# Safety Analysis Method of Mixed Failure Model using Temporal Bayesian Network

Li Wei[1], Bing-Wu Fang[2,3*]

[1] Department of management, Anhui Zhongao Institute of Technology, China
[2] School of Information Engineering, Anhui Finance and Trade Vocational College, China
[3] Key Laboratory of Safety-Critical Software, Nanjing University of Aeronautics and Astronautics, China
zixian_123@163.com, bingwufang@163.com

## Abstract

Dynamic Fault Tree (DFT) is used widely in the community of reliability and safety analysis of a complex system. DFT is a high-level modeling language lacking formal semantics, so we need to convert it to a mathematical model to analyze. The conventional analysis method can only solve the DFT with discrete or exponential distribution, but not the DFT with mixed distributions. To this end, we first propose a TBN framework to represent the DFT with mixed failure distribution by extending the BN and introduce Dirac delta functions and unit-step functions into the framework to represent the logical relationship and temporal relationship between the nodes, respectively. To run the standard BN inference algorithm over TBN, we fit the failure distribution of the nodes by using *k*-piece and *n*-degree polynomials. We then propose a transformation method from DFT to TBN and prove the equivalence of the transformation. Finally, the analysis of the DFT model of the X2000 avionics system shows that our approach can effectively analyze the reliability of mixed distribution failure models. Moreover, the accuracy and efficiency of the analysis are significantly better than current mainstream methods.

**Keywords:** Dynamic fault tree, Safety analysis, Mixed distribution failure model, Temporal Bayesian Networks

## 1 Introduction

Dynamic fault tree (DFT) has been widely used in reliability modeling of complex dynamic systems in the fields of aerospace, automotive electronics, and nuclear power because of its intuitive, concise, and good description capability [1-2]. DFT, a high-level modeling language, lacks formal semantics and needs to be transformed into a mathematical model for analysis. These models include binary decision graph, Markov chain, and Petri net, which can accurately analyze the DFT with discrete or exponential distributions [3-4]. However, these models are all faced with the infamous state space explosion problem, that is, the number of states grows exponentially with the number of components comprised in the DFT. Therefore, they are time-consuming and inefficient for the analysis of complex DFT.

To this end, researchers use Bayesian network (BN) for solving the DFT because the state of any node in BN only depends on the state of its neighbors, which effectively alleviates the problem of state space explosion, and the method also improves the modeling and analysis ability of DFT [5-6]. Boudali and Dugan proposed a discrete-time Bayesian network (DTBN) to analyze DFT in which mission time was partitioned into a finite number of time intervals [7]. Each root node of the DTBN has a finite number of states which equals to the number of time intervals. By partition, the conditional probability table (CPT) of the DTBN node can represent sequential failure, redundancy failure, and functional dependency failure of the components. The inference algorithm of BN can run over DTBN. However, the increase in the number of time intervals results in some huge and intractable CPT. To reduce the dimension of the CPT, Khakzad decomposed the CPT of the DTBN node into some intermediate nodes, which transformed the DFT into a chain BN structure [8]. Fang used a decision tree to represent the CPT and proposed a hierarchical DTBN inference algorithm to improve the analysis efficiency [9]. Marquez developed a hybrid BN to incorporate both discrete and continuous variables [10]. They used a dynamic time discretization method to improve the accuracy and efficiency of DTBN analysis. In this method, a finer interval partition is performed in the high-density region of the failure distribution to overcome the poor accuracy of the DTBN with a uniform partition. To analyze the DFT with continuous-time failure probability density function (PDF), Boudali and Dugan proposed a continuous-time BN (CTBN) framework in which one can perform various analyses, including reliability, sensitivity, and uncertainty analyses, and all the analyses allow the user to obtain closed-form solutions [11].

However, Existing methods can only analyze the DFT with discrete or exponential distributions and cannot effectively analyze the DFT with mixed distributions. To solve this problem, we present a temporal Bayesian network (TBN) framework for the analysis of the DFT with mixed distributions. We first extend BN to TBN by introducing the Dirac function and unit step function into the BN to express the logical relationship and temporal relationship among its nodes, respectively. We then propose a transformation method from DFT to TBN and prove the equivalence of the transformation. Because the failure distribution of nodes in TBN follows different distributions, and these operations among distributions, such as integration, marginalization, and

*Corresponding Author: Bing-Wu Fang; E-mail: bingwufang@163.com
DOI: 10.53106/160792642022072304008

multiplication, are not closed-form solutions, the standard BN inference algorithm cannot run on TBN. To this end, we use *k*-piece and *n*-degree polynomials to fit the failure distribution of these nodes, so that all parameters in the TBN are represented uniformly by *k*-piece and *n*-degree polynomials. Since the family of polynomials is closed under integration, marginalization, and multiplication, the BN inference algorithms can run on TBN. Our method can adjust the network parameters *k* and *n* to trade-off between the efficiency and accuracy of the analysis and avoid the state space explosion. By applying this method, one can solve a variety of DFT including unreliability, importance indices, and diagnosis, etc.

The rest of this paper is organized as follows: In Section 2, we propose an TBN framework based on the BN. Section 3 present the method of converting DFT to TBN. We prove the equivalence of the conversion in Section 4. In Section 5, we provide a case study and discuss analysis results. Section 6 give a conclusion and future research.

# 2 TBN Framework

The dynamic logic gates of DFT, such as SEQ, PAND and Spare, are used to model the failure scenario of temporal sequence. However, in the standard BN, the CPT expressing the relationship between nodes cannot express temporal relationship and continuous conditional probability distribution (CPD). Therefore, we propose a TBN to represent the DFT with mixed failure distribution by extending the BN.

## 2.1 Representation of Temporal Relationship

In the TBN formalism, we first divide the time domain [0, *T*] of the nodes representing primary components of the DFT into *k* disjoint time intervals, where *T* is mission time, and *k* is the time granularity. Then, the time domain of the failure distribution of the nodes is similarly divided, and an *n*-degree polynomial is used to fit the failure distribution piece in the time interval (see 2.2).

