Available online at www.sciencedirect.com
SCIENCE DIRECT®
Reliability Engineering and System Safety 84 (2004) 141–148
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Posbist fault tree analysis of coherent systems

Hong-Zhong Huang[a,*], Xin Tong[a], Ming J. Zuo[b]

[a]School of Mechanical Engineering, Dalian University of Technology, Dalian 116023, China
[b]Department of Mechanical Engineering, University of Alberta, Edmonton, Alberta, T6G 2G8, Canada

Received 12 June 2003; revised 20 October 2003; accepted 7 November 2003

Abstract

When the failure probability of a system is extremely small or necessary statistical data from the system is scarce, it is very difficult or impossible to evaluate its reliability and safety with conventional fault tree analysis (FTA) techniques. New techniques are needed to predict and diagnose such a system's failures and evaluate its reliability and safety. In this paper, we first provide a concise overview of FTA. Then, based on the posbist reliability theory, event failure behavior is characterized in the context of possibility measures and the structure function of the posbist fault tree of a coherent system is defined. In addition, we define the AND operator and the OR operator based on the minimal cut of a posbist fault tree. Finally, a model of posbist fault tree analysis (posbist FTA) of coherent systems is presented. The use of the model for quantitative analysis is demonstrated with a real-life safety system.

Keywords: Posbist reliability theory; Fault tree; Coherent system; Structure functions; Possibility distributions; Posbist fault tree analysis

1. Introduction

Fault tree analysis (FTA) is a powerful and computationally efficient technique for analyzing and predicting system reliability and safety. Many theoretical advances and practical applications have been achieved in this field to date. FTA is based on Boolean algebra and probability theory and is consistent with conventional reliability theory. It assumes that exact probabilities of events are given and many failure data are available. However, many modern systems are highly reliable and thus, it is often very difficult to obtain sufficient statistical data to estimate precise failure rates or failure probabilities. Moreover, the inaccuracy in system models that is caused by human errors is difficult to deal with solely by means of the probist reliability theory[1]. These fundamental problems of probist reliability theory have led researchers to look for new models or new reliability theories which do not have the shortcomings of the classical probabilistic definition of reliability. Among others, we mention Tanaka et al. [1], Singer [2], Onisawa [3], Cappelle and Kerre [4], Cremona and Gao [5], Utkin and Gurov [6] and Cai et al. [7–9] who have all tried to define reliability in terms other than probabilistic ones. According to [10], several forms of fuzzy reliability theories, including profust reliability theory [7], posbist reliability theory [8], and posfust reliability theory, are proposed using new assumptions, such as the possibility assumption and the fuzzy-state assumption, in place of the probability assumption or the binary-state assumption. For systems with extremely small failure probabilities or when necessary statistical data is scarce, posbist reliability theory demonstrates its advantages over probist reliability theory [6,8,9].

Owing to this, it is necessary to develop a new model of FTA corresponding to posbist reliability theory to evaluate system reliability and safety. In this paper, based on posbist reliability theory, event failure behavior is characterized in the context of possibility measures. A model of posbist fault tree analysis (posbist FTA) is proposed for predicting and diagnosing failures and evaluating reliability and safety of systems. The model of posbist FTA in posbist reliability theory plays a role that is analogous—though not completely—to that of probist FTA (Conventional FTA) in probist reliability

* Corresponding author. Tel.: +1-780-989-3374; fax: +1-780-492-2200.
E-mail address: hzhhuang@dlut.edu.cn (H.-Z. Huang).

[1] The reliability theory based on the PRObability assumption and the BInary-STate assumption is probist reliability theory, i.e. conventional reliability theory.

0951-8320/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2003.11.002

theory. As will be seen in the sequel, the model of posbist FTA constructed in this paper, where the failure behavior of the basic events is characterized in the context of possibility measures, is different from various reported models of fuzzy probist FTA, where the basic events are considered as fuzzy numbers. Furthermore, it will be noted that the proposed model corresponds to posbist reliability theory developed by Cai [8].

2. A concise overview of fault tree analysis

Conventional fault tree analysis was first applied to the analysis of system reliability by Watson in 1961. A fault tree is a logic diagram consisting of a top event and a structure delineating the ways in which the top event may occur. Up to now, the scope of conventional FTA has expanded from the aviation/space industry and nuclear industry to electronics, electric power, and the chemical industry as well as mechanical engineering, traffic, architecture, etc. It is a mature tool for analyzing coherent systems.

