2 Comparisons with partial testing strategies

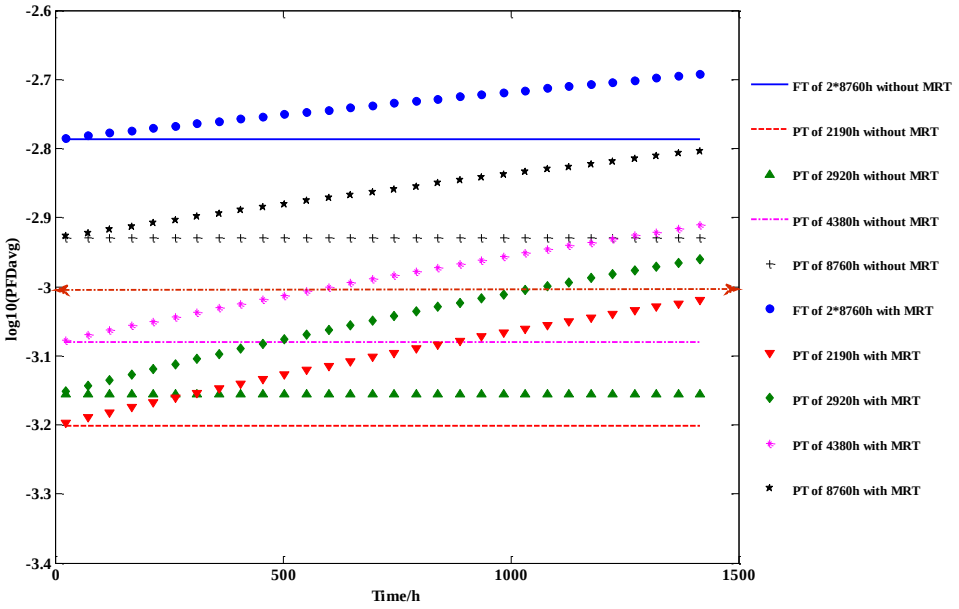
PT strategies	1oo1 system				1oo2 system			
	α=1		α=2		α=1		α=2	
	PFD_{avg}	$Log_{10}(PFD_{avg})$	PFD_{avg}	$Log_{10}(PFD_{avg})$	PFD_{avg}	$Log_{10}(PFD_{avg})$	PFD_{avg}	$Log_{10}(PFD_{avg})$
1460h	1.87E-02	-1.73	5.58E-04	-3.25	4.47E-04	-3.35	8.33E-07	-6.08
2190h	1.95E-02	-1.71	6.30E-04	-3.20	4.70E-04	-3.33	1.07E-06	-5.97
2920h	2.02E-02	-1.69	6.99E-04	-3.16	4.92E-04	-3.31	1.30E-06	-5.89
4380h	2.17E-02	-1.66	8.31E-04	-3.08	5.34E-04	-3.27	1.71E-06	-5.77
Without PT	3.42E-02	-1.47	1.63E-03	-2.79	1.55E-03	-2.81	4.81E-06	-5.32

