Inference algorithms for the useful life of safety instrumented systems under small failure sample data

Mao, Qi; Wang, Haiqing; Yang, Ming; Hu, Jason

DOI
10.1016/j.psep.2022.12.024

Publication date
2023

Document Version
Final published version

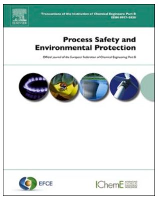
Published in
Process Safety and Environmental Protection

Process Safety and Environmental Protection 170 (2023) 783–790

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.journals.elsevier.com/process-safety-and-environmental-protection



Inference algorithms for the useful life of safety instrumented systems under small failure sample data

Qi Mao [a], Haiqing Wang [a,*], Ming Yang [b], Jason Hu [c]

[a] *China University of Petroleum (East China) Electromechanic Engineering College, Qingdao, China*
[b] *Safety and Security Science Section, Department of Values, Technology, and Innovation, Faculty of Technology, Policy, and Management, Delft University of Technology, the Netherlands*
[c] *Covestro Polymers (China) Co., Ltd, Shanghai Chemical Industry Park, China*

ARTICLE INFO

Keywords:
Safety instrumented systems
Useful life
Reliability
Small samples
Failure rate

ABSTRACT

Safety instrumented systems(SIS) have been widely used in petroleum and chemical plants to detect and respond to dangerous events and prevent them from developing into accidents. The in-service time of SIS does not exceed its useful life is one of the crucial assumptions of IEC functional safety standards. The testing method recommended in the IEC standard is essentially a chi-square testing, where the testing effect is proportional to the sample size and, therefore, not suitable for testing the type of data distribution under small samples. In this paper, a rapid inference method of useful life (RIUL) is proposed to: i) determine whether the distribution type of failure data is exponential under small samples with the help of Anderson-Darling testing, and ii) use the Bayesian sequential testing method for estimating the useful life. The sequential posterior odds ratio testing is introduced to test the equipment failure rate one by one. The proposed RIUL approach is applied to the liquid-level protection circuit of the hot high-pressure separator. The engineering simulation results show that compared with IEC standard methods, the proposed method can be performed with fewer failure data, providing a theoretical basis for reasonable maintenance and replacement of equipment.

1. Introduction

In the chemical industry, Safety instrumented systems (SIS) maintain chemical plants in a safe condition by detecting hazardous events and performing the required safety actions, in the event of a failure of such equipment, the dynamic risk level of the plant will be affected (Zhang et al., 2019; Mkhida et al., 2014). The SIS consists of three parts: sensor, logic controller and final component (Śliwiński, 2018). Safety integrity level (SIL) is one of the key indicators to measure the safety function of SIS (Chebila, 2018; Jahanian, 2017), it is determined by calculating the average probability of failure on demand (PFD_{avg}) (Wang et al., 2004; Chang et al., 2011). In the calculation of PFD_{avg} in IEC standard (IEC61508, 2016; Timms, 2009), it is considered that the failure rate of SIS is constant, that is, the in-service time of the SIS is in the range of useful life. Suppose the in-service time of SIS exceeds its useful life, the failure rate will increase rapidly, resulting in meaningless PFD_{avg} calculation results (IEC61508, 2016).

On the other hand, the field failure data of SIS are small (Brissaud et al., 2017), The IEC standard requires a large amount of failure data to conclude that equipment's in-service time has exceeded its useful life, which is contrary to its high reliability (Meng et al., 2018).

To ensure the safe operation of SIS in the proof test cycle, Xie et al. (2019) demonstrated how data-driven methods identify significant influencing factors for SIS failure. It was helpful to obtain a more accurate equipment failure rate. Chebila (2020) provided a binomial failure rate model for evaluating the performance of safety instrumented systems. The calculated PFDavg was more accurate because the effect of common cause failure is taken into account. Jahanian and Mahboob (2016) introduced a risk-based optimization approach to the SIL determination process to reduce the risk to as low as practically possible. de Lira-Flores et al. (2019) proposed an MINLP approach for solving the plant layout problem by optimizing the design of safety instrumented systems. This method based on the constant failure rate, the loss caused by SIS spurious trip and failure action was calculated. Sravanthi et al. (2017) proposed an inherently fail-safe electronic logic circuit with very low unsafe failure probability to achieve equivalent or lesser unsafe failure probability.

However, the premise of the above research results is that the in-

[*] Correspondence to: China University of Petroleum (East China), China.
E-mail address: wanghaiqing@upc.edu.cn (H. Wang).

https://doi.org/10.1016/j.psep.2022.12.024
Received 5 October 2022; Received in revised form 5 December 2022; Accepted 8 December 2022
Available online 15 December 2022

service time of SIS does not exceed its useful life. Therefore, their conclusions do not apply to the full life cycle of SIS, only to the part where the failure rate is constant. Thus, the research results in this paper have essential engineering value for the reliability assessment of SIS.

At present, there are few research results on the useful life of safety instrumented systems. ISA TR84.00.03 (2019) defines useful life as the portion where the random failure rate can be considered constant. IEC61508.2. (2016) indicates that useful life often lies within a range of 8–12 years. Stephen (2015) summarizes the range of SIS equipment useful life and proposes a series of management measures. Shao et al. (2022) proposed a multi-stage BNs model to predict the remaining useful life of the equipment. This method is only applicable to the late stage of equipment operation. Unfortunately, many SIL certificates in circulation today do not estimate the useful life, so it is essential to carry out this work.

How to quickly judge whether the in-service time of SIS exceeds its useful life in the case of a small failure sample data needs to solve two main problems: First, in the case of small samples and unknown distribution parameters, determine whether the distribution type of equipment failure data is exponential distribution; Second, the need to quickly determine whether the reliability index (failure rate) meets the Bayesian sequential testing requirements.

Based on SIS equipment failure data, we propose a method of rapid inference of useful life (RIUL) for SIS equipment, the RIUL proposed in this paper can use as few failure data as possible to judge whether the in-service time of SIS exceeds its useful life. RIUL overcomes the disadvantage of poor timeliness of IEC testing method. Estimating useful life helps the plant to maintain or replace equipment in time.