In addition, we introduce Dirac delta functions and unit-step functions into the framework as the components of the CPD of non-root nodes to represent the logical relationship and temporal relationship between the nodes, respectively.

In summary, the primary components of the DFT may fail in different time intervals, so, in the TBN, the failure order of all components can be expressed, and CPDs represented by these two functions can express the logical relationship and timing relationship between nodes Therefore, the TBN can represent the semantics of DFT. The definitions of these two functions on the interval [0, $\infty$) are as follows.

**Definition 1**. Dirac delta functions

$$\delta(x)=\begin{cases}0 & x\neq 0\\ \infty & x=0\end{cases}, \text{ and } \int_0^{\infty}\delta(x)\mathrm{d}x=1$$

By definition, we may regard the Dirac delta function as a PDF. Although the value $\delta(0)$ is undefined, we can interpret it as probability 1. Consider the normal PDF with mean 0 and variance $\sigma$^2. Its moment-generating function has a value of 1 when $\sigma$^2→0, so the value of $\delta(0)$ can be regarded as probability 1.

**Definition 2.** Unit-step functions

$$u(x)=\begin{cases}0 & x<0\\ 1 & x\geq 0\end{cases}$$

$\delta(x)$ is the derivative of $u(x)$ with respect to $x$. $u(x)$ can be regarded as the limit of the cumulative distribution functions of the Gaussian random variable with mean 0 and variance $\sigma$^2 when $\sigma$^2→0.

## 2.2 Piecewise Fitting of Failure Distributions

When analyzing DFT with mixed failure distribution, the distributions of nodes in the TBN may be exponential, Weibull distribution, Gaussian distribution, and so on, and the multiplication and integration of these distributions are not a closed-form. Therefore, it is impossible to run the automatic reasoning algorithm in the TBN that runs well in the BN.

To solve this problem, in each time interval, we use a *n*-degree polynomial to fit the corresponding the failure distribution piece. That is, the failure distribution of the node is fitted by a *k*-piece and *n*-degree polynomial. In addition, the CPD represented by Dirac functions and unit step functions are also piecewise polynomials in nature. Therefore, all parameters in the TBN are represented by piecewise polynomials which are closed under multiplication, integration, and addition, so, the inference algorithm of the BN can run on the TBN.

**Definition 3.** A one-dimensional function $f$: R→R is said to be a *k*-piece and *n*-degree polynomials function if it is a piecewise function of the form:

$$f(x)=\begin{cases}\sum_{i=0}^{n}a_{ij}x^{i}, & x\in\Omega_j, j=0,...,k-1,\\ 0, & otherwise,\end{cases}$$

where $\Omega_0$, …, $\Omega_{k-1}$ are disjoint intervals in R that do not depend on $x$, and $a_{ij}$ are constants and $a_{nj}\neq 0$ for all $i, j$.

We construct the *k*-piece and *n*-degree polynomial to fit the failure distribution of the node by using Newton interpolation with Chebyshev points in each time interval. Newton interpolation in the interval can eliminate the Runge phenomenon and choosing the Chebyshev point as the interval interpolation point can further improve the fitting accuracy. As a result, a polynomial with small *k* and *n* can fit the failure distribution of the node accurately. We can effectively adjust TBN complexity and accuracy by adjusting parameters *k* and *n*. For the interval ($a$, $b$), the *n* Chebyshev points are given by

$$x_j=\frac{1}{2}(a+b)+\frac{1}{2}(b-a)\cos\frac{2j-1}{2n}\pi, j=1,\ldots,n$$

# 3 Converting DFT to TBN

## 3.1 Conversion Steps from DFT to TBN

The DFT is converted to TBN by two steps of structure conversion and parameter mapping. Figure 1 shows the conversion process from DFT to TBN. In the structure conversion, the primary components, gates, and the system

(top events) of the DFT are converted into root nodes, intermediate nodes, and a leaf node of the TBN, respectively. In the parameter mapping, the PDF of the component is mapped to the marginal distribution of the corresponding root node, and the semantics of the gate is mapped to the CPD of the corresponding intermediate node. After transformation, the nodes in TBN are divided into three categories: the root node corresponds to the component of the system, the intermediate node corresponds to the subsystem, and the leaf node corresponds to the system.

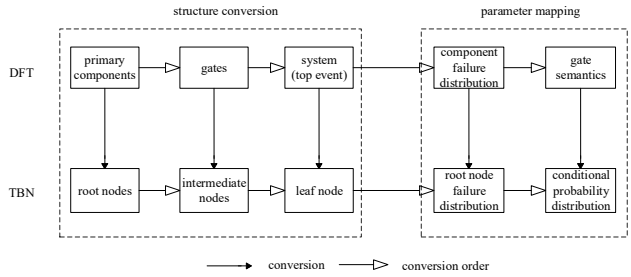


**Figure 1.** Conversion steps from DFT to TBN

## 3.2 Structure Conversion

The structure from DFT to BN shows in Figure 2 and Figure 3, in which *X* and *Y* denote the input component, and *Z* denotes the subsystem. Figure 2(a), Figure 2(b), and Figure 2(c) are AND, OR, and PAND gates of the DFT, respectively, and they have the same TBN structure, as shown in Figure 2(d). Figure 3(a) shows a Spare gate. Figure 3(b) and Figure 3(c) show the corresponding TBN structures of the WSP and CSP, respectively, and the TBN structure of the HSP is the same as the AND gate shown in Figure 2(d).