4.3 Contribution from delayed repairs

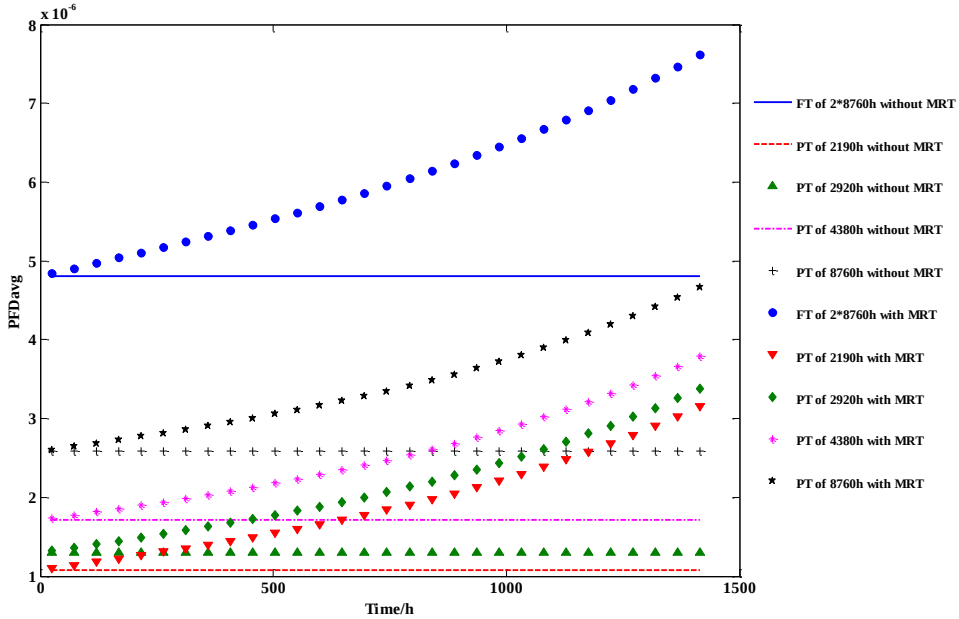
Due to the particulars of subsea applications, the repair cannot be initiated immediately even when the DU failures are detected. In order to examine effects of the non-negligible repair time, different values are assigned to MRT, MRTF, and MRTP (assuming MRTF = MRTP = MRT), while keeping the PT strategies from intervals of 2190h, 2920h, 4380h to 8760h for 1oo1 and 1oo2 HIPPS valves in this study. The other input data is $\alpha = 2$, $\lambda_{DU} = 4.00E\text{-}06$, $\tau = 2*8760h$ for FT only, and $\alpha = 2$, $\lambda_{FT} = 2.00E\text{-}06$, $\lambda_{PT} = 3.464E\text{-}06$ for FT with PT. Fig. 4 presents the PFD_{avg} from the contributions of PT and FT considering MRT or not. As shown in Fig. 4 (a) and (c), the values of PFD_{avg} with MRT are more than those without MRT, and they increase over MRT for 1oo1 system linearly and 1oo2 system non-linearly given the same PT interval, respectively. It should be noted that the effect of the repair time on PFD_{avg} becomes larger if managers don't take any decisions for the failed channel. It is also seen from Fig. 4 (b) and (d) that the values of $Log_{10}(PFD_{avg})$ of such 1oo1 system, marked by the dot-dash line, are more than -3.3, while they are always less than -3.3 for 1oo2 system for different MRT. It means the particular SIF of such a valve cannot meet the maximum allowed $PFD_{FE,avg}$, while it is always meet the maximum value for 1oo2 system given different testing strategies. Based on such unavailability analysis, the proposed formulas also provide an opportunity as an adequate tool to determine the MRT that satisfies the given conditions.



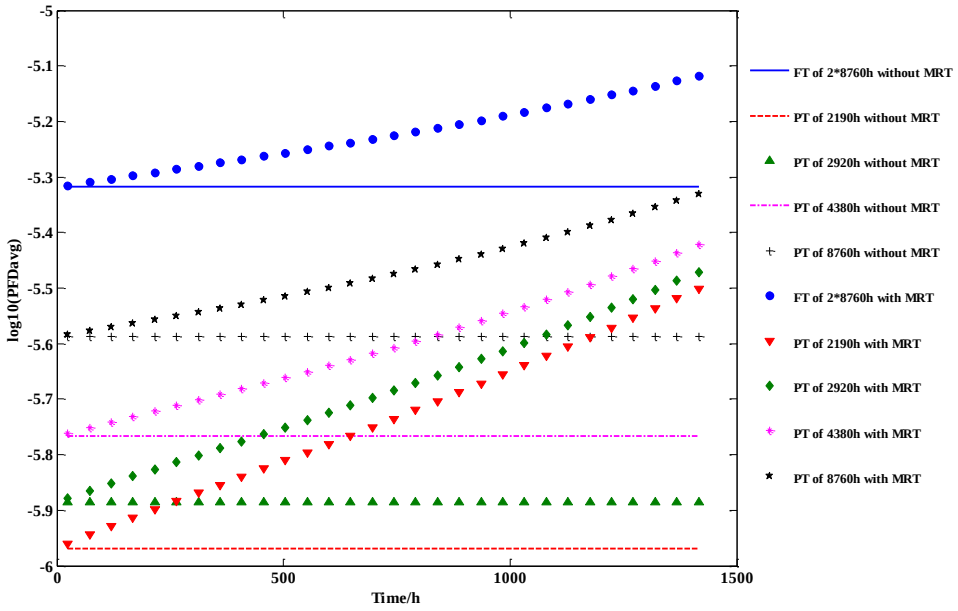
(a)


log10(PFDavg)
Time/h
FT of 2*8760h without MRT
PT of 2190h without MRT
PT of 2920h without MRT
PT of 4380h without MRT
PT of 8760h without MRT
FT of 2*8760h with MRT
PT of 2190h with MRT
PT of 2920h with MRT
PT of 4380h with MRT
PT of 8760h with MRT

(b)


x 10^-6
PFDavg
Time/h
FT of 2*8760h without MRT
PT of 2190h without MRT
PT of 2920h without MRT
PT of 4380h without MRT
PT of 8760h without MRT
FT of 2*8760h with MRT
PT of 2190h with MRT
PT of 2920h with MRT
PT of 4380h with MRT
PT of 8760h with MRT

(c)



(d)

Fig. 4 Contribution from delayed repair time under different testing strategies 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

Based on the realistic parameters from the real-world system, the proposed method provides a guide to choose the optimized testing strategies considering partial testing and delayed repair for decision-making, which also give an opportunity to guarantee safety with the acceptable costs.

