Reliability Analysis of Complex System Based on Dynamic Fault Tree and Dynamic Bayesian Network

Zhiqiang LI, Junyuan GU, Tingxue XU, Linyu FU, Jin AN, Qi DONG
Department of Ordnance Science and Technology
Naval Aeronautical & Astronautical University
Yantai, China
18663813941@163.com, 763607429@qq.com, xtx1962@163.com, 2249949260@qq.com
137331253@qq.com, lance0527@163.com

***Abstract*—Traditional static fault tree analysis is widely used to analyze the reliability of complex systems in different fields. To improve their reliability and availability values of complex redundant systems, lots of dynamic gates are used, such as Priority AND (PAND) Gate, Spare Gate, Sequence Enforcing (SEQ) Gate and Functional Dependency (FDEP) Gate. And dynamic fault tree developed on the basis of Markov chain is applied. In order to reduce calculation and avoid finding minimal cut set, dynamic Bayesian network is introduced. And then methods to convert dynamic fault tree events into corresponding Bayesian network nodes are put forward and conditional probability tables are determined by domain experts and logic relations between nodes. At last, an aviation electric system is taken for example. According to its dynamic fault tree model, dynamic Bayesian network model is established, and expanded from the first time slice to the second time slice. The results show that the reliability of aviation electric system decreases gradually when there is no repair. And it will maintain at a high level when repair measures are taken. Through importance analysis, weak nodes in design are pointed out.**

Keywords- dynamic fault tree; Markov chain; dynamic Bayesian network; conditional probability table

I. INTRODUCTION

Traditional fault tree[1, 2] refers to static fault tree (SFT) composed of static gates, such as OR Gate, AND Gate, Two-out-of-three Gate. Static fault tree was put forward by Watson and Haasl in 1961 in Bell laboratory. After then, it was applied in weapon system, aviation industry and nuclear industry. Static fault tree centers on the failure of system. From top down, according to logic relationship and system structure, a fault tree is established vividly. By determining minimal cut set, failure modes and mechanism of the system are obtained. Through qualitative and quantitative analysis, reliability of top event is calculated and weak points are pointed out. However, static fault tree can only express logic relationship with static gates. When it comes to complex systems with redundancy design or a trigger, its disadvantages become obvious. To deal with these problems, dynamic fault tree (DFT) was introduced in 1992 by Prof. Dugan to capture the dynamic mechanism of components in a complex system with sequence depending events[3-5]. In section 2, special dynamic gates of DFT are analyzed briefly. A short introduction of dynamic Bayesian network (DBN) is included in section 3, as well as methods to convert DFT dynamic gates into DBN models. A case is taken for example in section 4 to explain the efficiency of modeling with DBN in terms of dynamic system.

II. SPECIAL DYNAMIC GATES OF DYNAMIC FAULT TREE

Dynamic fault tree was put forward on the basis of Markov Chain (MC). Typical dynamic gates are set according to corresponding MC process[5, 6].

A. Priority AND (PAND) Gate

PAND Gate in DFT is an extension of AND Gate in SFT with an order of component failure. In Fig. 1(a), an example for a PAND Gate is showed, with one output event and two input events. The output event will happen only when component A and B fail simultaneously and component A fails before component B. If only one component fails or component B fails before component A, the output event will not happen.