To our best knowledge, this is the first attempt to investigate and inference the useful life of safety instrumented systems. The rest of the paper is organized as follows: The traditional useful life hypothesis testing method is introduced in Section 2. Then the RIUL inference method is proposed in Section 3. The two methods are applied to the level interlock protection circuit of the hot high-pressure separator respectively and the differences of the calculated results are compared and analyzed in Section 4. Finally, some conclusions are drawn, and further works are presented in Section 5.

2. Traditional useful life hypothesis testing

The IEC testing method assumes that during the useful life period, the equipment failure rate is constant, as shown in Fig. 1 (Catelani et al., 2018).

IEC standard points out that the constant failure rate hypothesis testing is equivalent to the testing of the exponential distribution, and the null hypothesis H is set as:

$$H: F(t) = 1 - e^{-\lambda t} \tag{1}$$

where λ is the equipment failure rate. To test hypothesis H, the total operating time of the equipment T_0 need to be collected, which can be expressed as (IEC60605.6, 2007):

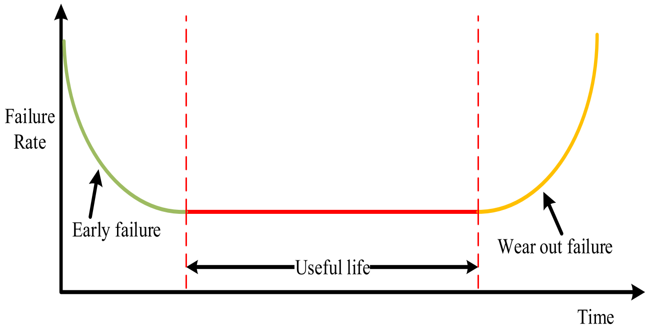


Fig. 1. The range of useful life.

$$T_0 = \sum_{i=1}^{r} t_i + (n - r + 1)t_r \tag{2}$$

where r is the number of equipment failures; t_i $(i = 1,2,3,\ldots,r)$is the equipment failure time; n is the total number of equipment.

$$T_k = \sum_{i=1}^{k} t_i + (n - r)t_k \tag{3}$$

where $T_k(k = 1,2,3,\ldots r)$ is the cumulative time when equipment failure occurs, statistical test value χ^2 is:

$$\chi^2 = 2\sum_{i=1}^{r-1} \ln \frac{T_0}{T_k} \tag{4}$$

When H is true, using the memoryless nature of exponential distribution, it can be shown that χ^2 obeys χ^2 distribution with degree of freedom 2d. For a given significance level σ , the rejection domain W of the hypothesis testing is:

$$W = \left\{\chi^2 \le \chi^2_{\sigma/2}\left(2d\right) or \chi^2 \ge \chi^2_{1-\sigma/2}\left(2d\right)\right\} \tag{5}$$

The accuracy of the χ^2 testing is positively correlated with the number of failure data, and the testing effect is generally more ideal when $r > 200$.

3. Rapid inference method of useful life

3.1. Determining the type of distribution of failure data

In the traditional hypothesis testing methods of data distribution type, χ^2 and KS testing are commonly used. The test result of χ^2 testing is ideal when the sample number is large. The effect of KS testing needs to be improved when the sample data distribution parameters are unknown. Due to the lack of field failure data of SIS equipment and the distribution parameters of the failure data recorded in the field are unknown, the χ^2 and KS testing are not suitable. Anderson-darling testing can judge the distribution type of equipment failure data in the case of small samples (Zhang, 2021). Its testing performance is better than KS testing under the same testing conditions. When we use the recorded failure data for parameter estimation, related studies show that the testing effect of this method is weakly correlated with the accuracy of parameter estimation (D'Agostino, 1986). In this paper, we propose a method that determines whether the distribution type of small sample failure data is exponential distribution.

Step 1: Assume that the distribution type of SIS equipment failure data are exponential distribution. To simplify the calculation process, using maximum likelihood estimation or moment estimation to obtain the failure rate λ (Toroody et al., 2020).

Step 2: Calculate the discrete distance A_n^2, Compare it with the critical value(CV). A_n^2 can be used to measure whether the failure data belong to the exponential distribution cluster, and its expression can be expressed as (Heo et al., 2013):

$$A_n^2 = r\int_{-\infty}^{+\infty} \frac{\{F_r(t) - F(t)\}^2}{F(t)(1 - F(t))} dF(t) \tag{6}$$

where $F(t)$ is the distribution function of failure data; $F_r(t)$ is the empirical probability density function of failure data. In practical engineering, A_n^2 can be expressed as:

$$A_n^2 = -r - \sum_{i=1}^{r}\left[\left(\frac{2i-1}{r}\right)\{\ln F_r(t_i) + \ln(1 - F_r(t_{r+1-i}))\}\right] \tag{7}$$

where $F_r(t_i)$ is the probability integral transformation function, and the process of determining the critical value is shown in Fig. 2.

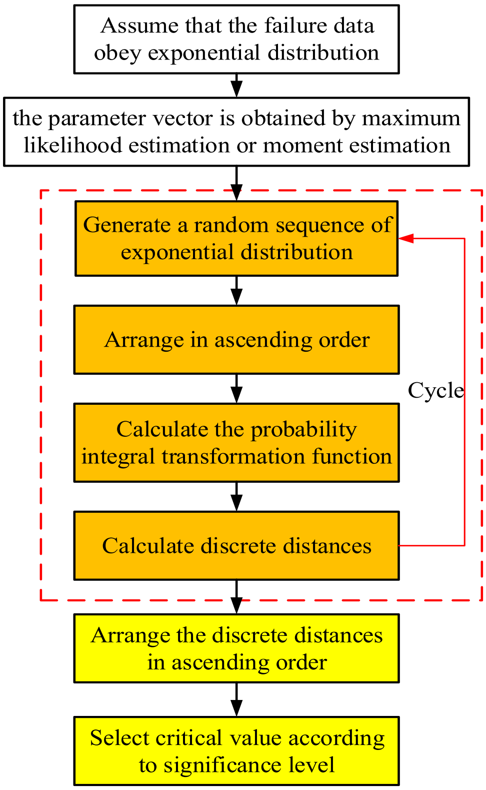

Assume that the failure data obey exponential distribution
the parameter vector is obtained by maximum likelihood estimation or moment estimation
Generate a random sequence of exponential distribution
Arrange in ascending order
Calculate the probability integral transformation function
Calculate discrete distances
Cycle
Arrange the discrete distances in ascending order
Select critical value according to significance level

Fig. 2. Critical value determination process.

