Petroleum Science 18 (2021) 1813–1828

Contents lists available at ScienceDirect

Petroleum Science

journal homepage: www.keaipublishing.com/en/journals/petroleum-science

Original Paper

Parameter uncertainty modeling of safety instrumented systems

Bao-Ping Cai [a, *], Wen-Chao Li [a], Yong-Hong Liu [a], Yan-Ping Zhang [a], Yi Zhao [a], Xiang-Di Kong [a], Zeng-Kai Liu [a], Ren-Jie Ji [a], Qiang Feng [b]

[a] *College of Mechanical and Electronic Engineering, China University of Petroleum, Qingdao, 266580, Shandong, China*
[b] *School of Reliability and Systems Engineering, Beihang University, Beijing, 100191, China*

ARTICLE INFO

Article history:
Received 27 April 2020
Accepted 26 November 2020
Available online 2 September 2021

Edited by Xiu-Qiu Peng

Keywords:
Safety integrity level
Dynamic Bayesian network
Monte Carlo
Parameter uncertainty

ABSTRACT

In this study, a novel safety integrity level (SIL) determination methodology of safety instrumented systems (SISs) with parameter uncertainty is proposed by combining multistage dynamic Bayesian networks (DBNs) and Monte Carlo simulation. A multistage DBN model for SIL determination with multiple redundant cells is established. The models of function inspection test interval and function inspection test stages are alternately connected to form the multistage DBNs. The redundant cells can have different *M* out of *N* voting system architectures. An automatic modeling of conditional probability between nodes is developed. The SIL determination of SISs with parameter uncertainty is constructed by using the multistage DBNs and Monte Carlo simulation. A high-pressure SIS in the export of oil well-platform is adopted to demonstrate the application of the proposed approach. The SIL and availability of the SIS and its subsystems are obtained. The influence of single subsystem on the SIL and availability of the SIS is studied. The influence of single redundant element on the SIL and availability of the subsystem is analyzed. A user-friendly SIL determination software with parameter uncertainty is developed on MATLAB graphical user interface.

© 2021 The Authors. Publishing services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

In accordance with IEC 61508 and IEC 61511, a safety instrumented system (SIS) is composed of a sensor subsystem, a controller subsystem and an actuator subsystem. It can achieve one or more safety instrumented functions. Safety integrity level (SIL) refers to the possibility that SISs can perform the safety instrument function as required under specified conditions and within a specified time. SIL is a performance index required by SISs. In the SIL determination of SISs, many uncertain factors are usually introduced. The uncertain factors for SIL determination are those that cause the final result to be biased during SIL determination. The uncertain factors for SIL determination can be classified into three categories: model, artificial, and parameter uncertainties. Model uncertainty refers to the incompleteness of the model and the limitation of the method to build the model. Model uncertainty is introduced when the model is built and calculated. Artificial uncertainty refers to the uncertainty caused by policies, operating procedures, and operators' execution ability. It is difficult to theorize, but its influence cannot be ignored. Parameter uncertainty is mainly due to the lack of historical failure data or the uncertainty caused by the interaction of multiple uncertain parameters (Kanjilal and Manohar, 2020; Martin et al., 2019; Wang and Qiu, 2012; Xu et al., 2012; Jin et al., 2012). For SISs with short life cycle and minimal failure parameters, the average of failure probability on demand (PFD_{avg}) of the system can be obtained through precise calculation if uncertain problems are disregarded. The results may differ from those that consider the effects of uncertainty. However, they are at the same discrete level, that is, the same SIL level. For SISs with long life cycle and large failure parameters, small uncertainty causes the PFD_{avg} of the system to fluctuate greatly. PFD_{avg} exceeds the original discrete interval, that is, wrong SIL determination result is obtained. This condition seriously affects the staff's design and application of the SIS and causes great potential risks to production activities. The operating cycle of SISs used in the process industry is long. Considering the fixed cost, equipment with high cost and extremely low failure parameters are not adopted. The deviation of determination results can be reduced, and the accuracy of SIL determination results can be improved through the analysis of uncertain factors with important influence (Wang et al., 2017;

* Corresponding author.
E-mail address: caibaoping@upc.edu.cn (B.-P. Cai).

https://doi.org/10.1016/j.petsci.2021.08.011

1995-8226/© 2021 The Authors. Publishing services by Elsevier B.V. on behalf of KeAi Communications Co. Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Nomenclature

Acronyms

SIL	Safety Integrity Level
SISs	Safety Instrumented Systems
SIF	Safety Instrumentation Functions
DBNs	Dynamic Bayesian Networks
BNs	Bayesian Networks
MooN	M out of N voting system
NS	normal state
SD	safety detected failure state
SU	safety undetected failure state
SS	safety failure state
DD	dangerous detected failure state
DU	dangerous undetected failure state
SPLCIC	safety programmable logic controller
LMVs	lower main shut-off electromagnetic valve
UMVs	upper main shut-off electromagnetic valve
WVs	wing electromagnetic valve
LMV	lower main shut-off ball valve
UMV	upper main shut-off ball valve
WV	wing ball valve
PT	pressure transmitter
IMP	impulse line
SPLCIC	safety programmable logic controller analog input channel
SPLCIP	safety programmable logic controller analog input processing
SPLCMP	safety programmable logic controller main processing
SPLCOP	safety programmable logic controller digital output processing
SPLCOC	safety programmable logic controller digital output
EV	electromagnetic valve
BV	ball valve

Notion and definition

PFD	failure probability on demand
PFS	probability of failing safely
PFD_{avg}	average of failure probability on demand
PFS_{avg}	average of safe failure probability
Δt	self-diagnosis interval
TI	test interval
TS	system running time
T_{ST}	function inspection test time
IF	channel independent failure nodes
CF	common cause failure nodes
CN	channel state nodes
U	cell state nodes
S	system state nodes
ω	common cause failure weight
n_{S}	number of channels with security failure
n_{D}	number of channels with dangerous failure
n_{SD}	number of channels with security detected failure
n_{SU}	number of channels with security undetected failure
n_{DD}	number of channels with dangerous detected failure
n_{DU}	number of channels with dangerous detected failure
MTTR	mean time to repair
MTSR	mean time to system restoration
C_{D}	hazard failure diagnostic coverage
μ_{TR}	repair rate
μ_{SR}	system restoration rate
λ_{T}	total failure rate
λ_{SDN}	detected independent safety failure rate
λ_{SUN}	undetected independent safety failure rate
λ_{DDN}	detected independent dangerous failure rate
λ_{DUN}	undetected independent dangerous failure rate
λ_{SDC}	detected common cause safety failure rate
λ_{SUC}	undetected common cause safety failure rate
λ_{DDC}	detected common cause dangerous failure rate
λ_{DUC}	undetected common cause dangerous failure rate
ε	test coverage rate
μ_{SD}	maintenance rate of safety detected failure
μ_{SU}	maintenance rate of safety undetected failure
μ_{DD}	maintenance rate of dangerous detected failure
μ_{DU}	maintenance rate of dangerous undetected failure
γ_{SD}	degradation rate of safety detected failure
γ_{SU}	degradation rate of safety undetected failure
γ_{DD}	degradation rate of dangerous detected failure
γ_{DU}	degradation rate of dangerous undetected failure

Freeman, 2012; Ulmeanu, 2012). Therefore, determining the SIL of SISs with uncertainty is valuable.

The model and artificial uncertainties are difficult to be analyzed quantitatively. Thus, parameter uncertainty is the focus of SIL determination. Many methods are used to address the SIL determination under parameter uncertainty. Freeman and Summers (2016) discussed the influence of uncertainty on the failure probability on demand (*PFD*) calculation in SISs and proposed a method to deal with the uncertainty of *PFD* calculation based on variance contribution analysis method. Sallak et al. (2008) presented a new confidence method for determining SIL. This method usesfailure rate and fuzzy probability to evaluate the *PFD* and SIL of SIS with uncertainty of failure rate. Piesik et al. (2016) introduced a new functional safety analysis method that considers the probabilistic model sensitivity of SISs and the uncertainty of probabilistic results. Wang et al. (2004) discussed the influence of data uncertainty on SIL calculation and proposed a procedure to solve the problem of data uncertainty in SIL determination of SISs. Chang et al. (2015) developed a new method by combining Monte Carlo simulation and fuzzy set to solve the uncertainty problem in SIL determination. The difficulty of SIL evaluation under parameter uncertainty is mainly the SIL determination. Many scholars proposed several qualitative (Śliwiński, 2018), semi quantitative, and quantitative methods for SIL determination, such as reliability block diagram (Ding et al., 2014), fault tree (Freeman, 2020), Markov graphs (Azizpour and Lundteigen, 2019), layer of protection analysis, and hazardous event severity matrix. Several of these methods are complex and difficult to apply, whereas others have important limitations for complex SISs, including binary variable problems (Soro et al., 2010) and state space explosion problems (Schlosser, 2020). Markov graphs are the commonly used method for SIL determination. IEC 61508 gives the solution steps with Markov and specifies the problem. The main problem with Markov graphs is that the number of states increases exponentially when the number of components of the system under study increases. Therefore, building Markov graphs and performing calculations without drastic approximations become quickly intractable by hand. Consequently, a quantitative comprehensive method is needed for SIL determination.

Bayesian networks (BNs) are widely used in reliability assessment, risk analysis, prediction, and fault diagnosis (Cai et al. 2015, 2016, 2017, 2020; Weber et al., 2012; Wang et al., 2010; Simon et al., 2008). Dynamic BNs (DBNs) are a long-established extension to BNs. DBNs have an advantage in representing uncertain knowledge in dynamic systems. They can be used to model the dynamic process of SISs. Recently, DBNs are used in safety risk analysis. Simon et al. (2019) calculated the availability integrated test duration and test strategy of SIS by using DBNs. Cai et al. (2016a,b) proposed a SIL determination method for different redundant architectures by using DBNs. SIL determination using DBNs can be quantitative and simple. However, SISs have many failure and multistage characteristics in the system life cycle. Many SISs in the process industry have multiple redundant cells. Thus, a comprehensive DBN model should be created for the SIL determination.

A novel SIL calculation methodology of SISs is proposed by combining multistage DBNs and Monte Carlo simulation. This method is used to address the SIL determination problem of SISs with multiple redundant cells under uncertain parameters. The rest of this paper is organized as follows. Section 2 proposes the SIL determination method with parameter uncertainty for SISs. Section 3 uses a high-pressure SIS in the export of oil well platform as an example to illustrate the proposed method. Section 4 develops a software package for SIL determination woth parameter uncertainty on MATLAB. Section 5 summarizes this work.

2. SIL determination method with parameter uncertainty

2.1. Structural modeling of the SIL determination model

SISs have the function of self-diagnosis, and SISs conduct self-diagnosis every Δt time. The failure detected by self-diagnosis of the system is called the detected failure, otherwise, it is called the undetected failure. After running *TI* time, SISs conduct a periodic function inspection test. The purpose of function inspection test is to detect dangerous failures of the system that are not detected in self-diagnosis. As shown in Fig. 1, the system running time *TS* contains multiple periodic function inspection test interval stage *TI* and function inspection test stage T_{ST}. The function inspection test interval stage and function inspection test stage models can be represented by two different DBN models. The models of function inspection test interval and function inspection test stages are alternately connected to form the multistage DBNs for the SIL determination of SISs. In Fig. 1, the solid and dotted lines are the directed transition lines between time slice. The directed transition lines in the purple box represent the time-varying law of nodes in the function inspection test interval stage. The directed transition lines in the green box represents the time-varying law of nodes in the function inspection test stage. The solid lines represent the directed transition line that plays a major role, and the dashed line represents the directed transition line that plays a supplementary role. The main difference depends on the degree of influence of nodes on the next time slice node. A SIS is composed of a sensor subsystem, a controller subsystem, and an actuator subsystem. A single subsystem is composed of several redundant cells. The redundant cells can have different *M* out of *N* voting system (MooN) architectures. The common redundant architectures are 1oo1, 1oo1D, 1oo2, 2oo2, 1oo2D, 2oo2D, 1oo3, 2oo3, and 2oo4 (Jahanian, 2015).

The time slice topology of BNs is shown in Fig. 2 *n* represents the number of channels of different redundant architectures. When $n = 1$, no common cause failure exists in the model. The red line represents the single-channel model architecture. The redundant architectures with the same number of channels have the same model structure. They are distinguished by conditional probability between nodes.The solid and dotted lines in Fig. 2 represent the interaction between nodes in the time slice.