The pioneering work on fuzzy fault tree analysis (fuzzy FTA) belongs to Tanaka et al. [1]. They treated probabilities of basic events as trapezoidal fuzzy numbers, and applied the fuzzy extension principle to calculating the probability of the top event. At the same time, they defined an index function analogous to importance measures for evaluating to what extent a basic event contributes to the top event. Singer [2] analyzed fuzzy reliability by using L–R type fuzzy numbers. He considered the relative frequencies of the basic events as fuzzy numbers and used possibility instead of probability measures. However, these approaches cannot be applied to a fault tree with repeated events. In order to deal with repeated basic events, Soman and Misra [11] provided a simple method for fuzzy FTA based on the α-cut method, also known as resolution identity. This method was then extended to deal with multistate FTA [12]. Sawyer and Rao [13] used the α-cut method to calculate the failure probability of the top event in fuzzy FTA of mechanical systems. Huang [14] employed fuzzy fault tree to analyze railway traffic safety. Many other results on fuzzy FTA are reported in [15–19].

There is one common characteristic in the above-mentioned works: the notion of fuzziness is introduced to conventional FTA and the probabilities of events are fuzzified into the fuzzy numbers in the unit interval [0,1]. However, we note that these works are based on probist FTA (i.e. conventional FTA). More precisely, we can say that these works fall within the scope of fuzzy probist FTA.

Furuta and Shiraishi [20] proposed a kind of importance measure using fuzzy integrals assuming that the basic events in a fault tree are fuzzy. Feng and Wu [21] developed a model of profust FTA based on the theory of 'probability of fuzzy events' and provided partial quantitative analysis when the state space is discrete. Their model is based on two assumptions: (1) the failure behavior of components is defined in a fuzzy way and (2) the probability assumption is used.

Based on the foregoing overview, we can itemize the main categories of the methods of FTA to date:

(1) Probist FTA (conventional FTA),
(2) Fuzzy probist FTA (or fuzzy FTA), and
(3) Profust FTA (corresponding to profust reliability theory).

Furthermore, we can find that the study of fuzzy probist FTA is confined to the algorithm itself, the cited engineering applications are overly simplified, and the obtained results lack comparability. On the other hand, the study of profust FTA has appeared only recently and the study of posbist FTA is not reported at all.

3. Posbist reliability theory based on state variables

Posbist reliability theory was developed by Cai in 1991, in an attempt to give an alternative to probabilistic reliability theory. It is based on the following two assumptions [8]:

(1) The possibility assumption: The system failure behavior is fully characterized in the context of possibility measures.
(2) The binary-state assumption: The system demonstrates only two crisp states: fully functioning or completely failed. At any time the system is in one of the two states.

Though the system states are defined precisely, we cannot determine accurately the system state at a specified future instant. According to the possibility assumption, this uncertainty is characterized by possibility measures rather than probability measures; therefore, the system state can be treated as a fuzzy variable. However, we should note that such a fuzzy variable takes only one (i.e. fully functioning) or zero (i.e. completely failed) as its value.

For ease of reference, in the following we provide some essential concepts in posbist reliability theory. For more details, refer to [8].

Definition 3.1. A fuzzy variable is a real valued function defined on a possibility space $(U, \Phi, P_{\mathrm{oss}})$, where U is the universe of discourse, Φ is the discrete topology on U (that is, the power set or the class of all subsets of U), and the scale, P_{oss}, which is a mapping from U to [0,1], satisfies the following properties:

(1) $P_{oss}(\Theta) = 0$ and $P_{oss}(U) = 1$, where Θ denotes the empty set.
(2) For any arbitrary collection of sets A_α of Φ,

$$P_{oss}\left(\bigcup_\alpha A_\alpha\right) = \sup_\alpha P_{oss}(A_\alpha).$$

Definition 3.2. The possibility distribution function of a fuzzy variable X, denoted by π_X, is a mapping from R (the set of real numbers) to the unit interval [0,1] and is given by $\pi_X(x) = P_{oss}\{v : X(v) = x\}$ for all $x \in R$.

