Reliability Engineering and System Safety 174 (2018) 71–81

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Reliability analysis of complex multi-state system with common cause failure based on evidential networks

Jinhua Mi [a,b], Yan-Feng Li [b,*], Weiwen Peng [b], Hong-Zhong Huang [b]

[a] School of Automation Engineering, University of Electronic Science and Technology of China, No. 2006, Xiyuan Avenue, West Hi-Tech Zone, Chengdu, Sichuan 611731, China

[b] Center for System Reliability and Safety, University of Electronic Science and Technology of China, No. 2006, Xiyuan Avenue, West Hi-Tech Zone, Chengdu, Sichuan 611731, China

ARTICLE INFO

Keywords:
Complex multi-state system
Evidence theory
Bayesian network
Common cause failure group

ABSTRACT

With the increasing complexity and size of modern advanced engineering systems, the traditional reliability theory cannot characterize and quantify the complex characteristics of complex systems, such as multi-state properties, epistemic uncertainties, common cause failures (CCFs). This paper focuses on the reliability analysis of complex multi-state system (MSS) with epistemic uncertainty and CCFs. Based on the Bayesian network (BN) method for reliability analysis of MSS, the Dempster-Shafer (DS) evidence theory is used to express the epistemic uncertainty in system through the state space reconstruction of MSS, and an uncertain state used to express the epistemic uncertainty is introduced in the new state space. The integration of evidence theory with BN which called evidential network (EN) is achieved by adapting and updating the conditional probability tables (CPTs) into conditional mass tables (CMTs). When multiple CCF groups (CCFGs) are considered in complex redundant system, a modified β factor parametric model is introduced to model the CCF in system. An EN method is proposed for the reliability analysis and evaluation of complex MSSs in this paper. The reliability analysis of servo feeding control system for CNC heavy-duty horizontal lathes (HDHLs) by this proposed method has shown that CCFs have considerable impact on system reliability. The presented method has high computational efficiency, and the computational accuracy is also verified.

1. Introduction

The multi-state system (MSS) was firstly proposed by Barlow and Wu, it has been proved that lots of industrial systems belong to MSS, such as electrical power system, pipe transmission system, production and manufacturing system, aerospace system [1–3]. Those systems can define the multi-state characteristics of components accurately by analyzing the system failure process and tracking the effect of the change of component performance on the system reliability. There are four types of methods used for reliability analysis of MSS, including multi-state fault tree method [4], Markov process method [5,6], Monte-Carlo simulation (MCS) method [7,8] and universal generating function (UGF) method [9,10]. The MSS plays a critical role in the reliability analysis and assessment of complex system and also has broad application foreground.

The uncertainty caused by lack of data and scarcity of information is one of the most challenging issues in MSS reliability analysis. When the system state performances and state probabilities cannot be exactly defined and obtained, sometimes the bounds of system states and state probabilities can be expressed by some linguistic forms. Then the probability based methods are no longer applicable to this kind of system. Some non-probabilistic methods are developed, including Dempster-Shafer evidence theory (DSET) [11], fuzzy theory [12–15], probability-box [16–18], interval theory [19], possibility theory [20], Bayesian method [21], etc. The DS evidence theory has a flexible axiomatic system to describe uncertainty, and also has an independent frame to process uncertainty in system [22,23]. It has been widely used for uncertainty modeling, quantification, reasoning and mitigation in reliability engineering [24–26].

Bayesian network (BN) has been widely used in reliability and safety analysis because of its obvious advantages in multi-state and non-deterministic fault logic description [27–29]. Evidence theory allows an analyst to distribute the probability mass in overlapping regions of the sample space, which is useful when there are significant uncertainty and conflicting evidence. There are many researches on BN based on evidence theory. Simon et al. [30,31] analyzed reliability of complex system with epistemic uncertainty by using of BN, where evidence theory is used to quantify system uncertainty. Then the evidential networks

* Corresponding author.
E-mail addresses: yanfengli@uestc.edu.cn (Y.-F. Li), hzhuang@uestc.edu.cn (H.-Z. Huang).

https://doi.org/10.1016/j.ress.2018.02.021
Received 7 December 2016; Received in revised form 14 February 2018; Accepted 14 February 2018
Available online 16 February 2018
0951-8320/

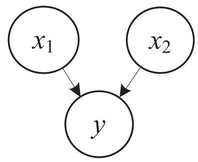

Fig. 1. A sample multi-state BN.

(ENs) also have been used for the reliability and performance evaluation of system with imprecise knowledge [32]. Zhao et al. [33] studied the influence of incomplete original parameters and subjective parameters on the reliability of distribution system by using BN and evidence theory. Simon et al. [31] developed the combination method of BN and evidence theory for reliability analysis of multi-state system (MSS). Detailed illustrations of the concepts of EN and its application have been given in [34]. It is shown that evidence theory can handle the imprecise information in system and get more useful information than interval analysis method.

This paper introduces a multi-state EN method for reliability analysis of complex system with CCFGs based on evidence theory and BN. The remaining of this paper is organized as follows. In Section 2, the node definition and network reasoning of multi-state EN are introduced. In Section 3, when the multiple CCF groups (CCFGs) are considered in complex redundant system, a modified β factor parametric model is introduced to model the CCF in system. This comprehensive method is used to analyze the reliability of an example system and a feeding control system of CNC heavy-duty horizontal lath (HDHL) in Section 4. Finally, conclusions are drawn in Section 5.

2. Multi-state evidential network

2.1. The node definition of multi-state evidential network

For a sample BN with three nodes shown in Fig. 1, it is assumed that the nodes x_1 and x_2 are three state nodes, the state space is $\Lambda = \{0, 1, 2\}$. Where $x_i = 0, 1, 2$ represent the success, partial failure and complete failure of the corresponding component. When the epistemic uncertainty exists in system, an added state $x_i = [0, 1, 2]$ is defined to represent the uncertain state of node x_i. Then the frame of discernment $D = \{0, 1, 2, [0, 1, 2]\}$ is defined under evidence theory, and the basic mass assignment (BMA) which corresponding to basic probability assignment (BPA) in BN is m: $2^D \to [0, 1]$, its power set can be expressed as

$$2^D = \{m(x = \emptyset) = 0; m(x = 0); m(x = 1); m(x = 2); m(x = [0, 1, 2])\}. \tag{1}$$

For an event $A : \{x = 0\}$ on the frame of discernment D, and $B \subseteq A$, then the belief function of event A is

$$Bel(A) = \sum_{B \subseteq A} m(B) = m(x = 0). \tag{2}$$

Eq. (2) represents the belief degree (the measure of belief) of event $A : x = 0$. It is the lower bound of belief interval when the probability of uncertain information is not counted in the BMA [31]. Based on the definition of plausibility function, the plausibility function of event A can be gotten by

$$Pl(A) = \sum_{B \cap A \neq \emptyset} m(B) = m\{x = 0\} + m\{x = [0, 1, 2]\}. \tag{3}$$

Accordingly, the interval probability of event A can be calculated by Eqs. (2) and (3), and it can be expressed as $[P](A) = [Bel(A), Pl(A)]$. Similarly, the interval probabilities of other nonempty events under the frame of discernment D can be computed as well.

When the corresponding components of nodes x_1 and x_2 are parallel or series, the conditional probability table (CPT) of node y under evidence theory can be derived and transformed into conditional mass table (CMT). Then the belief reliability of node y: $Bel(y = 0)$ can be obtained by BN reasoning as

$$Bel(y = 0) = \sum_{x_1, x_2} Bel(y = 0 | x_1, x_2) Bel(x_1) Bel(x_2). \tag{4}$$

The plausibility reliability $Pl(y = 0)$ is

$$Pl(y = 0) = \sum_{x_1, x_2} Pl(y = 0 | x_1, x_2) Pl(x_1) Pl(x_2). \tag{5}$$

The actual reliability of node y: $P(y = 0)$ will belongs to interval $[Bel(y = 0), Pl(y = 0)]$.