The structure of the multistage DBNs is divided into four layers. The first layer of the model is the failure factor node layer. The nodes in this layer include channel independent failure nodes IF*nt x* and common cause failure nodes CF*t x* They represent the failure factors affecting the system. The failure factor nodes contain normal state (NS), safety detected failure state (SD), safety undetected failure state (SU), dangerous detected failure state (DD), and dangerous undetected failure state (DU). The second layer is the channel state node layer. They represent the channel state in single cell under the influence of failure factors. The channel state nodes contain five states: NS, SD, SU, DD, and DU. The third layer is the cell state node layer. They represent the state of single redundant cell of the system. The cell state nodes contain four states: NS, safety failure state (SS), DD, and DU. The fourth layer is the system state node layer. They represent the state of the subsystem being

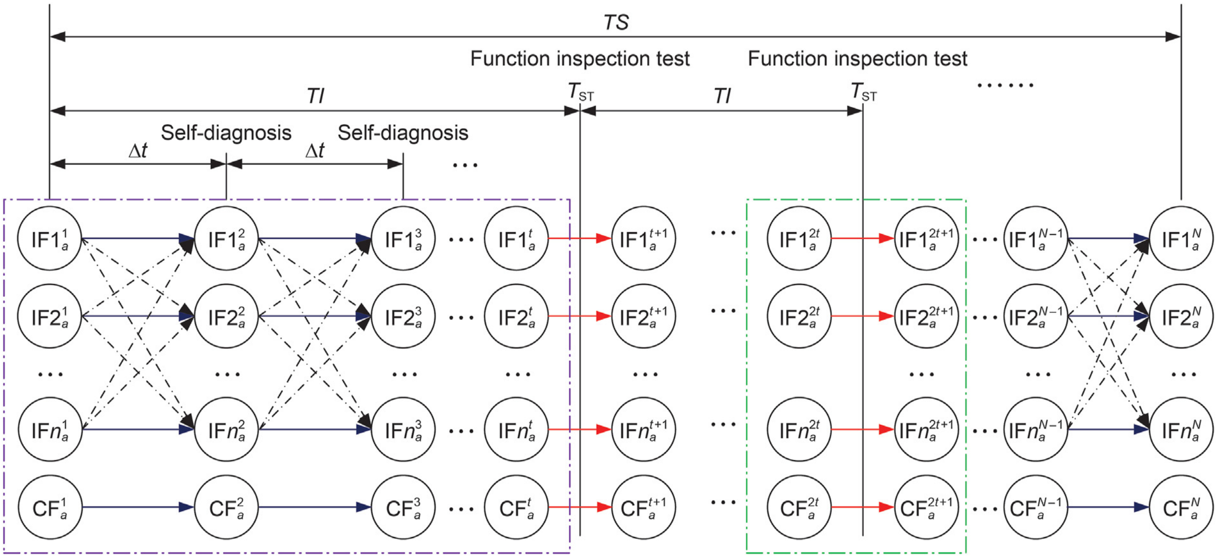

TS
Function inspection test
Function inspection test
TI
T_{ST}
TI
T_{ST}
......
Self-diagnosis
Self-diagnosis
Δt
Δt
...
$IF1_a^1$ $IF1_a^2$ $IF1_a^3$ ... $IF1_a^t$ $IF1_a^{t+1}$ ... $IF1_a^{2t}$ $IF1_a^{2t+1}$ ... $IF1_a^{N-1}$ $IF1_a^N$
$IF2_a^1$ $IF2_a^2$ $IF2_a^3$ ... $IF2_a^t$ $IF2_a^{t+1}$ ... $IF2_a^{2t}$ $IF2_a^{2t+1}$ ... $IF2_a^{N-1}$ $IF2_a^N$
...
IFn_a^1 IFn_a^2 IFn_a^3 ... IFn_a^t IFn_a^{t+1} ... IFn_a^{2t} IFn_a^{2t+1} ... IFn_a^{N-1} IFn_a^N
CF_a^1 CF_a^2 CF_a^3 ... CF_a^t CF_a^{t+1} ... CF_a^{2t} CF_a^{2t+1} ... CF_a^{N-1} CF_a^N

Fig. 1. Multistage DBNs for SIL determination.

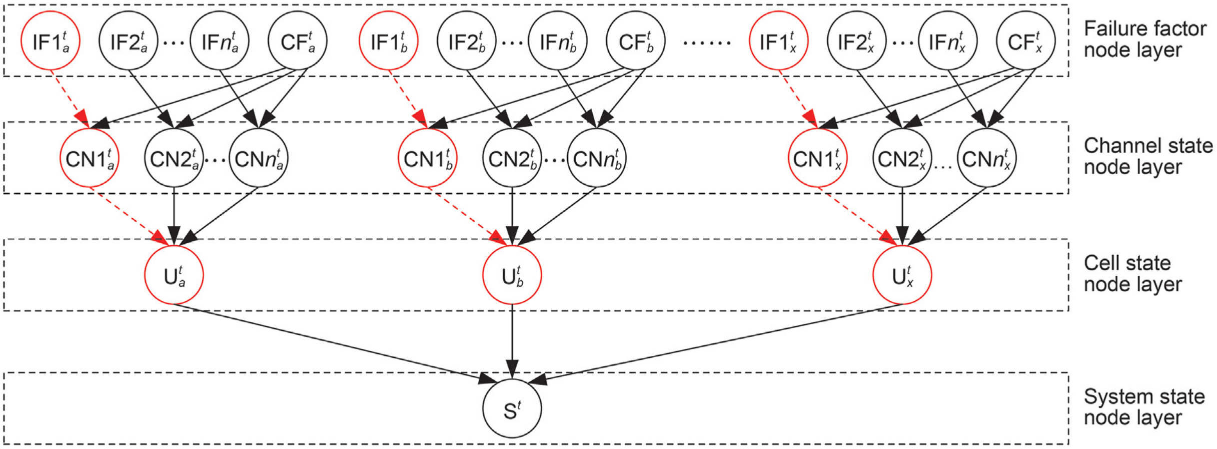


Fig. 2. Time slice topology of BNs.

evaluated. The system state node contains four states: NS, SS, DD, and DU.

The model structure in function inspection test stage is composed of two time slices of the DBNs in adjacent test interval stage. The static time slice of the model in function inspection test stage is the same as function inspection test interval stage. The failure factor nodes do not interact with each other during function inspection test stage. The interslice transition of failure factor nodes is shown in Fig. 3. The solid lines in Fig. 3 represent the state transitions of nodes between time slices during the function inspection test stage.

2.2. Parameter modeling of SIL determination model

2.2.1. Conditional probability within the time slice

The state of the channel state nodes CN is jointly determined by nodes IF and CF. The state only depends on node IF for 1oo1 and 1oo1D architecture. The flow chart of conditional probability modeling of nodes CN is shown in Fig. 4. The established rules are as follows:

Rule 1: when the state of nodes IF and CF is the same, the state of node CN is the same as theirs.
Rule 2: when the states of nodes IF and CF are different and the state of node IF is NS, then the state of node CN is the same as node CF.
Rule 3: when the states of nodes IF and CF are different and the state of node CF is NS, then the state of node CN is the same as node IF.
Rule 4: when the states of nodes IF and CF are different and the states of nodes IF and CF are not in NS, then the probability of node CN in the state of node CF is ω, and the probability in the state of node IF is $1-\omega$. The common cause failure weight parameter is defined as ω (the default is $\omega = 1$).

The state of cell state nodes U is determined by nodes CN. The flow chart of conditional probability modeling of nodes U is shown in Fig. 5. The established rules are as follows:

Rule 1: when the number of channels with security failure (n_S) is greater than safety fault tolerance (*SFT*), the cell experiences security failure. Specifically, the state of the node is SS.
Rule 2: when the number of channels with dangerous failure (n_D) is greater than hardware fault tolerance (*HFT*), the cell with MooN architecture experiences dangerous failure. If at least one safety detected failure or dangerous detected failure occurs, the cell experiences dangerous detected failure. Specifically, the state of the node is DD, otherwise the state of the node is DU.
Rule 3: when the number of channels with dangerous detected failure (n_{DU}) is greater than *HFT* for the *M* out of *N* voting system with diagnostic (MooND) architecture, the cell experiences dangerous failure. If at least one safety detected failure or dangerous detected failure occurs, the cell experiences dangerous detected failure. Specifically, the state of the node is DD, otherwise the state of the node is DU.

The subsystem of SIS is composed of several different cells. The state of system state node S is determined by nodes U. The conditional probability of node S depends on the actual connection relationship of redundant cells.

2.2.2. Conditional probability in function inspection test interval stage

The process of establishing the conditional probability of independent failure node IF during function inspection test interval

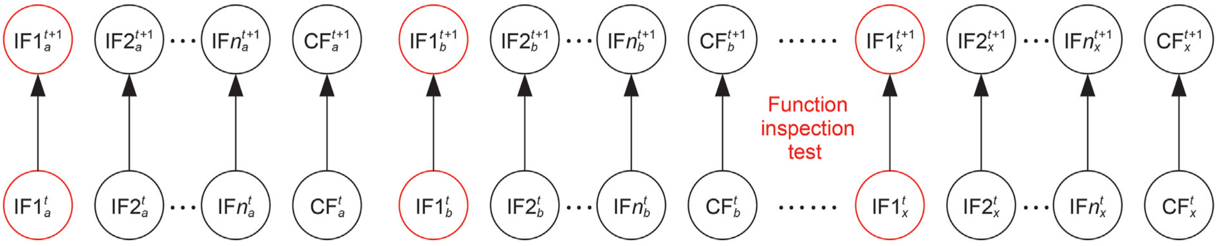


Fig. 3. Transition of failure factor nodes during function inspection test stage.

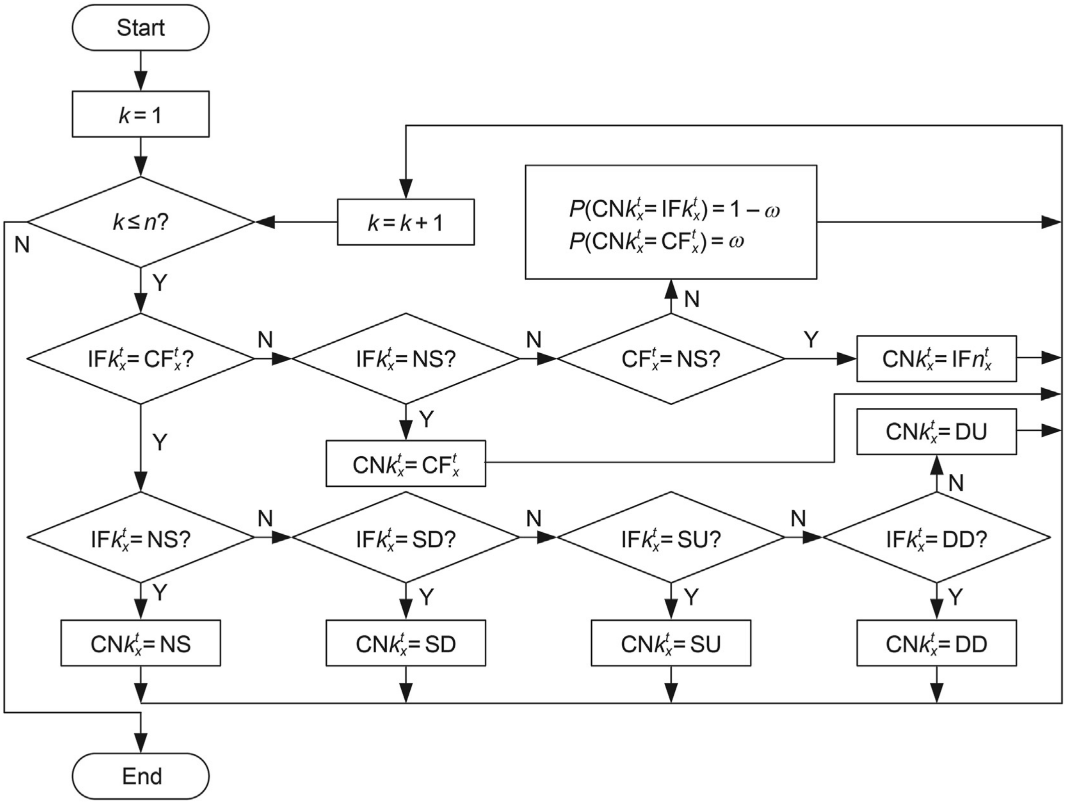

Start
$k=1$
$k\leq n?$
$k=k+1$
$P(\mathrm{CN}k_x^t=\mathrm{IF}k_x^t)=1-\omega$
$P(\mathrm{CN}k_x^t=\mathrm{CF}_x^t)=\omega$
N
Y
$\mathrm{IF}k_x^t=\mathrm{CF}_x^t?$
$\mathrm{IF}k_x^t=\mathrm{NS}?$
$\mathrm{CF}_x^t=\mathrm{NS}?$
$\mathrm{CN}k_x^t=\mathrm{IF}n_x^t$
$\mathrm{CN}k_x^t=\mathrm{CF}_x^t$
$\mathrm{CN}k_x^t=\mathrm{DU}$
$\mathrm{IF}k_x^t=\mathrm{NS}?$
$\mathrm{IF}k_x^t=\mathrm{SD}?$
$\mathrm{IF}k_x^t=\mathrm{SU}?$
$\mathrm{IF}k_x^t=\mathrm{DD}?$
$\mathrm{CN}k_x^t=\mathrm{NS}$
$\mathrm{CN}k_x^t=\mathrm{SD}$
$\mathrm{CN}k_x^t=\mathrm{SU}$
$\mathrm{CN}k_x^t=\mathrm{DD}$
End

Fig. 4. Conditional probability modeling of nodes CN.