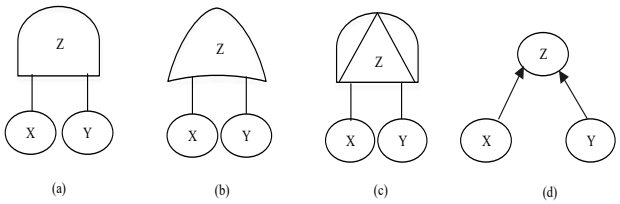


**Figure 2.** AND, OR and PAND gates of DFT and the corresponding TBN structures

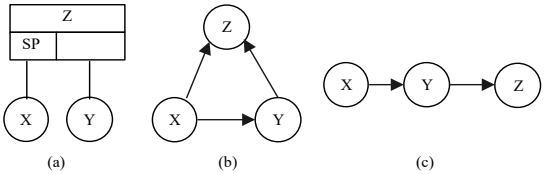


**Figure 3.** The Spare gate of DFT and the corresponding TBN structures

## 3.3 Semantics Mapping

We use the CPD of the non-root node of the TBN to represent the logical semantics of the DFT gate. Let *x*, *y* and *z* denote the failure time of *X*, *Y*, and *Z*, respectively, and assume that the components *X*, *Y* fail not at the same time.

### 3.3.1 TBN Parameters of AND Gate

The AND gate has more than two input components, which can be primary components or subsystems. When all input components fail, the AND gate subsystem fails. According to the AND gate failure mechanism, the dependence of the AND subsystem *Z* and the input components *X*, *Y* is

$$f_{\mathrm{AND}}(z|x,y)=u(x-y)d(z-x)+u(y-x)d(z-y) \quad \textbf{(1)}$$

where $u(x\text{-}y)$ $\delta(z\text{-}x)$ indicates that the *X* fails after the *Y*, and the failure of the *Z* depends on the *X*. $u(y\text{-}x)$ $\delta(z\text{-}y)$ indicates that the *X* fails before the *Y*, and failure of the *Z* depends on the *Y*.

### 3.3.2 TBN Parameters of OR Gate

The OR gate has more than two input components, which can be primary components or subsystems. When at least one of the input components fails, the OR gate subsystem fails. According to the OR gate failure mechanism, the dependence of the OR subsystem *Z* and the input components *X*, *Y* is

$$f_{\mathrm{OR}}(z|x,y)=u(x-y)d(z-y)+u(y-x)d(z-x) \quad \textbf{(2)}$$

where $u(x-y)d(z-y)$ indicates that the *X* fails after the *Y* and the failure of the *Z* depends on the *Y*. $u(y-x)d(z-x)$ indicates that the *X* fails before the *Y* and failure of the *Z* depends on failure of the *X*.

### 3.3.3 TBN Parameters of PAND Gate

The PAND has more than two input components, which can be primary components or subsystems. The PAND subsystem fails when the components fail by the order from left to right. According to the PAND failure mechanism, the dependence of the PAND subsystem *Z* and the input components *X*, *Y* is

$$f_{\mathrm{PAND}}(z\mid x,y)=u(y-x)\delta(z-y)+u(x-y)\delta(z-\infty) \quad \textbf{(3)}$$

where $u(y-x)\delta(z-y)$ indicates that the *X* fails before the *Y* and the failure of the *Z* depends on the *Y*. $u(x-y)\delta(z-\infty)$ indicates that the *X* fails after the *Y* and the subsystem *Z* does not fail.

### 3.3.4 TBN Parameters of SP Gate

The spare gate has one primary component and one or more spare parts. When the primary component fails, it is replaced by the first spare. When the spare fails, it is replaced by the next spare, and so on. When all spares fail, the spare gate fails. We first map the semantics of the WSP into TBN. According to the failure mechanism of the WSP, the CPD of *Z* is the same as that of the AND gate and the CPD of *Y* is given by Theorem 1.

**Theorem 1**. In the TBN structure corresponding to the WSP, the CPD of the node *Y* is expressed by

$$f_{\mathrm{WSP}}(y|x)=u(x\text{-}y)\alpha f_Y(y)(1\text{-}F_Y(y))^{\alpha-1}+u(y\text{-}x)f_Y(y)(1\text{-}F_Y(x))^{\alpha-1} \quad \textbf{(4)}$$

where $f_Y(y)$ and $F_Y(y)$ represent the PDF and the CDF of $Y$, respectively. $\alpha$ is the dormancy factor of the spare gate and $\alpha \in (0, 1)$.

**Proof.** The failure rate of $Y$ is determined by its working state. When $Y$ is active, its failure rate is $\lambda(t)$; When $Y$ is in standby, its failure rate is $a\,\lambda(t)$. Thus, the conditional failure rate of $Y$ is expressed as follows:

$$\lambda(y \mid x) = u(x - y)a\,\lambda(y) + u(y - x)\lambda(y) \quad \textbf{(5)}$$

According to the relationship between failure rate and failure distribution, the CPD $f_{\mathrm{WSP}}(y \mid x)$ of $Y$ is expressed by

$$f_{\mathrm{WSP}}(y|x) = \lambda(y \mid x)e^{-\int_0^y \lambda(t|x)\,\mathrm{dt}} \quad \textbf{(6)}$$

Substituting Equation (5) into Equation (6), then we get the following expression:

$$\begin{aligned} f_{\mathrm{WSP}}(y|x) &= (u(x\text{-}y)\alpha\lambda(y) + u(y\text{-}x)\lambda(y))e^{-\int_0^y \lambda(t|x)\,\mathrm{dt}} \\ &= u(x\text{-}y)\alpha\lambda(y)e^{-\int_0^y u(x-t)\alpha\lambda(t)\,\mathrm{dt}}e^{-\int_0^y u(t-x)\lambda(t)\,\mathrm{dt}} \\ &+ u(y\text{-}x)\lambda(y)e^{-\int_0^y u(x-t)\alpha\lambda(t)\,\mathrm{dt}}e^{-\int_0^y u(t-x)\lambda(t)\,\mathrm{dt}} \end{aligned}$$