After 10,000 cycles, the regression equation for the critical value can be expressed as:

$$\begin{cases} CV = 0.6278 - \dfrac{0.0175}{\sqrt{n}} - \dfrac{0.1138}{n} - \dfrac{0.5672}{n^2} & \sigma = 0.01 \\ CV = 0.7441 - \dfrac{0.0011}{\sqrt{n}} - \dfrac{0.0493}{n} - \dfrac{0.3652}{n^2} & \sigma = 0.02 \\ CV = 0.8648 - \dfrac{0.0478}{\sqrt{n}} - \dfrac{0.2719}{n} - \dfrac{1.2466}{n^2} & \sigma = 0.05 \end{cases} \tag{8}$$

If A_n^2 is greater than CV, it indicates that the in-service time of the SIS has exceeded its useful life. Chemical plant needs to take a series of maintenance measures for the SIS.

3.2. Bayesian sequential testing for failure rate

The failure rate of SIS may increase gradually in the equipment wear-out phase due to fatigue or wear and tear. To guarantee its high-reliability requirement, the upper limit of its failure rate needs to be limited. If A_n^2 is less than CV in step 2, continue to record equipment failure time t_i ($i = 1,2,3,\ldots m$). To determine whether equipment failure rate is greater than upper limit, giving the following hypothetical scheme.

Define the null and alternative hypotheses as follows: null hypothesis H_0: $\lambda_\mathrm{n} \leq \lambda_\mathrm{m}$; alternative hypothesis H_1: $\lambda_\mathrm{n} > \lambda_\mathrm{m}$. where λ_n is the equipment failure rate, λ_m is the Bayesian estimation of the failure rate. Since the risks in the hypothetical scheme are inevitable, thus when defining $\lambda_\mathrm{n} \leq \lambda_\mathrm{m}$, accepting H_0 with probability no less than $1 - \varphi$, when $\lambda_\mathrm{n} > \lambda_\mathrm{m}$, rejecting H_0 with probability no higher than ν. Where φ is the producer risk, ν is the user risk (φ means the probability that in-service time does not exceed useful life, but is judged to exceed it. This error causes damage to the producer. ν has the opposite meaning of φ).

Combined with the OREDA database and Bayesian theory, a more accurate equipment failure rate can be obtained (Yang et al., 2015). Combined with the idea of Bayesian and sequential test, this paper proposes a Bayesian sequential testing method for failure rate. We can obtain the upper limit of failure rate based on Bayesian estimation: λ_m. Judging one by one whether the failure rate λ_n exceeds λ_m, if $\lambda_\mathrm{n} > \lambda_\mathrm{m}$, the in-service time of SIS is considered to have exceeded its useful life.

Step 3: Determine λ_m based on Bayesian estimation. Since the failure rate of SIS is constant, considering its reparability, its total number of equipment failures meets the Poisson distribution (Toroody et al., 2020; Yazdi et al., 2022):

$$P\left(r|\lambda\right) = \frac{(\lambda T)^r e^{-\lambda T}}{r!} \tag{9}$$

$$T = \sum_{i=1}^{r} t_i + \sum_{j=n-r+1}^{n} t_j \tag{10}$$

where T is the accumulated operating time before the SIS failure; λ is the equipment failure rate in the industrial database; and r is the number of equipment failures; n is the total number of equipment; t_i is the operating time before the i-th equipment failure; t_j is the operating time before the j-th equipment failure.

Bayesian estimation using the squared loss function (Kiapour and Nematollahi, 2011), the Bayesian estimate of the failure rate λ is denoted as λ_m and can be expressed:

$$\lambda_m = \int_0^\infty \lambda g(\lambda|r)d\lambda = \frac{\Gamma(r+\alpha+1)}{\Gamma(r+\alpha)(T+\beta)} = \frac{r+\alpha}{T+\beta} \tag{11}$$

where r is the number of equipment failures; T is the accumulated operating time before the SIS failure.

When the Mean column and the n/τ column are not identical under the same equipment classification in the OREDA database, the prior distribution parameters can be expressed as (OREDA, 2015):

$$\begin{cases} \beta = \dfrac{Mean}{SD^2} \\ \alpha = \left(\dfrac{Mean}{SD}\right)^2 \end{cases} \tag{12}$$

Step 4: Bayesian sequential testing of failure rate. Based on φ、ν and λ_m, determining one by one whether λ_n is greater than λ_m. Let $\Theta_1 = \{\theta{:}\lambda_\mathrm{n} \leq \lambda_\mathrm{m}\}$, $\Theta_2 = \{\theta{:}\lambda_\mathrm{n} > \lambda_\mathrm{m}\}$, the prior distribution function of λ_n is $Ga(\delta_\pi,\gamma_\pi)$, by the nature of the conjugate distribution, its posterior distribution function is $Ga(\delta_1, \gamma_1)$. Relevant parameters can be expressed as:

$$\begin{cases} \delta_1 = \delta_\pi + r \\ \gamma_1 = \gamma_\pi + \sum_{i=1}^{m} t_i \end{cases} \tag{13}$$

$$\begin{cases} E(t_i) = \dfrac{\delta_\pi}{\gamma_\pi} \\ Var(t_i) = \dfrac{\delta_\pi}{{\gamma_\pi}^2} \end{cases} \tag{14}$$

Where r is the number of equipment failures; t_i($i = 1.m$)is the equipment failure time; $E(t_i)$ and $Var(t_i)$ are the mathematical expectation and variance. The prior failure time can be obtained by Monte Carlo simulation (Jiang et al., 2022). For example, using $1/\lambda_\mathrm{m}$ as the scaling parameter, through Monte Carlo simulation, 50 uniform random number in the interval of (0−1) are generated. Substituted the random number into the inverse function of the failure distribution function to calculate a series of failure times, and 20 of them are intercepted and recorded as group 1. Use the same method to get other data groups. Calculate the mathematical expectation and variance of each group of data, the calculations result of each group are summed and then averaged.