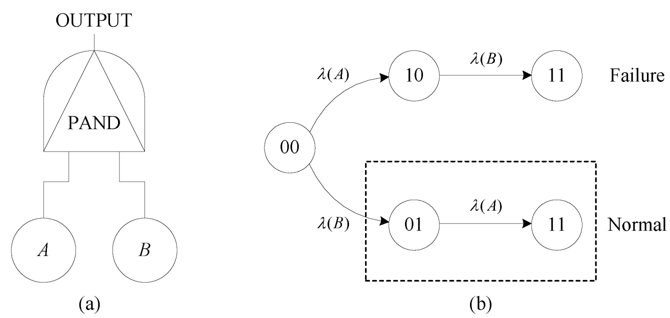

Figure 1. PAND Gate in DFT and its MC model

MC model related to PAND Gate in Fig. 1(a) is displayed in Fig. 1(b). Here $\{xy\}$ represents the state of component A and B, and 0 is for normal, 1 is for failure. $\lambda(A)$ and $\lambda(B)$ are failure rates of component A and B respectively. From MC model, it's obvious that violating the order of failure will not cause the failure of the PAND system. In most model of DFT, components are not repairable, so that MC moves towards one-way without return. In reliability analysis, the part locating in dashed box can be omitted.

This research is supported by Natural Science Foundation of China (No. 51605487), China Postdoctoral Science Foundation (2016M592965)

B. Sequence Enforcing (SEQ) Gate

SEQ Gate is defined as that the failure of the second component B is forbidden before the failure of the first component A presented in Fig. 2. Top event will happen only if component A fails before B. In terms of PAND Gate, failure is allowed in any order, while in SEQ Gate only one order is allowed. With its corresponding MC model, it's easy to understand the principle of SEQ.

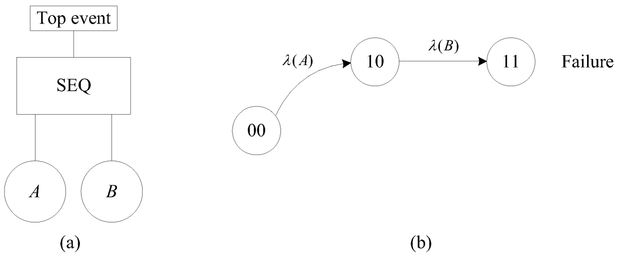

Figure 2. SEQ Gate in DFT and its MC model

C. Warm Spare (WSP) Gate

Spare Gate can be divided into three kinds, Cold Spare (CSP) Gate, Warm Spare (WSP) Gate and Hot Spare (HSP) Gate. Behaviors of spare events (spare components) contained in Spare Gate are different when in active mode and in standby mode. In active mode, the failure rate of component i is λ_i, while in standby mode, its failure rate of component i is $k_i \cdot \lambda_i$. A DFT with HSP and its MC model is showed in Fig. 3.

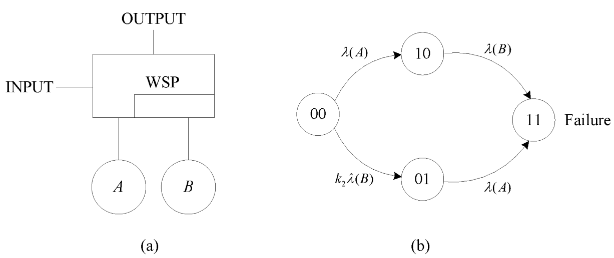

Figure 3. Spare Gate in DFT and its MC model

Spare component B will change its state immediately from standby mode into active mode when component A fails. CSP Gate and HSP Gate are special cases of WSP Gate. If $k_i = 0$, WSP Gate becomes CSP Gate. If $k_i = 1$, WSP Gate becomes HSP Gate. Spare components can be shared and repeated, and corresponding mechanism is relatively complex.

D. Functional Dependency (FDEP) Gate

FDEP Gate is consisted of three parts, a trigger event, unrelated events and related events, showed in Fig. 4. If the trigger happens, all inputs $(A_1, A_2, \cdots, A_n)$ linked to the gate will happen immediately. Failure of unrelated events has no influence on DFT. FDEP Gate is widely used in controlling systems through regulating related events.