The first term indicates that the $Y$ fails before the $X$. Since the $Y$ is independent of the $X$, $u(x\text{-}t) = 1$ and $u(t\text{-}x) = 0$. The second term indicates that the $Y$ fails after the X, where the first integral term indicates that the $Y$ is in the standby state and the second integral term indicates that the $X$ has failed, and the $Y$ transitions from the standby state to the active state. Substituting $l(t) = f(t)/(1\text{-}F(t))$, where $F(t) = 1 - e^{-\int_0^t \lambda(\tau)d\tau}$ into the above formula we have:

$$\begin{aligned} f_{\mathrm{WSP}}(y|x) &= u(x\text{-}y)\alpha\lambda(y)e^{-\int_0^y \alpha\lambda(t)\,\mathrm{dt}} \\ &+ u(y\text{-}x)\lambda(y)e^{-\int_0^x \alpha\lambda(t)\,\mathrm{dt}}e^{-\int_x^y \lambda(t)dt} \\ &= u(x\text{-}y)\alpha\lambda(y)(e^{-\int_0^y \lambda(t)\,\mathrm{dt}})^{\alpha} \\ &+ u(y\text{-}x)\lambda(y)(1\text{-}F_Y(x))^{\alpha}e^{-\int_0^y \lambda(t)\,\mathrm{dt}+\int_0^x \lambda(t)\,\mathrm{dt}} \\ &= u(x\text{-}y)\alpha f_Y(y)(1\text{-}F_Y(y))^{\alpha-1} \\ &+ u(y\text{-}x)f_Y(y)(1\text{-}F_Y(x))^{\alpha-1} \end{aligned}$$

According to the failure mechanism of the HSP gate, the CPD of $Z$ is represented by Equation (1), which is equivalent to that of the AND gate. Substituting $\alpha$=1 into Equation (4), we can get the CPD of $Y$ as follows:

$$f_{\mathrm{HSP}}(y \mid x) = f_Y(y) \quad \textbf{(7)}$$

For the CSP gate, substituting $\alpha$=1 into Equation (4) we have: $f_{CSP}(y \mid x) = u(y - x)f_Y(y)(1 - F_Y(x))^{-1}$. Since $Y$ is in the cold standby state before $X$ fails, $f_Y(y)$is replaced by $f_Y(y - x)$ and $F_Y(x) = 0$. Therefore, the CPD of $Y$ is reduced to

$$f_{\mathrm{CSP}}(y \mid x) = u(y - x)f_Y(y - x) \quad \textbf{(8)}$$

According to the failure mechanism of the CSP gate, When the $Y$ fails, the $Z$ fails, that is, the failure behaviors of $Y$ and $Z$ are the same. Therefore, we get the CPD of $Z$ as follows:

$$f_{\mathrm{CSP}}(z \mid y) = d(z - y) \quad \textbf{(9)}$$

**Theorem 2.** Equations (1) to (4), (7) to (9) are all normalized CPDs.

**Proof.** For the AND gate, according to definition 1 and Equation (1), we get:

$$\begin{aligned} \int_0^{\infty} f_{\mathrm{AND}}(z \mid x, y)dz &= u(x - y)\int_0^{\infty}\delta(z - x)dz \\ &+ u(y - x)\int_0^{\infty}\delta(z - y)dz \\ &= u(x - y) + u(y - x) = 1. \end{aligned}$$

For the PAND gate, according to definition 1 and Equation (3), we get:

$$\begin{aligned} \int_0^{\infty} f_{\mathrm{PAND}}(z \mid x, y)dz &= u(y - x)\int_0^{\infty}\delta(z - y)dz \\ &+ u(x - y)\int_0^{\infty}\delta(z - \infty)dz \\ &= u(y\text{–}x) + u(x\text{–}y) = 1. \end{aligned}$$

For the WSP gate, according to definition 2 and Equation (4), we get:

$$\begin{aligned} \int_0^{\infty} f_{\mathrm{WSP}}(y \mid x)dy &= \int_0^{\infty} u(x - y)\,\alpha f_Y(y)(1 - F_Y(y))^{\alpha-1}dy \\ &+ \int_0^{\infty} u(y - x)f_Y(y)(1 - F_Y(y))^{\alpha-1}dy \\ &= \int_0^{x} \alpha f_Y(y)(1 - F_Y(y))^{\alpha-1}dy \\ &+ \int_x^{\infty} f_Y(y)(1 - F_Y(x))^{\alpha-1}dy = 1. \end{aligned}$$

Similarly, the CPDs of the OR gate, HSP gate and CSP gate are also all normalized.

# 4 Equivalence of Conversion

In order to ensure the correctness of the DFT to TBN structural conversion (Figure 2 and Figure 3) and semantic mapping (Equation (1) to (4), Equation (7) to (9)), in this section, from the perspective of probability calculation, we prove equivalence of DFT gate and corresponding node of TBN.

**Definition 4.** Probability Calculations Equivalence. Let $\mathrm{Pr}_{\mathrm{DFT}}(z' \le t)$ denote the failure probability of gate $Z$' in DFT, and $\mathrm{Pr}_{\mathrm{TBN}}(z \le t)$ denote the failure probability of corresponding node $Z$ in TBN, if $\mathrm{Pr}_{\mathrm{DFT}}(z' \le t) = \mathrm{Pr}_{\mathrm{TBN}}(z \le t)$, then it is said that the gate $Z$' and the node $Z$ are probability calculations equivalence.