2.2. The multi-state evidential network reasoning

In order to use BN with the evidence theory, there should be an adaption in the transformation of the CPTs into CMTs. For a multi-state EN with n root nodes $x_1, x_2, \cdots, x_n$, and the leaf node which represents the final statement of system is denoted as y, the state number of the ith root node x_i and leaf node y are l_i and l_y, respectively. The relation between the state probability of leaf node y and root nodes can be expressed as

$$P\left(y = y^j \middle| x_1 = x_1^{k_1}, \cdots, x_n = x_n^{k_n}\right) = \frac{P\left(y = y^j, x_1 = x_1^{k_1}, \cdots, x_n = x_n^{k_n}\right)}{P\left(x_1 = x_1^{k_1}, \cdots, x_n = x_n^{k_n}\right)}, \tag{6}$$

where $1 \le j \le k_y$, $1 \le i \le n$ and $1 \le k_i \le l_i$. Suppose that the interval probability of node x_i at state k_i is

$$[P]\left(x_i = x_i^{k_i}\right) = \left[Bel\left(x_i^{k_i}\right), Pl\left(x_i^{k_i}\right)\right], \tag{7}$$

where $Bel(x_i^{k_i})$ and $Pl(x_i^{k_i})$ can be calculated by the CMT of those nodes.

The conditional probability of non-leaf node y of EN is

$$[P]\left(y = y^j \middle| x_1 = x_1^{k_1}, \cdots, x_n = x_n^{k_n}\right) = \left[Bel\left(y^j\right), Pl\left(y^j\right)\right]. \tag{8}$$

The probability of node y on jth state can be gotten by

$$P\left(y = y^j\right) = P\left(y = y^j \middle| x_1 = x_1^{k_1}, \cdots, x_n = x_n^{k_n}\right) P\left(x_1 = x_1^{k_1}\right) \cdots P\left(x_n = x_n^{k_n}\right). \tag{9}$$

Based on the former reasoning method, the probability of leaf node $T = T_v$ can be expressed as

$$[P](T = T_v) = \left[Bel(T = T_v), Pl(T = T_v)\right], \tag{10}$$

where the lower bound $Bel(T = T_v)$ is the belief probability and can be calculated by

$$\begin{aligned} Bel(T = T_v) &= \sum_{x_1, \cdots, x_n, y_1, \cdots, y_m} Bel(x_1, \cdots, x_n, y_1, \cdots, y_m, T = T_v) \\ &= \sum_{\pi(T)} Bel(T = T_v | \pi(T)) \prod_{j=1}^{m} \sum_{\pi(y_1)} Bel\left(y_j \middle| \pi(y_j)\right) \prod_{i=1}^{n} Bel\left(x_i^{k_i}\right) \\ &= \sum_{\pi(T)} Bel(T = T_v | \pi(T)) \sum_{\pi(y_1)} Bel\left(y_1 \middle| \pi(y_1)\right) \times \cdots \\ &\quad \times \sum_{\pi(y_m)} Bel\left(y_m \middle| \pi(y_m)\right) \times \cdots \times Bel\left(x_1 = x_{1,k_1}\right) \\ &\quad \times \cdots \times Bel\left(x_n = x_{n,k_n}\right). \end{aligned} \tag{11}$$

The upper bound $Pl(T = T_v)$ is the plausibility probability and can be computed by

$$\begin{aligned} Pl(T = T_v) &= \sum_{x_1, \cdots, x_n, y_1, \cdots, y_m} Pl(x_1, \cdots, x_n, y_1, \cdots, y_m, T = T_v) \\ &= \sum_{\pi(T)} Pl(T = T_v | \pi(T)) \prod_{j=1}^{m} \sum_{\pi(y_1)} Pl\left(y_j \middle| \pi(y_j)\right) \prod_{i=1}^{n} Pl\left(x_i^{k_i}\right) \end{aligned}$$

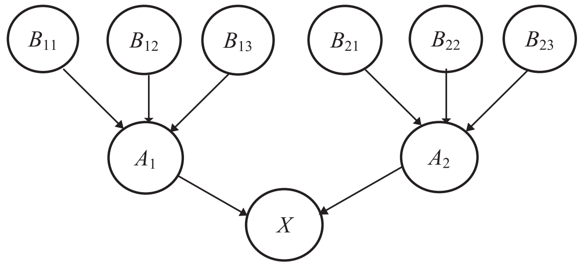

Fig. 2. Case Bayesian network.

Table 1
The state probabilities of root nodes.

Node	0	1	2	[0,1,2]
B_{i1}	0.9991	1.7×10^{-4}	2.5×10^{-4}	4.8×10^{-4}
B_{i2}	0.9989	–	6.3×10^{-4}	4.7×10^{-4}
B_{i3}	0.9986	3.1×10^{-4}	5.4×10^{-4}	5.5×10^{-4}

$$= \sum_{\pi(T)} Pl\left(T = T_v | \pi(T)\right) \sum_{\pi(y_1)} Pl\left(y_1 \middle| \pi(y_1)\right) \times \cdots \times \sum_{\pi(y_m)} Pl\left(y_m \middle| \pi(y_m)\right) \times \cdots \times Pl\left(x_1 = x_{1,k_1}\right) \times \cdots \times Pl\left(x_n = x_{n,k_n}\right). \tag{12}$$

The probability of leaf node can be obtained by the former forward reasoning of BN, the posterior probability of root nodes can be deduced by backward reasoning. When $T = T_v$, the posterior probability of root node $x_i = x_{i,k_i}$ can be computed by

$$[P]\left(x_i = x_{i,k_i} | T = T_v\right) = \begin{bmatrix} \min\left(Bel\left(x_i = x_{i,k_i} | T = T_v\right), Pl\left(x_i = x_{i,k_i} | T = T_v\right)\right), \\ \max\left(Bel\left(x_i = x_{i,k_i} | T = T_v\right), Pl\left(x_i = x_{i,k_i} | T = T_v\right)\right) \end{bmatrix}, \tag{13}$$

where

$$Bel\left(x_i = x_{i,k_i} | T = T_v\right) = \frac{Bel\left(x_i = x_{i,k_i}, T = T_v\right)}{Bel\left(T = T_v\right)}, \tag{14}$$

$$Pl\left(x_i = x_{i,k_i} | T = T_v\right) = \frac{Pl\left(x_i = x_{i,k_i}, T = T_v\right)}{Pl\left(T = T_v\right)}, \tag{15}$$

where $Bel(x_i = x_{i,k_i}, T = T_v)$ and $Pl(x_i = x_{i,k_i}, T = T_v)$ are the belief and plausibility joint probability of root nodes and leaf node. The root nodes and leaf node of EN reflect the fault causes and fault state properties of system. Therefore, the system state probability can be computed by forward reasoning of EN, which also realizes a quantitative description of system fault states. The backward reasoning of EN can estimate the posterior probability of fault causes based on system failure state, and also can implement the system failure prediction and judgment. The latter possesses certain guiding significance for improving the reliability of a complex system.

2.3. Introductory example

An example multi-state BN from Ref. [35] is employed by this paper as shown in Fig. 2. Based on the state definition method in Section 2.1, the fourth state [0, 1, 2] is used to describe the uncertainty for each root nodes in the presence of reliability uncertainty. The state probabilities of root nodes are listed in Table 1. And the CMT of non-leaf nodes A_1 and A_2 are shown in Table 2. Since the non-leaf nodes A_1 and A_2 have 3 certain states, the CPT of leaf node X is shown in Table 3. The EN will be evolved as Fig. 3.