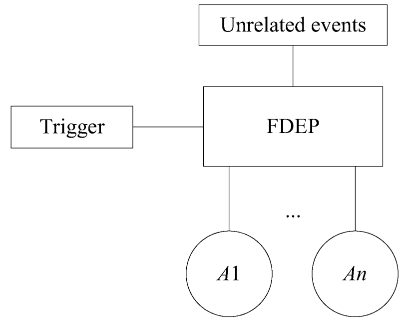

Figure 4. FDEP gate in DFT

III. Dynamic Bayesian Network Modifying Dynamic Fault Tree

Usually, modularization is applied in DFT analysis. At the beginning of calculation, we need to define independent modules in fault tree. If a module is in a static state, binary decision diagram (BDD) can be utilized. If a module is in a dynamic state, Markov chain is available. However, the overall states in Markov chain will increase rapidly with the number of components. This is the so-called combinatory explosion[7, 8]. It becomes obvious that Markov chain cannot be applied for DFT model with large size in many cases.

A. Dynamic Bayesian network

Dynamic Bayesian network[9, 10] developed on the basis of static BN and hidden Markov model is an extension of BN by introducing temporal dependencies. DBN includes a series of time slices and each one is composed by a static BN. A DBN with N nodes is expressed as $N = \langle\langle V, T_n, E\rangle, P\rangle$ including two parts, a directed acyclic graph (DAG) with N nodes denoted as $\langle V, T_n, E\rangle$ and conditional probability tables related to every node denoted as P. Element in node set $V = \{V_1, V_2, \cdots, V_N\}$ represents variable, and it can be a component or just a state of the system. Time slices, denoted as $T_n = \{[t_0, t_1), \cdots, [t_{i-1}, t_i), \cdots, [t_{n-1}, t_n), [t_n, \infty)\}$, are units of time period during which variables happen. And E is a directed edge of nodes representing the relationship between the nodes. A typical DBN model is showed is in Fig. 5. A DBN with T time slices is showed in Fig. 5(a), and then comes an initial BN model and a BN model with two time slices.

Transition probability between two time slices can be denoted as

$$P(X_t \mid X_{t-1}) = \prod_{i=1}^{N} P(X_{t,i} \mid pa(X_{t,i})) \qquad (1)$$

Herein, X_t and X_{t-1} represent the variables at time slice t and $t\text{-}1$ respectively. $X_{t,i}$ represents the i^{th} node in slice t, and its parent nodes are denoted as $pa(X_{t,i})$.

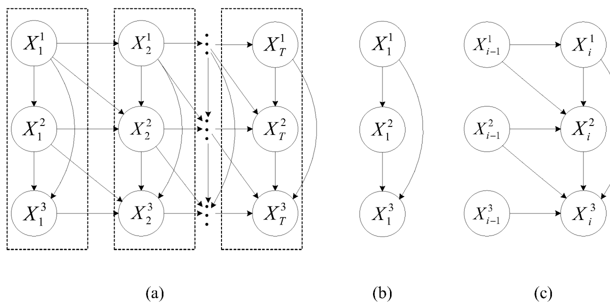

Figure 5. A typical DBN model

Unrolling the T time slices, its joint distribution probability can be obtained as follow

$$P(X_{1:T}) = \prod_{i=1}^{T} \prod_{i=1}^{N} P(X_t^i \mid pa(X_t^i)) \tag{2}$$

B. Converting DFT gates to DBN model

DBN model corresponding to PAND Gate in DFT is showed in Fig. 6(a). The probability distribution of root node X is denoted as[4, 11]

$$\begin{cases} P(X = [(x-1)\Delta, x\Delta)] = e^{-\lambda_X x\Delta}(e^{\lambda_X \Delta} - 1), (0 < x \le n) \\ P(X = [T, \infty]) = \int_T^\infty \lambda_X e^{-\lambda_X t} dt = e^{-\lambda_X T} \end{cases} \tag{3}$$