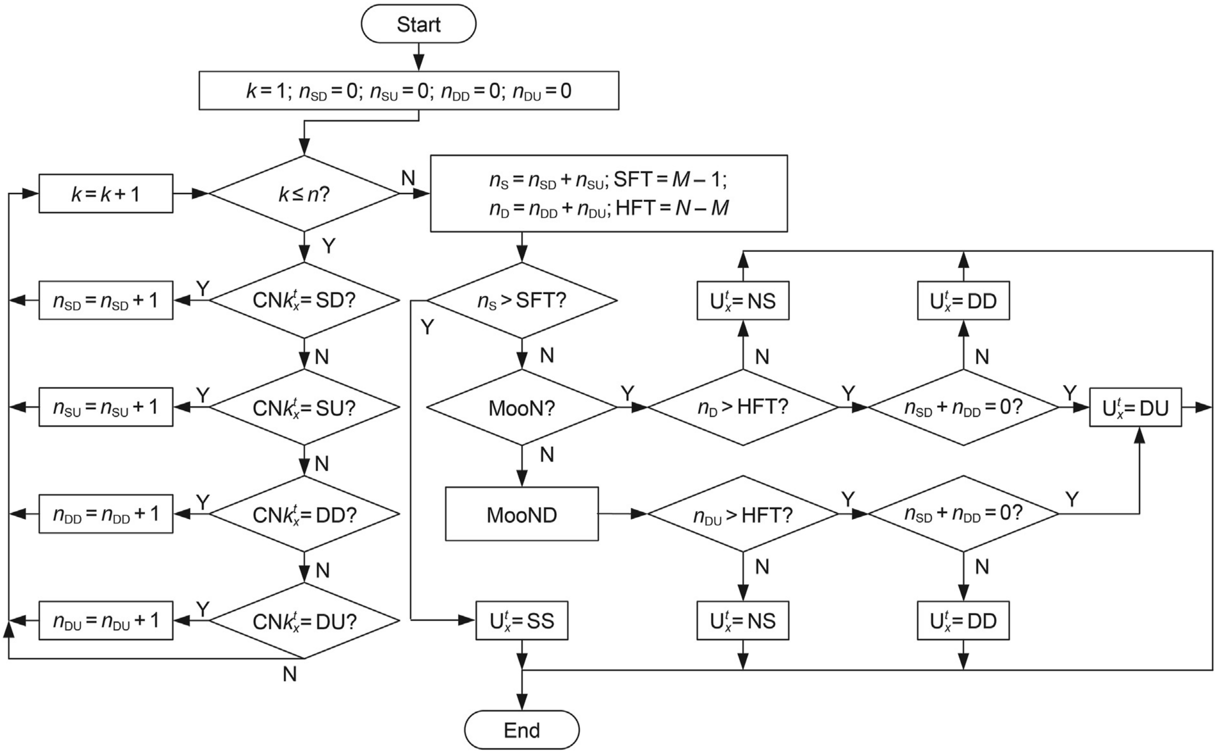

Start
$k=1;\ n_{\mathrm{SD}}=0;\ n_{\mathrm{SU}}=0;\ n_{\mathrm{DD}}=0;\ n_{\mathrm{DU}}=0$
$k=k+1$
$k\leq n?$
N
$n_{\mathrm{S}}=n_{\mathrm{SD}}+n_{\mathrm{SU}};\ \mathrm{SFT}=M-1;$
$n_{\mathrm{D}}=n_{\mathrm{DD}}+n_{\mathrm{DU}};\ \mathrm{HFT}=N-M$
Y
$n_{\mathrm{SD}}=n_{\mathrm{SD}}+1$
$\mathrm{CN}k_x^t=\mathrm{SD}?$
$n_{\mathrm{SU}}=n_{\mathrm{SU}}+1$
$\mathrm{CN}k_x^t=\mathrm{SU}?$
$n_{\mathrm{DD}}=n_{\mathrm{DD}}+1$
$\mathrm{CN}k_x^t=\mathrm{DD}?$
$n_{\mathrm{DU}}=n_{\mathrm{DU}}+1$
$\mathrm{CN}k_x^t=\mathrm{DU}?$
$n_{\mathrm{S}}>\mathrm{SFT}?$
MooN?
MooND
$n_{\mathrm{D}}>\mathrm{HFT}?$
$n_{\mathrm{DU}}>\mathrm{HFT}?$
$n_{\mathrm{SD}}+n_{\mathrm{DD}}=0?$
$n_{\mathrm{SD}}+n_{\mathrm{DD}}=0?$
$\mathrm{U}_x^t=\mathrm{NS}$
$\mathrm{U}_x^t=\mathrm{DD}$
$\mathrm{U}_x^t=\mathrm{DU}$
$\mathrm{U}_x^t=\mathrm{SS}$
$\mathrm{U}_x^t=\mathrm{NS}$
$\mathrm{U}_x^t=\mathrm{DD}$
End

Fig. 5. Conditional probability modeling of nodes U.

stage is shown in Fig. 6. This process represents the degradation, self-diagnosis, and maintenance of independent failure node IF during function inspection test interval stage. This process can be used to model and analyze the structures of heterogeneous

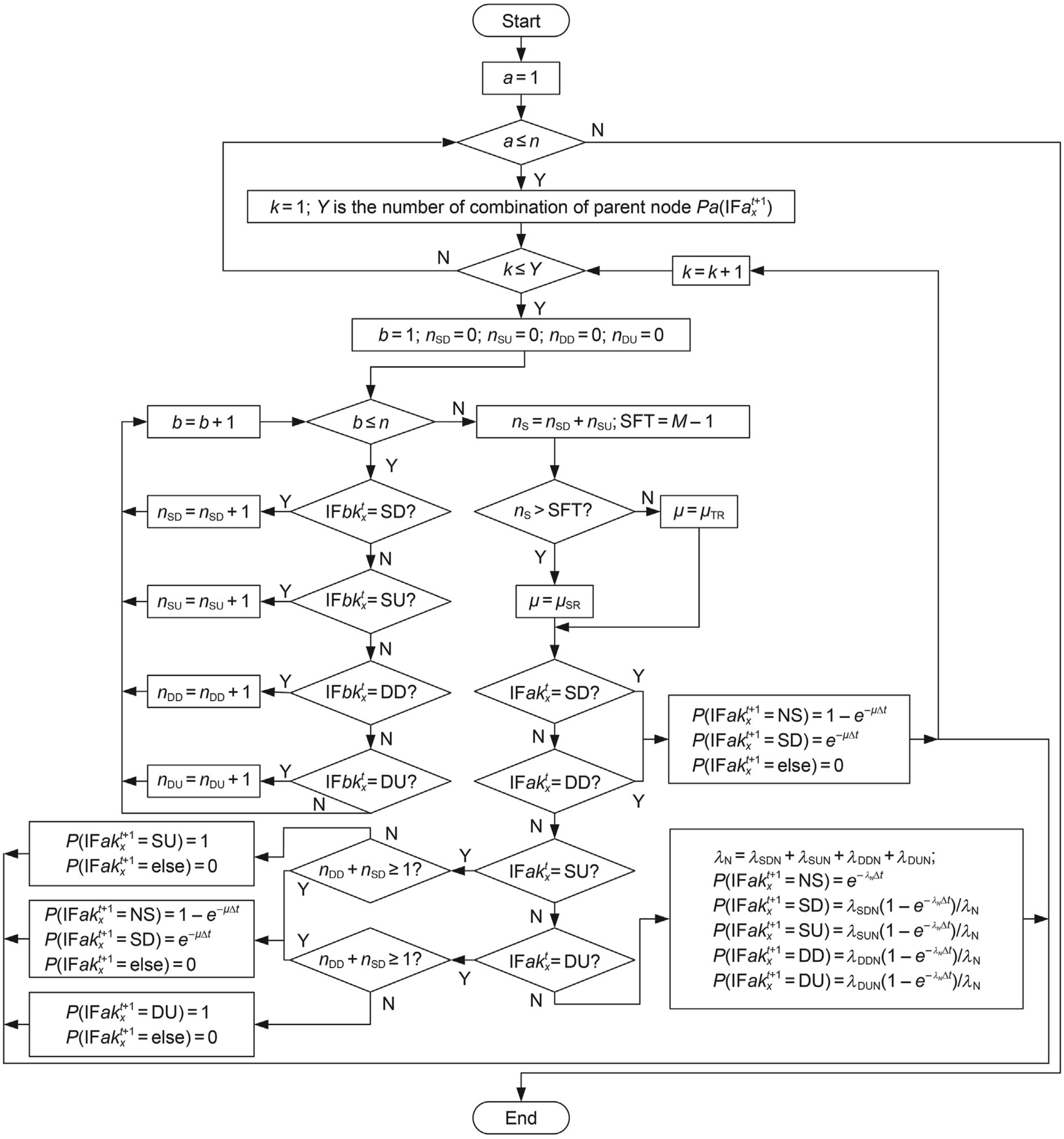

Start
$a = 1$
$a \le n$
N
Y
$k = 1$; Y is the number of combination of parent node $Pa(\mathrm{IF}a_x^{t+1})$
N
$k \le Y$
$k = k + 1$
Y
$b = 1$; $n_{SD} = 0$; $n_{SU} = 0$; $n_{DD} = 0$; $n_{DU} = 0$
$b = b + 1$
$b \le n$
N
$n_S = n_{SD} + n_{SU}$; $SFT = M - 1$
Y
$n_{SD} = n_{SD} + 1$
Y
$\mathrm{IF}bk_x^t = SD?$
$n_S > SFT?$
N
$\mu = \mu_{TR}$
N
Y
$n_{SU} = n_{SU} + 1$
Y
$\mathrm{IF}bk_x^t = SU?$
$\mu = \mu_{SR}$
N
$n_{DD} = n_{DD} + 1$
Y
$\mathrm{IF}bk_x^t = DD?$
$\mathrm{IF}ak_x^t = SD?$
Y
$P(\mathrm{IF}ak_x^{t+1} = NS) = 1 - e^{-\mu\Delta t}$
$P(\mathrm{IF}ak_x^{t+1} = SD) = e^{-\mu\Delta t}$
$P(\mathrm{IF}ak_x^{t+1} = else) = 0$
N
N
$n_{DU} = n_{DU} + 1$
Y
$\mathrm{IF}bk_x^t = DU?$
$\mathrm{IF}ak_x^t = DD?$
N
Y
$P(\mathrm{IF}ak_x^{t+1} = SU) = 1$
$P(\mathrm{IF}ak_x^{t+1} = else) = 0$
N
N
$n_{DD} + n_{SD} \ge 1?$
Y
$\mathrm{IF}ak_x^t = SU?$
Y
$\lambda_N = \lambda_{SDN} + \lambda_{SUN} + \lambda_{DDN} + \lambda_{DUN}$;
$P(\mathrm{IF}ak_x^{t+1} = NS) = e^{-\lambda_N\Delta t}$
$P(\mathrm{IF}ak_x^{t+1} = SD) = \lambda_{SDN}(1 - e^{-\lambda_N\Delta t})/\lambda_N$
$P(\mathrm{IF}ak_x^{t+1} = SU) = \lambda_{SUN}(1 - e^{-\lambda_N\Delta t})/\lambda_N$
$P(\mathrm{IF}ak_x^{t+1} = DD) = \lambda_{DDN}(1 - e^{-\lambda_N\Delta t})/\lambda_N$
$P(\mathrm{IF}ak_x^{t+1} = DU) = \lambda_{DUN}(1 - e^{-\lambda_N\Delta t})/\lambda_N$
$P(\mathrm{IF}ak_x^{t+1} = NS) = 1 - e^{-\mu\Delta t}$
$P(\mathrm{IF}ak_x^{t+1} = SD) = e^{-\mu\Delta t}$
$P(\mathrm{IF}ak_x^{t+1} = else) = 0$
N
Y
$n_{DD} + n_{SD} \ge 1?$
$\mathrm{IF}ak_x^t = DU?$
Y
N
N
$P(\mathrm{IF}ak_x^{t+1} = DU) = 1$
$P(\mathrm{IF}ak_x^{t+1} = else) = 0$
End

Fig. 6. Conditional probability of nodes IF during function inspection test interval stage.

redundant architecture and special degradation.

The process of establishing the conditional probability of common cause failure node CF during function inspection test interval stage is shown in Fig. 7. This process represents the degradation, self-diagnosis, and maintenance of common cause failure node CF during function inspection test interval stage. It can be used to model and analyze the complex degradation and the influence of common cause failure.

2.2.3. Conditional probability in function inspection test stage

The function inspection test is mainly affected by test coverage rate ε, maintenance parameters, and degradation parameters. The maintenance parameters of function inspection test can be specifically divided into maintenance rate of safety detected failure μ_{SD}, maintenance rate of safety undetected failure μ_{SU}, maintenance rate of dangerous detected failure μ_{DD}, and maintenance rate of dangerous undetected failure μ_{DU}. The degradation parameters of function inspection test can be specifically divided into degradation rate of safety detected failure γ_{SD}, degradation rate of safety undetected failure γ_{SU}, degradation rate of dangerous detected failure γ_{DD}, and degradation rate of dangerous undetected failure γ_{DU}.

The conditional probability table of nodes during the function inspection test stage is shown in Table 1, where $\gamma = \gamma_{SD}+\gamma_{SU}+\gamma_{DD}+\gamma_{DU}$.

2.3. SIL determination with parameter uncertainty

The SIL determination with parameter uncertainty is shown in Fig. 8. This process combines the multistage DBNs and Monte Carlo simulation (Zou et al., 2019; Innal et al., 2016; Gao et al., 2019;