Table 2
CMT of non-leaf nodes A_1 and A_2.

b_{11}, b_{21}	b_{12}, b_{22}	b_{13}, b_{23}	a_1, a_2					
			Bel			*Pl*		
			0	1	2	0	1	2
0	0	0	1	0	0	1	0	0
0	0	1	0	1	0	0	1	0
0	0	2	0	0	1	0	0	1
0	0	[0,1,2]	0	0	0	1	1	1
0	2	0	0	0	1	0	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
[0,1,2]	[0,1,2]	2	0	0	1	0	0	1
[0,1,2]	[0,1,2]	[0,1,2]	0	0	0	1	1	1

Table 3
CPT of leaf node X.

a_1	a_2	x		
		0	1	2
0	0	1	0	0
0	1	1	0	0
0	2	1	0	0
1	0	1	0	0
1	1	0	1	0
1	2	0	1	0
2	0	1	0	0
2	1	0	1	0
2	2	0	0	1

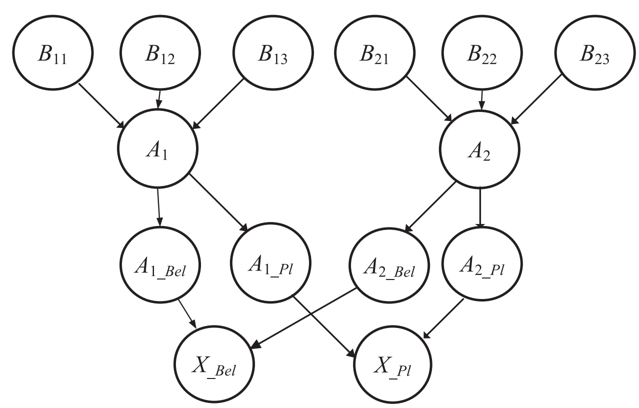

Fig. 3. The evolved evidential network.

Table 4
The belief and plausibility marginal probabilities of non-leaf nodes A_1 and A_2.

Non-leaf nodes	State	*Bel*	*Pl*
A_1, A_2	0	0.996604	0.998101
	1	4.790082×10^{-4}	1.976844×10^{-3}
	2	1.419367×10^{-3}	2.917203×10^{-3}

Based on the EN reasoning method in Section 2.2, the marginal probability distribution of non-leaf nodes A_1 and A_2 can be computed and listed in Table 4. The state probabilities of leaf node X is obtained and shown in Table 5.

Table 5
The state probabilities of leaf node X.

Non-leaf nodes	State	*Bel*	*Pl*
X	0	0.997003	0.999976
	1	1.589226×10^{-6}	1.534954×10^{-5}
	2	2.014604×10^{-6}	8.459324×10^{-6}

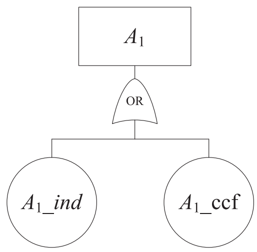

Fig. 4. Fault tree explicit modeling method for component with CCF.

The mid-value of interval probability of root nodes are chosen as the inputs of EN, the probability distribution of leaf node can be computed and

$$\begin{aligned} P(X=0) &= 0.999995 \\ P(X=1) &= 2.275775\times10^{-6} \\ P(X=2) &= 2.557409\times10^{-6}. \end{aligned} \tag{16}$$

Comparing the results of Eq. (16) with Table 5, it can be found that the precise state probability of leaf node X is located between the belief probability and the plausibility probability gotten by the introduced evidence theory based method. This indicates that the result obtained by this method is correct and effective.

3. Reliability modeling of system with multiple CCFGs

3.1. A modified β factor model for common cause failure groups

Considering the dependent failure caused by interior physical interactions of components and human interactions in system, the β factor parametric model [36] has been widely used for such cases. Assume that P_t is the total failure probability of a component; it can be expanded into an independent contribution P_{ind} and a dependent contribution P_{ccf}, which are functions of time t respectively. When the component is assumed to follow the exponential distribution, λ_t, λ_{ind} and λ_{ccf} are the failure rates of entire system, independent part, and the dependent part respectively. Then parameter β can be defined as the fraction of the total failure probability attributable to dependent failures [35,36], and can be mathematically described as

$$\begin{aligned} \beta &= \frac{P_{ccf}}{P_t} = \frac{P_{ccf}}{P_{ind}+P_{ccf}} = \frac{(1-\exp(-\lambda_{ccf}\cdot t))}{(1-\exp(-\lambda_t\cdot t))} \\ &= \frac{(1-\exp(-\lambda_{ccf}\cdot t))}{(1-\exp(-\lambda_{ind}\cdot t))+(1-\exp(-\lambda_{ccf}\cdot t))}. \end{aligned} \tag{17}$$

The value of β-factor can be obtained by the direct use of field data and experts' experience [35–37].

In order to present how the β factor model works, a simple deduction is performed for a single component within the FTA model. For a parallel system with two identical components, and $P(A_1)=P(A_2)=P_A$, the failure probability of system can be computed as:

$$P_{sys} = P(A_1)P(A_2) = P_A^2 \tag{18}$$

For the basic component A, as shown in Fig. 4, the failure probability of A can be divided into two proportions: independent part and CCF part, and it can be expressed as

$$P_A = P_{A\_ind} + P_{A\_ccf} \tag{19}$$

And the CCF part, the failure probability is

$$P_{A\_ccf} = \beta P_A \tag{20}$$

By using the former explicit modeling method, the failure probabilities of component A_1 and A_2 are both divided into independent part and CCF part. Then based on the standard β-factor model and Eq. (17), the probability of CCF part can be obtained and $P_{A_1\_ccf} = P_{A_2\_ccf} = \beta P_A$. The parallel system with two components also can be further expressed as Fig. 5(a). The system failure event Sys can be simplified by using Boolean algebra operation rules and expressed as

$$\begin{aligned} Sys &= A_1A_2 = (A_1\_ind + A_1\_ccf)(A_2\_ind + A_2\_ccf) \\ &= (A_1\_ind + A\_ccf)(A_2\_ind + A\_ccf) \\ &= A_1\_ind\cdot A_2\_ind + A\_ccf\cdot(A\_ccf + A_1\_ind + A_2\_ind) \\ &= A_1\_ind\cdot A_2\_ind + \underbrace{A\_ccf\cdot A\_ccf}_{A\_ccf} \\ &\quad + \underbrace{A\_ccf\cdot A_1\_ind}_{0} + \underbrace{A\_ccf\cdot A_2\_ind}_{0} \\ &= A_1\_ind\cdot A_2\_ind + A\_ccf \end{aligned} \tag{21}$$

Finally, the system with consideration of CCF can be simplified and shown as Fig. 5(b).

Then the failure probability of system can be obtained by Eq. (21) and

$$\begin{aligned} P(Sys) &= P(A_1\_ind\cdot A_2\_ind + A\_ccf) \\ &= P(A_1\_ind)\cdot P(A_2\_ind) + P(A\_ccf) \\ &= (1-\beta)P(A)\cdot(1-\beta)P(A) + \beta P(A) \end{aligned} \tag{22}$$

When a single component fails simultaneously within multiple CCFGs [37,38], a modified β factor parametric model is used to express the coupling mechanism. The explicit modeling of component A with multiple CCFGs is shown in Fig. 6.

The failure probability of component A is then given as

$$\begin{aligned} P(A) &= P(A\_ind) + P(A\_ccf) \\ &= P(A\_ind) + P(A\_CCFG_1 \cup \cdots \cup A\_CCFG_k) \\ &= P(A\_ind) + P(A\_CCFG_1) + \cdots P(A\_CCFG_k) \end{aligned} \tag{23}$$

In this way, the failure probability of component A is divided into CCF parts and independent part as follow

$$\begin{aligned} P_{A\_ccf} &= P_{A\_CCFG_1} + P_{A\_CCFG_2} + \cdots + P_{A\_CCFG_k} \\ &= \beta_1P_A + \beta_2P_A + \cdots + \beta_kP_A = P_A\sum_{i=1}^{k}\beta_i \end{aligned} \tag{24}$$

$$P_{A\_ind} = \left(1-\sum_{i=1}^{k}\beta_i\right)P_A \tag{25}$$

3.2. Model limitation and solution

Because the β-factors are obtained by expert judgments, there exists the limitation of this modified β factor parametric model for $(\beta_1+\beta_2+\cdots+\beta_k)>1$. In this case, the failure probability of CCF part is larger than the probability of total components. To cope with this limitation in this model, a proportional reduction factor (PRF) method [37,38] is applied in this paper. The PRF factor is defined as

$$\mathrm{PRF} = \frac{1}{\sum_{j=1}^{k}\beta_j} \tag{26}$$

Then a set of new reduced β factor are generated as

$$\boldsymbol{\beta} = [\beta'_1, \beta'_2, \cdots, \beta'_k] = \mathrm{PRF}[\beta_1, \beta_2, \cdots, \beta_k]. \tag{27}$$