Where $X = [(x-1)\Delta, x\Delta]$ represents failure of X during the period of $[(x-1)\Delta, x\Delta]$. $X = [T, \infty]$ represents that X will not fail during the period of T. λ_X is failure rate of X obeying exponential distribution. If component A and B fail simultaneously, the top event will happen. Conditional probability distribution of node X_{PAND} is given by

$$\begin{aligned} &P_{x,y,z} = P(X_{PAND} = [(z-1)\Delta, z\Delta] \mid A = [(x-1)\Delta, x\Delta], \\ &B = [(y-1)\Delta, y\Delta]) = \begin{cases} 1, (0 < x \le y = z \le n) \\ 0, (0 < y \le x \le n) \end{cases} \end{aligned} \tag{4}$$

$$\begin{cases} P_{x,\infty,\infty} = P(X_{PAND} = [T, \infty) \mid A = [(x-1)\Delta, x\Delta], B = [T, \infty)) = 1 \\ P_{\infty,y,\infty} = P(X_{PAND} = [T, \infty) \mid A = [T, \infty), B = [(y-1)\Delta, y\Delta]) = 1 \\ P_{\infty,\infty,\infty} = P(X_{PAND} = [T, \infty) \mid A = [T, \infty), B = [T, \infty)) = 1 \end{cases} \tag{5}$$

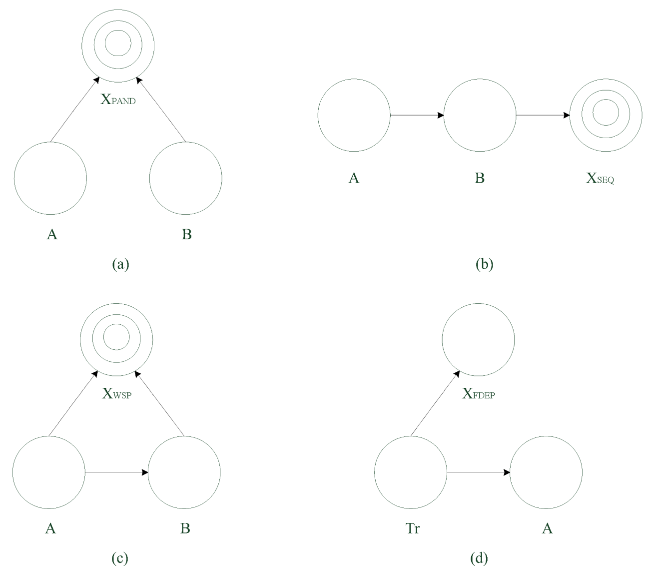

Figure 6. DBN model of dynamic gate in DFT

DBN model corresponding to SEQ Gate in DFT is showed in Fig. 6(b). Conditional probability distribution of node B is given by

$$\begin{aligned} P_{x,y} &= P(B = [(y-1)\Delta, y\Delta] \mid A = [(x-1)\Delta, x\Delta],) \\ &= \begin{cases} 0, (0 < y < x \le n) \\ 1 - \dfrac{\lambda_a (e^{(\lambda_a - \lambda_b)\Delta} - 1)}{(\lambda_a - \lambda_b)(e^{\lambda_a \Delta} - 1)}, (0 < y = x \le n) \\ \dfrac{\lambda_a e^{-(\lambda_a - \lambda_b)(y-x)\Delta}(e^{(\lambda_a - \lambda_b)\Delta} - 1)(e^{\lambda_b \Delta} - 1)}{(\lambda_a - \lambda_b)(e^{\lambda_a \Delta} - 1)}, (0 < x < y \le n) \end{cases} \end{aligned} \tag{6}$$

$$\begin{cases} P_{x,\infty} = P(B = [T, \infty) \mid A = [(x-1)\Delta, x\Delta]) = 1 - \sum\limits_{0 < y \le n} P_{x,y} \\ P_{\infty,\infty} = P(B = [T, \infty) \mid A = [T, \infty)) = 1 \end{cases} \tag{7}$$

Conditional probability distribution of node X_{SEQ} is denoted as

$$\begin{cases} P_{y,y} = P(X_{SEQ} = [(y-1)\Delta, y\Delta] \mid B = [(y-1)\Delta, y\Delta]) = 1 \\ P_{\infty,\infty} = P(X_{SEQ} = [T, \infty) \mid B = [T, \infty)) = 1 \end{cases} \tag{8}$$