Definition 3.3. Given a possibility space (U, Φ, P_{oss}), the sets $A_1, A_2, \cdots, A_n \subset \Phi$ are said to be mutually unrelated if for any permutation of the set $\{1, 2, \ldots, n\}$, denoted by $i_1, i_2, \cdots, i_k$ for $1 \le k \le n$,

$$P_{oss}(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_n})$$
$$= \min(P_{oss}(A_{i_1}), P_{oss}(A_{i_2}), \cdots, P_{oss}(A_{i_n})).$$

Definition 3.4. Given a possibility space (U, Φ, P_{oss}), the fuzzy variables $X_1, X_2, \ldots, X_n$ are said to be mutually unrelated if for any permutation of the set $\{1, 2, \ldots, n\}$, denoted by $i_1, i_2, \ldots, i_k$, for $1 \le k \le n$, the sets

$$\{X_{i_1} = x_1\}, \{X_{i_2} = x_2\}, \ldots, \{X_{i_k} = x_k\}$$

are unrelated for all $x_1, x_2, \ldots, x_k \in R$.

Formally, we assume that the state of the system is determined completely by the states of the components, so the structure function of a system of n components is denoted by

$$\phi = \phi(X)$$

$$X = (X_1, X_2, \ldots, X_n) \tag{1}$$

where X is the system state vector and X_i represents the state of component i.

Assume that $X_1, X_2, \ldots, X_n$ and ϕ are all binary fuzzy variables defined on possibility space (U, Φ, P_{oss})

$$X_i : U \to \{0, 1\}, i = 1, 2, \ldots, n$$

$$\phi : U \to \{0, 1\}.$$

Then we assume

$$X_i = \begin{cases} 1, & \text{if the component } i \text{ is functioning} \\ 0, & \text{if the component } i \text{ is failed} \end{cases} \quad \textit{and}$$

$$\phi = \begin{cases} 1, & \text{if the system is functioning} \\ 0, & \text{if the system is failed} \end{cases}$$

According to above-mentioned analysis, the system posbist reliability, denoted by R, is defined as

$$R = P_{oss}(\phi = 1) \tag{2}$$

and the system posbist unreliability, denoted by F, is defined as

$$F = P_{oss}(\phi = 0). \tag{3}$$

Furthermore, we note that the system reliability defined in terms of system states coincides with the system reliability defined in terms of system lifetimes. Refer to [8] for more details on posbist reliability theory in terms of system states.

4. Posbist fault tree analysis of coherent systems

4.1. Basic definitions of coherent systems

Here we give several basic redefinitions of coherent systems that are indispensable to the model of posbist FTA that we will construct. Refer to [22] for a more detailed treatment of coherent systems.

Definition 4.1.1. In the context of posbist reliability theory, the ith component is irrelevant to the structure ϕ if ϕ is constant in z_i, that is,

$$\phi(1_i, Z) = \phi(0_i, Z)$$

for all $(\bullet_i, Z)$. Otherwise the ith component is relevant to the structure. Here we employ notations

$$(1_i, Z) = (z_1, \ldots, z_{i-1}, 1, z_{i+1}, \ldots, z_n)$$

$$(0_i, Z) = (z_1, \ldots, z_{i-1}, 0, z_{i+1}, \ldots, z_n)$$

$$(\bullet_i, Z) = (z_1, \ldots, z_{i-1}, \bullet, z_{i+1}, \ldots, z_n)$$

Definition 4.1.2. A system of components is coherent in the context of posbist reliability theory if (1) every component of it is relevant to the system and (2) its structure function ϕ is increasing in every component. We can denote a coherent system by ϕ, or more precisely by (C, ϕ), where the set C is a set of integers designating the components.

To be brief, coherent systems are monotone systems wherein no unit irrelevant to the system exists since the units irrelevant to the system are removed by Boolean calculation after their reliability behavior is analyzed. We will use possibility measures rather than probability measures to characterize the failure behavior of coherent systems. We note that the definition of coherent systems here is the same as that of coherent systems in conventional reliability theory. This is because the binary-state assumption is also valid in posbist reliability theory [8].