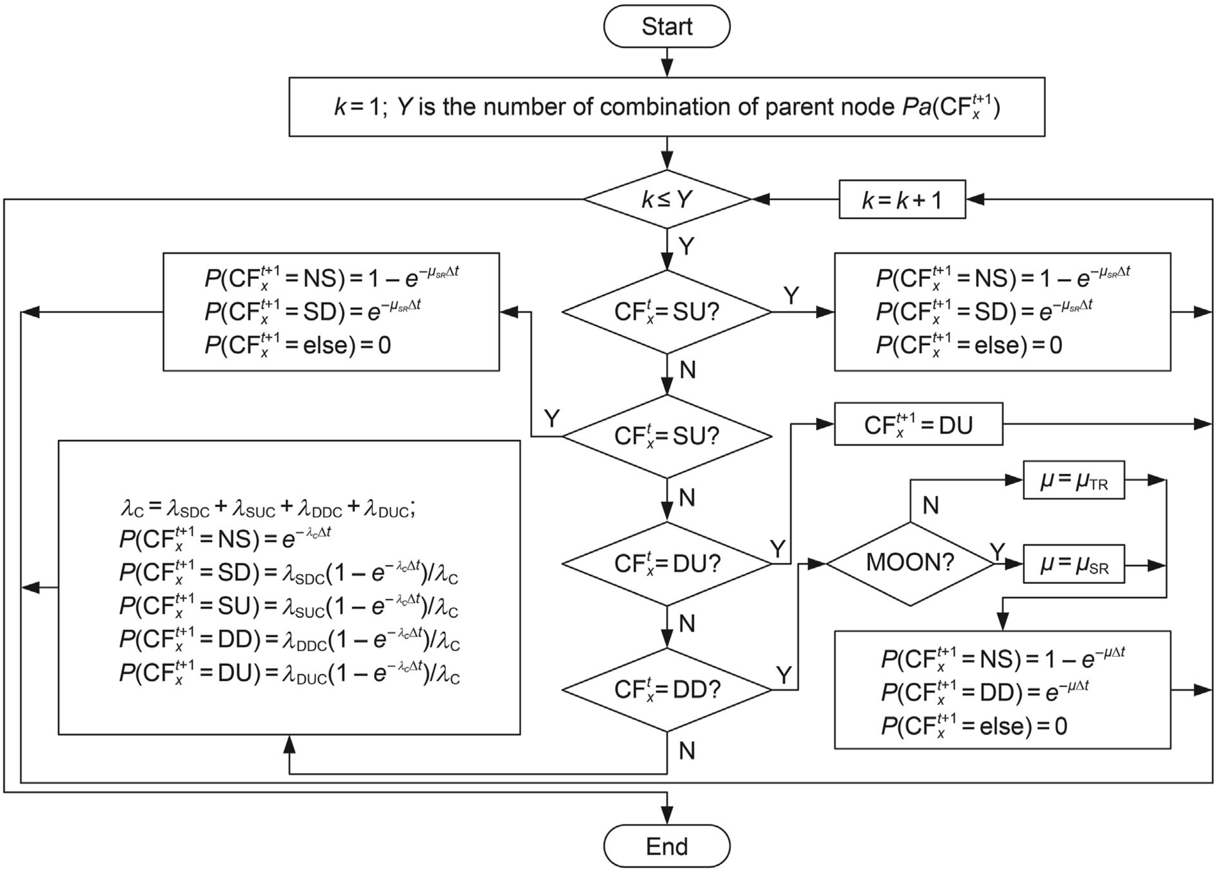

Start
k = 1; Y is the number of combination of parent node Pa(CF$_x^{t+1}$)
k ≤ Y
k = k + 1
Y
CF$_x^t$ = SU?
Y
P(CF$_x^{t+1}$ = NS) = 1 − e$^{-\mu_{SR}\Delta t}$
P(CF$_x^{t+1}$ = SD) = e$^{-\mu_{SR}\Delta t}$
P(CF$_x^{t+1}$ = else) = 0
N
CF$_x^t$ = SU?
Y
P(CF$_x^{t+1}$ = NS) = 1 − e$^{-\mu_{SR}\Delta t}$
P(CF$_x^{t+1}$ = SD) = e$^{-\mu_{SR}\Delta t}$
P(CF$_x^{t+1}$ = else) = 0
N
CF$_x^t$ = DU?
Y
CF$_x^{t+1}$ = DU
N
CF$_x^t$ = DD?
Y
MOON?
N
μ = μ$_{TR}$
Y
μ = μ$_{SR}$
P(CF$_x^{t+1}$ = NS) = 1 − e$^{-\mu\Delta t}$
P(CF$_x^{t+1}$ = DD) = e$^{-\mu\Delta t}$
P(CF$_x^{t+1}$ = else) = 0
N
λ$_C$ = λ$_{SDC}$ + λ$_{SUC}$ + λ$_{DDC}$ + λ$_{DUC}$;
P(CF$_x^{t+1}$ = NS) = e$^{-\lambda_C\Delta t}$
P(CF$_x^{t+1}$ = SD) = λ$_{SDC}$(1 − e$^{-\lambda_C\Delta t}$)/λ$_C$
P(CF$_x^{t+1}$ = SU) = λ$_{SUC}$(1 − e$^{-\lambda_C\Delta t}$)/λ$_C$
P(CF$_x^{t+1}$ = DD) = λ$_{DDC}$(1 − e$^{-\lambda_C\Delta t}$)/λ$_C$
P(CF$_x^{t+1}$ = DU) = λ$_{DUC}$(1 − e$^{-\lambda_C\Delta t}$)/λ$_C$
End

Fig. 7. Conditional probability of nodes CF during function inspection test interval stage.

Table 1
Conditional probability table of nodes during function inspection test stage.

Before function inspection test	After function inspection test				
	NS	SD	SU	DD	DU
NS	$1-\gamma$	γ_{SD}	γ_{SU}	γ_{DD}	γ_{DU}
SD	μ_{SD}	$1-\mu_{SD}$	0	0	0
SU	μ_{SU}	$(1-\mu_{SU})\varepsilon$	$(1-\mu_{SU})(1-\varepsilon)$	0	0
DD	μ_{DD}	0	0	$1-\mu_{DD}$	0
DU	μ_{DU}	0	0	$(1-\mu_{DU})\varepsilon$	$(1-\mu_{DU})(1-\varepsilon)$

Kaczor et al., 2016; Chen et al., 2020; Koneshloo et al., 2018).

Expert assessment is used to calculate the parameter range for the equipment. Expert assessment mainly uses fuzzy number to express the parameters. It integrates the evaluation data of experts by using an ordered weighted average algorithm.

Expert assessment is based on triangular fuzzy number theory. The form of triangular fuzzy number is $\tilde{T}_f = (T_f^L, T_f^M, T_f^U)$, where *TL f* represents the lower limit of the fuzzy interval, *TM f* represents the intermediate value of the fuzzy interval, and *TU f* represents the upper limit of the fuzzy interval. The greater the difference between *TL f* (*TU f*) and *TM f*, the greater the fuzziness of the data. When *TL f* = *TM f* = *TU f*, the data become accurate. If *n* experts assess the parameters of the equipment, the triangular fuzzy number of the *k*'th expert assessment value is $\tilde{T}_f = (T_f^L, T_f^M, T_f^U)$. The assessment process is as follows.

Step 1: Calculate the arithmetic average $\tilde{T}_a = (T_a^L, T_a^M, T_a^U)$ of the expert's assessment. *TL a TM a*, and *TU a* are expressed as follows:

$$T_a^L = \frac{\sum_{k=1}^{n} T_k^L}{n}, T_a^M = \frac{\sum_{k=1}^{n} T_k^M}{n}, T_a^U = \frac{\sum_{k=1}^{n} T_k^U}{n}, k = 1, 2, 3, \ldots\ldots \tag{1}$$

Step 2: Calculate distance measure $d(\tilde{T}_{\mathrm{k}}, \tilde{T}_a)$ between each expert's assessment result and arithmetic average $d(\tilde{T}_{\mathrm{k}}, \tilde{T}_a)$ is as follows:

$$d\left(\tilde{T}_{\mathrm{k}}, \tilde{T}_a\right) = \left(\left|T_k^L - T_{\mathrm{a}}^L\right| + \left|T_k^M - T_{\mathrm{a}}^M\right| + \left|T_k^U - T_{\mathrm{a}}^U\right|\right) \Big/ 3. \tag{2}$$

Step 3: Calculate the similarity of each expert's assessment, and $s(\tilde{T}_{\mathrm{k}}, \tilde{T}_a)$ is expressed as follows:

$$s\left(\tilde{T}_{\mathrm{k}}, \tilde{T}_a\right) = 1 - \frac{\mathrm{d}\left(\tilde{T}_{\mathrm{k}}, \tilde{T}_a\right)}{\sum_{k=1}^{n} \mathrm{d}\left(\tilde{T}_{\mathrm{k}}, \tilde{T}_a\right)}. \tag{3}$$

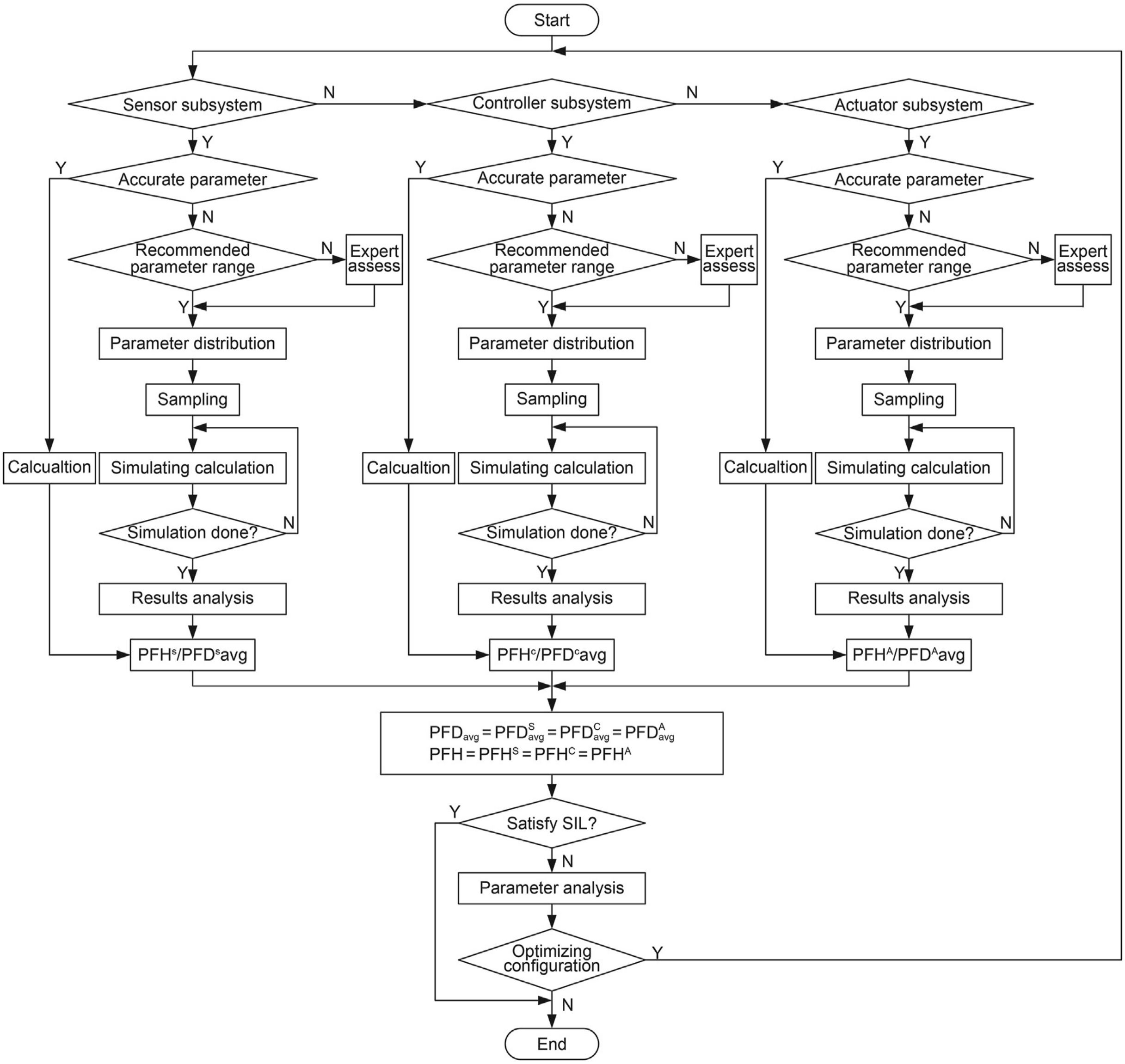


Fig. 8. SIL determination with parameter uncertainty.

Step 4: Calculate the weight coefficient w_k of each expert's assessment and obtain the assessment results $\tilde{T}$. $\tilde{T}$ is expressed as follows:

$$\tilde{T} = \left(T^L, T^M, T^U\right) = \sum_{k=1}^{n} w_k \tilde{T}_k = \tilde{T}_k \sum_{k=1}^{n} \frac{s\left(\tilde{T}_k, \tilde{T}_a\right)}{\sum\limits_{k=1}^{n} s\left(\tilde{T}_k, \tilde{T}_a\right)} \tilde{T}_k \cdot \tag{4}$$

3. Case study

3.1. Modeling of a high-pressure SIS in the export of oil well platform

Oil platforms work in harsh environments, such as permanent frozen zone, deep sea, and desert. The operation of oil well platform requires high safety and availability. The coordination of SISs ensures the safe operation of the platform. The design and validation of the SISs of platform must strive for enhanced safety at low cost (Zhang and Hu, 2013; Zhang et al., 2019; Hu et al., 2014; Eshiet and Sheng, 2018).

A platform contains multiple oil wells. Each well contains multiple safety instrumentation functions (SIF): high-pressure SIF, low-pressure SIF, high-flow SIF, low-flow SIF, and gas detection SIF. A single SIS can perform multiple SIFs. Fig. 9 shows a typical high-pressure SIS in the export of oil well platform. The function of the SIS is to shut down the system when an abnormal high pressure occurs in the oil pipeline.

The block diagram of high-pressure SIS in the export of oil well platform is shown in Fig. 10. The high-pressure SIS is mainly composed of a sensor subsystem, a controller subsystem, and an actuator subsystem. When the two pressure transmitters installed by 1oo2 architecture detect abnormal high pressure in the oil pipeline, they send a signal to the safety programmable logic controller (SPLC) through the impulse line and the analog input channel. The SPLC includes analog input processing, main

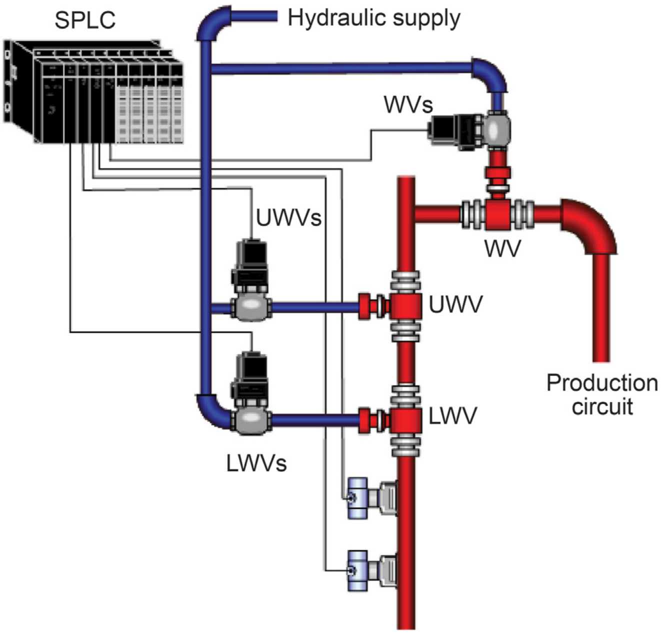


Fig. 9. Typical high-pressure SIS in the export of oil well platform.

processing, and digital output processing. The SPLC sends a closing instruction to the electromagnetic valve (EV) through the digital output channel. The lower main shut-off EV (LMVs), upper main shut-off EV (UMVs), and wing EV (WVs) are installed by 1oo3 architecture. The EV controls the corresponding ball valve (BV) to close the pipeline. The lower main shut-off BV (LMV), upper main shut-off BV (UMV), and wing BV (WV) are installed by 1oo3 architecture.