5. Reliability block diagram driven Petri net modeling

In this section, the reliability block diagram (RBD) driven Petri net is adopted to check SIS unavailability and to validate the model derived from the analytic theory. Petri net approach is suggested in the IEC61508 and ISO/TR 12489 [3, 4] as a powerful way for safety/dependability modeling and calculations especially considering testing strategies of SISs [1, 11]. The stochastic Petri net with predicates and assertions [38] is applied in this study to model unavailability of the HIPPS valve system.

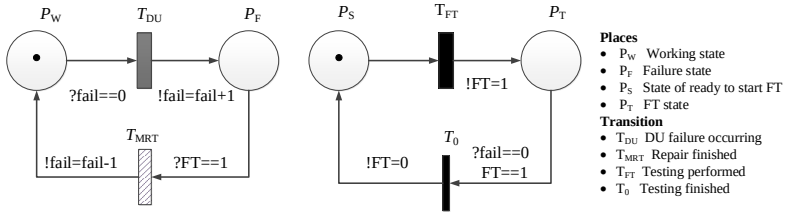
A typical Petri net consists of places, transitions, tokens and directed arcs connecting places and transitions as well as all types of mathematical variables and available logic operators [4]. Among them, places are used to model local states or conditions, while the transition is used to model local events. Tokens are dynamic elements, illustrated as black bullets and assigned to places. The distribution of tokens in the places can be used to reflect the corresponding condition or a system state. The variables represent indicators and act on the validation of transition (predicates) and can also be modified when firing transition (assertions). More details about Petri nets can be found in [4, 5, 11, 39]. The Petri net module in the GRIF software [38] is employed to model the behavior of complex dynamic systems for performance evaluation with 95% confidence intervals, and they are calculated to provide a more practical explanation as well as to better assess the failure distribution of the system [40, 41].

5.1 Petri net modeling for 1oo1 and 1oo2 systems

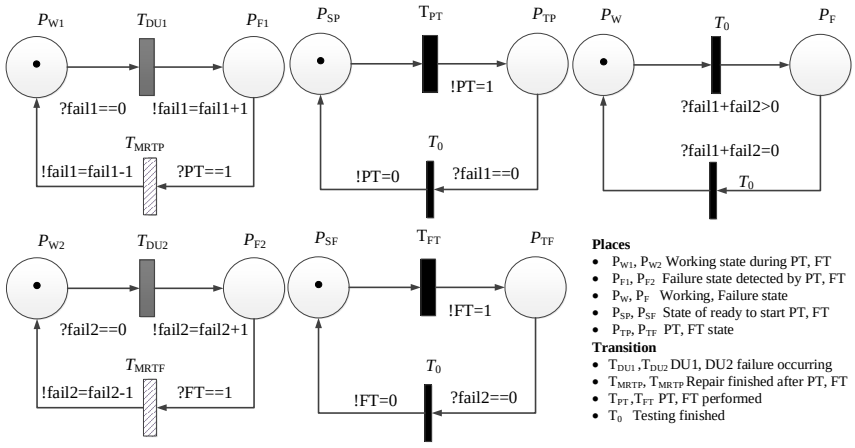
RBD driven Petri net models for 1oo1 system and 1oo2 system[29] are developed under different testing strategies considering MRT as presented in Fig. 5 and Fig. 6, respectively. In these models, what different places and transition represent are explained, respectively. In addition, a bar with gradient color refers to a transition with Weibull firing time, meaning that the failure times are Weibull distributed. A thick bar with black color and white color of slash is for the transition with constant firing time, meaning that tests and repair are performed at the constant intervals, respectively. And a thin bar with black color is used to represent an immediate transition (zero firing time), ignoring the testing time, since they are much shorter than the testing interval. 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 [2, 11, 29].

Fig. 5(a) shows the Petri net model for 1oo1 system under FT without PT. It is seen that a DU-failure will occur when the token in P_W is removed by the transition T_{DU} and deposited to P_F. Proof tests are reflected by firing T_{FT} and depositing a token from Ps to P_T. The predicate "?*fail*==0" means that a necessary firing condition of T_{DU} is the variable '*fail'* with the value of 0. And the assertion "!*fail* = *fail*+1" means that the value of the variable '*fail'* is added with 1 after the firing of T_{DU}. Similarly, the assertion "!*FT*=1" means that a proof test is performed. Transitions T_{MRT} and T_0 express the two situations in a proof test. If a DU-failure in the SIS is revealed, T_{MRT} can be fired with the predicate "?*FT*==1". The assertion "!*fail* = *fail*-1" means that a DU failure is repaired after firing T_{MRT}. While in case no DU-failure occurs, T_0 is fired with the predicate "?*fail*==0". After firing T_0, the assertion "!*FT* = *0*" represents that the test is finished.