Definition 4.1.3. A path set, denoted by P, of a coherent system (C, ϕ) in the context of posbist reliability theory is a subset of C that makes ϕ functioning. P is minimal if any real subset of it will not make ϕ functioning. A cut set, denoted by K, of a coherent system (C, ϕ) is a subset of C that makes ϕ failed. K is minimal if any real subset of it will not make ϕ failed.

Suppose a coherent system ϕ in the context of posbist reliability theory with p minimal path sets $(P_1, P_2, \ldots, P_p)$ and k minimal cut sets $(K_1, K_2, \ldots, K_k)$. Define

$$P_j(X) = \bigcap_{i \in P_j} x_i$$

and

$$K_j(X) = \bigcup_{i \in K_j} x_i.$$

Then the structure function ϕ can be expressed as

$$\phi(X) = \bigcup_{j=1}^{p} P_j(X) = \max_{1 \le j \le p} \min_{i \in P_j} x_i \tag{4}$$

or

$$\phi(X) = \bigcap_{j=1}^{k} K_j(X) = \min_{1 \le j \le k} \max_{i \in K_j} x_i. \tag{5}$$

4.2. Basic assumptions

It is necessary for the construction of the model of posbist FTA to make the following assumptions:

(1) The states of events are crisp: occurrence or non-occurrence. However, the event state is uncertain at a given future instant.
(2) The failure behaviors of events are characterized in the context of possibility measures. Furthermore, the possibility distribution functions of events have been obtained by adopting a certain technique (or several techniques) for estimating possibility distributions.
(3) The events are mutually unrelated.

4.3. Construction of the model of posbist fault tree analysis

According to the equivalent conversion of special logic gates [23], we can convert an arbitrary fault tree of coherent systems into a basic fault tree that consists only of AND gates, OR gates and basic events.

4.3.1. The structure function of posbist fault tree

Consider a coherent system S of n components. The failure of the system is the top event and the failures of the components are basic events. Since the system and its components demonstrate only two crisp states, i.e. fully functioning or completely failed, we can use 0 and 1 to represent the states of the top event and basic events. Thus, we assume

$$X_i = \begin{cases} 1, & \text{if the basic event } i \text{ occurs} \\ 0, & \text{if the basic event } i \text{ does not occur} \end{cases} \quad i = 1, 2, \ldots, n$$

$$\varphi(X) = \begin{cases} 1, & \text{if the top event occurs} \\ 0, & \text{if the top event does not occur} \end{cases}$$

$$X = (X_1, X_2, \ldots, X_n).$$

Then the function $\varphi(X)$ is called the structure function of a posbist fault tree. We can call it a posbist fault tree $\varphi(X)$, or more precisely, a posbist fault tree $(C, \varphi(X))$, where the set C is a set of integers designating basic events.

Analogous to the conventional fault tree, we can easily obtain the following results:

For a posbist fault tree consisting of AND gates, we have

$$\varphi(X) = \prod_{i=1}^{n} X_i = \min(X_1, X_2, \cdots, X_n). \tag{6}$$

For a posbist fault tree consisting of OR gates, we have

$$\varphi(X) = 1 - \prod_{i=1}^{n} (1 - X_i) = \max(X_1, X_2, \ldots, X_n). \tag{7}$$

Definition 4.3.1.1. A path set, denoted by P_a, of a posbist fault tree $\varphi(X)$ is a subset of C that will not make the top event occur. P_a is minimal if any real subset of it will make the top event occur. A cut set, denoted by K_u, of a posbist fault tree $\varphi(X)$ is a subset of C that makes the top event occur. K_u is minimal if any real subset of it will not make the top event occur.

Then, suppose a fault tree $\varphi(X)$ of a coherent system with p minimal path sets $(P_{a1}, P_{a2}, \ldots, P_{ap})$ and k minimal cut sets $(K_{u1}, K_{u2}, \ldots, K_{uk})$. Define

$$P_{\mathrm{aj}}(X) = \bigcap_{i \in P_{aj}} x_i$$

and

$$K_{uj}(X) = \bigcup_{i \in K_{uj}} x_i.$$

Thus, the structure function $\varphi(X)$ of the posbist fault tree can be expressed as

$$\varphi(X) = \bigcap_{j=1}^{p} P_{aj}(X)$$

$$= \min_{1\le j\le p} \max_{i\in P_{aj}} x_i. \tag{8}$$

or

$$\varphi(X) = \bigcup_{j=1}^{k} K_{uj}(X)$$
$$= \max_{1\le j\le k} \min_{i\in K_{uj}} x_i. \tag{9}$$