The sensor subsystem is composed of a pressure transmitter (PT) cell, an impulse line (IMP) cell, and a safety programmable logic controller analog input channel (SPLCIC) cell. The PT cell is composed of two pressure transmitters installed with 1oo2 architecture. The uncertain parameter failure rate (λ_T/h^{-1}) of pressure transmitters obeys lognormal distribution λ_T ~ log N (−13.475, 0.18645). The IMP cell is composed of an impulse line installed with 1oo1 architecture.The uncertain parameter λ_T of impulse line obeys lognormal distribution λ_T ~ log N (−15.249, 0.15792). The SPLCIC cell is composed of an analog input channel installed with 1oo1 architecture. The uncertain parameter mean time to system restoration (*MTSR*/h) of analog input channel obeys uniform distribution *MTSR* ~ unif (43.2, 100.8).

The controller subsystem is composed of a safety programmable logic controller analog input processing (SPLCIP) cell, a safety programmable logic controller main processing (SPLCMP) cell, and a safety programmable logic controller digital output processing

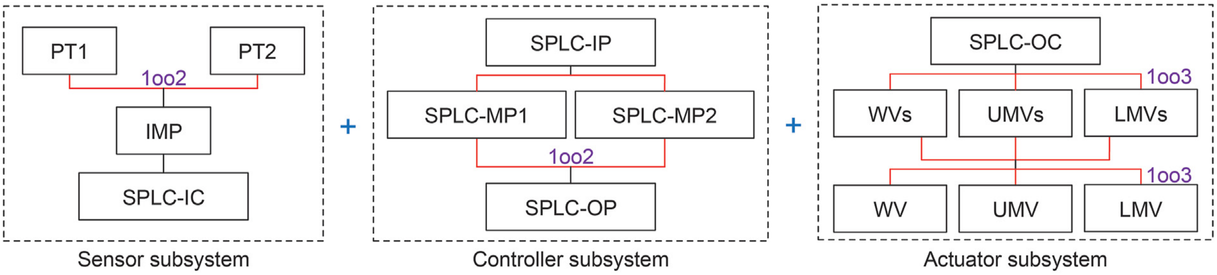


Fig. 10. Block diagram of high-pressure SIS in the export of oil well platform.

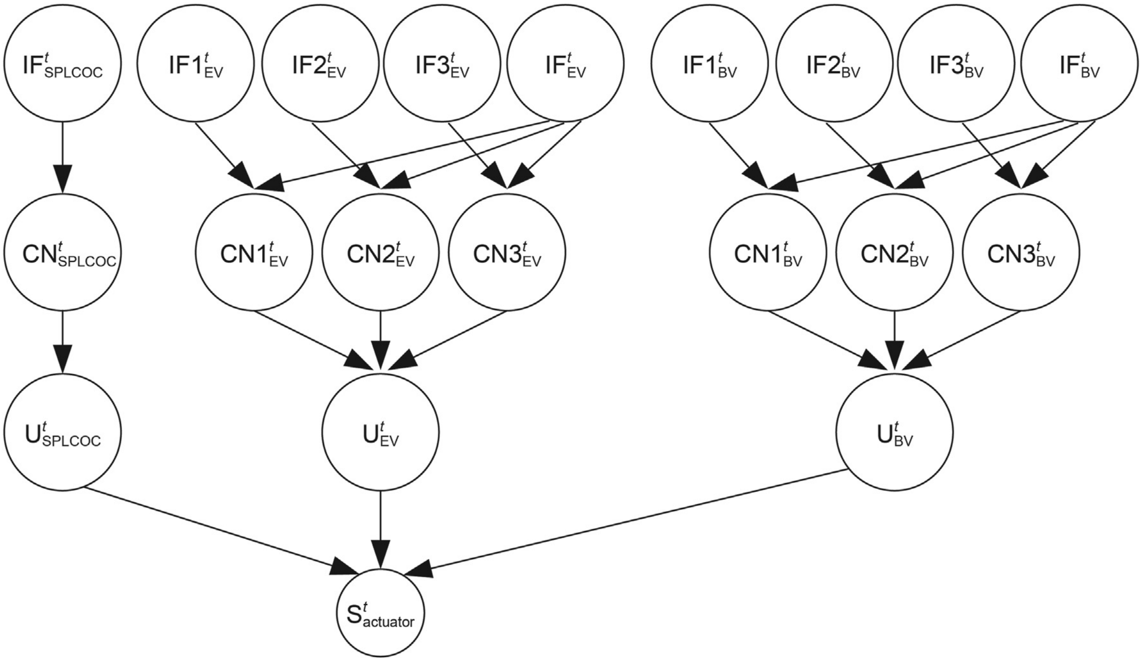


Fig. 11. Time slice topology of actuator subsystem with BNs.

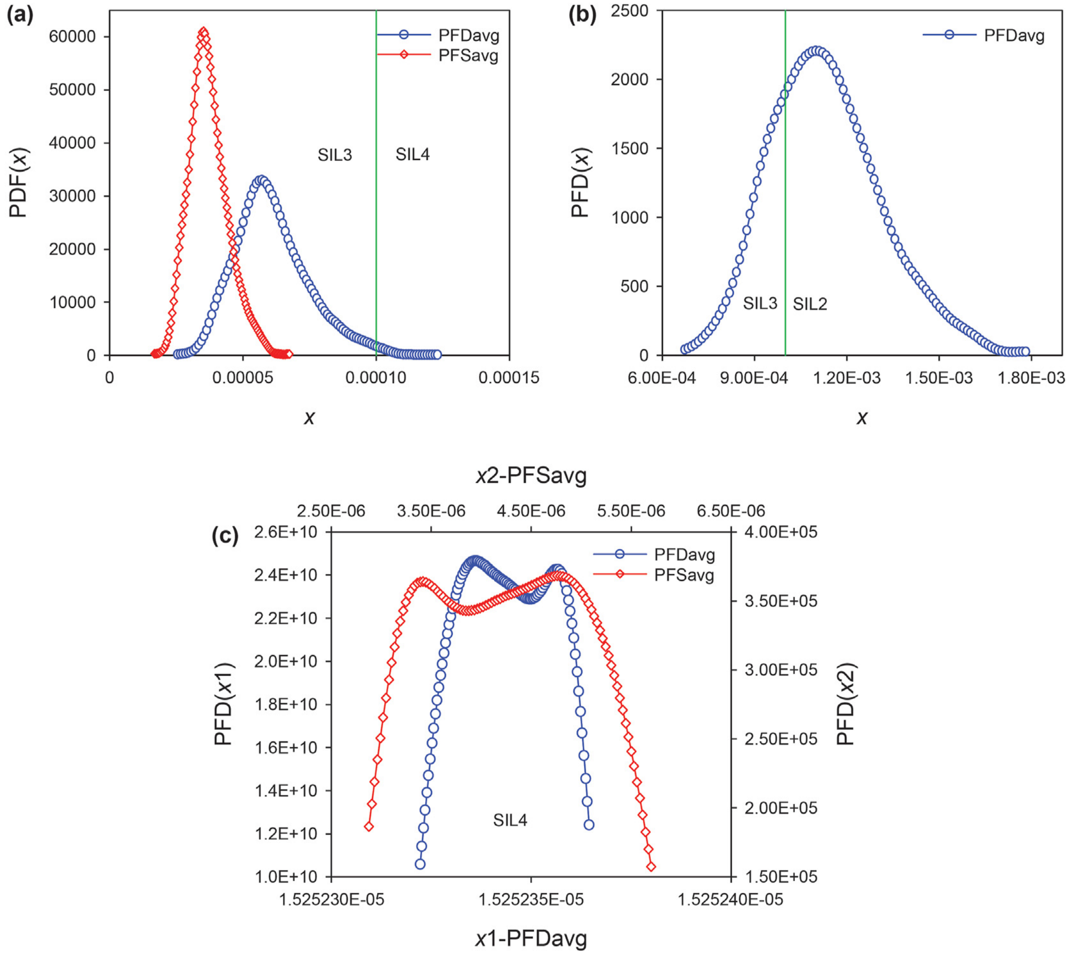


Fig. 12. Probability density function of single cell of the sensor subsystem **a** PT cell, **b** IMP cell, and **c** SPLCIC cell.

Table 2
Interval estimation of PFD_{avg} and PFS_{avg} in single cell of sensor subsystem.

Subsystem cell	PFD_{avg}	PFS_{avg}
PT cell	$[3.74 \times 10^{-5}, 5.71 \times 10^{-5}, 9.45 \times 10^{-5}]$	$[2.45 \times 10^{-5}, 3.53 \times 10^{-5}, 5.41 \times 10^{-5}]$
IMP cell	$[8.07 \times 10^{-4}, 1.10 \times 10^{-3}, 1.55 \times 10^{-3}]$	–
SPLCIC cell	1.52×10^{-5}	$[2.96 \times 10^{-6}, 4.76 \times 10^{-6}, 5.59 \times 10^{-6}]$

(SPLCOP) cell. The SPLCIP cell is composed of an analog input processor installed with 1oo1 architecture. The uncertain parameter *MTSR* of analog input processor obeys uniform distribution *MTSR* ~ unif (50.4, 93.6). The SPLCMP cell is composed of two main processors installed with 1oo2 architecture. The uncertain parameter λ_T of main processors obeys lognormal distribution λ_T ~ log*N* (−11.337, 0.15792). The SPLCOP cell is composed of a digital output processor installed with 1oo1 architecture. The uncertain parameter hazard failure diagnostic coverage (C_D) of digital output processor obeys normal distribution C_D ~ norm (0.8, 0.05).

The actuator subsystem is composed of a safety programmable logic controller digital output channel (SPLCOC) cell, an EV cell, and a BV cell. The SPLCOC cell is composed of a digital output channel installed with 1oo1 architecture, and the uncertain parameter mean time to repair *MTTR* (*h*) of digital output channel obeys uniform distribution *MTTR* ~ unif (19.2, 28.8). The EV cell is composed of three EVs installed with 1oo3 architecture, and the uncertain parameter failure rate λ_T of EVs obeys lognormal distribution λ_T ~ log*N* (−12.071, 0.15792). The BV cell is composed of three BVs installed with 1oo3 architecture, and the uncertain parameter failure rate λ_T of BVs obeys lognormal distribution λ_T ~ log*N* (−12.867, 0.17333).

The time slice topology of actuator subsystem with BNs is shown in Fig. 11. The SPLCOC cell is a single-channel 1 out of 1 architecture. The EV cell is 1 out of 3 architecture consisting of LMVs, UMVs, and WVs. The BV cell is 1 out of 3 architecture consisting of LMV, UMV, and WV. The nodes of the actuator subsystem model are described as follows.

The failure factor of the first layer consist of nine nodes. The nodes are SPLCOC channel independent failure (single-channel equipment does not consider common cause failure), LMV channel independent failure, UMV channel independent failure node, WV channel independent failure node, EV cell common cause failure, LMV channel independent failure, UMV channel independent failure node, WV channel independent failure node, and EV cell common cause failure nodes. The channel state nodes consists of seven nodes. The nodes are SPLCOC channel state, LMV channel state, UMV channel state, WV channel state, LMV channel state,

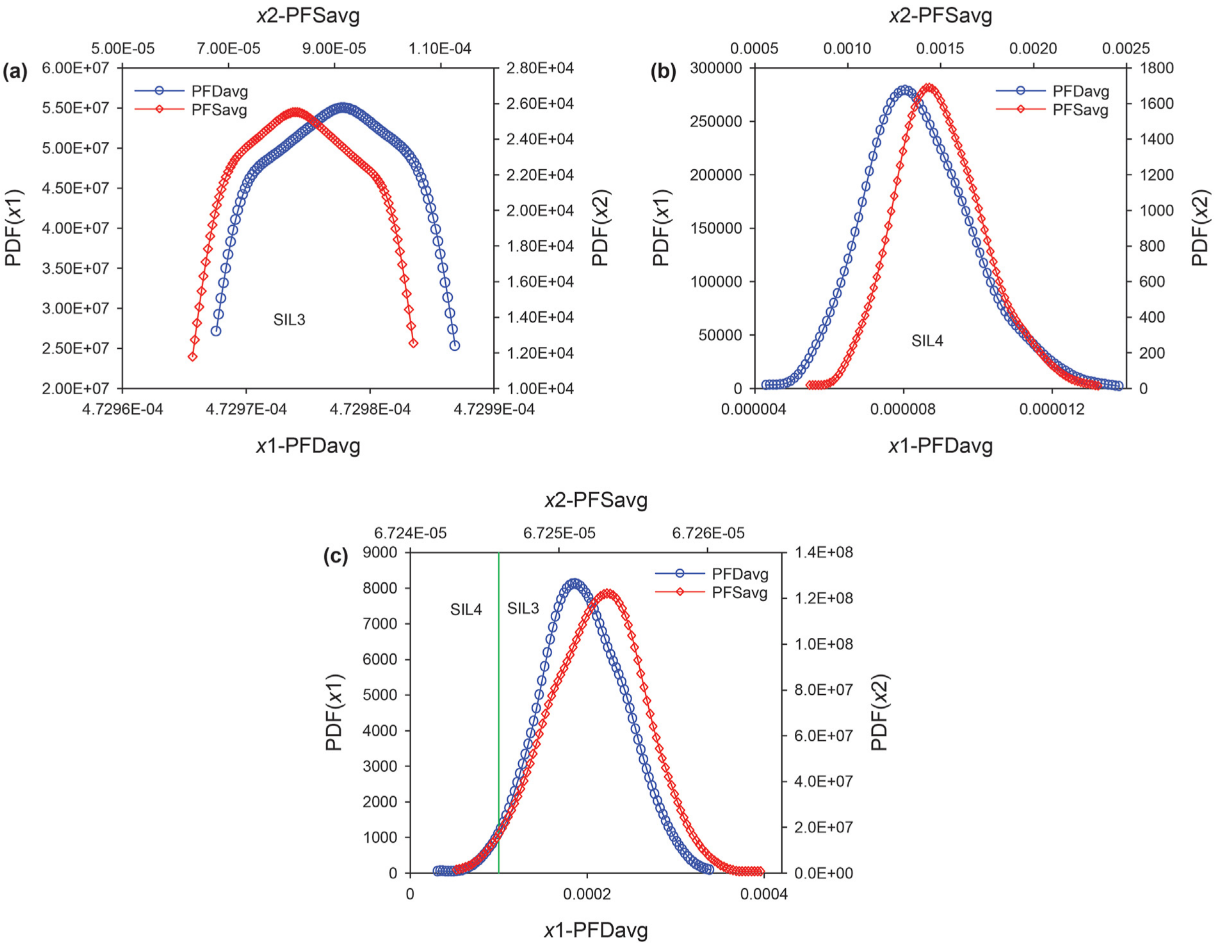


Fig. 13. Probability density function of a single cell of the controller subsystem **a** SPLCIP cell, **b** SPLCMP cell, and **c** SPLCOP cell.