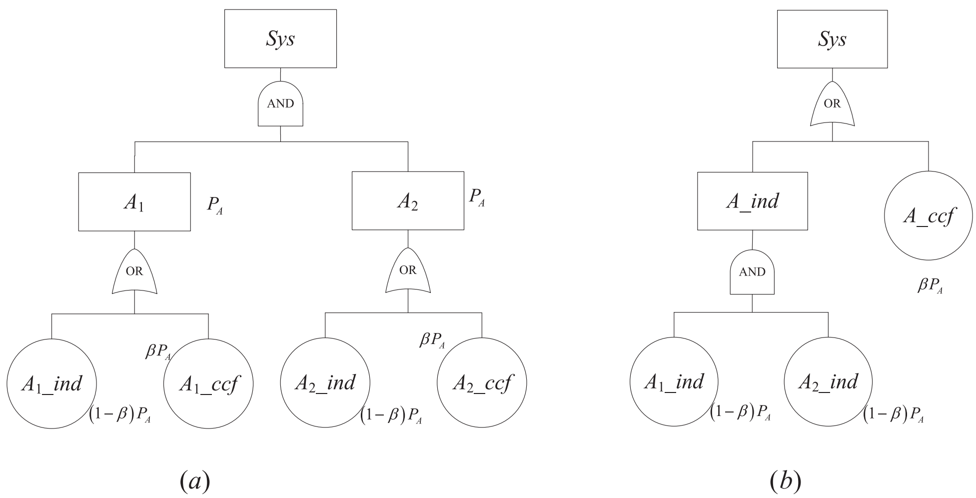

Fig. 5. (a) Fault tree of two components parallel system with CCF; (b) Simplify fault tree of system.

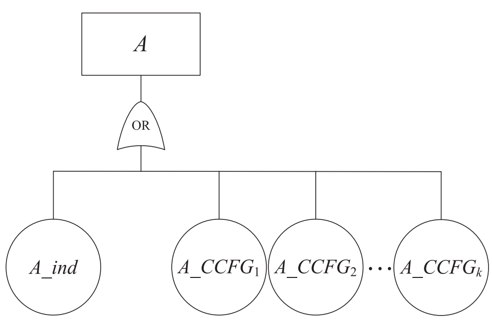

Fig. 6. Explicit modeling of multiple CCFGs within fault tree.

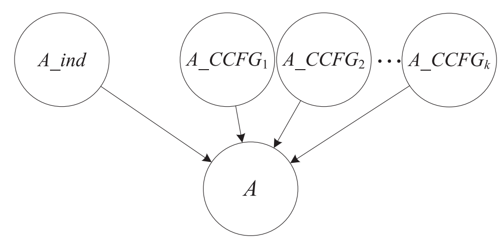

Fig. 7. BN node with CCFGs.

In this way, the failure probability of CCF parts and independent part are rewritten as

$$P_{A\_ccf} = P_A \sum_{i=1}^{k} \beta'_i \tag{28}$$

$$P_{A\_ind} = \left(1 - \sum_{i=1}^{k} \beta'_i\right) P_A = 0 \tag{29}$$

The essence of the PRF method is an equilibrium process of the accumulated common cause parts on β factor, which has weaken the contradiction of the common cause part beyond the total failure probability to some extent. And the PRF method is just one of the methods which can be used to solve this kind of logical contradiction; any other method capable of dealing with such contradictions may be applicable.

3.3. The Bayesian network node with CCFGs

When CCFs is considered in system reliability modeling, the failure of system can be divided into independent part and CCF part. The independent part means the failure of system caused a single cause. The CCF part represents the simultaneous failure of multiple components which caused by a common coupling mechanism, then those components constitute a CCFG. For component A which exists in multiple CCFGs that denoted as $CCFG_1$, $CCFG_2$, ⋯, $CCFG_k$, by using the fault tree explicit modeling of multiple CCFGs in Section 3.2 and translate the fault tree into BN, as shown in Fig. 7.

When the independent failure probability of node A is $P(A_{ind})$, the corresponding β factors of common cause nodes are $\beta_1, \beta_2, \cdots, \beta_k$. When $(\beta_1 + \beta_2 + \cdots + \beta_k) < 1$, the failure probability of node A can be calculated by Eqs. (22)–(26) and

$$P'(A) = P(A_{ind}) + P(A_{ccf}) = P(A_{ind}) + \frac{\sum_{i=1}^{k} \beta_i}{1 - \sum_{i=1}^{k} \beta_i} P(A_{ind})$$
$$= \frac{1}{1 - \sum_{i=1}^{k} \beta_i} P(A_{ind}) \tag{30}$$

When the sum of β factors is larger than 1, that is $(\beta_1 + \beta_2 + \cdots + \beta_k) > 1$, by using the PRF method in Section 3.2, the failure probability of node A can be computed by Eqs. (26)–(29) and

$$P'(A) = P'_{A\_ccf} + P'_{A\_ind} = P_A \sum_{i=1}^{k} \beta'_i + 0 = P_A \cdot PRF \cdot \sum_{i=1}^{k} \beta_i. \tag{31}$$

4. Reliability analysis of feeding control system for CNC HDHLs with multiple CCFGs

4.1. Fault tree modeling of feeding control system

The lathes are basic machine tools for manufacturing cylindrical parts. In recent years, the DL series computer numerical control (CNC) heavy-duty horizontal lathes (HDHLs) have been widely used in the transportation, energy, and aviation industries. High availability of the CNC HDHL is required to maximize the efficiency and benefit of these manufacturing industries [37]. The DL series horizontal lathes are computer numerical control (CNC) types which are used for the turning operation of rotational parts with outside and inside surface, such as axles and disc, and have the following work axes: X axis of tool head lateral movement, Z axis of tool head longitudinal movement, U_1 axis of left gang tool movement and U_2 axis of right gang tool movement. Fig. 8

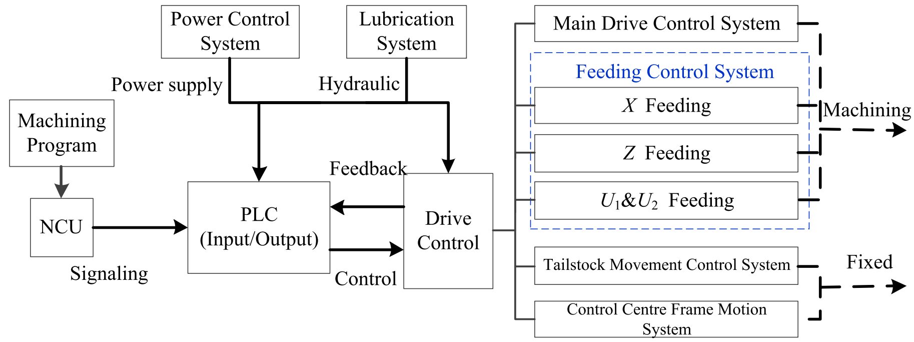

Fig. 8. Functional block diagram of electrical control and drive system for the DL series CNC HDHL.