Partial tests are modeled by introducing two types of failures with the variables of '*fail*1', '*fail*2' for 1oo1 system, as illustrated in Fig. 5 (b). the values of '*fail*1' and '*fail*2' stand for whether DU failures are detected by PT or FT respectively. In this model, the DU1-failure or DU2-failure will occur when the token in P_{W1}/ P_{W2} is removed to P_{F1}/ P_{F2}. Proof tests and partial tests are reflected by firing T_{FT} and T_{PT}, depositing two tokens to P_{TP} and P_{TF}, respectively. The same method is used to model the operation with a Petri net with predicates and assertions when partial tests are involved. In addition, the predicate "?*fail*1 + *fail*2 > 0" means that at least the system is in a complete failing state in FT or PT, and the predicate of "? *fail*1 + *fail*2 == 0" represents that the system is restored in both FT and PT.



(a)

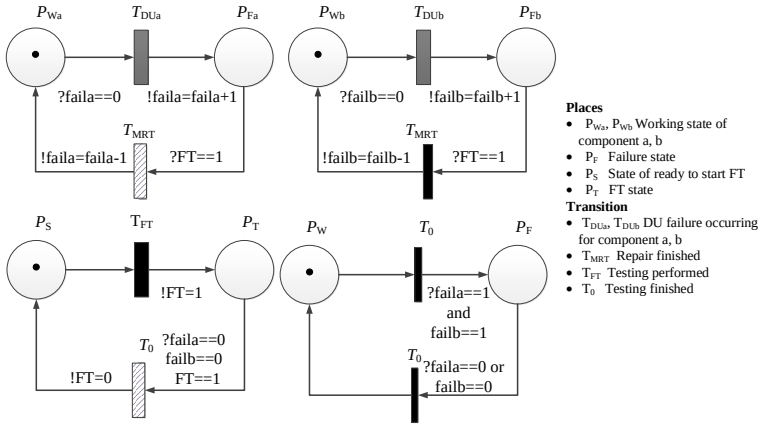


(b)

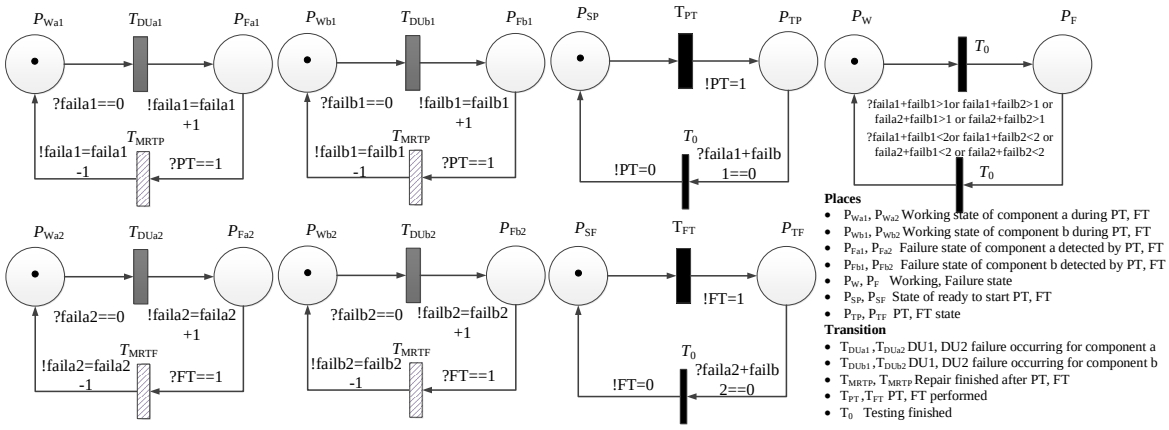
Fig. 5 Petri net models for 1oo1 system under (a) FT without PT and (b) FT with PT

The Petri net model for 1oo2 system under FT without PT can follow Fig. 6(a) while building a relationship between the component *a* and *b*. It is seen that the values of "*faila*" and "*failb*" stand for whether there are DU failures in the component *a* and *b*, respectively. The occurrence of DU-failures and proof testing process are modeled in the same way as used for 1oo1system under FT without PT. In addition, while in case no DU-failure occurs, T_0 is fired with the predicate "?*faila*==0, *failb*==0". The predicate of "?*faila* == 1 and *failb* == 1" means that the system is 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.

Partial tests for1oo2 system can also be modeled by a Petri net with predicates and assertions, as illustrated in Fig. 6(b). The DU1-failure, DU2-failure, FT, and PT are modeled in the same way as used for 1oo1system under FT with PT. In addition, while in case no DU-failure occurs during PT, T_0 is fired with the predicate "?*faila1+failb1*==0", and for FT, T_0 is fired with the predicate "?*faila2+failb2*==0". 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 number of iterations for 1oo1 system and 1oo2 system in Petri net models is set with 1.0E+7 times and 1.0E+8 times, respectively.