4.3.2. Estimation of possibility distributions

The estimation of possibility distributions is a crucial step in the application of possibilistic reliability theory (for example, posbist reliability theory). In the theory of possibilistic reliability, the concept of a possibility distribution plays a role that is analogous—though not completely—to that of a probability distribution in the theory of probabilistic reliability. Because the concept of membership functions bears a close relation to the concept of possibility distributions [24], in this paper, we believe that all the methods for generating membership functions can be used to construct the relevant possibility distributions in principle. For more details of methods for generating membership functions (i.e. the methods for generating possibility distributions), we can refer to [25–28]. However, we should realize that it might be difficult, if not impossible, to come up with a general possibility distribution method which will work for all applications. Much future work is yet to be done on this subject.

Here, we present two techniques for estimating possibility distributions from probability distributions.

(i) Bijective transformation method

Let $X = \{x_i | i = 1, 2, \ldots, n\}$ be the universe of discourse. If the histograms (or the probability distribution) of the variable X is ranged in a decreasing rate:

$p(x_1) \ge p(x_2) \ge \ldots \ge p(x_n)$

then, the corresponding possibility distribution can be constructed as follows:

$$\pi_X(x_i) = \sum_{j=1}^{n} \min(p(x_i), p(x_j)) = ip(x_i) + \sum_{j=i+1}^{n} p(x_j). \tag{10}$$

Generally, the histograms can be renormalized by setting the maximal value to 1, i.e.

$$\pi_X(x_i) = \frac{p(x_i)}{\max_{i=1}^{n} p(x_i)} \tag{11}$$

where $(p(x_i))_{1\le i\le n}$ is a histogram of X.

(ii) Conservation of uncertainty method

As the name suggests, this method is based on the principle of uncertainty conservation [29]. When uncertainty is transformed from one theory T_1 to another T_2, the following requirements must be met:

(1) The amount of inherent uncertainty should be preserved when the transformation is made from T_1 to T_2.
(2) All relevant numerical values in T_1 must be converted to their counterparts in T_2 by an appropriate scale.

The method is:

$$\pi_X(x_i) = \left[\frac{p(x_i)}{p(x_1)}\right]^{\alpha}, \alpha \in [0, 1]. \tag{12}$$

Sometimes, the immediate judgments of experts or technologists are used to construct possibility distributions. In that case, most of the universes of discourse are discrete.

It should be pointed out that we usually combine or use several methods for constructing possibility distributions in order to obtain all the possibility distribution functions of the fuzzy variables involved.

4.3.3. Quantitative analysis

According to posbist reliability theory based on state variables (i.e. system states) and the basic assumptions in Section 4.2, we have:

The failure possibility of the basic event i is

$$P_{\text{oss}_i} = P_{\text{oss}}(X_i = 1). \tag{13}$$

The failure possibility of the top event is

$$P_{\text{oss}_T} = P_{\text{oss}}(\varphi = 1). \tag{14}$$

Theorem 1. *For the AND gate, the operator is*

$$P_{\text{oss}_T}^{\text{AND}} = \min(P_{\text{oss}_1}, P_{\text{oss}_2}, \cdots, P_{\text{oss}_n}). \tag{15}$$

Proof.

$$\begin{aligned} P_{\text{oss}_T}^{\text{AND}} &= P_{\text{oss}}(\varphi = 1) \\ &= P_{\text{oss}}\left(\prod_{i=1}^{n} X_i = 1\right) = P_{\text{oss}}(\min(X_1, X_2, \cdots, X_n) = 1) \\ &= P_{\text{oss}}(X_1 = 1, X_2 = 1, \cdots, X_n = 1). \end{aligned}$$

Since the basic events are mutually unrelated, we have

$$\begin{aligned} P_{\text{oss}_T}^{\text{AND}} &= \min(P_{\text{oss}}(X_1 = 1), P_{\text{oss}}(X_2 = 1), \ldots, P_{\text{oss}}(X_n = 1)) \\ &= \min(P_{\text{oss}_1}, P_{\text{oss}_2}, \ldots, P_{\text{oss}_n}) \qquad \square \end{aligned}$$