The sequential probability ratio method is to make a likelihood ratio, where the likelihood ratio is replaced by the posterior odds ratio S_n of the likelihood function on Θ_1 and Θ_2:

$$S_n = \frac{\int_{\Theta_2} \pi\left(\lambda_n|x\right)d\lambda}{\int_{\Theta_1} \pi\left(\lambda_n|x\right)d\lambda} = \frac{\int_0^{\lambda_m} \lambda_n^{\delta_1 - 1}\exp\left(-\gamma_1\lambda_n\right)d\lambda}{\int_{\lambda_m}^{+\infty} \lambda_n^{\delta_1 - 1}\exp\left(-\gamma_1\lambda_n\right)d\lambda} \tag{15}$$

Let $y = 2\gamma_1\lambda_\mathrm{n}$, we can get:

$$S_n = \frac{\int_0^{2\gamma_1\lambda_m} y^{\delta_1 - 1}e^{-\frac{y}{2}}dy}{\int_{2\gamma_1\lambda_m}^{+\infty} y^{\delta_1 - 1}e^{-\frac{y}{2}}dy} = \frac{\int_0^{2\gamma_1\lambda_m} K_{2\delta_1}(\chi^2)d\chi^2}{\int_{2\gamma_1\lambda_m}^{+\infty} K_{2\delta_1}(\chi^2)d\chi^2} = \frac{1 - K_{2\delta_1}(2\gamma_1\lambda_m)}{K_{2\delta_1}(2\gamma_1\lambda_m)} \tag{16}$$

where $K_{2\alpha1}(2\gamma_1\lambda_\mathrm{m})$ denotes the probability that the random variable is less than $2\gamma_1\lambda_\mathrm{m}$. Random variable obeys χ^2 distribution with degrees of freedom of $2\delta_1$. The decision thresholds A and B are introduced, and the following test law is given:

1) When $S_n \leq A$, stop recording failure data and accept $H0$;.
2) When $S_n \geq B$, stop recording failure data and accept $H1$;.
3) When $A < S_n < B$, continue to record failure data and do not make a decision.

According to the idea of the Bayes testing, the decision thresholds A and B are:

$$\begin{cases} A = \dfrac{\gamma_{\pi_1}}{\pi_0 - \delta_{\pi_0}} \\ B = \dfrac{\pi_1 - \gamma_{\pi_1}}{\delta_{\pi_0}} \end{cases} \tag{17}$$

where the expressions for π_0 and π_1 can be expressed as:

$$\begin{cases} \pi_0 = \int_{\lambda\in\Theta_1} dF^\pi(\lambda) \\ \pi_1 = \int_{\lambda\in\Theta_2} dF^\pi(\lambda) \end{cases} \tag{18}$$

where the expressions for $\delta_{\pi0}$and $\gamma_{\pi1}$ can be expressed as:

$$\begin{cases} \delta_{\pi_0} = \int_{\lambda\in\Theta_1}\left[\int_{B_n}\prod_{i=1}^{n} f(x_n|\theta)dx\right]dF^\pi(\lambda) \\ \gamma_{\pi_1} = \int_{\lambda\in\Theta_2}\left[\int_{D_n}\prod_{i=1}^{n} f(x_n|\theta)dx\right]dF^\pi(\lambda) \end{cases} \tag{19}$$