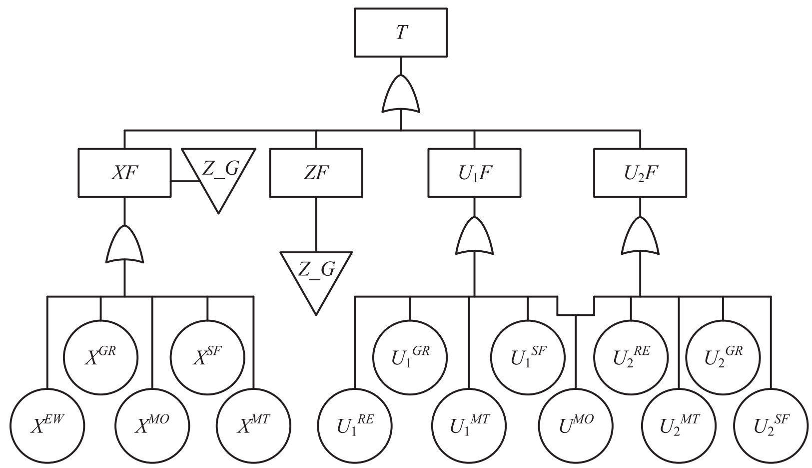

Fig. 9. Fault tree model of the feeding control system.

shows the functional block diagram of the electrical control and drive system for such DL series horizontal lathes. The feeding control system include three subsystems: *X, Z*, as well as U_1 and U_2 axes feeding control systems. A signal generated by 611D-type servo driven module (*Mo*) is transmitted through electric cable (*Ew*) to control the motor (*Mt*) in *X* axis feeding control system. There exists a speed feedback device (*Sf*). The grating scales (*Gr*) feedback the straightness of *X* axis to *Mo* to adjust the feed speed and direction. The electrical control of *Z*, U_1 and U_2 axes is almost the same as that of *X* axis, excepting the difference introduced in Section 1. Although U_1 and U_2 axes share a 611D-type servo driven module, they have different current relays (*Re*).

The main functional failure modes of the system can be obtained by the functional analysis and failure mechanism analysis of feeding control system, which include motor cannot be started, overshooting of axes, short circuit, damage of electronic units, exceed standards of geometric accuracy, crack of structure, etc. Then the “functional failure of feeding control system” has been chosen as the top event in FTA, the fault tree of feeding control system is built and shown in Fig. 9.

The meanings of the notations in Fig. 9 are as following: *T* denotes the functional failure of feeding control system; *XF, ZF*, U_1F and U_2F are the functional failures of *X, Z*, U_1 and U_2 axes feeding control systems. The basic components of each axes feeding control system include *Gr, Sf, Ew, Mo, Mt* and *Re*. Therefore, in the fault tree model, the failure events of basic components are noted by two parts: the code of axes and the code of each component. For example, X^{Ew} represents the *Ew* failure of *X* axis feeding control system, and the other notations follow the similar interpretations.

4.2. The BN modeling and CCFGs fusion

From Fig. 9, components of the same types are used in different subsystems of feeding control system, an external shock or interior component physical interactions may cause the failure of those components simultaneously. So when considering the CCF caused by human interactions, system function correlation and environment, the following common cause events or CCFGs will exist in system.

Table 6
The failure rates and failure probabilities of components.

Code	Failure rate $\lambda(\times 10^{-6}/\text{h})$	Failure probability ($t = 3000$ h)
MO	0.2	0.0006
EW	0.6	0.0018
GR	2	0.0060
MT	7	0.0208
SF	0.5	0.0015
RE	2	0.0060

1) $C^{MO} = \{X^{MO}, Z^{MO}, U^{MO}\}$, which means the motors of different subsystems fail at the same time by one influence factor. Based on expert experience, the common cause factor $\beta^{MO} = 0.1$.
2) $C^{GR} = \{X^{GR}, Z^{GR}, U_1^{GR}, U_2^{GR}\}$, $C^{SF} = \{X^{SF}, Z^{SF}, U_1^{SF}, U_2^{SF}\}$ and $\beta^{GR} = 0.2$, $\beta^{SF} = 0.15$.
3) $C^{EW} = \{X^{EW}, Z^{EW}\}$, $C^{RE} = \{X^{RE}, Z^{RE}\}$ and $\beta^{EW} = \beta^{RE} = 0.15$.
4) When X^{MT} exists in multiple CCFGs, and expressed as $CCFG_1^{MT} = \{X^{MT}, Z^{MT}\}$, $\{X^{MT}, U_1^{MT}\}$, $\{X^{MT}, U_2^{MT}\}$, $\{Z^{MT}, U_1^{MT}\}$, $\{Z^{MT}, U_2^{MT}\}$, $\{U_1^{MT}, U_2^{MT}\}$; $CCFG_2^{MT} = \{X^{MT}, Z^{MT}, U_1^{MT}\}$, $\{X^{MT}, Z^{MT}, U_2^{MT}\}$, $\{Z^{MT}, U_1^{MT}, U_2^{MT}\}$ and $CCFG_3^{MT} = \{X^{MT}, Z^{MT}, U_1^{MT}, U_2^{MT}\}$. The corresponding common cause factors of two components, three components and four components failure simultaneously are $\beta_1^{MT} = 0.25$, $\beta_2^{MT} = 0.2$ and $\beta_3^{MT} = 0.15$.

The failure rates and failure probabilities of system components at $t = 3000$ h are listed in Table 6.

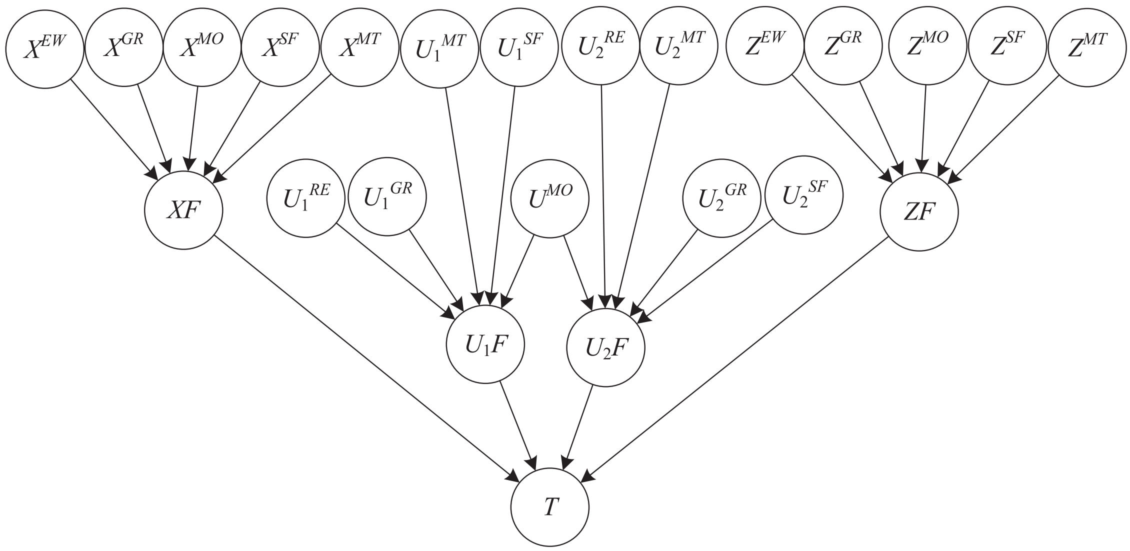

Fig. 10. The system BN with consideration of CCF.

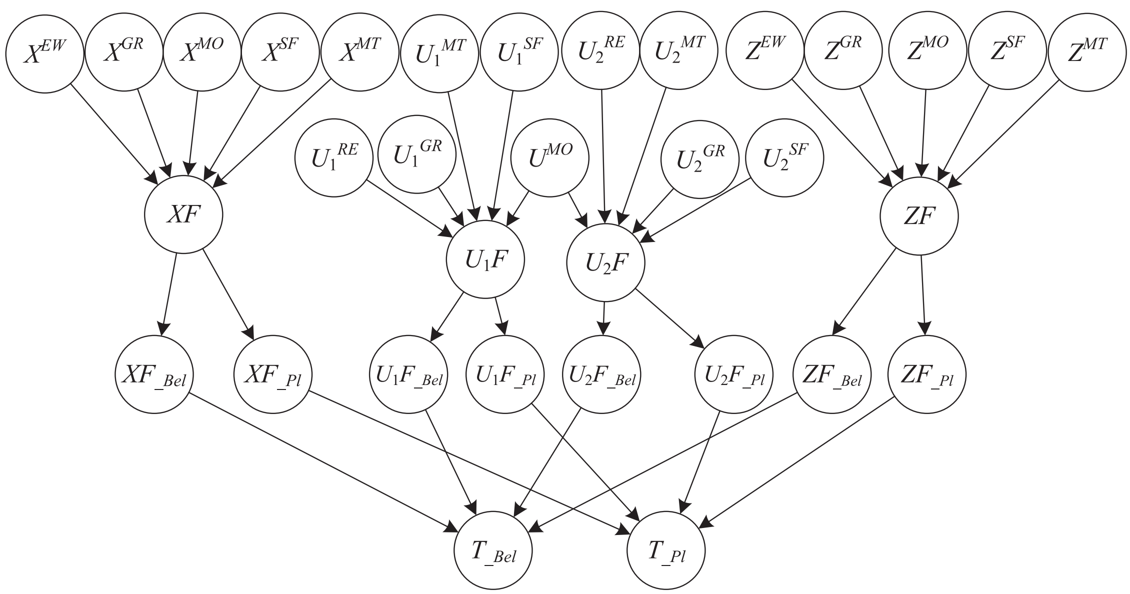

Fig. 11. System EN model.