Table 3
Interval estimation of PFD_{avg} and PFS_{avg} in single cell of controller subsystem.

Subsystem's cell	PFD_{avg}	PFS_{avg}
SPLCIP cell	4.72×10^{-4}	$[6.44 \times 10^{-5}, 8.25 \times 10^{-5}, 1.04 \times 10^{-4}]$
SPLCMP cell	$[5.74 \times 10^{-6}, 8.04 \times 10^{-6}, 1.18 \times 10^{-5}]$	$[1.05 \times 10^{-3}, 1.44 \times 10^{-3}, 2.03 \times 10^{-3}]$
SPLCOP cell	$[1.02 \times 10^{-4}, 1.86 \times 10^{-4}, 2.92 \times 10^{-4}]$	$[6.7241 \times 10^{-5}, 6.7248 \times 10^{-5}]$ $6.7254 \times 10^{-5}]$

UMV channel state, and WV channel state nodes. The cell state nodes consists of three nodes. The nodes are SPLCOC cell state, EV cell state, and BV cell state nodes. The system state node layer is the state node of the actuator subsystem.

3.2. Results and discussions

The research results are obtained through Monte Carlo simulation by using the established multistage DBNs.The simulation number is set as $N = 10^3$ to ensure the accuracy of the test samples. The results are statistically analyzed as follows.

3.2.1. Results and analysis of sensor subsystem

The average of failure probability on demand (PFD_{avg}) is the evaluation parameter of SIL under low demand mode. The average of safe failure probability (PFS_{avg}) is the evaluation parameter of availability. The probability density functions of PFD_{avg} and PFS_{avg} of single cell of the sensor subsystem are shown in Fig. 12. When the confidence degree is 5%, the upper limit, mean value, and lower limit of interval estimation of PFD_{avg} and PFS_{avg} in single cell of the sensor subsystem are given in Table 2.

In the confidence interval, the SIL of the PT cell is SIL4, the SIL of the IMP cell is SIL3-SIL2, and the SIL of the SPLCIC cell is SIL4. The SIL of the SPLCIC cell is the highest in the sensor subsystem. The cell that restricts the SIL of the sensor subsystem is the IMP cell. No safety failures occur in the IMP cell. The cell that restricts the availability of the sensor subsystem is the PT cell. The availability of SPLCIC cell is higher than the PT cell. The uncertainty of λ_T has great influence on the SIL and availability determination results in the sensor subsystem. As shown in Fig. 12c, the uncertain parameter *MTSR* has minimal influence on the SIL determination of the SPLCIC cell and can be ignored. However, it affects availability. Therefore, parameter uncertainty has different effects on the SIL and availability determination in the SISs. Thus, determining the SIL and availability of SISs at the same time is valuable.

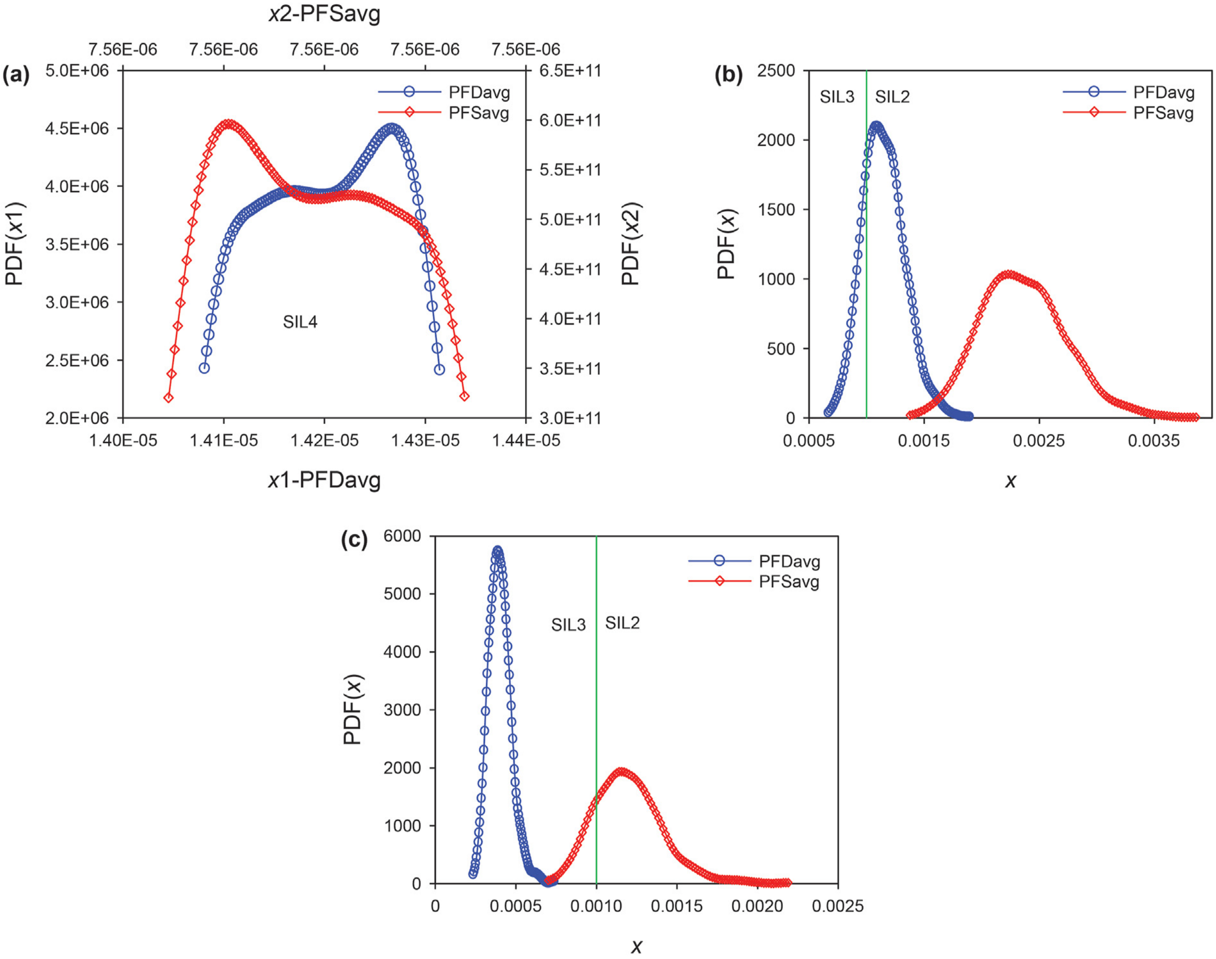


Fig. 14. Probability density function of a single cell of the actuator subsystem **a** SPLCOC cell, **b** EV cell, and **c** BV cell.

Table 4
Interval estimation of PFD_{avg} and PFS_{avg} in single cell of actuator subsystem.

Subsystem's cell	PFD_{avg}	PFS_{avg}
SPLCOC cell	[1.409×10^{-5}, 1.427×10^{-5}, 1.431×10^{-5}]	7.56×10^{-6}
EV cell	[8.02×10^{-4}, 1.09×10^{-3}, 1.56×10^{-3}]	[1.68×10^{-3}, 2.23×10^{-3}, 3.18×10^{-3}]
BV cell	[2.76×10^{-4}, 3.89×10^{-4}, 5.63×10^{-4}]	[8.23×10^{-4}, 1.16×10^{-3}, 1.67×10^{-3}]

3.2.2. Results and analysis of controller subsystem

The probability density function of PFD_{avg} and the PFS_{avg} of single cell of the controller subsystem are shown in Fig. 13. When the confidence degree is 5%, the upper limit, mean value, and lower limit of the interval estimation of PFD_{avg} and PFS_{avg} in the single cell of the controller subsystem are given in Table 3.

In the confidence interval, the SIL of the SPLCIP cell is SIL3, the SIL of the SPLCMP cell is SIL4, and the SIL of the SPLCOP cell is SIL3. The SIL of the SPLCMP cell is the highest in the controller subsystem. The cell that restricts the SIL of the controller subsystem is the SPLCIP cell. Compared with the uncertainty of *MTSR*, C_D, and λ_T in the controller subsystem, the uncertainty of C_D has greater influence on the SIL determination, and the uncertainty of *MTSR* has a lower influence. The cell that restricts the availability of the controller subsystem is the SPLCMP cell. Therefore, the architecture 1oo2 improves the SIL and reduces the availability of the cell. Compared with the uncertainty of *MTSR*, C_D, and λ_T in the controller subsystem, the uncertainty of λ_T has a greater influence on the availability, and the uncertainty of C_D has a lower influence.

3.2.3. Results and analysis of actuator subsystem

The probability density function of PFD_{avg} and the PFS_{avg} of a single cell of the actuator subsystem are shown in Fig. 14. When the confidence degree is 5%, the upper limit, mean value, and lower limit of the interval estimation of PFD_{avg} and PFS_{avg} in single cell of the actuator subsystem are given in Table 4.

In the confidence interval, the SIL of the SPLCOC cell is SIL4, the SIL of the EV cell is SIL3-SIL2, and the SIL of the BV cell is SIL3. The SIL of the SPLCOC cell is the highest in the controller subsystem. The cell that restricts the SIL and availability of the actuator subsystem is the EV cell. Therefore, the EV cell is the most crucial part for strengthening the actuator subsystem. The SIL and availability of EV cell can be improved by replacing parts with low failure rate or selecting a suitable architecture. Compared with the uncertainty of *MTTR* and λ_T in the actuator subsystem, the uncertainty of λ_T has a greater influence on the SIL and availability determination. The uncertainty of *MTTR* has small influence on SIL and availability determination. The uncertainty parameters of the EV cell and BV cell are λ_T, and the BV cell is more affected by uncertainty parameter λ_T.

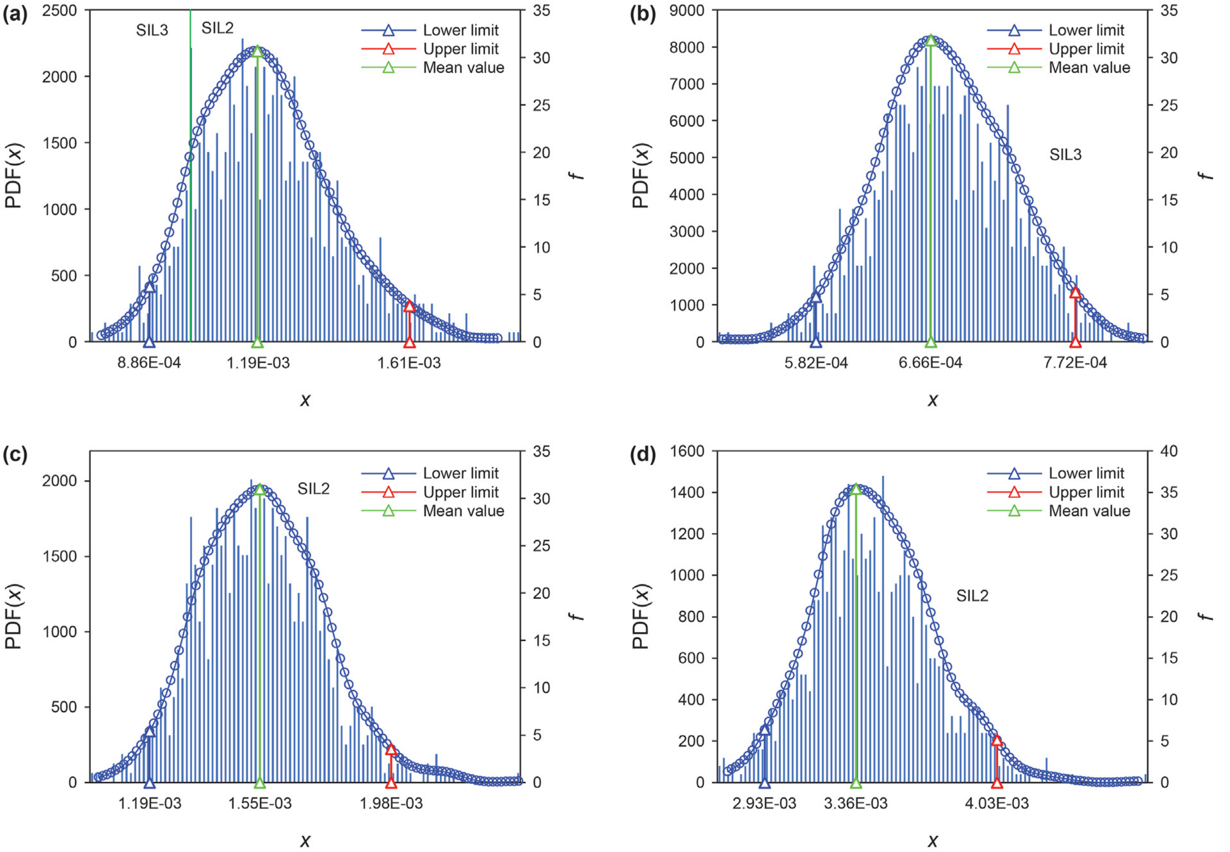


Fig. 15. *PFD*$_{avg}$ statistical histogram and probability density function of the SIS and a singlesubsystem **a** sensor subsystem, **b** controller subsystem, **c** actuator subsystem, and **d** SIS.