Theorem 2. *For the OR gate, the operator is*

$$P^{\mathrm{OR}}_{\mathrm{oss}_T} = \max(P_{\mathrm{oss}_1}, P_{\mathrm{oss}_2}, \dots, P_{\mathrm{oss}_n}). \tag{16}$$

Proof.

$$P^{\mathrm{OR}}_{\mathrm{oss}_T} = P_{\mathrm{oss}}(\varphi = 1) = P_{\mathrm{oss}}(\max(X_1, X_2, \dots, X_n) = 1)$$

$$= P_{\mathrm{oss}}((X_1 = 1) \cup (X_2 = 1) \cup \dots \cup (X_n = 1))$$

$$= \max(P_{\mathrm{oss}}(X_1 = 1), P_{\mathrm{oss}}(X_2 = 1), \dots, P_{\mathrm{oss}}(X_n = 1))$$

$$= \max(P_{\mathrm{oss}_1}, P_{\mathrm{oss}_2}, \dots, P_{\mathrm{oss}_n}) \qquad \square$$

Theorem 3. *For a posbist fault tree $\varphi(X)$ of a coherent system with mutually unrelated basic events, suppose there are k minimal cut sets $(K_{u1}, K_{u2}, \dots, K_{uk})$. Let P_{oss_i} be the failure possibility of the basic event i. Then*

$$P_{oss_\mathrm{T}} = \max_{1 \le j \le k} \left(\min_{i \in K_{uj}} P_{oss_\mathrm{i}}\right). \tag{17}$$

Proof. From Eq. (9), we have

$$\varphi(X) = \bigcup_{j=1}^{k} K_{uj}(X) = \max_{1 \le j \le k} \min_{i \in K_{uj}} x_i.$$

Since all the basic events of the posbist fault tree are mutually unrelated, we may arrive at

$$P_{\mathrm{oss}}(K_{uj}(X) = 1) = P_{\mathrm{oss}}(\min_{i \in K_{uj}} x_i = 1) = \min_{i \in K_{uj}} (P_{\mathrm{oss_i}}).$$

The above equation is due to Theorem 1. Then according to Theorem 2, we have

$$P_{\mathrm{oss}_T} = P_{\mathrm{oss}}(\varphi(X) = 1)$$

$$= P_{\mathrm{oss}}(\max_{1 \le j \le k} K_{uj}(X) = 1)$$

$$= \max_{1 \le j \le k} (\min_{i \in K_{uj}} P_{\mathrm{oss}_i})$$

where we can find that the unrelatedness of $\{K_{uj}(X), j = 1, 2, \dots, k\}$ is not required. $\square$

Thus, as long as we know the failure possibility of every basic event, we can use the above-mentioned operators to obtain the failure possibility of the top event.

5. Example

Consider the problem of a failure caused by the break of the hoisting rope of a crane. For a failure analysis of a broken hoisting rope, we can refer to [30]. In [30], the authors concluded that the main reasons for the failure of the crane's hoisting rope were fatigue and poor inspection. But they considered only the failures of the steel wires themselves. In fact, there are many factors (materials and/or human errors) that caused the break of the hoisting rope of the crane. It is not enough to consider the failure of the steel wires only.

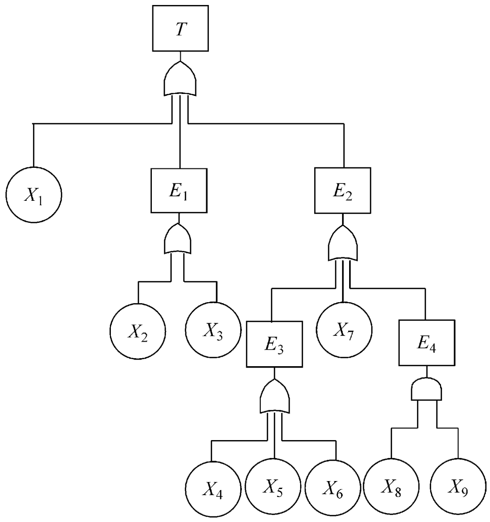

Fig. 1. The fault tree of a failure of the rope on a crane.