(a)



(b)

Fig. 6 Petri net models for 1oo2 system under (a) FT without PT and (b) FT with PT

5.2 Verification for PFD_{avg} under FT strategies

Numerical examples are illustrated under different FT strategies for Fig. 5 and Fig. 6, based on the following data which is $\alpha = 2$, $\tau_{PT} = 2920$ h, and MRT = 0, while other parameters are following those used in Section 4.1. PFD_{avg} results are obtained both from the proposed formulas based on Eqs. (8) and (15) and the Petri-net simulation for 1oo1 system, as listed in Table 3 where the 95% confidence intervals of a probability sample are calculated. Results for 1oo2 system are also obtained in the same way, as listed in Table 4. Take 1oo1 system with the FT interval of 2*8760h for instance, PFD_{avg} under FT without PT, lies in the 95% confidence interval from 1.62E-4 to 1.66E-4, with the best estimate being 1.64E-4 that is nearly close to the values of 1.63E-4 obtained with formulas. Approximation formulas developed for FT are therefore verified by the closeness of the results from the Petri net simulation. Noting that when FT interval of 5*8760h is modeled for 1oo2 system considering PT, there is a big difference between them. It may be partly explained that such simulation models ignore the effects that the failure doesn't occur in the previous testing period, and such effects on 1oo2 system are larger than those on 1oo1system.

Table 3 Comparisons of proposed formulas and Petri-net models under FT with PT for1oo1 system

FT strategies	Without PT				With PT			
	PFD_{avg} from Eq.(8)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval	PFD_{avg} from Eq.(15)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval
8760h	4.09E-4	4.12E-4	1.43E-2	[4.03E-4, 4.21E-4]	2.39E-4	2.40E-4	8.99E-3	[2.34E-4,2.46E-4]
2*8760h	1.63E-3	1.64E-3	2.86E-2	[1.62E-3, 1.66E-3]	6.99E-4	7.03E-4	1.54E-2	[6.93E-4, 7.13E-4]
3*8760h	3.67E-3	3.68E-3	4.28E-2	[3.65E-3, 3.71E-3]	1.36E-3	1.37E-3	2.23E-2	[1.36E-3, 1.38E-3]
4*8760h	6.51E-3	6.53E-3	5.68E-2	[6.49E-3, 6.57E-3]	2.23E-3	2.24E-3	2.92E-2	[2.22E-3, 2.36E-3]
5*8760h	1.01E-2	1.02E-2	7.07E-2	[1.02E-2, 1.02E-2]	3.30E-3	3.27E-3	2.60E-2	[3.25E-3, 3.29E-3]

Table 4 Comparisons of proposed formulas and Petri-net models under FT with PT for1oo2 system

FT strategies	Without PT				With PT			
	PFD_{avg} from Eq.(9)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval	PFD_{avg} from Eq.(16)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval
8760h	3.01E-7	2.60E-7	3.00E-4	[2.01E-7, 3.19E-7]	1.29E-7	1.23E-7	1.67E-4	[9.03E-8, 1.56E-7]
2*8760h	4.81E-6	4.83E-6	1.27E-3	[4.58E-6, 5.08E-6]	1.30E-6	8.84E-7	4.03E-4	[8.05E-7, 9.63E-7]
3*8760h	2.42E-5	2.44E-5	2.86E-3	[2.38E-5, 2.50E-5]	5.03E-6	3.19E-6	7.93E-4	[3.03E-6, 3.35E-6]
4*8760h	7.61E-5	7.62E-5	5.05E-3	[7.52E-5, 7.72E-5]	1.32E-5	8.49E-6	1.35E-3	[8.23E-6, 8.75E-6]
5*8760h	1.84E-4	1.84E-4	7.84E-3	[1.82E-4, 1.86E-4]	1.07E-3	1.84E-5	2.03E-3	[1.80E-5 1.88E-5]

5.3 Verification for PFD_{avg} under PT strategies

In order to validate the PFD_{avg} formulas under partial testing strategies, Petri net models for 1oo1 system and 1oo2 system are shown as in Fig. 5 (b) and Fig. 6 (b). The input data is the same as used in Section 4.2. The different PT strategies for both 1oo1 and 1oo2 systems are given a proof test interval of 2*8760h with MRT = 0 as listed in Tables 5 and 6. PFD_{avg} results are obtained both from the proposed formulas based on Eqs. (15) and (16) and the Petri-net simulation, as listed in Tables 3 and 4. Take 1oo1 system with the PT interval of 4380h for instance, PFD_{avg} with $\alpha = 1$, lies in the 95% confidence interval from 2.15E-2 to 2.17E-2, with the best estimate being 2.16E-2 that is nearly close to the value of 2.17E-2 obtained with the formulas. Approximation formulas developed for 1oo1 system are verified by the closeness of the results from the Petri net simulation. The results obtained by the former are seen to be somewhat higher than the results obtained by using the latter for 1oo2 system, but still acceptable for most practical purposes.