Based on the transformation method of fault tree to BN and the modified β factor model, the fault tree of feeding control system can be transformed to BN and decomposed by explicit modeling method. When CCFs are considered, the root nodes of BN can be decomposed into independent parts and common cause parts. Then the system BN with consideration of CCFGs can be depicted in Fig. 10 as follows.

The BN of Fig. 10 is the same as system BN structure without considering CCF, the difference is the redefinition of the probabilities of root nodes, then CCF of each components can be taken into consideration. The failure probabilities of components in Table 6 are independent probabilities, then the root nodes' actual failure probabilities can be updated by modified β factor model.

For component A which is not included in multiple CCFGs, the updated failure probabilities of this kind of basic components can be calculated by Eq. (30) and $P'(EW) = 0.0021$, $P'(RE) = 0.0071$, $P'(GR) = 0.0075$, $P'(SF) = 0.0018$, $P'(MO) = 0.0007$. For component MT which is included in multiple CCFGs, the failure probability of MT can be computed by Eq. (30) since it does not meet the limitation that the sum of β factors of different CCFGs is larger than 1, then

$$
\begin{aligned}
P'(MT) &= P(MT_{ind}) + P(MT_{ccf}) \\
&= P(MT_{ind}) + P((CCFG_1^{MT})) + P((CCFG_2^{MT})) \\
&\quad + P((CCFG_3^{MT})) \\
&= P(MT_{ind}) + \left(\frac{\sum_{i=1}^{3} \beta_i^{MT}}{1 - \sum_{i=1}^{3} \beta_i^{MT}} \right) P(MT_{ind}) \\
&= \frac{1}{1 - \sum_{i=1}^{3} \beta_i^{MT}} P(MT_{ind})
\end{aligned}
\tag{32}
$$

Because $(\beta_1^{MT} + \beta_2^{MT} + \beta_3^{MT}) < 1$, the logical contradiction of modified β factor model does not exist here. So, the failure probability of this kind of components with consideration of CCFs can be calculated directly, and $P'(MT) = 0.0520$.

Table 7
The state probabilities of components at $t = 3000$ h with CCF.

Component	State			
	0	1	2	[0,1,2]
MO	0.9993	–	0.0007	–
EW	0.9979	–	0.0021	–
GR	0.9925	–	0.0075	–
MT	0.9304	0.0089	0.0520	0.0087
SF	0.9982	–	0.0018	–
RE	0.9929	–	0.0071	–

4.3. Reliability analysis of feeding control system by using EN

As the main power take-off components of Horizontal lathe, the work state of motors will affect the processing efficiency directly. Therefore, in this paper, there exists an intermediate state between the perfect work state and failure state of the motors of DL series horizontal lathes, called derating work state. So the state space of motors can be expressed as {0, 1, 2}, where, 0 is the perfect working state, 1 is the derating working state and 2 represents failure state. The other components of system are all considered as two-state component. Due to the complexity of the system, the coupling between components and the lack of data, there is a significant amount of epistemic uncertainty which can be represented by an uncertain state [0,1,2] in the state space of system. Assume that the life of all components obey exponential distribution, the basic components state probabilities of feeding control system can be obtained base on existing studies or experts experience and listed in Table 7.

By using the EN node definition and probability reasoning method introduced in Sections 2.1 and 2.2, the conditional mass table (CMT) of non-leaf nodes of EN in Fig. 10 can be gotten. Table 8 is the CMT of non-leaf nodes *XF, ZF,* U_1F and U_2F.

Then the system EN model can be shown as Fig. 11, and the CMT of leaf node *T* is shown in Table 9. By using the multi-state EN reasoning method in Section 2.2, the belief probabilities and plausibility probabilities of non-leaf nodes *XF, ZF,* U_1F and U_2F can be obtained and listed in Table 10.

The belief and plausibility probabilities of leaf node *T* can be calculated by Eqs. (11) and (12), and

$$Bel(T=0) = P(T\_Bel=0) = \sum_{XF,ZF,U_1F,U_2F} Bel(XF,ZF,U_1F,U_2F,T=0)$$

Table 9
The CMT of leaf node *T*.

XF	*ZF*	U_1F	U_2F	(OR)*T*					
				$T_{\_Bel}$			$T_{\_Pl}$		
				0	1	2	0	1	2
0	0	0	0	1	0	0	1	0	0
0	0	0	1	0	1	0	0	1	0
0	0	0	2	0	0	1	0	0	1
0	0	1	0	0	1	0	0	1	0
0	0	1	1	0	1	0	0	1	0
0	0	1	2	0	0	1	0	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
2	2	2	1	0	0	1	0	0	1
2	2	2	2	0	0	1	0	0	1

$$\begin{aligned} &= \sum_{XF,ZF,U_1F,U_2F} Bel(T=0|XF,ZF,U_1F,U_2F)\prod_{i=1}^{n} Bel\left(x_i^{k_i}\right) \\ &= \sum_{XF,ZF,U_1F,U_2F} Bel(T=0|XF,ZF,U_1F,U_2F) \\ &\times Bel(XF)Bel(ZF)Bel(U_1F)Bel(U_2F) \end{aligned} \quad (33)$$

$$\begin{aligned} Pl(T=0) &= P(T\_Pl=0) \\ &= \sum_{XF,ZF,U_1F,U_2F} Pl(XF,ZF,U_1F,U_2F,T=0) \\ &= \sum_{XF,ZF,U_1F,U_2F} Pl(T=0|XF,ZF,U_1F,U_2F)\prod_{i=1}^{n} Pl\left(x_i^{k_i}\right) \\ &= \sum_{XF,ZF,U_1F,U_2F} Pl(T=0|XF,ZF,U_1F,U_2F)Pl(XF)Pl(ZF) \\ &\times Pl(U_1F)Pl(U_2F) \end{aligned} \quad (34)$$

Then the state belief probabilities and plausibility probabilities of leaf node *T* under epistemic uncertainty can be calculated. Table 11 shows the results of system state probabilities when considering the influence of CCFs and without CCFs. In order to illustrate the influence of epistemic uncertainty on system, the uncertain state of component *MT* is classified as perfect work state 0. Then the state probabilities of system at $t = 3000$ h are calculated and also listed in Table 11.

Based on the previous assumption that the lifetime of components obey exponential distribution, and the derating working state is regarded as perfect state. From the belief and plausibility probability of

Table 8
The CMT of non-leaf nodes *XF, ZF,* U_1F and U_2F.

X^{EW} Z^{EW}	X^{GR} Z^{GR}	X^{MO} Z^{MO}	X^{SF} Z^{SF}	X^{MT} Z^{MT}	(OR) *XF, ZF,* U_1F, U_2F					
U^{RE}	U^{GR}	U^{MO}	U^{SF}	U^{MT}	*Bel*			*Pl*		
					0	1	2	0	1	2
0	0	0	0	0	1	0	0	1	0	0
0	0	0	0	1	0	1	0	0	1	0
0	0	0	0	2	0	0	1	0	0	1
0	0	0	0	[0,1,2]	0	0	0	1	1	1
0	0	0	2	0	0	0	1	0	0	1
0	0	0	2	1	0	0	1	0	0	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
2	2	2	2	0	0	0	1	0	0	1
2	2	2	2	1	0	0	1	0	0	1
2	2	2	2	2	0	0	1	0	0	1
2	2	2	2	[0,1,2]	0	0	1	0	0	1

Table 10
The state belief and plausibility probabilities of non-leaf nodes of BN.