**Theorem 3.** The failure distributions of the corresponding TBN nodes $Z$ of the AND, OR, and PAND gates are represented by Equations (10) to (12), respectively, which are normalized failure distributions and satisfy the probability calculations equivalence.

$$f_{Z_{\mathrm{AND}}}(z) = F_X(z)f_Y(z) + F_Y(z)f_X(z) \quad \textbf{(10)}$$

$$f_{Z_{\mathrm{OR}}}(z) = f_X(z) + f_Y(z) - (F_X(z)F_Y(z))' \quad \textbf{(11)}$$

$$fz_{PAND}(z)\, F_X(z)\, f_Y(z) + \delta(z-\infty) \int_0^{\infty} f_Y(y)(1-F_Y(y))dy \quad \textbf{(12)}$$

**Proof.** Let the factors of the TBN nodes *X*, *Y* and *Z* in Figure 2 be $f(x)$, $f(y)$, $f(x,y,z)$, respectively and $f(x) = f_X(x)$, $f(y) = f_Y(x)$, $f(x,y,z) = f_{Z|X,Y}(z \mid x,y)$. According to the BN principle, the marginalized distribution of node Z is represented as follows.

$$\begin{aligned} f_Z(z) &= (f(x) f(y) f(x,y,z))^{-\{X,Y\}} \\ &= ((f(x) f(x,y,z))^{-X} f(y))^{-Y} \end{aligned} \quad \textbf{(13)}$$

*A. AND gate*

Substituting Equation (1) into Equation (13) and eliminating variable *x*, we get:

$$\begin{aligned} &((\phi(x)\,\phi(x,y,z))^{-x} \\ &= \int_0^{\infty} (u(y-x)\ \delta(z-y) + u(x-y)\delta(z-x)) f_X(x)dx \\ &= \delta(z-y) \int_0^{\infty} u(y-x) f_X(x)dx \\ &+ \int_0^{\infty} u(x-y)\delta(z-x) f_X(x)dx \\ &= \delta(z-y) F_X(y) + u(z-y) f_X(z). \end{aligned}$$

Next, eliminating the variable *Y*, we get:

$$\begin{aligned} &((\phi(x)\,\phi(x,y,z))^{-X}\phi(y))^{-Y} \\ &= \int_0^{\infty} \delta(z-y)\, F_X(y) f_Y(y)dy + \int_0^{\infty} u(z-y)\, f_X(z) f_Y(y)dy \\ &= F_X(z) f_Y(z) + F_Y(z) f_X(z) \end{aligned}$$

Therefore, Equation (10) holds. Since the integral of Equation (10) $\int_0^{\infty} f_{Z_{\mathrm{AND}}}(z)\mathrm{d}z = [F_X(z)F_Y(z)]_0^{\infty} = 1$, it is a normalized probability density distribution. The failure probability of *Z* in the interval$[0,t]$ $F_Z(t) = Pr(z \le t) = F_X(t)\ F_Y(t)$, which is equivalent to the result of the algebraic analysis method [12]. Similarly, the OR gate can be proved.

*B. PAND gate*

Substituting Equation (3) into Equation (13) and eliminating variable *x*, we get:

$$\begin{aligned} &((\phi(x)\,\phi(x,y,z))^{-X} \\ &= \int_0^{\infty} (u(y-x)\ \delta(z-y) + u(x-y)\ \delta(z-\infty)) f_X(x)dx \\ &= \delta(z-y) \int_0^{\infty} (u(y-x) f_X(x)dx \\ &\quad + \delta(z-\infty)) \int_0^{\infty} u(x-y) f_X(x)dx \\ &= \delta(z-y)\, F_X(y) + \delta(z-\infty)(1-F_X(y)). \end{aligned}$$

Next, eliminating the variable *Y*, we get:

$$\begin{aligned} &((f(x) f(x,y,z))^{-X} f(y))^{-Y} \\ &= \int_0^{\infty} d(z-y) F_X(y) f_Y(y)dy + d(z-\infty) \int_0^{\infty} (1-F_X(y)) f_Y(y)dy \\ &= F_X(z) f_Y(z) + d(z-\infty) \int_0^{\infty} (1-F_X(y)) f_Y(y)dy \end{aligned}$$

Therefore, Equation (12) holds. Since the integral of Equation (12)

$$\begin{aligned} &\int_0^{\infty} f_{Z_{\mathrm{PAND}}}(z)\mathrm{d}z = \int_0^{\infty} F_X(z) f_Y(z)\mathrm{d}z + \int_0^{\infty} \delta(z-\infty)\mathrm{d}z \int_0^{\infty} f_Y(y)(1-F_X(y))\mathrm{d}y \\ &= \int_0^{\infty} F_X(z) f_Y(z)\mathrm{d}z + (1-\int_0^{\infty} f_Y(y) F_X(y)\mathrm{d}y) \int_0^{\infty} \delta(z-\infty)\mathrm{d}z \\ &= \int_0^{\infty} F_X(z) f_Y(z)\mathrm{d}z + (1-\int_0^{\infty} f_Y(y) F_X(y)\mathrm{d}y) = 1, \end{aligned}$$

It is also a normalized PDF. The failure probability of *Z* in the interval [0, *t*]

$$\begin{aligned} &Fz_{PAND}(t) = Pr(z \le t) \int_0^t F_X(z) f_Y(z)dz \\ &+ (1- \int_0^t F_X(y) f_Y(y)dy) \int_0^{\infty} \delta(z-\infty)dz \\ &= \int_0^t F_X(z) f_Y(z)dz, \end{aligned}$$

which is equivalent to the calculation of the algebraic analysis method [12].