DBN model corresponding to WSP Gate in DFT is showed in Fig. 6(c). Let's assume failure rate of component A and spare part B is λ, and dormancy factor is k. Conditional probability distribution of node B can be calculated by

$$P_{x,y}=P(B=[(y-1)\Delta,y\Delta]\mid A=[(x-1)\Delta,x\Delta])$$
$$=\begin{cases} e^{-k\lambda_y\Delta}(e^{k\lambda\Delta}-1),(0<y<x\le n) \\ \dfrac{e^{-k\lambda_y\Delta}}{e^{\lambda\Delta}-1}\left(e^{(1+k)\lambda\Delta}-\dfrac{1+k}{k}e^{k\lambda\Delta}+\dfrac{1}{k}\right),(0<x=y\le n) \\ \dfrac{e^{k\lambda\Delta}-1}{k}e^{\lambda(x-y-k_x)\Delta},(0<x<y\le n) \end{cases} \tag{9}$$

$$\begin{cases} P_{x,\infty}=P(B=[T,\infty)\mid A=[(x-1)\Delta,x\Delta])=1-\sum_{0<y\le n}P_{x,y} \\ P_{\infty,y}=P(B=[(y-1)\Delta,y\Delta]\mid A=[T,\infty))=e^{-k\lambda_y\Delta}(e^{k\lambda\Delta}-1) \\ P_{\infty,\infty}=P(B=[T,\infty)\mid A=[T,\infty))=1-\sum_{0<y\le n}P_{\infty,y} \end{cases} \tag{10}$$

Conditional probability distribution of node X_{WSP} is given as

$$P_{x,y,z}=P(X_{WSP}=[(z-1)\Delta,z\Delta]\mid A=[(x-1)\Delta,x\Delta],$$
$$B=[(y-1)\Delta,y\Delta])=\begin{cases}1,(z=\max(x,y)) \\ 0,(z\ne\max(x,y))\end{cases} \tag{11}$$

$$\begin{cases} P_{x,\infty,\infty}=P(X_{WSP}=[T,\infty)\mid A=[(x-1)\Delta,x\Delta],B=[T,\infty))=1 \\ P_{\infty,y,\infty}=P(X_{WSP}=[T,\infty)\mid A=[T,\infty),B=[(y-1)\Delta,y\Delta])=1 \\ P_{\infty,\infty,\infty}=P(X_{WSP}=[T,\infty)\mid A=[T,\infty),B=[T,\infty))=1 \end{cases} \tag{12}$$

DBN model corresponding to FDEP Gate in DFT is showed in Fig. 6(d). Conditional probability distribution of node A is denoted as

$$P_{x,y}=P(A=[(y-1)\Delta,y\Delta]\mid Tr=[(x-1)\Delta,x\Delta])$$
$$=\begin{cases} e^{-\lambda_A y\Delta}(e^{\lambda\Delta}-1),(0<y<x\le n) \\ 1-\sum_{y<x}P_{x,y},(0<y=x\le n) \\ 0,(0<x<y\le n) \end{cases} \tag{13}$$

$$\begin{cases} P_{\infty,y}=P(A=[(y-1)\Delta,y\Delta]\mid Tr=[T,\infty))=e^{-\lambda_y\Delta}(e^{\lambda\Delta}-1) \\ P_{\infty,\infty}=P(A=[T,\infty)\mid Tr=[T,\infty))=1-\sum_{0<y\le n}P_{\infty,y} \end{cases} \tag{14}$$

Conditional probability distribution of node X_{FDEP} is calculated by

$$\begin{cases} P_{x,x}=P(X_{FDEP}=[(x-1)\Delta,x\Delta]\mid Tr=[(x-1)\Delta,x\Delta])=1 \\ P_{\infty,\infty}=P(X_{FDEP}=[T,\infty)\mid Tr=[T,\infty))=1 \end{cases} \tag{15}$$