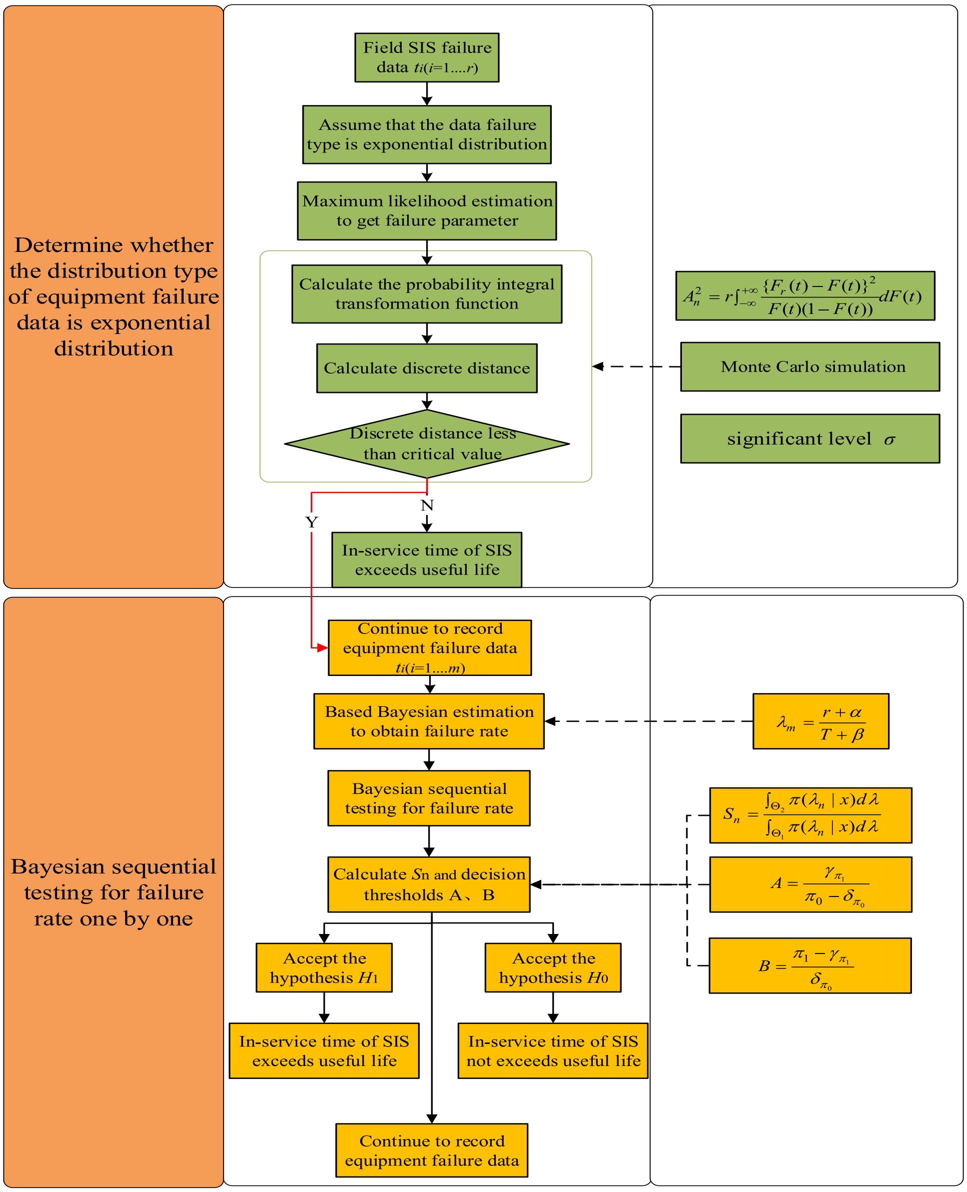

Determine whether the distribution type of equipment failure data is exponential distribution
Field SIS failure data ti(i=1....r)
Assume that the data failure type is exponential distribution
Maximum likelihood estimation to get failure parameter
Calculate the probability integral transformation function
Calculate discrete distance
Discrete distance less than critical value
$A_n^2 = r\int_{-\infty}^{+\infty}\frac{\{F_r(t) - F(t)\}^2}{F(t)(1 - F(t))}dF(t)$
Monte Carlo simulation
significant level σ
Y
N
In-service time of SIS exceeds useful life
Bayesian sequential testing for failure rate one by one
Continue to record equipment failure data ti(i=1....m)
Based Bayesian estimation to obtain failure rate
$\lambda_m = \frac{r + \alpha}{T + \beta}$
Bayesian sequential testing for failure rate
$S_n = \frac{\int_{\Theta_2}\pi(\lambda_n | x)d\lambda}{\int_{\Theta_1}\pi(\lambda_n | x)d\lambda}$
Calculate Sn and decision thresholds A、B
$A = \frac{\gamma_{\pi_1}}{\pi_0 - \delta_{\pi_0}}$
$B = \frac{\pi_1 - \gamma_{\pi_1}}{\delta_{\pi_0}}$
Accept the hypothesis H1
Accept the hypothesis H0
In-service time of SIS exceeds useful life
In-service time of SIS not exceeds useful life
Continue to record equipment failure data

Fig. 3. The flow of the rapid inference method of useful life.

When H_0 is accepted, the in-service time of the SIS does not exceed its useful life; When H_1 is accepted, the in-service time of SIS equipment exceeds its useful life. The flow of the rapid inference method of useful life is shown in Fig. 3.

4. Case study

Hydrocracking is a conversion process in which hydrocarbon molecules of petroleum distillate are cracked and hydrogenated on the catalyst surface at a higher reaction temperature and pressure to form smaller hydrocarbon molecules. Due to its advantages of strong adaptability of raw materials and clean products, the technology is becoming one of the key technologies for improving the quality of oil products and the high efficiency of raw oil processing. The process flow of the hydrocracking unit is shown in Fig. 4.

The hot high-pressure separator is a critical process equipment in the hydrocracking process, and its liquid level control results directly affect the effect of hydrogenation reaction (Yousefi and Hernandez, 2019). If the liquid level is too high, the liquid is quickly brought into the circulating hydrogen compressor, which will damage the compressor.

The liquid level interlock protection circuit is composed of a liquid level sensor of the two out of three (2oo3) voting structure, a logical controller of the one out of one (1oo1) voting structure, and a final element of the one out of two (1oo2) voting structure. One of its main functions is: when the liquid level of the reactor reaches the preset high trigger value, the logic controller sends a shutdown signal to the final element, and the valves are opened to ensure that the liquid level in the reactor is at a safe and controllable level.

Without loss of generality, the LOPA report (Fang et al., 2007; Markowski and Kotynia, 2011) shows that the safety integrity level of this level interlock circuit needs to meet the requirements of SIL2. The chemical plant perform a three year proof test interval, assuming that the PFD of the equipment returns to 0 after the proof test (Wu et al., 2018). The equipment failure data related to this liquid level interlock circuit in the industrial database (OREDA, 2015) are shown in Table 1.

The instrumentation preventive maintenance strategy developed by the plant states that the useful life of the final element ranges from 10 to 15 years, and the main failure mode considered here is FTO (Failure To Open) (ISO14224, 2016). Field equipment failure time of the valves x_i are shown in Table 2 (Data from a petrochemical plant field project).

Setting the significant level $\sigma = 0.05$ and $i = 15$, the testing results for the type of distribution of small sample failure data can be obtained from Eqs. (7)–(8), and the calculated results are shown in Table 3.

From Table 3, the A_n^2 of valve B is greater than the CV, the failure data do not fit the assumption of exponential distribution (constant failure rate), the in-service time of the valve B has exceeded its useful life. The chemical plant need to take a series of preventive maintenance measures for valve B. The in-service time of valve A still does not exceed its useful life, it is necessary to continue to record its failure data.

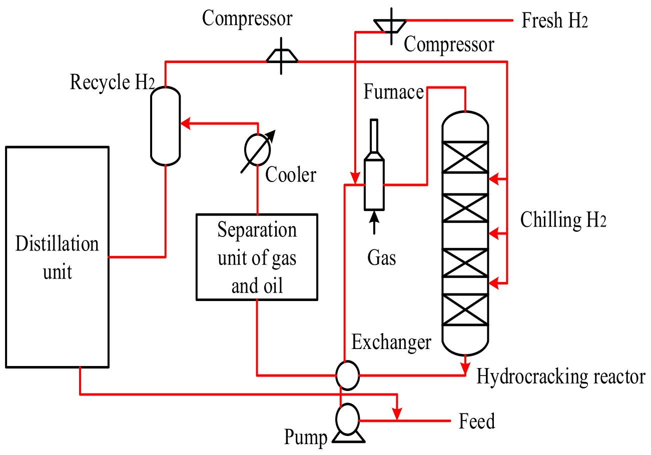


Fig. 4. Process flow of hydrocracking unit.

Table 1
Failure data of liquid level interlock protection circuit.