**Theorem 4.** The failure distributions of TBN nodes *Z* in Figure 3(b), Figure 3(c) and Figure 2(d) are represented by Equations (14) to (16), respectively, which are normalized failure distributions and satisfy the probability calculations equivalence.

$$\begin{aligned} fz_{WSP}(z) = f_Y(z) \int_0^z f_X(x)(1-F_Y(x))^{\alpha-1}dx \\ + f_X(z)(1-(1-F_Y(z)^{\alpha}) \end{aligned} \quad \textbf{(14)}$$

$$f_{Z_{\mathrm{HSP}}}(z) = f_Y(z)F_X(z) + f_X(z)F_Y(z) \quad \textbf{(15)}$$

$$fz_{CSP}(z) = \int_0^z f_X(x) f_Y(z-x)\, dx \quad \textbf{(16)}$$

**Proof.** The marginal distribution of the corresponding TBN node *Z* of the WSP gate can be represented as follows.

$$\begin{aligned} f_{Z_{\mathrm{WSP}}}(z) &= (f(x) f(x,y) f(x,y,z))^{-\{X,Y\}} \\ &= ((f(x,y) f(x,y,z))^{-Y} f(y))^{-X} \end{aligned} \quad \textbf{(17)}$$

Substituting Equation (4) into Equation (17) and eliminating variable *X*, we get:

$$\begin{aligned} &(\phi(x,y)\,\phi(x,y,z))^{-Y} \\ &= \int_0^{\infty} (u(y-x)\ \delta(z-y) + u(x-y)\ \delta(z-x)) f_{X|Y}(x|y)dy \\ &= \int_0^{\infty} (u(y-x)\ \delta(z-y)\, u(x-y)\ \alpha f_Y(y)(1-F_Y(y))^{\alpha-1}dy \\ &+ \int_0^{\infty} (u(y-x)\ \delta(z-y)\, u(y-x) f_Y(y)(1-F_Y(x))^{\alpha-1}dy \\ &+ \int_0^{\infty} (u(x-y)\ \delta(z-x)\, u(x-y)\ \alpha f_Y(y)(1-F_Y(y))^{\alpha-1}dy \\ &+ \int_0^{\infty} (u(x-y)\ \delta(z-x)\, u(y-x) f_Y(y)(1-F_Y(x))^{\alpha-1}dy \\ &= \int_0^{\infty} (u(y-x)\ \delta(z-y) f_Y(y)(1-F_Y(x))^{\alpha-1}dy \\ &+ \int_0^{\infty} (u(x-y)\ \delta(z-x)\ \alpha f_Y(y)(1-F_Y(y))^{\alpha-1}dy \\ &= (u(z-x) f_Y(z)(1-F_Y(x))^{\alpha-1} \\ &+ \delta(z-x) \int_0^{\infty} \alpha f_Y(y)(1-F_Y(y))^{\alpha-1}dy \\ &= u(z-x) f_Y(z)(1-F_Y(x))^{\alpha-1} + \delta(z-x)(1-(1-F_Y(x))^{\alpha} \end{aligned}$$

Next, eliminating the variable *Y*, we get Equation (14)

$$\begin{aligned} &((\phi(x,y)\,\phi(x,y,z))^{-Y}\phi(x))^{-x} \\ &= \int_0^{\infty} (u(z-x) f_Y(z)(1-F_Y(x))^{\alpha-1} f_X(x)dx \\ &+ \int_0^{\infty} \delta(z-x)(1-(1-F_Y(x))^{\alpha}) f_X(x)dx \\ &= f_Y(z) \int_0^{\infty} f_X(x)(1-F_Y(x))^{\alpha-1}dx + f_X(z)(1-(1-F_Y(z)^{\alpha}). \end{aligned}$$

For the HSP gate (i.e., $\alpha = 1$), Equation (14) reduces into Equation (15) which is the same as Equation (10). This is because in the HSP gate, the spare part is in a hot backup state, that is, the spare part and the main part work at the same time, the failure behavior of the two is completely independent, and its failure mechanism is the same as the AND gate.

For the CSP gate, the marginal distribution of the corresponding TBN node $Z$ can be represented as follows.

$$f_{Z_{CSP}}(z) = (f(x)f(x,y)f(y,z))^{-\{X,Y\}} = ((f(x,y)f(y,z))^{-Y} f(x))^{-X} \quad \textbf{(18)}$$

Substituting Equation (8) and (9) into Equation (18) and eliminating variable $Y$, we get:

$$\begin{aligned}&(\phi(x,y)\phi(y,z))^{-Y}\\ &=\int_0^{\infty} \delta(z-y)u(y-x)f_Y(y-x)dy\\ &= u(z-x)f_Y(z-x)f_X(x).\end{aligned}$$

Next, eliminating the variable $Y$, we get Equation (16).

Since the integral in Equation (14) and Equation (16) may not have an analytic solution, the equivalence of the calculation of failure probability under arbitrary distribution cannot be proved. However, we can prove the equivalence of failure probability calculation under exponential distribution. Assuming that the failure distribution of components $X$ and $Y$ follow the exponential distribution with parameter $l$, then,

$$\begin{aligned}f_{Z_{WSP}}(z) &= \lambda e^{-\lambda z}\int_0^z \lambda e^{-\alpha\lambda z}\,dx + \lambda e^{-\lambda z}(1-e^{-\alpha\lambda z})\\ &= \frac{1+\alpha}{\alpha}(\lambda e^{-\lambda z} - \lambda e^{-(1+\alpha)\lambda z})\end{aligned}$$

and the failure probability of $Z_{\mathrm{WSP}}$ in the interval [0, $t$]

$$\begin{aligned}F_{Z_{\mathrm{WSP}}}(t) &= \Pr(z \le t) = \int_0^t \frac{1+\alpha}{\alpha}(\lambda e^{-\lambda z} - \lambda e^{-(1+\alpha)\lambda z})\,dz\\ &= \frac{1+\alpha}{\alpha}(1-e^{-\lambda t}) - \frac{1}{\alpha}(1-e^{-(1+\alpha)\lambda t}).\end{aligned}$$

Similarly, for the CSP gate

$$f_{Z_{\mathrm{CSP}}}(z) = \int_0^z f_X(x)f_Y(z-x)\,dx = \lambda^2 z e^{-\lambda z}$$

and the failure probability of Z_CSP in the interval [0, $t$]

$$F_{Z_{\mathrm{CSP}}}(t) = \Pr(z \le t) = 1 - e^{-\lambda t} - \lambda t e^{-\lambda t}.$$

The failure probabilities of $Z_{\mathrm{WSP}}$ and $Z_{\mathrm{CSP}}$ in the interval [0, $t$] are equal to those calculated by Markov chain analysis method [1].