The fault tree of a failure of the hoisting rope of a crane has been constructed in Fig. 1. By means of the technique for analyzing a fault tree, we can derive almost all the main reasons for the failure of the crane's hoisting rope. The events of the fault tree are illustrated in Table 1.

For a failure such as that of the hoisting rope of a crane, it is often very difficult to estimate precise failure rates or failure probabilities of individual components or failure events. This is because the failure events consist of not only the failure of components (e.g. drawback of materials) but also human factors (e.g. insufficient inspection). According to Zadeh's consistency principle [24], it may be feasible to

Table 1
The events and the failure possibility of every basic event of the fault tree

Symbol	Event	Failure possibility
T	Broken	
E_1	Hoisting objects aslant	
E_2	Inadequate strength	
E_3	Drawback of manufacturing	
E_4	Drawback of use	
X_1	Overloading	0.05
X_2	Dragging	0.03
X_3	Hoisting objects alternately	0.004
X_4	Drawback of materials	0.002
X_5	Drawback of machining	0.001
X_6	Insufficient inspection	0.003
X_7	Unsuitable diameter	0.005
X_8	Inadequate overhauling	0.02
X_9	Arriving at limit of failure	0.5

use possibility measures as a rough estimate of probability measures.

Using the judgments of experts or technologists, we can obtain the failure possibility of every basic event illustrated in Table 1. Thus, we can deduce the failure possibility of the top event by use of the technique presented in this paper.

According to Eq. (16), we arrive at

$$P_{\rm oss}(E_1) = \max(P_{\rm oss}(X_2), P_{\rm oss}(X_3)) = \max(0.03, 0.004) = 0.03.$$

$$P_{\rm oss}(E_3) = \max(P_{\rm oss}(X_4), P_{\rm oss}(X_5), P_{\rm oss}(X_6)) = \max(0.002, 0.001, 0.003) = 0.003.$$

$$P_{\rm oss}(E_2) = \max(P_{\rm oss}(E_3), P_{\rm oss}(E_4)) = \max(0.003, 0.02) = 0.02.$$

Further, according to Eq. (15), we arrive at

$$P_{\rm oss}(E_4) = \min(P_{\rm oss}(X_8), P_{\rm oss}(X_9)) = \min(0.02, 0.5) = 0.02.$$

In this way, we can arrive at the failure possibility of the top event according to Eq. (16)

$$P_{\rm oss}(T) = \max(P_{\rm oss}(X_1), P_{\rm oss}(E_1), P_{\rm oss}(E_2)) = \max(0.05, 0.03, 0.02) = 0.05.$$

6. Concluding remarks

(1) The model of posbist FTA constructed in this paper can be used to evaluate the failure possibility of those systems, in which the statistical data is scarce or the failure probability is extremely small (e.g. 10^{-7}). It is very difficult, however, to evaluate the safety and reliability of such systems using conventional FTA.

(2) As long as the failure possibilities of basic events can be obtained, the failure possibility of the top event can be derived according to the technique outlined in this paper. Thus, it is crucial to estimate possibility distributions of basic events. In this paper, we have pointed out that all the methods for generating membership functions can be used to construct the relevant possibility distributions in principle, and we have provided several methods for constructing possibility distributions. Nevertheless, further research is needed.

(3) We should note that the model of posbist FTA proposed in the present paper, where the uncertainty is characterized in the context of possibility measures rather than probability measures, is different from the reported models of fuzzy FTA and the model of profust FTA.

Acknowledgements

We gratefully acknowledge the financial support of the National Science Foundation of China (under the contract number 50175010), the Excellent Young Teachers Program of the Ministry of Education, China (under the contract number 1766), National Excellent Doctoral Dissertation Special Foundation, China (under the contract number 200232), and the Natural Sciences and Engineering Research Council of Canada. Constructive suggestions and comments from the referees and editors are very much appreciated.