IV. A CASE FOR EXAMPLE

An aviation electric system consists three parts, a GNC subsystem (G) with component *e*, a computer subsystem (WSP) with component *c* and *d* and a redundant bus subsystem (CAN) with component *a* and *b*, displayed in Fig. 7. Failure of any subsystem will lead to the failure of AES. According to conversion methods in Section 3, DBN model of DFT of AES is established in Fig. 8. Conditional probability tables of DBN are based on the logic relationship of events. In order to analyze quantitatively, failure rate of events are obtained according to historical failures and experts' experience listed as follows, $\lambda_a=\lambda_b=0.002h^{-1}$, $\lambda_c=\lambda_d=0.003h^{-1}$, $\lambda_e=0.001h^{-1}$, $k=0.1$.

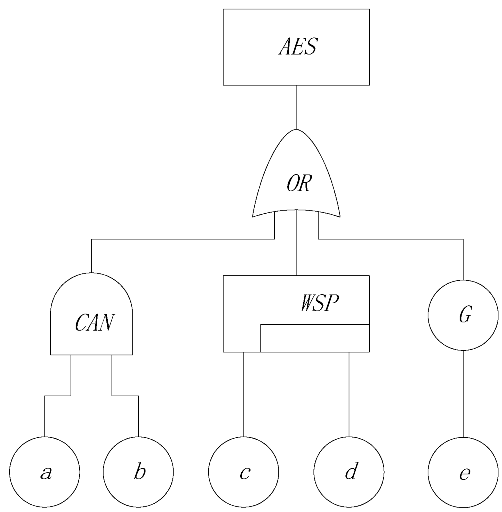

Figure 7. DFT model of AES

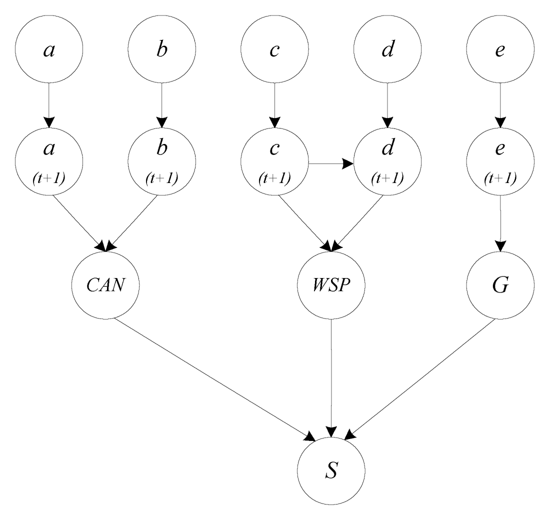

Figure 8. DBN model of AES

By expanding DBN model of AES from time slice *t=1* to *t=2*, an expanded DBN model is obtained, showed in Fig. 9.