Equipment Type	Component	Failure rate/ h	Common cause failure β	MTTR/ h
Level sensor	LT A/B/C	2.20E-5	0.02	8
Logic controller	LC	4.82E-7	–	12
Final element	FE A/B	2.51E-5	0.02	24

For comparison, the calculated results of the useful life hypothesis testing in the IEC method can be determined according to Eqs. (1)–(5), as shown in Table 4.

The comparison of Tables 3 and 4 shows that the IEC method has a certain lag when the equipment failure data is small ($i = 15$). According to IEC method, it is concluded that the in-service time of valve B does not exceed its useful life. However, according to Table 3, the failure rate of valve B is no longer constant. Thus, if the IEC method is used, chemical plant cannot adjust the maintenance strategy in time.

Based on the existing failure data in Table 2, valve A can continue to be in service. Referring to the plant instrument maintenance strategy, valve A has entered the wear-out phase. To ensure safety interlock circuit meets SIL2 level during the proof test cycle, need to limit the upper limit of failure rate. Since the *Mean* value of valve A in the OREDA database is 11.3 and the *SD* value is 7.48, the $\lambda_{\rm m}$ of valve A can be obtained as 2.89E-5/h according to Eqs. (11)–(12).

The subsequent Bayesian sequential testing statistical inference needs to analyze its prior information to obtain the prior distribution parameters of the failure rate. Using $1/\lambda_{\rm m}$ as the scaling parameter, 15 groups of simulation data are generated by Monte Carlo simulation (Intercept 20 failure data per group). Some prior simulation data generated by the simulation are shown in Table 5.

According to Eqs. (13)-(14) and the prior simulation data in Table 5, the prior distribution parameters can be obtained as $\delta_1 = 13.818$, $\gamma_1 = 448{,}398.28$.

Assume that both φ and ν are 0.1 (The definitions of φ and ν are detailed in Section 3.2), two groups failure data $x_{\rm n}$ (n = 1,2,3,4) and $y_{\rm n}$ are colleted from the field maintenance records. Where $x_1 = 91{,}452$ h, $x_2 = 95{,}037$ h, $x_3 = 98{,}053$ h, and $x_4 = 102{,}420$ h; $y_1 = 91{,}055$ h, $y_2 = 94{,}637$ h, $y_3 = 99{,}053$ h, and $y_4 = 104{,}755$ h. Use the RIUL inference method to test $x_{\rm n}$ and $y_{\rm n}$ one by one. According to Eqs. (15)–(19), the hypothesis testing results of $x_{\rm n}$ and $y_{\rm n}$ are shown in Fig. 5.

As seen in Fig. 5, when the equipment failure time is x_1, x_2, or x_3, respectively, the posterior odds ratio all satisfies $A<S_{\rm n}<B$. According to the test law in subsection 2.2, the null hypothesis H_0 (failure rate $\lambda_{\rm n} \le \lambda_{\rm m}$) cannot be accepted yet, the relationship between the in-service time and useful life cannot be judged. Thus, the decision result is: Record failure data continuously and don't make decision. When the equipment failure time is x_4 or y_4, the posterior odds ratio satisfies $S_{\rm n} > B$, according to the decision rule, accepts the alternative hypothesis H_1 (failure rate $\lambda_{\rm n} > \lambda_{\rm m}$) and concludes that the in-service time of equipment exceeds its useful life.

For comparison, the hypothesis testing results of $x_{\rm n}$ and $y_{\rm n}$ in the IEC method are given in Table 6.

As can be seen from Table 6, when the failure time is x_4 or y_4, the hypothetical testing method in IEC standard still cannot reject the assumption of the constant failure rate. The comparison results in Fig. 6 and Table 6 show that the RIUL method requires only a few (four) failure data to conclude that the in-service time of equipment exceeds its useful life, however the traditional IEC method requires more failure data to reach the same conclusions.

Poor timeliness of IEC method will lead to an improper estimation of useful life. If the Valve A is maintained or replaced according to the calculations of this method, in the equipment wear-out phase, the

Table 2
Failure time of the valves in FTO mode.

Number	Failure time/h														
Valve A	1754	3542	6874	10,254	11,245	14,258	20,145	25,478	37,485	52,458	68,452	80,526	85,456	89,214	90,457
Valve B	1845	3568	5727	11,458	22,457	29,874	38,956	50,231	62,742	71,548	78,956	80,475	82,451	84,753	87,235

Table 3
Testing results for the distribution type of failure data.

Number	Discrete distance A_n^2	Critical value	Exponential distribution assumption	Whether in-service time of equipment exceeds its useful life
Valve A	0.411	0.829	Accept	No
Valve B	0.847	0.829	Reject	Yes

Table 4
Results of useful life hypothesis testing in IEC method.

Number	Statistical test value χ^2	Range of reject domain *W*	Constant failure rate assumption	Whether in-service time of equipment exceeds its useful life
Valve A	28.555	15.308–44.461	Accept	No
Valve B	32.792	15.308–44.461	Accept	No

theoretical calculation of PFD_{avg} and the actual value will have a gap (the SIL level of the safety interlock circuit does not meet the SIL2). It will lead to serious production safety accidents.

To illustrate the impact of useful life estimation on PFD, using the equipment failure rate in Table 1 as a benchmark, the formula for calculating PFD is detailed in Ding et al. (2017). If the failure rate is constant in the proof test cycle, the PFD curve of the valve A and liquid level interlock protection circuit are shown in Fig. 6.

From Fig. 6, assuming that equipment failure rate is constant, PFD changes little in proof test cycle. The PFD_{avg} of the liquid level interlock circuit in the fourth proof test cycle is 0.0097, which meets the SIL2 level ($0.001 \le \text{PFD} < 0.01$). However, the test results in Table 6 show that the failure rate of valve A at x_4 has exceeded λ_m, indicating that the failure rate of valve A in the fourth proof test cycle is no longer constant. The gradual increase of failure rate will lead to PFD_{avg} greater than 0.01 in the fourth proof test cycle. If the equipment is not replaced in time, the safety production of the plant will be seriously affected.

5. Conclusions

The useful life of a safety instrumented systems is a crucial reliability indicator. Since few manufacturers offer this indicator voluntarily, the

Table 6
Hypothesis testing results in IEC method.