3.2.4. Results and analysis of the SIS

The *PFD*$_{avg}$ statistical histogram and probability density function of the SIS and single subsystem are shown in Fig. 15. When the confidence degree is 5%, the upper limit, mean value, and lower limit of the interval estimation of *PFD*$_{avg}$ of the SIS and single subsystem are shown. The SIL of the sensor subsystem is SIL3-SIL2, and most of the intervals are at SIL2. The SIL of the controller subsystem is SIL3, the SIL of the actuator subsystem is SIL2, and the SIL of the SIS is SIL2. The SIL of the sensor subsystem is most affected by uncertainty parameters. The controller subsystem is least affected by uncertainty parameters during the SIL determination. The actuator subsystem has the greatest influence on the SIL determination of the SIS. The controller subsystem has the least influence on the SIL determination of the SIS.

The *PFS*$_{avg}$ statistical histogram and probability density function of the SIS and single subsystem are shown in Fig. 16. When the confidence degree is 5%, the upper limit, mean value, and lower limit of the interval estimation of *PFS*$_{avg}$ of the SIS and single subsystem are shown. The availability of the sensor subsystem is most affected by uncertainty parameters. Therefore, the SIS should focus on the parameter uncertainty on the sensor subsystem. The actuator subsystem is least affected by uncertainty parameters for availability. The actuator subsystem has the greatest influence on the availability of the SIS. The sensor subsystem has the least influence on the availability of the SIS. Combined with the previously analyzed results, the EV cell of the actuator subsystem have the lowest SIL and availability. Thus, the EV should be optimized first in the SIS.

Fig. 17 shows the *PFD*$_{avg}$/*PFD* and *PFS*$_{avg}$/*PFS* of the SIS with the change in running time. The increase in SIL and availability of the SIS is modest after the first year. This condition is because the inspection test and maintenance rates of components are assumed to be higher than 90%. With long running time of the SIS, the SIL and availability can be inferred from the image.

4. SIL determination software development

A user-friendly SIL determination software with parameter uncertainty is developed on MATLAB graphical user interface. The SIL and availability of SIS and its subsystems can be determined on the software by using the proposed method in Section 2. The software is suitable for multiple redundant cells, such as a subsystem composed by 1oo2, 1oo1, and 1oo3. It mainly consists of main and calculation interfaces. As shown in Fig. 18, the SIL and availability of the high-pressure SIS in the export of oil well platform are determined in the main interface. The SIL and availability of single subsystem are calculated separately, and the percentage of each cell's influence on the subsystem SIL and availability is displayed. As shown in Fig. 19, the SIL and availability of redundant architecture with uncertain parameter λ are determined in the calculation interface. The interface is different for different uncertain parameters. The redundant architecture and uncertain parameter of a single cell are selected in the main interface. Parameter, such as failure parameter, maintenance parameter, degradation parameter, test coverage rate, and confidence degree, are inputted in the calculation interface. After calculation, the values of *PFD*$_{avg}$ and *PFS*$_{avg}$ of the cell are outputted, and the probability density function curves of *PFD*$_{avg}$ and *PFS*$_{avg}$ are displayed.

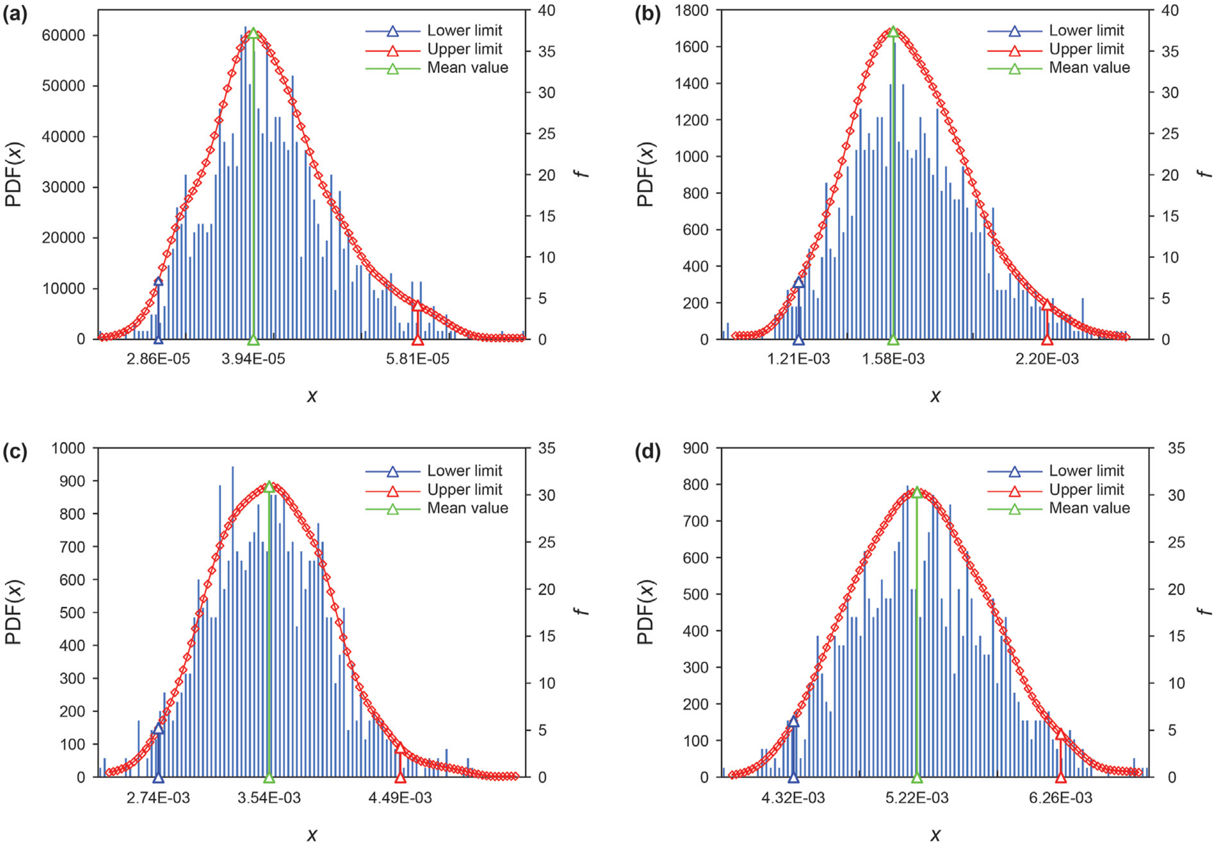


Fig. 16. PFS_{avg} statistical histogram and probability density function of the SIS and a single subsystem **a** sensor subsystem, **b** controller subsystem, **c** actuator subsystem, and **d** SIS.

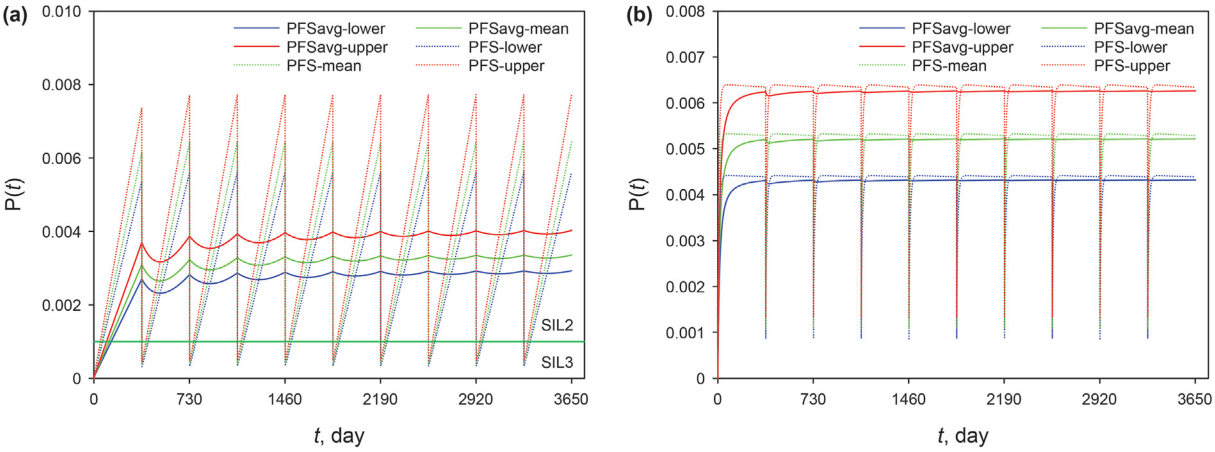
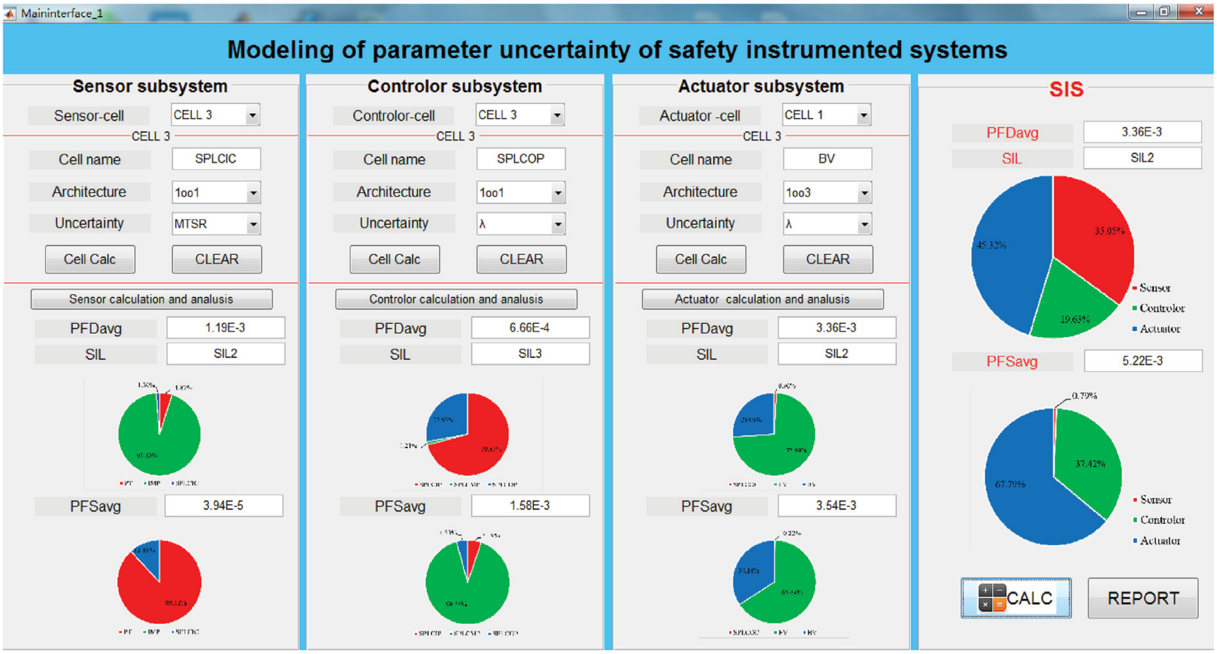


Fig. 17. PFD_{avg}/PFD and PFS_{avg}/PFS of the SIS subsystem **a** PFD_{avg}/PFD and **b** PFS_{avg}/PFS.

5. Conclusion

This study proposes a novel SIL determination methodology of SISs with parameter uncertainty by combining multistage DBNs and Monte Carlo simulation. This methodology can solve the SIL determination problem with parameter uncertainty of multicell redundant architecture and is applicable to common Moon architectures. A high-pressure SIS in the export of oil wellplatform is adopted to demonstrate the application of the proposed approach. The results show that the SIL of the high-pressure SIS is SIL2. The SIL of the sensor subsystem is most affected by uncertainty parameters. The availability of the sensor subsystem is most affected by uncertainty parameters. The actuator subsystem has the greatest influence on the SIL and availability of high-pressure SIS. Comparing the SIL and availability results of single subsystem and single cell with different uncertain parameters, the uncertainty of maintenance parameters *MTTR* and *MTSR* has small effect on the determination results. Although some cells, such as IMP units in the sensor subsystem, are easily overlooked in the general evaluation, they have important effects on the SIL and availability of SIS. The results show that the proposed methodology can be used to calculate the SIL and availability of SISs with multiple redundant