Table 5 Comparisons of proposed formulas and Petri-net model under partial testing with α for 1oo1 system

PT strategies	α = 1				α = 2			
	PFD_{avg} from Eq.(15)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval	PFD_{avg} from Eq.(15)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval
1460h	1.87E-2	1.88E-2	1.07E-1	[1.87E-2, 1.89E-2]	5.58E-4	5.62E-4	1.46E-2	[5.53E-4,5.71E-4]
2190h	1.95E-2	1.95E-2	1.07E-1	[1.94E-2, 1.96E-2]	6.30E-4	6.32E-4	1.49E-2	[6.23E-4, 6.41E-4]
2920h	2.02E-2	2.02E-2	1.07E-1	[2.01E-2, 2.03E-2]	6.99E-4	7.03E-4	1.54E-2	[6.93E-4, 7.13E-4]
4380h	2.17E-2	2.16E-2	1.09E-1	[2.15E-2, 2.17E-2]	8.31E-4	8.36E-4	1.65E-2	[8.35E-4, 8.37E-4]
Without PT	3.42E-2	3.42E-2	1.48E-1	[3.41E-2, 3.43E-2]	1.63E-3	1.64E-3	2.86E-2	[1.62E-3, 1.66E-3]

Table 6 Comparisons of proposed formulas and Petri-net model under partial testing with α for 1oo2 system

PT strategies	α = 1				α = 2			
	PFD_{avg} from Eq.(16)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval	PFD_{avg} from Eq.(15)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval
1460h	4.47E-4	4.23E-4	1.41E-2	[4.20E-4, 4.26E-4]	8.33E-7	5.72E-7	3.48E-4	[5.04E-7, 6.40E-7]

2190h	4.70E-4	4.37E-4	1.42E-2	[4.34E-4, 4.40E-4]	1.07E-6	6.94E-7	3.66E-4	[6.22E-7, 7.66E-7]
2920h	4.92E-4	4.51E-4	1.43E-2	[4.48E-4, 4.54E-4]	1.30E-6	8.84E-7	4.03E-4	[8.05E-7, 9.63E-7]
4380h	5.34E-4	4.81E-4	1.46E-2	[4.78E-4, 4.84E-4]	1.71E-6	1.23E-6	4.79E-4	[1.14E-6, 1.32E-6]
Without PT	1.55E-3	1.55E-3	2.80E-2	[1.54E-3, 1.56E-3]	4.81E-6	4.83E-6	1.27E-3	[4.58E-6, 5.08E-6]

5.4 Verification for PFD_{avg} under delayed repairs

MRT is introduced in these Petri-net models and the effects of delayed repairs on the unavailability are analyzed for subsea HIPPS valves. Such models for 1oo1 system and 1oo2 system with delayed repair can follow Fig. 5 and Fig. 6 with the value of MRT=MRTF=MRTP=168 when a DU-failure is revealed by a proof test or a partial test, meaning that the bar of T_{MRT} will be fired when a value is assigned. The input data for FT and PT is following that used in section 4.3. We can conduct PFD_{avg} calculation for different partial testing strategies during a full proof test (τ =2* 8760h), as listed in Tables 7 and 8. Take 1oo1 system with the PT interval of 4380h for instance, PFD_{avg} with MRT, lies in the 95% confidence interval from 8.65E-4 to 8.85E-4, with the best estimate being 8.75E-4 that is nearly close to the value of 8.78E-4 obtained with the formulas. It can be also seen that the two methods give the rather close results under different scenarios.

Table 7 Comparisons of proposed formulas and Petri-net model under testing strategy with MRT for 1oo1 system

Testing strategies	Without MRT				With MRT			
	PFD_{avg} from Eqs. (8) and (15)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval	PFD_{avg} from Eqs. (8) and (15)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval
FT of 2*8760h	1.63E-3	1.64E-3	2.86E-2	[1.62E-3, 1.66E-3]	1.68E-3	1.67E-3	2.89E-2	[1.65E-3,1.69E-3]
PT of 2190h	6.30E-4	6.32E-4	1.49E-2	[6.23E-4, 6.41E-4]	6.68E-4	6.73E-4	1.52E-2	[6.64E-4, 6.82E-4]
PT of 2920h	6.99E-4	7.03E-4	1.54E-2	[6.93E-4, 7.13E-4]	7.46E-4	7.43E-4	1.57E-2	[7.33E-4, 7.53E-4]
PT of 4380h	8.31E-4	8.36E-4	1.65E-2	[8.26E-3, 8.46E-3]	8.78E-4	8.75E-4	1.68E-2	[8.65E-4, 8.85E-4]
PT of 8760h	1.18E-3	1.18E-3	2.08E-2	[1.17E-3, 1.19E-3]	1.22E-3	1.21E-3	2.12E-2	[1.20E-3, 1.22E-3]

Table 8 Comparisons of proposed formulas and Petri-net model under testing strategy with MRT for 1oo2 system