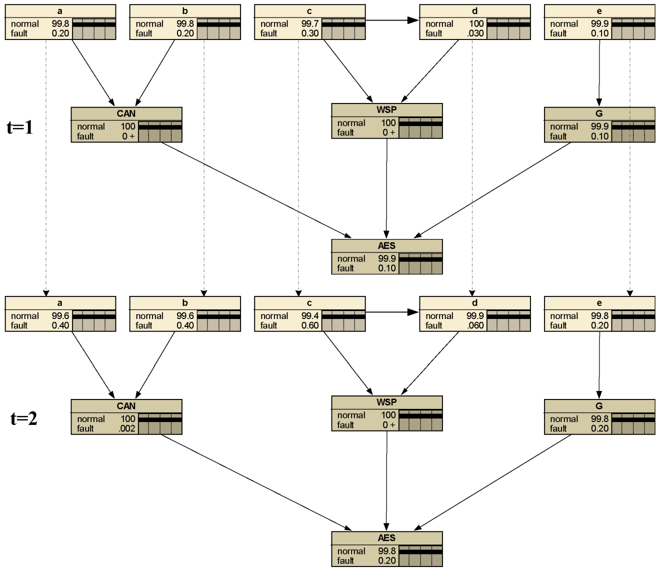

Figure 9. DBN model from *t=1* to *t=2*

After modeling DBN, the reliability of AES can be calculated at given time. Probability curves of node *AES* and its subsystems are showed in Fig. 10, which are consistent with traditional fault tree analysis by referring to literature [3]. Probability values decrease with time going on. When $t=1000$, reliability of AES almost reaches 0, while G_e reaches about 37%. Because it's an OR Gate between node *AES* and its parent nodes, it become obvious that node WSP contributes more to the fall of reliability of the system. And from Fig. 11, a conclusion can be drawn that node *d* and *e* offer more mutual information than other nodes and they're the most important node in reliability analysis. So in reliability design and distribution, more attention should be paid to them.

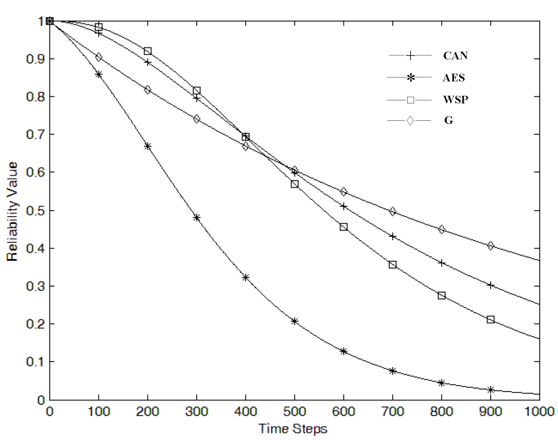

Figure 10. Reliability curves of AES without repair

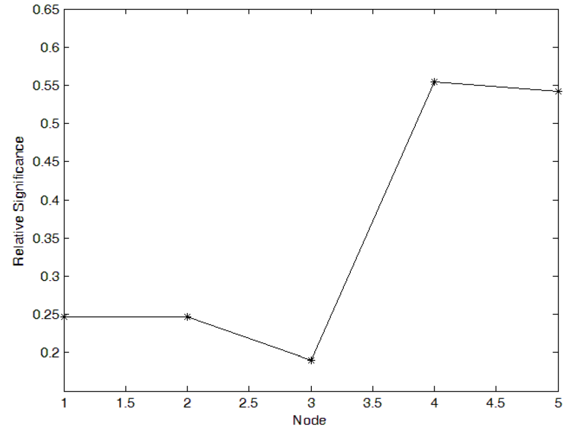

Figure 11. Relative significance of nodes in AES

Above, we discuss the reliability of AES without repair. However, for important equipment repair is a non-negligible factor. The repair rates of components *a-e* are given as $u_a = u_b = 0.15h^{-1}$, $u_c = u_d = 0.10h^{-1}$, $u_e = 0.20h^{-1}$. Then reliability curves of AES and its subsystems are plotted in Fig. 12. Because of repair, the reliability of AES maintains a high level above 0.994. The reliability of subsystem G is relatively higher. And the reliability of WSP and CAN are almost 1. It's obvious that node *e* is the weak node of the system with repair. So in reliability design and assignment, component with high reliability should be adopted.