# 5 Case Study

In this section, we verify the effectiveness of the TBN method by analyzing the DFT model of the X2000 avionics system in [13], and use SamIamv3.0 (http://reasoning.cs.ucla.edu/samiam) as an auxiliary tool to analyze TBN and DTBN models.

## 5.1 Model Conversion

According to the method of conversion DFT to TBN in Section 3, we first convert the structure of the DFT of the X2000 system in [13] to the structure of TBN as shown in Figure 4. The leaf node NC in TBN indicates a top event which is that the network is cut off due to the failure of the bus set or computer nodes.

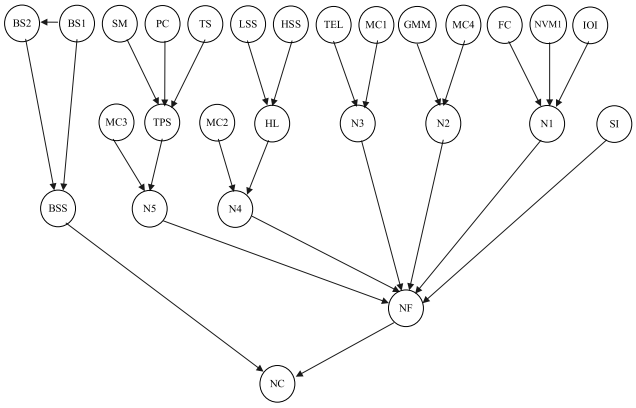


**Figure 4.** TBN of X2000 avionics system

Then, we map the logic semantics of gates of The DFT into the corresponding nodes of the TBN. The detailed mapping is shown in Table 1.

## 5.2 Safety Analysis for the X2000

We conduct 2 groups of experiments to verify the safety analysis capability of the TBN method. The first group assumes that the failure distribution of each primary component follows an exponential distribution, in which traditional DFT analysis methods, such as CTMC, can give exact solutions. The second group assumes that the primary components follow different types of distributions (mixture distributions), in which traditional analytical methods are intractable.

The parameters of the two groups of experiments are set as follows: In the first group, the failure distribution of each primary component follows the exponential distribution with parameter $l$ = 0.05, and the DTBN time granularity $n$ is 20. In the second group, the failure distribution of components FC, MC1, MC2, MC3 and MC4 follow the exponential distribution with a parameter of $l$ = 0.05, respectively, and the remaining components follow the Weibull distribution with a shape parameter of 5 and a scale parameter of 100, respectively. In the two groups, the failure rate coefficient $\alpha$ in WSP is equal to 0.5, and the TBN uses a 3-piece and 5-degree polynomial to fit the node's failure probability distribution function. Figure 5 plots the cumulative failure distribution of the top event which are calculated by the TBN method during 100h mission time using two different sets of parameters, which also shows that TBN method can effectively analyze models with mixed distribution.

## 5.3 Performance Analysis

Under the first group of parameter settings in Section 5.2, we use CTMC, TBN and DTBN to analyze the DFT of X2000, respectively. In this setting, the CTMC method can obtain an analytical solution, that is, an exact solution. Therefore, the performance of the TBN method and the DTBN method can

be compared based on the exact solution. Figure 6 plots the change trend of absolute error between the solution of TBN and the solution of DTBN and the exact solution respectively within the mission time of 100h.

Here, the absolute error is the absolute value of the difference between the numerical solution and the exact solution at the same time point, the maximum absolute error is the maximum value of the absolute error at the same time point, and the average error is the average of the absolute errors over the mission time.

The maximum error of the TBN method is 2.1‰, and the average error is 0.227‰. However, the DTBN method has a maximum error of 15.4‰ and an average error of 3.2‰. The error shows that the accuracy of the TBN method is significantly better than that of the DTBN method. The running time of TBN is 12.62ms and the DTBN is 79.82m without considering the fitting time of failure distribution in the TBN and the discretization time of failure distribution in the DTBN.

**Table 1.** The relationship between TBN nodes

| Sub-system | Component/ Subsystem | Logic Relationship | Semantics Representation |
|---|---|---|---|
| NC | BSS, NF | OR | The semantics of the NC is represented by Equation (2), where z represents NC, x represents BSS, and y represents NF. |
| BSS | BS1, BS2 | WSP | The semantics of between BS1 and BS2 is represented by Equation (4), where x represents BS1, and y represents BS2.The semantics of the BSS is represented by Equation (1), where z represents BSS. |
| NF | SI, N1-N5 | AND | The semantics of NF is represented by a three-level AND subsystem. |
| N1 | IOI,NVM1,FC | OR | The semantics of N1 is represented by a two-level OR subsystem. |
| N2 | MC4, GMM | OR | The semantics of the N2 is represented by Equation (2), where z represents N2, x represents MC4, and y represents GMM. |
| N3 | MC1, TEL | OR | The semantics of the N3 is represented by Equation (2), where z represents N3, x represents MC1, and y represents TEL. |
| N4 | MC2, HL | OR | The semantics of the N4 is represented by Equation (2), where z represents N4, x represents MC2, and y represents HL. |
| N5 | MC3, TPS | OR | The semantics of the N5 is represented by Equation (2), where z represents N5, x represents MC3, and y represents TPS. |
| HL | HSS, LSS | AND | The semantics of HL is represented by Equation (1), where z represents HL, x represents HSS, and y represents LSS. |
| TPS | TS, PC, SM | AND | The semantics of TPS is represented by a two-level AND subsystem. |