Testing strategies	Without MRT				With MRT			
	PFD_{avg} from Eqs. (9) and (16)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval	PFD_{avg} from Eqs. (9) and (16)	PFD_{avge} from Petri net	σ (PFD_{avge})	95% confidence interval
FT of 2*8760h	4.81E-6	4.83E-6	1.27E-3	[4.58E-6, 5.08E-6]	5.04E-6	4.98E-6	1.28E-3	[4.73E-6, 5.23E-6]
PT of 2190h	1.07E-6	6.94E-7	3.66E-4	[6.22E-7, 7.66E-7]	1.22E-6	7.71E-7	3.78E-4	[6.97E-7, 8.45E-7]
PT of 2920h	1.30E-6	8.84E-7	4.03E-4	[8.05E-7, 9.63E-7]	1.45E-6	9.70E-7	4.17E-4	[8.88E-7, 1.05E-6]
PT of 4380h	1.71E-6	1.23E-6	4.79E-4	[1.14E-6, 1.32E-6]	1.86E-6	1.32E-6	4.94E-4	[1.22E-6, 1.42E-6]
PT of 8760h	2.58E-6	2.65E-6	8.14E-4	[2.49E-6, 2.81E-6]	2.73E-6	2.77E-6	8.29E-4	[2.61E-6, 2.93E-6]

6. Concluding remarks

A methodology for reliability modeling of SISs final elements has been presented in this study. The main benefit of the proposed approach can focus on different operational issues, such as partial tests and delayed repairs. Approximation formulas for PFD_{avg} have been developed by introducing conditional probability in subsequent partial testing intervals, and Weibull rules are adopted for modeling the degradation effects. Delayed restoration is considered and different scenarios for calculation of mean repair time have been developed to demonstrate effects on the reliability.

In the case study, a focus is given to 1oo1 and 1oo2 HIPPS valves. The most difficult challenge concerning the approximations is to handle the degradation effects in a series of subsequent partial testing intervals. Investigations of shape parameters have indicated that maintenance strategies can be made to predicate the PFD_{avg} given different proof testing periods including partial testing or not, which also provide a method for determining the suitable types of valves under limitations of testing. The contributions of PFD_{avg} from partial tests have been demonstrated in improving the performance of valves in different cases. The experiments have shown that PFD_{avg} is increasing under subsequent partial testing intervals, but it is reduced compared that without PT. Decision should be made based on the maximum allowed $PFD_{FE,avg}$, so as to choose appropriate partial testing strategies with given conditions. The effects on the reliability from delayed restoration have shown that the values of PFD_{avg} are increased over MRT but they can also provide an adequate tool to determine the MRT under given requirements and different partial testing strategies.

The current paper is restricted to SISs with simple configurations. For SISs with reasonably independent components, an extension of the current work is to establish a formula for the unavailability of a single component and combine such unavailability through Fault trees. Petri nets and Monte Carlo simulation can be also used for SISs with dependent components. The common cause failures and process demand could be taken into account. In addition, the other operational and testing issues (staggered testing) in the subsea environment need to be addressed in the further study.

Acknowledgment

This research is supported by the research project from China University of Petroleum (Beijing). The authors will be grateful for the reviewers' and editor's helpful comments.

References

[1] Liu Y, Rausand M. Reliability effects of test strategies on safety-instrumented systems in different demand modes. Reliability Engineering & System Safety. 2013;119:235-43.

[2] Liu Y, Rausand M. Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems. Reliability Engineering & System Safety. 2016;145:366-72.

[3] IEC61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission; 2010.

[4] ISO. ISO/TR12489: Petroleum, petrochemical and natural gas industries— Reliability modelling and calculation of safety systems. BSI Standards Publication; 2016.

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

[6] Longhi AEB, Pessoa AA, Garcia PAdA. Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. Reliability Engineering & System Safety. 2015;142:525-38.

[7] Cai B, Xie M, Liu Y, Liu Y, Feng Q. Availability-based engineering resilience metric and its corresponding evaluation