Node	State					
	Bel			*Pl*		
	0	1	2	0	1	2
XF	0.919180	0.008793	0.063432	0.927775	0.017388	0.072027
ZF	0.919180	0.008793	0.063432	0.927775	0.017388	0.072027
U_1F	0.914575	0.008749	0.068125	0.923127	0.017301	0.076677
U_2F	0.914575	0.008749	0.068125	0.923127	0.017301	0.076677

Table 11
The state probabilities of leaf node *T*.

Leaf node *T*		Considering CCFGs		
State		0	1	2
Epistemic uncertainty	Belief Prob.	0.706706	0.027431	0.232005
	Plausibility Prob.	0.733514	0.056553	0.280306
Ignore uncertainty	State Prob.	0.733514	0.028204	0.238282
Leaf node *T*		Without considering CCFGs		
State		0	1	2
Epistemic uncertainty	Belief Prob.	0.808964	0.030368	0.119782
	Plausibility Prob.	0.838640	0.062523	0.161703
Ignore uncertainty	State Prob.	0.838640	0.031195	0.122977

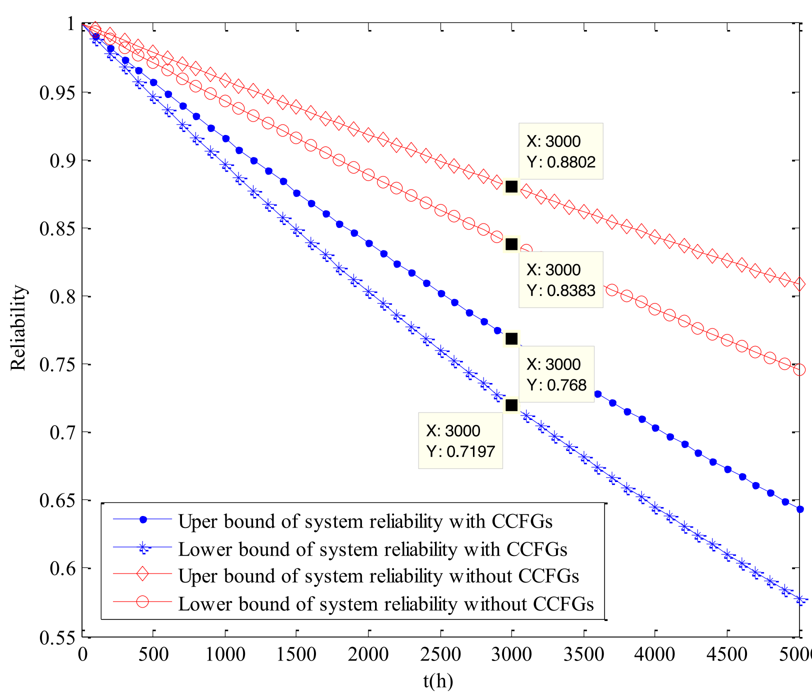

Fig. 12. The contrast curves of the influence of epistemic uncertainty and CCFGs to system reliability.

feeding control system at state 2 in Table 11, it has shown that the failure probability interval and failure rate interval of system at $t = 3000$ h is [0.232005, 0.280306] and $[8.7991\times10^{-5}, 1.0964\times10^{-4}]$/h respectively when consider the influence of epistemic uncertainty and CCFGs. When the CCFGs are ignored, the system failure probability interval will be [0.119782, 0.161703], and failure rate interval is $[4.2529\times10^{-5}, 5.8794\times10^{-5}]$/h. The contrast curves of system reliability with consideration of CCF are also obtained and shown in Fig. 12. From Fig. 12 we know that when the influence of uncertainty is ignored, the failure probability and failure rate of system are 0.238282 and 9.072629×10^{-5}/h. And when the CCF and uncertainty are both ignored, the corresponding failure probability and failure rate of feeding control system are 0.122977 and 4.374068×10^{-5}/h. Finally, the contrast curves of system reliability with epistemic uncertainty are shown in Fig. 13.

This section has built an fault tree model of the feeding control system of a DL series horizontal lath. The evidence theory is induced to quantify the epistemic uncertainty caused by lack of data and information in this system, and combined with BN model formed an EN to

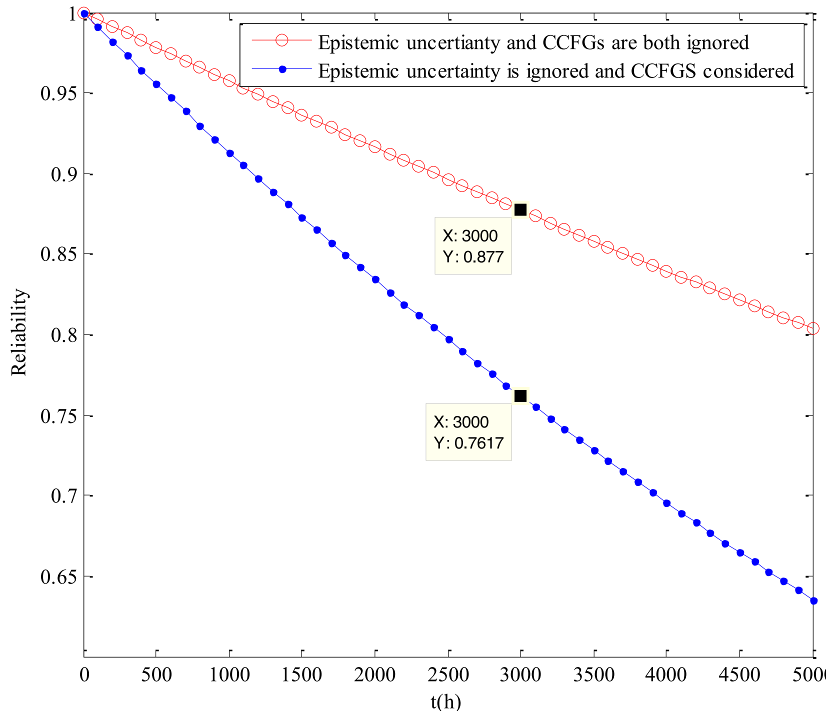

Fig. 13. The contrast curves of the influence of CCFGs to system reliability without considering epistemic uncertainty.

realize the system reliability indexes calculation. A modified β factor model is used to model the CCFGs in the system. From Table 11 and Fig. 12, when the influence of epistemic uncertainty to system is included, system reliability interval at $t = 3000$ h is [0.808964, 0.838640] without considering CCFs, and when the influence of CCFs is also considered, the reliability interval is [0.706706, 0.733514]. This shows that CCFs has considerable impact on system reliability. The system state probabilities in Table 11 when the epistemic uncertainty is ignored are between the corresponding belief probabilities and plausibility probabilities, which verify the accuracy of results. From the results, we can see that the lower bound and upper bound of system reliability are with six digits of accuracy, which means the reliability uncertainty interval is with high accuracy, and sometimes it can be seen as a certain interval. It is essential to distinguish this with the system reliability is accurate and not uncertain. That is to say the system reliability is uncertain but in a relatively certain interval.

5. Conclusions

This paper introduces a reliability analysis method for complex MSS with epistemic uncertainty based on EN. The epistemic uncertainty of system is quantified by adding an uncertain state of root nodes in the multi-state EN, and the state space is then constructed. After that, the belief function and plausibility function are defined using evidence theory. Based on the BN forward reasoning, the measure system reliability and failure probability can be computed. The case study confirms the feasibility of this comprehensive method, and realized a quantitative analysis of system failure state. The backward reasoning can get the posterior probability of failure causes based on the system failure state, and provide guidance for predicting the system failure types.