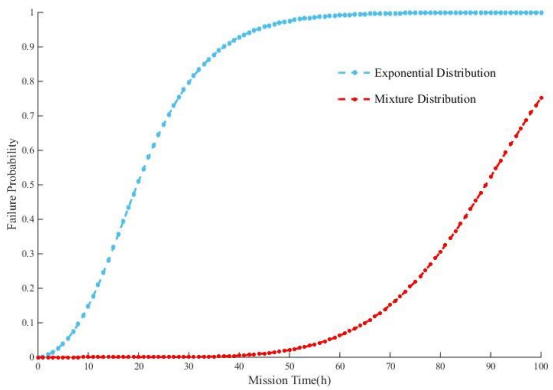


**Figure 5.** CDF of the X2000 system under exponential and mixed distributions respectively

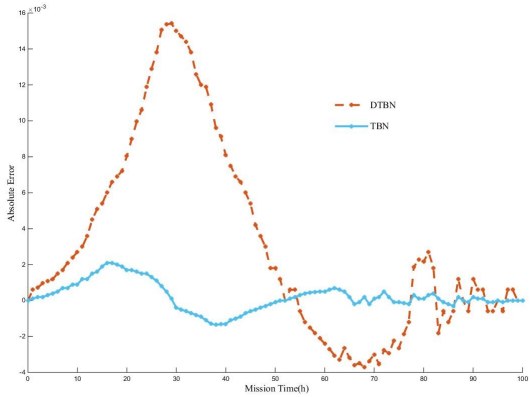


**Figure 6.** Absolute error of TBN and DTBN

# 6 Conclusion

In this paper, we propose a method in which the analysis of the mixture failure model is reduced to the TBN inference problem. The approach can trade-off between computational efficiency and accuracy by adjusting the parameters $k$ and $n$, and effectively avoid the local state explosion problem of the DTBN method. Further research is to extend the method to analyze the cascade spare gate and the spare gate with a shared pool.

# Acknowledgements

This work was supported by Domestic Visiting Program for Outstanding Young Teachers of Colleges and Universities in Anhui Province (Grant No GXGNFX2021215), Major Research Projects of Natural Science of Colleges and Universities in Anhui Provincial (Grant No. KJ2021ZD0175), Academic Support Project for Outstanding Talents of Discipline (Professional) in Anhui Province (Grant No. GXBJZD32), and Key Laboratory of Safety-Critical Software (Nanjing University of Aeronautics and Astronautics), Ministry of Industry and Information Technology research project (Grant No. NJ2019006).

# References

[1] J. B. Dugan, K. J. Sullivan, D. Coppit, Developing a Low-Cost High-Quality Software Tool for Dynamic Fault-Tree analysis, *IEEE Transactions on Reliability*, Vol. 49, No. 1, pp. 49-59, March, 2000.

[2] K. Li, S. Jin, Z. He, Q. Yang, S. Lin, Critical Component Identification and Reliability Enhancement of AC Metro Traction Substation using FTA and Sequential Monte Carlo Simulation, *International Journal of Performability Engineering*, Vol. 16, No. 12, pp. 1862-1874, December, 2020.

[3] L. Xing, B. A. Morrissette, J. B. Dugan, Combinatorial Reliability Analysis of Imperfect Coverage Systems Subject to Functional Dependence, *IEEE Transactions on Reliability*, Vol. 63, No. 1, pp. 367-382, March, 2014.

[4] J. Hu, S. Chen, D. Chen, J. Kang, H. Wang, Model-based Safety Analysis for an Aviation Software Specification, *International Journal of Performability Engineering*, Vol. 16, No. 2, pp. 238-254, February, 2020.

[5] P. Weber, G. Medina-Oliva, C. Simon, B. Lung, Overview on Bayesian Networks Applications for Dependability, Risk Analysis and Maintenance Areas, *Engineering Applications of Artificial Intelligence*, Vol. 25, No. 4, pp. 671-682, June, 2012.

[6] D. Liu, C. Y. Zhang, W. Xing, R. Li, Reliability Analysis of Phased-Mission Systems Using Bayesian Networks, *Annual Reliability and Maintainability Symposium*, Las Vegas, NV, USA, 2008, pp. 21-26.

[7] H. Boudali, J. B. Dugan, A Discrete-Time Bayesian Network Reliability Modeling and Analysis Framework, *Reliability Engineering & System Safety*, Vol. 87, No. 3, pp. 337-349, March, 2005.

[8] N. Khakzad, F. Khan, P. Amyotte, Risk-Based Design of Process Systems Using Discrete-Time Bayesian Networks, *Reliability Engineering and System Safety*, Vol. 109, pp. 5-17, January, 2013.

[9] B. W. Fang, Z. Q. Huang, Y. Wang, Y. Li, A Novel Safety Analysis Method of Hybrid System on Hybrid Bayesian Network, *Acta Electronica Sinica*, Vol. 45, No. 12, pp. 2896-2902, December, 2017.

[10] D. Marquez, M. Neil, N. Fenton, Improved Reliability Modeling Using Bayesian Networks and Dynamic Discretization, *Reliability Engineering and System Safety*, Vol. 95, No. 4, pp. 412-425, April, 2010.

[11] H. Boudali, J. B. Dugan, A Continuous-Time Bayesian Network Reliability Modeling, and Analysis Framework, *IEEE Transactions on Reliability*, Vol. 55, No. 1, pp. 86-97, March, 2006.

[12] G. Merle, J. Roussel, J. Lesage, A. Bobbio, Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events, *IEEE Transactions on Reliability*, Vol. 59, No. 1, pp. 250-261, March, 2010.

[13] Z. H. Tang, J. B. Dugan, Minimal Cut Set/Sequence Generation for Dynamic Fault Trees, *Annual Symposium Reliability and Maintainability*, Los Angeles, CA, USA, pp. 207-213, 2004.

# Biographies

**Li Wei** received her B.S. degree in management science from University of Science and Technology of China, and received her M.S. degree in management science from Hefei University of Technology. Her current research interests include system reliability, machine learning.

**Bing-Wu Fang** received his B.S. and M.S. degrees in computer science from University of Science and Technology of China, and he received his Ph.D. degree in computer science and technology from Nanjing University of Aeronautics and Astronautics. His current research interests include software safety and reliability, Bayesian deep learning.