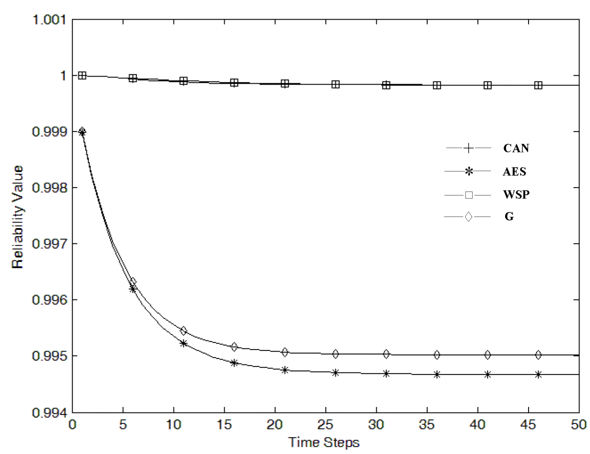

Figure 12. Reliability curves of AES with repair

V. CONCLUSIONS

To overcome the disadvantages of SFT, DFT is introduced into complex systems with dynamic gates such as PAND Gate, SEQ Gate, FDEP Gate and WSP Gate to improve the reliability and availability. To avoid combinatory explosion in using MC method and difficulty in obtaining minimal cut set, DBN is applied.

(1) Dynamic Bayesian network has an advantage in simplifying DFT events, and can reason forward and backward. The same nodes in DFT model can be

represented by only one node in DBN, and relations between nodes can be denoted by conditional probability tables easily.

(2) Through importance analysis, weak nodes in complex systems can be pointed out and corresponding maintenance measures can be taken immediately.

(3) For system without repairable components, period test and maintenance are needed to offer a stable operation environment. And for system with repairable components, test period and maintenance personnel should be optimal according to the desired reliability demand.

ACKNOWLEDGMENT

This research is supported by Natural Science Foundation of China (No. 51605487), China Postdoctoral Science Foundation (2016M592965).

REFERENCES

[1] H. Langsetb, L. Portinale, "Bayesian networks in reliability," Reliab. Eng. Syst. Safe., vol. 92, pp. 92-108, 2007.

[2] A. G. Wilsona, A. V. Huzurbazar, "Bayesian networks for multilevel system reliability," Reliab. Eng. Syst. Safe., vol. 92, pp. 1413-1420, 2007.

[3] M. Cepin, B. Mavko, "A dynamic fault tree," Reliab. Eng. Syst. Safe., vol. 75, pp. 83-91, 2002.

[4] Z. K. Liu, Y. H. Liu, B. P. Cai, D. W. Zhang, C. Zheng, "Dynamic Bayesian network modeling of reliability of subsea blowout preventer stack in presence of common cause failures," J. Loss. Prevent. Proc., vol. 38, pp. 58-66, 2015.

[5] O. Yevkin, "An efficient approximate markov chain method in dynamic fault tree analysis," Qual. Reliab. Eng. Int., vol. 32, pp. 1509-1520, 2016.

[6] L. J. Guo, J. X. Kang, "An extended HAZOP analysis approach with dynamic fault tree," J. Loss. Prevent. Proc., vol. 38, pp. 224-232, 2015.

[7] E. L. Droguett, M. C. Moura, C. M. Jacinto, M. F. S. Jr, "A semi-Markov model with Bayesian belief network based human error probability for availability assessment of downhole optical monitoring systems," Simul. Model. Pract. Th., vol. 16, pp. 1713-1727, 2008.

[8] H. Tjelmeland, P. Arnesen, "Fully Bayesian binary markov random field models: prior specification and posterior simulation," Scand. J. Stat., vol. 42, pp. 967-987, 2015.

[9] N. Khakzad, M. M. Aliabadi, I. M. E. Zarei, A. Azadeh, "Dynamic safety assessment of natural gas stations using Bayesian network," J. Hazard. Mater., vol. 321, pp. 830-840, 2017.

[10] L. M. Zhang, X. G. Wu, M. J. Skibniewski, B. B. Zhong, Y. J. Lu, "Bayesian-network-based safety risk analysis in construction projects," Reliab. Eng. Syst. Safe., vol. 131, pp. 29-39, 2014.

[11] S. Barua, X. D. Gao, H. Pasman, M. S. Mannan, "Bayesian network based dynamic operational risk assessment," J. Loss. Prevent. Proc., vol. 41, pp. 399-410, 2016.