CCF is an important failure mode in complex system, so the reliability analysis of MSS with consideration of both epistemic uncertainty and CCF are also investigated in this paper. When CCFGs exist in system, a modified β factor model is introduced and integrated with evidence theory based on BN, and realize the state expression and probability reasoning for complex system with epistemic uncertainty and CCFGs. The reliability analysis of the feeding control system of DL series HDHLs by this method has shown that, the proposed comprehensive method has high computing efficiency and theoretical value. In engineering practice, sometimes it is difficult to get enough data and the data are with large uncertainties, therefore this method also has relative practical value with enough good data and sufficient evidence. This paper the nodes of EN are described as discrete variables, so when the system inputs contain both discrete and continuous variables, how to use the hybrid BN method to realize system reliability modeling and system probability reasoning, and how to express and synthesize the multiple complex characteristics are worthwhile further studying and discussing.

Acknowledgments

This research was partially supported by NSFC under the contract number 51775090 and 51405065, the Pre-research Project of General Armament Department under the contract number 41403040103, and the Open Project of Traction Power State Key Laboratory of Southwest Jiaotong University under the contract number TPL 1410.

References

[1] Gu YK, Li J. Multi-state system reliability: a new and systematic review. Procedia Eng 2012;29:531–6.
[2] Massim Y, Zeblah A, Benguediab M, Ghouraf A, Meziane R. Reliability evaluation of electrical power systems including multi-state considerations. Electr Eng 2006;88(2):109–16.
[3] Li YF, Zio E. A multi-state model for the reliability assessment of a distributed generation system via universal generating function. Reliab Eng Syst Saf 2012;106:28–36.
[4] Xue J. On multistate system analysis. IEEE Trans Reliab 1985;34(4):329–37.
[5] Lisnianski A, Elmakias D, Laredo D, Haim HB. A multi-state Markov model for a short-term reliability analysis of a power generating unit. Reliab Eng Syst Saf 2012;98(1):1–6.
[6] Liu YW, Kapur KC. Reliability measures for dynamic multi-state nonrepairable systems and their applications to system performance evaluation. IIE Trans 2006;38:511–20.
[7] Zio E, Podofillini L, Levitin G. Estimation of the importance measures of multi-state elements by Monte Carlo simulation. Reliab Eng Syst Saf 2004;86(3):191–204.
[8] Ramirez-Marquez JE, Coit DV. Composite importance measures for multi-state systems with multi-state components. IEEE Trans Reliab 2005;54:517–29.

[9] Levitin G. The universal generating function in reliability analysis and optimization. Berlin, Germany: Springer-Verlag; 2005.
[10] Mi J, Li YF, Liu Y, Yang YJ, Huang HZ. Belief universal generating function analysis of multi-state systems under epistemic uncertainty and common cause failures. IEEE Trans Reliab 2015;64(4):1300–9.
[11] Zhang Z, Jiang C, Wang GG, Han X. First and second order approximate reliability analysis methods using evidence theory. Reliab Eng Syst Saf 2015;137:40–9.
[12] Mula J, Poler R, Garcia-Sabater JP. Material requirement planning with fuzzy constraints and fuzzy coefficients. Fuzzy Set Syst 2007;158(7):783–93.
[13] Li YF, Mi J, Liu Y, Yang YJ, Huang HZ. Dynamic fault tree analysis based on continuous-time Bayesian networks under fuzzy numbers. Proc Inst Mech Eng O-J Risk Reliab 2015;229(6):530–41.
[14] Li YF, Huang HZ, Zhang H, Xiao NC, Liu Y. Fuzzy sets method of reliability prediction and its application to a turbocharger of diesel engines. Adv Mech Eng 2013 Article ID 216192, 7 pages. doi:10.1155/2013/216192.
[15] Li YF, Huang HZ, Liu Y, Xiao N, Li H. A new fault tree analysis method: fuzzy dynamic fault tree analysis. Eksploat Niezawodn 2012;14(3):208–14.
[16] Mehl CH. P-boxes for cost uncertainty analysis. Mech Syst Signal Process 2013;37(1):253–63.
[17] Yang X, Liu Y, Zhang Y, Yue Z. Hybrid reliability analysis with both random and probability-box variables. Acta Mech 2015;226(5):1341–57.
[18] Mi J, Li YF, Yang YJ, Peng W, Huang HZ. Reliability assessment of complex electromechanical systems under epistemic uncertainty. Reliab Eng Syst Saf 2016;152:1–15.
[19] Sankararaman S, Mahadevan S. Likelihood-based representation of epistemic uncertainty due to sparse point data and/or interval data. Reliab Eng Syst Saf 2011;96(7):814–24.
[20] Lorini E, Prade H. Strong possibility and weak necessity as a basis for a logic of desires. In: Working papers of the ECAI workshop on weighted logics for artificial intelligence; 2012. p. 99–103.
[21] Soundappan P, Nikolaidis E, Haftka RT, Grandhi R, Canfield R. Comparison of evidence theory and Bayesian theory for uncertainty modeling. Reliab Eng Syst Saf 2004;85(1):295–311.
[22] Shah H, Hosder S, Winter T. Quantification of margins and mixed uncertainties using evidence theory and stochastic expansions. Reliab Eng Syst Saf 2015;138:59–72.
[23] Yang JP, Huang HZ, Liu Y, Li YF. Quantification classification algorithm of multiple sources of evidence. Int J Inf Technol Decis Mak 2015;14(5):1017–34.
[24] Zhou Q, Zhou H, Zhou Q, Yang F, Luo L, Li T. Structural damage detection based on posteriori probability support vector machine and Dempster–Shafer evidence theory. Appl Soft Comput 2015;36:368–74.
[25] Zhou J, Liu L, Guo J, Sun L. Multisensory data fusion for water quality evaluation using Dempster–Shafer evidence theory. Int J Distrib Sens Netw 2013;9(11):1–6.
[26] Kohlas J, Monney PA. A mathematical theory of hints: an approach to the Dempster–Shafer theory of evidence. Springer Science & Business Media; 2013.
[27] Pearl J. Fusion, propagation, and structuring in belief networks. Artif Intell 1986;29(3):241–88.
[28] Li YF, Mi J, Huang HZ, Xiao NC, Zhu SP. System reliability modeling and assessment for solar array drive assembly based on Bayesian networks. Eksploat Niezawodn 2013;16(2):117–22.
[29] Weber P, Simon C. Systems dependability assessment: benefits of Bayesian network models. ISTE Ltd and John Wiley & Sons Inc; 2016.
[30] Simon C, Weber P, Levrat E. Bayesian networks and evidence theory to model complex systems reliability. J Comput 2007;2(1):33–43.
[31] Simon C, Weber P, Evsukoff A. Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. Reliab Eng Syst Saf 2008;93(7):950–63.
[32] Simon C, Weber P. Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge. IEEE Trans Rel 2009;58(1):69–87.
[33] Zhao S, Wang H, Cheng D. Power distribution system reliability evaluation by DS evidence inference and Bayesian network method. In: IEEE 11th international conference on probabilistic methods applied to power systems; 2010. p. 654–8.
[34] Simon C, Weber P, Sallak M. Uncertainty of data and important measures. In: Volume 3 - security evaluation of SET systems coordinated by Jean-François Aubry. London and New Jersey: ISTE Ltd and John Wiley & Sons, Inc.; 2018. p. 119–69.
[35] Mi J, Li YF, Huang HZ, Liu Y, Zhang X. Reliability analysis of multi-state systems with common cause failure based on Bayesian networks. Eksploat Niezawodn 2013;15(2):169–75.
[36] Rausand M. Common-cause failures, in risk assessment. Hoboken, New Jersey: John Wiley & Sons, Inc; 2011. p. 469–95.
[37] Mi J, Li YF, Peng W, Yang Y, Huang HZ. Fault tree analysis of feeding control system for computer numerical control heavy-duty horizontal lathes with multiple common cause failure groups. J Shanghai Jiaotong Univ 2016;21(4):504–8.
[38] Kančev D, Čepin M. A new method for explicit modelling of single failure event within different common cause failure groups. Reliab Eng Syst Saf 2012;103:84–93.