References

[1] Tanaka H, Fan LT, Lai FS. Fault-tree analysis by fuzzy probability. IEEE Trans Reliab 1983;32:453–7.
[2] Singer D. A fuzzy set approach to fault tree and reliability analysis. Fuzzy Sets Sys 1990;34:145–55.
[3] Onisawa T. An approach to human reliability in man–machine systems using error possibility. Microelect. Reliab. 1988;27:87–103.
[4] Cappelle B, Kerre EE. On a possibilistic approach to reliability theory. In: Proceedings of the Second International Symposium on Uncertainty Analysis, Maryland MD; 1993. p. 415–418.
[5] Cremona C, Gao Y. The possibilistic reliability theory: theoretical aspects and applications. Struct Safety 1997;19(2):173–201.
[6] Utkin LV, Gurov SV. A general formal approach for fuzzy reliability analysis in the possibility context. Fuzzy Sets Syst 1996; 83:203–13.
[7] Cai KY, Wen CY, Zhang ML. Fuzzy states as a basis for a theory of fuzzy reliability. Microelec Reliab 1993;33(15):2253–63.
[8] Cai KY, Wen CY, Zhang ML. Fuzzy variables as a basis for a theory of fuzzy reliability in the possibility context. Fuzzy Sets Syst 1991;42: 145–72.
[9] Cai KY, Wen CY, Zhang ML. Posbist reliability behavior of fault-tolerant systems. Microelect Reliab 1995;35(1):49–56.
[10] Cai KY. System failure engineering and fuzzy methodology: an introductory overview. Fuzzy Sets Syst 1996;83:113–33.
[11] Soman KP, Misra KB. Fuzzy fault tree analysis using resolution identity and extension principle. Int J. Fuzzy Math 1993;1: 193–212.
[12] Misra KB, Soman KP. Multistate fault tree analysis using fuzzy probability vectors and resolution identity. In: Onisawa T, Kacprzyk J, editors. Reliability and safety analysis under fuzziness. Heidelberg: Physica-Verlag; 1995. p. 113–125.
[13] Sawyer JP, Rao SS. Fault tree analysis of mechanical systems. Microelect Reliab 1994;54(4):653–67.
[14] Huang HZ, Yuan X, Yao XS. Fuzzy fault tree analysis of railway traffic safety. Proceedings of the Conference on Traffic and Transportation Studies, ICTTS; 2000. 107–112.
[15] Pan HS, Yun WY. Fault tree analysis with fuzzy gates. Comput Ind Engng 1997;33(3–4):569–72.
[16] Lin CT, Wang MJJ. Hybrid fault tree analysis using fuzzy sets. Reliab Engng Sys Safety 1997;58:205–13.
[17] Suresh PV, Babar AK, Raj VV. Uncertainty in fault tree analysis: a fuzzy approach. Fuzzy Sets Sys 1996;83:135–41.
[18] Hua XY, Hu ZW, Fan ZY. A method to multistate fuzzy fault tree analysis. J Mech Strength 1998;20(1):35–40.
[19] Huo Y, Hou CZ, Liu SX. Application of fuzzy set theory in fault tree analysis. Chin J Mech Engng (English Edition) 1998;11(4): 326–32.

[20] Furuta H, Shiraishi N. Fuzzy importance in fault tree analysis. Fuzzy Sets Sys 1984;12:205–13.

[21] Feng J, Wu MD. The profust fault tree and its analysis. J Natl Univ Def Technol 2001;23(1):85–8.

[22] Barlow RE, Proschan F. Statistical theory of reliability and life testing: probability models. Holt: Rinehart and Winston; 1975.

[23] Mei QZ, Liao JS, Sun HZ. Introduction to system reliability engineering. Beijing: Science Press; 1987.

[24] Zadeh LA. Fuzzy sets as a basis for a theory of possibility. Fuzzy sets Sys 1978;1(1):3–28.

[25] Civanlar MR, Trussell HJ. Constructing membership functions using statistical data. Fuzzy Sets Sys 1986;18(1):1–13.

[26] Medasani S, Kim J, Krishnapuram R. An overview of membership function generation techniques for pattern recognition. Int J Approx Reason 1998;19:391–417.

[27] Medaglia AL, et al. An efficient and flexible mechanism for constructing membership functions. Eur J Oper Res 2002;139:84–95.

[28] Dubois D, Prade H. Unfair coins and necessity measures: towards a possibilistic interpretation of histograms. Fuzzy Sets Sys 1983;10:15–20.

[29] Klir G. A principle of uncertainty and information invariance. Int J General Sys 1990;17(2/3):249–75.

[30] Torkar M, Arzensek B. Failure of crane wire rope. Engng Failure Analysis 2002;9:227–33.