	Failure time	Statistical test value χ^2	Range of reject domain *W*	Constant failure rate assumption	Whether in-service time of equipment exceeds its useful life
x_n	x_1	29.865	16.791–46.979	Accept	No
	x_2	31.072	18.291–49.480	Accept	No
	x_3	32.181	19.806–51.966	Accept	No
	x_4	33.266	21.336–54.437	Accept	No
y_n	y_1	32.720	16.791–46.979	Accept	No
	y_2	34.096	18.291–49.480	Accept	No
	y_3	35.416	19.806–51.966	Accept	No
	y_4	36.739	21.336–54.437	Accept	No

Table 5
Partial prior simulation data.

	Failure time/h									
Group 1	1341	4330	6855	7465	9499	11,259	18,871	21,528	24,606	24,622
	25,162	25,231	26,941	34,790	48,007	50,992	56,373	70,485	89,598	93,533
Group 2	1729	2560	3890	6564	8392	9253	10,731	11,971	15,128	16,163
	20,288	30,637	30,804	43,552	44,049	44,669	67,465	78,085	92,691	94,979
Group 3	1743	3086	4032	9373	17,571	23,854	27,590	28,730	31,785	33,052
	36,979	45,961	51,205	57,092	68,830	72,959	76,051	83,562	88,754	93,251

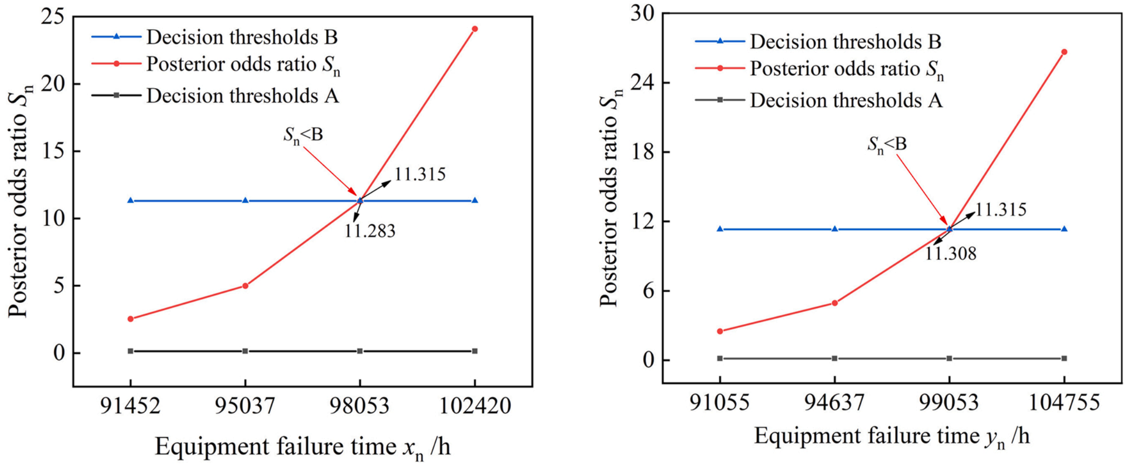


Fig. 5. Hypothesis testing results of x_n and y_n in RIUL method.

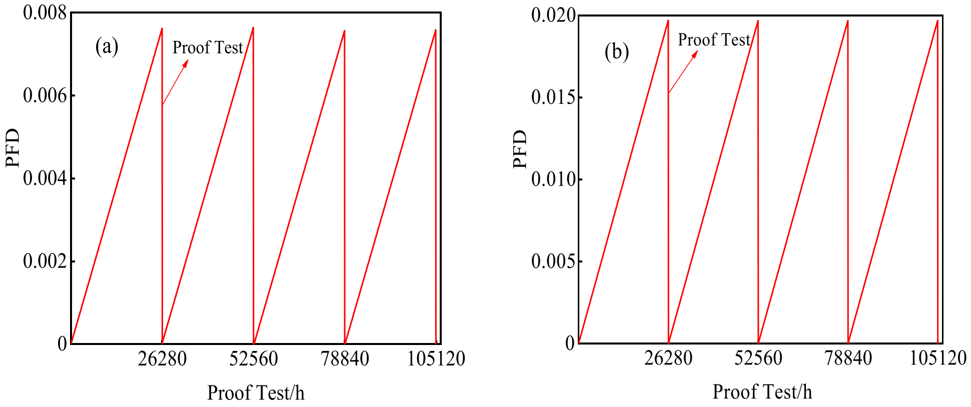


Fig. 6. PFD curve during the proof test cycle. (a) PFD curve of the valve A; (b) PFD curve of liquid level interlock circuit.

current IEC standard only gives an approximate range of the useful life. The useful life inference method given by IEC is poor timeliness. It requires a large amount of equipment failure data to reach a conclusion, contrary to SIS equipment's high reliability. Many scholars do not estimate the useful life when assuming a constant failure rate. How to accurately infer the useful life of equipment under small samples is of great engineering significance. Combined with the characteristics of SIS equipment failure data, this paper proposes the RIUL method. Use Anderson-Darling testing to determine whether the distribution type of failure data is exponential under small samples. After that, propose a Bayesian sequential testing method for the failure rate, judging one by one whether the failure rate λ_n exceeds λ_m. The proposed approach aims to overcome the disadvantage of poor timeliness of the IEC testing method. It is also convenient for scholars to estimate the useful life of the SIS equipment more accurately.

The case study shows that compared to the IEC method, the RIUL method requires only a few equipment failure data to conclude that in-service time exceeds useful life. The RIUL method can help the chemical plant adjust the equipment maintenance and replacement strategy in time and guarantee the SIL level meets the corresponding requirements of the LOPA analysis report, avoiding safety accidents caused by increasing failure rate.

The RIUL method still needs some improvement. A large amount of credible prior information can guarantee the accuracy of the RIUL method. In this paper, only the prior information of simulation data is used, which can be combined with various prior information, such as expert experience, in future works. For example, D-S evidence theory is one of the methods of combining multiple sources of prior information.

Declaration of Competing Interest

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

Acknowledgements

The authors gratefully acknowledge the financial support provided by the National Key R&D Program of China (2019YFB2006305).