Maininterface_1

Modeling of parameter uncertainty of safety instrumented systems

Sensor subsystem

Sensor-cell: CELL 3

CELL 3

Cell name: SPLCIC

Architecture: 1oo1

Uncertainty: MTSR

Cell Calc | CLEAR

Sensor calculation and analusis

PFDavg: 1.19E-3

SIL: SIL2

PFSavg: 3.94E-5

Controlor subsystem

Controlor-cell: CELL 3

CELL 3

Cell name: SPLCOP

Architecture: 1oo1

Uncertainty: λ

Cell Calc | CLEAR

Controlor calculation and analusis

PFDavg: 6.66E-4

SIL: SIL3

PFSavg: 1.58E-3

Actuator subsystem

Actuator -cell: CELL 1

CELL 3

Cell name: BV

Architecture: 1oo3

Uncertainty: λ

Cell Calc | CLEAR

Actuator calculation and analusis

PFDavg: 3.36E-3

SIL: SIL2

PFSavg: 3.54E-3

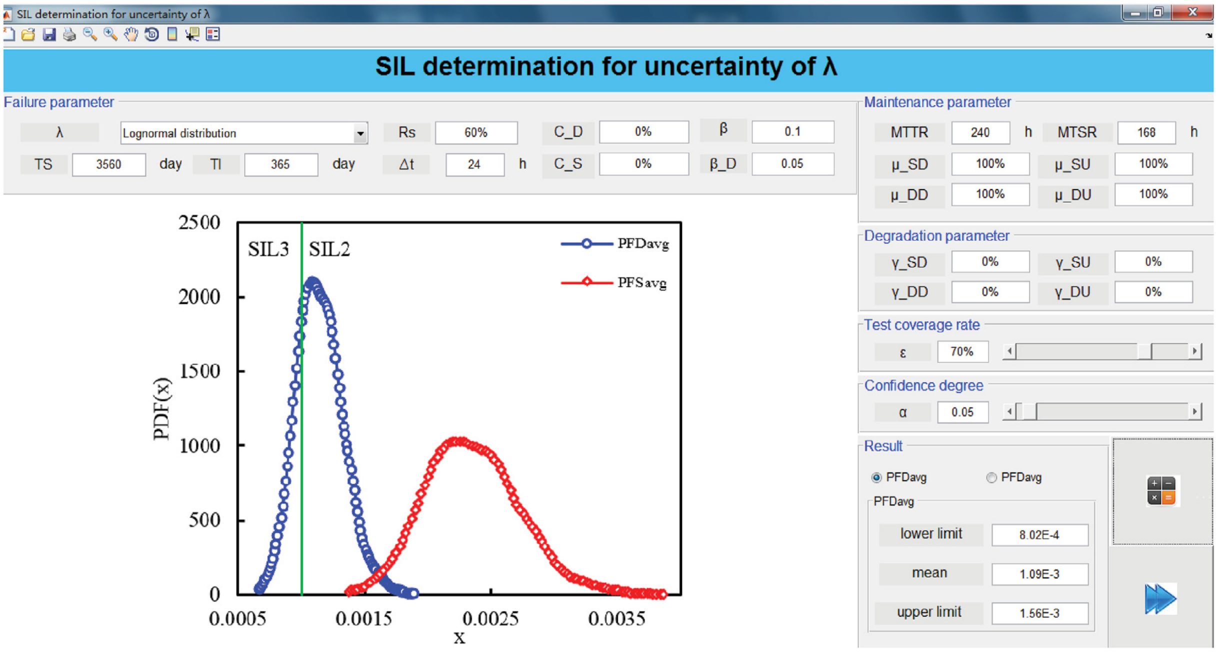
SIS

PFDavg: 3.36E-3

SIL: SIL2

PFSavg: 5.22E-3

Fig. 18. Main interface of the SIL determination software.



SIL determination for uncertainty of λ

SIL determination for uncertainty of λ

Failure parameter

λ: Lognormal distribution | Rs: 60% | C_D: 0% | β: 0.1

TS: 3560 day | TI: 365 day | Δt: 24 h | C_S: 0% | β_D: 0.05

Maintenance parameter

MTTR: 240 h | MTSR: 168 h

μ_SD: 100% | μ_SU: 100%

μ_DD: 100% | μ_DU: 100%

Degradation parameter

γ_SD: 0% | γ_SU: 0%

γ_DD: 0% | γ_DU: 0%

Test coverage rate

ε: 70%

Confidence degree

α: 0.05

Result

● PFDavg ○ PFDavg

PFDavg

lower limit: 8.02E-4

mean: 1.09E-3

upper limit: 1.56E-3

Fig. 19. Calculation interface of the SIL determination software.

cells and parameter uncertainty. This methodology can also be used to compare the influence of parameter uncertainty on single subsystem and the influence of different parameters on the evaluation results under uncertain conditions. The user-friendly SIL determination software with parameter uncertainty is developed on MATLAB graphical user interface. The PFD_{avg} and PFS_{avg} of single cell, single subsystem, and SIS can be calculated, and the contribution of single cell to the subsystem and the contribution of single subsystem to the SIS can be displayed.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 52171287, No.51779267, No.51707204), the National Key Research and Development Program of China (No.2019YFE0105100), the IKTPLUSS program of Research Council of Norway (No.309628), the Taishan Scholars Project (No.tsqn201909063), the Fundamental Research Funds for the Central Universities, that is, the Opening Fund of National Engineering Laboratory of Offshore Geophysical and Exploration

Equipment (No.20CX02301A), and the Science and Technology Support Plan for Youth Innovation of Universities in Shandong Province (No.2019KJB016).

References

Azizpour, H., Lundteigen, M.A., 2019. Analysis of simplification in markov-based models for performance assessment of safety instrumented system. Reliab. Eng. Syst. Saf. 183, 252–260. https://doi.org/10.1016/j.ress.2018.09.012.

Cai, B.P., Zhang, Y.P., Yuan, X.B., 2020. A dynamic-Bayesian-networks-based resilience assessment approach of structure systems: subsea oil and gas pipelines as A case study. China Ocean Eng. 34 (5), 597–607. https://doi.org/10.1007/s13344-020-0054-0.

Cai, B.P., Liu, H.L., Xie, M., 2016a. A real-time fault diagnosis methodology of complex systems using object-oriented Bayesian networks. Mech. Syst. Signal Process. 80, 31–44. https://doi.org/10.1016/j.ymssp.2016.04.019.

Cai, B.P., Liu, Y., Xie, M., 2017. A dynamic-Bayesian-network-based fault diagnosis methodology considering transient and intermittent faults. IEEE Trans. Autom. Sci. Eng. 14 (1), 276–285. https://doi.org/10.1109/TASE.2016.2574875.

Cai, B.P., Liu, Y., Fan, Q., 2016b. A multiphase dynamic Bayesian networks methodology for the determination of safety integrity levels. Reliab. Eng. Syst. Saf. 150, 105–115. https://doi.org/10.1016/j.ress.2016.01.018.

Cai, B.P., Liu, Y.H., Ma, Y.P., et al., 2015. Real-time reliability evaluation methodology based on dynamic Bayesian networks: a case study of a subsea pipe ram BOP system. ISA Trans. 58, 595–604. https://doi.org/10.1016/j.isatra.2015.06.011.

Chen, S.S., Wang, H.X., Jiang, H., et al., 2020. Risk assessment of corroded casing based on analytic hierarchy process and fuzzy comprehensive evaluation. Petrol. Sci. 18 (2), 591–602. https://doi.org/10.1007/s12182-020-00507-0.

Chang, K., Kim, S., Chang, D., et al., 2015. Uncertainty analysis for target SIL determination in the offshore industry. J. Loss Prev. Process. Ind. 34, 151–162. https://doi.org/10.1016/j.jlp.2015.01.030.

Ding, L., Wang, H., Kang, K., et al., 2014. A novel method for SIL verification based on system degradation using reliability block diagram. Reliab. Eng. Syst. Saf. 132, 36–45. https://doi.org/10.1016/j.ress.2014.07.005.

Eshiet, K.I.I., Sheng, Y., 2018. The performance of stochastic designs in wellbore drilling operations. Petrol. Sci. 15 (2), 335–365. https://doi.org/10.1007/s12182-018-0219-0.

Freeman, R.A., 2020. Error propagation and uncertainty analysis: application to fault tree analysis. Process Saf. Prog. 39 (2). https://doi.org/10.1002/prs.12080.

Freeman, R.R., 2012. Quantifying LOPA uncertainty. Process Saf. Prog. 31 (3), 240–247. https://doi.org/10.1002/prs.11493.

Freeman, R.R., Summers, A., 2016. Evaluation of uncertainty in safety integrity level calculations. Process Saf. Prog. 35 (4), 341–348. https://doi.org/10.1002/prs.11805.

Gao, P., Xie, L.Y., Pan, J., 2019. Reliability and availability models of belt drive systems considering failure dependence. Chin. J. Mech. Eng. 32 (1). https://doi.org/10.1186/s10033-019-0342-x.

Hu, X.W., Zhou, C.F., Duan, M.L., et al., 2014. Reliability analysis of marine risers with narrow and long corrosion defects under combined loads. Petrol. Sci. 11 (1), 139–146. https://doi.org/10.1007/s12182-014-0325-6.

Innal, F., Chebila, M., Dutuit, Y., 2016. Uncertainty handling in safety instrumented systems according to IEC 61508 and new proposal based on coupling Monte Carlo analysis and fuzzy sets. J. Loss Prev. Process. Ind. 44, 503–514. https://doi.org/10.1016/j.jlp.2016.07.028.

Jahanian, L., 2015. Generalizing PFD formulas of IEC 61508 for KooN configurations. ISA Trans. 55, 168–174. https://doi.org/10.1016/j.isatra.2014.07.011.

Jin, H., Lundteigen, M.A., Rausand, M., 2012. Uncertainty assessment of reliability estimates for safety-instrumented systems. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. 226 (6), 646–655. https://doi.org/10.1177/1748006X12462780.

Kanjilal, O., Manohar, C.S., 2020. Time variant reliability estimation of randomly excited uncertain dynamical systems by combined Markov chain splitting and Girsanov's transformation. Arch. Appl. Mech. 90 (11), 2363–2377. https://doi.org/10.1007/s00419-020-01726-y.

Kaczor, G., Mlynarski, S., Szkoda, M., 2016. Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams. J. Loss Prev. Process. Ind. 41, 31–39. https://doi.org/10.1016/j.jlp.2016.03.002.

Koneshloo, M., Aryana, S.A., Hu, X.N., 2018. The impact of geological uncertainty on primary production from a fluvial reservoir. Petrol. Sci. 15 (2), 270–288. https://doi.org/10.1007/s12182-018-0229-y.

Martin, V., Gbenga, O., Andrei, P., 2019. Fuzzy logic applied to value of information assessment in oil and gas projects. Petrol. Sci. 16 (5), 1208–1220. https://doi.org/10.1007/s12182-019-0348-0.

Piesik, E., Śliwiński, M., Barnert, T., 2016. Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects. Reliab. Eng. Syst. Saf. 152, 259–272. https://doi.org/10.1016/j.ress.2016.03.018.

Soro, I.W., Nourelfath, M., Ait-Kadi, D., 2010. Performance evaluation of multi-state degraded systems with minimal repairs and imperfect preventive maintenance. Reliab. Eng. Syst. Saf. 95 (2), 65–69. https://doi.org/10.1016/j.ress.2009.08.004.

Schlosser, R., 2020. Risk-sensitive control of Markov decision processes: a moment-based approach with target distributions. Comput. Oper. Res. 123. https://doi.org/10.1016/j.cor.2020, 104997.

Sallak, M., Simon, C., Aubry, J.F., 2008. A fuzzy probabilistic approach for determining safety integrity level. IEEE Trans. Fuzzy Syst. 16 (1), 239–248. https://doi.org/10.1109/TFUZZ.2007.903328.

Simon, C., Weber, P., Evsukoff, A., 2008. Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. Reliab. Eng. Syst. Saf. 93 (7), 950–963. https://doi.org/10.1016/j.ress.2007.03.012.

Simon, C., Mechri, W., Capizzi, G., 2019. Assessment of safety integrity level by simulation of dynamic Bayesian networks considering test duration. J. Loss Prev. Process. Ind. 57, 101–113. https://doi.org/10.1016/j.jlp.2018.11.002.

Śliwiński, M., 2018. Safety integrity level verification for safety-related functions with security aspects. Process Saf. Environ. Protect. 118, 79–92. https://doi.org/10.1016/j.psep.2018.06.016.

Ulmeanu, A.P., 2012. Analytical method to determine uncertainty propagation in fault trees by means of binary decision diagrams. IEEE Trans. Reliab. 61 (1), 84–94. https://doi.org/10.1109/TR.2012.2182812.

Wang, J., Qiu, Z.P., 2012. Fatigue reliability based on residual strength model with hybrid uncertain parameters. Acta Mech. Sin. 28 (1), 112–117. https://doi.org/10.1007/s10409-011-0536-7.

Wang, P.D., Zhang, J.G., Zhai, H., et al., 2017. A new structural reliability index based on uncertainty theory. Chin. J. Aeronaut. 30 (4), 1451–1458. https://doi.org/10.1016/j.cja.2017.04.008.

Wang, Y., West, H.H., Mannan, M.S., 2004. The impact of data uncertainty in determining Safety Integrity Level. Process Saf. Environ. Protect. 82 (B6), 393–397. https://doi.org/10.1205/psep.82.6.393.53199.

Wang, H.R., Ye, L.T., Xu, X.Y., et al., 2010. Bayesian networks precipitation model based on hidden markov analysis and its application. Sci. China Technol. Sci. 53 (2), 539–547. https://doi.org/10.1007/s11431-010-0034-3.

Weber, P., Medina-Oliva, G., Simon, C., et al., 2012. Overview on Bayesian networks applications for dependability risk analysis and maintenance areas. Appl. Artif. Intell. 25 (4), 671–682. https://doi.org/10.1016/j.engappai.2010.06.002.

Xu, M., Chen, T., Yang, X.H., 2012. The effect of parameter uncertainty on achieved safety integrity of safety system. Reliab. Eng. Syst. Saf. 99, 15–23. https://doi.org/10.1016/j.ress.2011.10.015.

Zhang, L.B., Hu, J.Q., 2013. Safety prognostic technology in complex petroleum engineering systems: progress, challenges and emerging trends. Petrol. Sci. 10 (4), 486–493. https://doi.org/10.1007/s12182-013-0299-9.

Zhang, S.Z., Wang, X., Cheng, Y.F., et al., 2019. Modeling and analysis of a catastrophic oil spill and vapor cloud explosion in a confined space upon oil pipeline leaking. Petrol. Sci. 17 (2), 556–566. https://doi.org/10.1007/s12182-019-00403-2.

Zou, H., Ye, Y.G., Zong, Q.G., et al., 2019. Monte Carlo simulations of the sensor head of imaging energetic electron spectrometer onboard a Chinese IGSO navigation satellite. Sci. China Technol. Sci. 62 (7), 1169–1181. https://doi.org/10.1007/s11431-017-9314-6.