methodology. Reliability Engineering & System Safety. 2018;172:216-24.
[8] Cai B, Kong X, Liu Y, Lin J, Yuan X, Xu H, et al. Application of Bayesian Networks in Reliability Evaluation. IEEE Transactions on Industrial Informatics. 2018:1-12.
[9] Cai B, Huang L, Xie M. Bayesian Networks in Fault Diagnosis. IEEE Transactions on Industrial Informatics. 2017.
[10] Wu S, Zhang L, Barros A, Zheng W, Liu Y. Performance analysis for subsea blind shear ram preventers subject to testing strategies. Reliability Engineering & System Safety. 2018;169:281-98.
[11] Signoret J-P, Dutuit Y, Cacheux P-J, Folleau C, Collas S, Thomas P. Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering & System Safety. 2013;113:61-75.
[12] Meng H, Kloul L, Rauzy A. Modeling patterns for reliability assessment of safety instrumented systems. Reliability Engineering & System Safety. 2018;180:111-23.
[13] Torres-Echeverría AC, Martorell S, Thompson HA. Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing. Reliability Engineering & System Safety. 2011;96:545-63.
[14] Jahanian H. Generalizing PFD formulas of IEC 61508 for KooN configurations. ISA Transactions. 2015;55:168-74.
[15] Jin H, Rausand M. Reliability of safety-instrumented systems subject to partial testing and common-cause failures. Reliability Engineering & System Safety. 2014;121:146-51.
[16] Hauge S, Hokstad P, Håbrekke S, Lundteigen MA. Common cause failures in safety-instrumented systems: Using field experience from the petroleum industry. Reliability Engineering & System Safety. 2016;151:34-45.
[17] Alizadeh S, Sriramula S. Impact of common cause failure on reliability performance of redundant safety related systems subject to process demand. Reliability Engineering & System Safety. 2018;172:129-50.
[18] Alizadeh S, Sriramula S. Unavailability assessment of redundant safety instrumented systems subject to process demand. Reliability Engineering & System Safety. 2018;171:18-33.
[19] Alizadeh S, Sriramula S. Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand. ISA Transactions. 2017;71:599-614.
[20] Jigar AA, Liu Y, Lundteigen MA. Spurious activation analysis of safety-instrumented systems. Reliability Engineering & System Safety. 2016;156:15-23.
[21] Lundteigen MA, Rausand M. Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. Reliability Engineering & System Safety. 2008;93:1208-17.
[22] Rahimi M, Rausand M. Monitoring human and organizational factors influencing common-cause failures of safety-instrumented system during the operational phase. Reliability Engineering & System Safety. 2013;120:10-7.
[23] Innal F, Chebila M, Dutuit Y. Uncertainty handling in safety instrumented systems according to IEC 61508 and new proposal based on coupling Monte Carlo analysis and fuzzy sets. Journal of Loss Prevention in the Process Industries. 2016;44:503-14.
[24] Wu X, Hillston J. Mission reliability of semi-Markov systems under generalized operational time requirements. Reliability Engineering & System Safety. 2015;140:122-9.
[25] Petroni F, Prattico F. Reliability measures for indexed semi-Markov chains applied to wind energy production. Reliability Engineering & System Safety. 2015;144:170-7.
[26] Guo H, Yang X. Automatic creation of Markov models for reliability assessment of safety instrumented systems. Reliability Engineering & System Safety. 2008;93:829-37.
[27] Jigar AA. Quantification of reliability performance: Analysis methods for safety instrumented system. 2013.
[28] Rogova E, Lodewijks G, Lundteigen MA. Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates. Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability. 2017;231.
[29] Wu S, Zhang L, Lundteigen MA, Liu Y, Zheng W. Reliability assessment for final elements of SISs with time dependent failures. Journal of Loss Prevention in the Process Industries. 2018;51:186-99.
[30] Lundteigen MA, Rausand M. Partial stroke testing of process shutdown valves: How to determine the test coverage.

Journal of Loss Prevention in the Process Industries. 2008;21:579-88.
[31] Summers A, Zachary B. Variable function voting solenoid-operated valve apparatus and testing method therefor. Google Patents; 2004.
[32] 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. Reliability Engineering & System Safety. 2016;150:160-70.
[33] Torres-Echeverría A, Martorell S, Thompson H. Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm. Reliability Engineering & System Safety. 2012;106:45-60.
[34] Pascual R, Louit D, Jardine AK. Optimal inspection intervals for safety systems with partial inspections. Journal of the Operational Research Society. 2011;62:2051-62.
[35] Bond K. IEC 61511-Functional Safety: Safety Instrumented Systems for the Process Industry Sector. ANNUAL SYMPOSIUM ON INSTRUMENTATION FOR THE PROCESS INDUSTRIES: INSTRUMENT SOCIETY OF AMERICA; 2002. p. 33-40.
[36] IEC61511. Functional safety—Safety instrumented systems for the process industry sector. International Electrotechnical Commission Std. 2003.
[37] Lundteigen MA, Rausand M. The effect of partial stroke testing on the reliability of safety valves. T Aven, J Vinnem (Eds), Risk, reliability and societal safety, Taylor & Francis 2007.
[38] GRIF. Version 2017, http://grif-workshop.com. 2017.
[39] IEC62551. Analysis techniques for dependability Petri net techniques2013.
[40] Grabaskas D, Nakayama MK, Denning R, Aldemir T. Advantages of variance reduction techniques in establishing confidence intervals for quantiles. Reliability Engineering & System Safety. 2016;149:187-203.
[41] Alban A, Darji HA, Imamura A, Nakayama MK. Efficient Monte Carlo methods for estimating failure probabilities. Reliability Engineering & System Safety. 2017;165:376-94.