References

Brissaud, F., 2017. Using field feedback to estimate failure rates of safety-related systems. Reliab. Eng. Syst. Saf. 159, 206–213.
Catelani, M., Ciani, L., Venzi, M., 2018. Failure modes, mechanisms and effect analysis on temperature redundant sensor stage. Reliab. Eng. Syst. Saf. 180, 425–433.
Chang, Y.J., Khan, F., Ahmed, S., 2011. A risk-based approach to design warning system for processing facilities. Process Saf. Environ. Prot. 89 (5), 310–316.
Chebila, M., 2018. Simultaneous evaluation of safety integrity's performance indicators with a generalized implementation of common cause failures. Process Saf. Environ. Prot. 117, 214–222.
Chebila, M., 2020. Generalized markovian consideration of common cause failures in the performance assessment of safety instrumented systems. Process Saf. Environ. Prot. 141, 28–36.
D'Agostino, R.B., 1986. Goodness-of-fit Techniques, New York: Marcel Dekker.
Ding, L., Wang, H., Jiang, J., et al., 2017. SIL verification for SRS with diverse redundancy based on system degradation using reliability block diagram. Reliab. Eng. Syst. Saf. 165, 170–187.
Fang, J.S., Mannan, M.S., Ford, D.M., 2007. Value at risk perspective on layers of protection analysis. Process Saf. Environ. Prot. 85 (1), 81–87.
Heo, J.H., Shin, H., Nam, W., et al., 2013. Approximation of modified Anderson-Darling test statistics for extreme value distributions with unknown shape parameter. J. Hydrol. 49 (30), 41–49.
IEC60605, 2007. Equipment reliability testing, Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity.
IEC61508, 2016. Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC61508, 2016. Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 6: Guidelines on the application of IEC 61508–2 and IEC 61508–3.
ISA TR84.00.03, 2019. Automation asset integrity of safety instrumented systems (SIS).
ISO14224, 2016. Petroleum, petrochemical and natural gas industries-collection and exchange of reliability and maintenance data for equipment.
Jahanian, H., 2017. Optimization, a rational approach to SIL determination. Process Saf. Environ. Prot. 109, 452–464.
Jahanian, H., Mahboob, Q., 2016. SIL determination as a utility-based decision process. Process Saf. Environ. Prot. 102, 757–767.
Jiang, S.Y., Chen, G.M., Zhu, Y., et al., 2022. Probabilistic approach for risk assessment of offshore hydrate wellbore during test production. Process Saf. Environ. Prot. 163, 574–584.
Kiapour, A., Nematollahi, N., 2011. Robust Bayesian prediction and estimation under a squared log error loss function. Stat. Probab. Lett. 81 (11), 1717–1724.
de Lira-Flores, J.A., López-Molina, A., Gutiérrez-Antonio, C., et al., 2019. Optimal plant layout considering the safety instrumented system design for hazardous equipment. Process Saf. Environ. Prot. 124, 97–120.
Markowski, A.S., Kotynia, A., 2011. "Bow-tie" model in layer of protection analysis. Process Saf. Environ. Prot. 89 (4), 205–213.
Meng, H.X., Kloul, L., Rauzy, A., 2018. Modeling patterns for reliability assessment of safety instrumented systems. Reliab. Eng. Syst. Saf. 180, 111–123.
Mkhida, A., Thiriet, J.M., Aubry, J.F., 2014. Integration of intelligent sensors in safety instrumented systems (SIS). Process Saf. Environ. Prot. 92 (2), 142–149.
OREDA, 2015. Offshore Reliability Data Handbook. DNV, Trondheim, Norway.
Shao, X.Y., Wang, Y.Y., Cai, B.P., et al., 2022. Remaining useful life prediction considering degradation interactions of subsea Christmas tree: a multi-stage modeling approach. Ocean. Eng. 264, 112455.
Śliwiński, M., 2018. Safety integrity level verification for safety-related functions with security aspects. Process Saf. Environ. Prot. 118, 79–92.
Sravanthi, S., Dheenadhayalan, R., Devan, K., 2017. An inherently fail-safe electronic logic design for a safety application in nuclear power plant. Process Saf. Environ. Prot. 111, 232–243.
Stephen, T., 2015. Useful Life of Safety Instrumented Systems. ISA Process Control and Safety Symposium.
Timms, C., 2009. Hazards equal trips or alarms or both. Process Saf. Environ. Prot. 87 (1), 3–13.
Toroody, A.B., Abaei, M.M., Arzaghi, E., 2020. On reliability challenges of repairable systems using hierarchical bayesian inference and maximum likelihood estimation. Process Saf. Environ. Prot. 135, 157–165.
Wang, Y., West, H.H., Mannan, M.S., 2004. The impact of data uncertainty in determining safety integrity level. Process Saf. Environ. Prot. 82 (6), 393–397.

Wu, S.N., Zhang, L.B., Lundteigen, M.A., et al., 2018. Reliability assessment for final elements of SISs with time dependent failures. J. Loss Prev. Process Ind. 51, 186–199.

Xie, L., Håbrekke, S., Liu, Y.L., et al., 2019. Operational data-driven prediction for failure rates of equipment in safety instrumented systems: a case study from the oil and gas industry. J. Loss Prev. Process Ind. 60, 96–105.

Yang, M., Khan, F., Lye, L., et al., 2015. Risk assessment of rare events. Process Saf. Environ. Prot. 98, 102–108.

Yazdi, M., Khan, F., Abbassi, R., 2022. Operational subsea pipeline assessment affected by multiple defects of microbiologically influenced corrosion. Process Saf. Environ. Prot. 158, 159–171.

Yousefi, A., Hernandez, M.R., 2019. Using a system theory based method (STAMP) for hazard analysis in process industry. J. Loss Prev. Process Ind. 61, 305–324.

Zhang, A.B., Zhang, T.L., Barros, A., et al., 2019. Optimization of maintenances following proof tests for the final element of a safety-instrumented system. Reliab. Eng. Syst. Saf. 196, 106779.

Zhang, S.B., 2021. A test for second-order stationarity of a time series based on the maximum of Anderson–Darling statistics. J. Stat. Plan. Infer.