Original Article

Institution of MECHANICAL ENGINEERS

Journal of RISK AND RELIABILITY

Proc IMechE Part O:
J Risk and Reliability
2014, Vol. 228(4) 371–381

DOI: 10.1177/1748006X14520824
pio.sagepub.com
SAGE

A new fault tree analysis approach based on imprecise reliability model

Zheng Liu, Yan-Feng Li, Li-Ping He, Yuan-Jian Yang and Hong-Zhong Huang

Abstract

Fault tree analysis is a powerful and computationally efficient technique for safety analysis and reliability prediction. It decomposes an undesired failure into multiple possible root causes by constructing a sub-event tree and spreading it into basic events. Classical reliability theory using probability theory to quantify the uncertainties of basic events encounters many challenges when failure data are limited. In this case, uncertainty quantification should be carried out based on subjective information, such as experts' assessment or engineers' experience. As a generalization of probability theory, imprecise probability theory can quantify subjective information as the upper and lower expectations or previsions. In this article, a fault tree analysis algorithm incorporating subjective information into imprecise reliability models of basic events is proposed to calculate the failure interval of lubricating oil warning system.

Keywords

Fault tree analysis, subjective information, imprecise reliability model, lubricating oil warning system

Date received: 15 October 2013; accepted: 19 December 2013

Introduction

There are more and more stringent requirements on the safety of large engineering systems due to the growing technical and environmental complexity, and it has stimulated the research and development of safety analysis methods and safety assessment procedures.[1] System safety analysis can be conducted both qualitatively and quantitatively.[2] Fault tree analysis (FTA) is a powerful diagnosis technique for qualitative safety analysis, and it is widely used to determine the root causes of undesired system failure event.[3] Conventional FTA is based on probability theory, which is consistent with conventional reliability theory.[4] The general assumption is that all probabilities or probability distributions involved are precise or perfectly known, and the system components are independent or their dependence is precisely known.[5] However, in many cases, it may be difficult or even impossible to determine the distribution parameters precisely due to the inherent uncertainty and uncontrollable variability.[6] Many specialists and scholars have found that statistical data and distribution information in practical reliability applications are often limited. Therefore, it might be more appropriate to quantify the reliability uncertainty based on subjective information, such as experts' judgments or engineers' experiences. Moreover, it is difficult for experts or engineers to quantify an event using a precise or deterministic number, rather imprecise descriptors or linguistic assessments may be more convenient for them.[7–9] In these cases, classical reliability theory cannot provide appropriate ways to quantify this kind of assessments. In the past few decades, many specialists and scholars have developed new models and reliability theories to facilitate these assessments, such as Tanaka et al.,[10] Soman and Misra[11] and Huang et al.[4,12] These studies pointed out that the probability of basic events can be treated as fuzzy numbers, and possibility measures can be used to quantify uncertainty instead of using probability ones. These models and methodologies focus on the basics of fault trees and introduce the fuzzy set theory and possibility theory into safety analysis. Besides, a growing number of subjective methodologies are used to evaluate system reliability and safety.

School of Mechanical, Electronic, and Industrial Engineering, University of Electronic Science and Technology of China, Chengdu, P.R. China

Corresponding author:
Li-Ping He, School of Mechanical, Electronic, and Industrial Engineering, University of Electronic Science and Technology of China, No. 2006, Xiyuan Avenue, West Hi-Tech Zone, 611731 Chengdu, Sichuan, P.R. China.
Email: lipinghe@uestc.edu.cn

Wang et al.[13] incorporate fuzzy set modeling and evidential reasoning to assess the safety requirement specifications; more information is available in Liu et al.[1] and Wang.[6]

In addition to the above theories, one concept that is called "imprecise probability," also known as "interval probability," has particularly been a growing area of research in recent years. Technically, imprecise probability is a generalization of probability theory, and its theoretical development, as well as applications in reliability engineering, has been reported in Utkin and Coolen,[5] Coolen[7] and Utkin.[14] Compared with classical reliability theory, imprecise reliability theory does not assume precise probabilities or probability distributions of reliability measures, and also there is no need to assume precisely known dependence relationship between basic events. It characterizes the uncertainty in terms of the upper and lower expectations, which is an appropriate alternative to uncertainty and imprecision quantification. In many engineering practices, assessments and judgments often come from different experts and engineers. In that case, imprecise probability theory can provide a unified tool to fuse these heterogeneous assessments into one model via natural extension.[8] Natural extension is an effective method to quantify uncertainties, but sometimes it is intractable because of large dimensionality, which restricts its wide applications. To promote the application, some simplified algorithms of a natural extension must be developed.[7] By FTA, system safety analysis can be resolved to qualitative and quantitative analyses of its minimum cut sets and path sets, which are subsets of its all components; it reduced the complexity of the system to some extent, as well as the complexity of a natural extension.

Study on imprecise reliability theory made some significant progresses on the theoretical aspect, but there are few applications in real-world projects. Lubricating oil warning system[15] is a critical component in aircraft engine. Owing to the complicated working environment, there are many uncertain factors influencing its safety, which are very difficult to be quantified by classical probability theory. Therefore, imprecise reliability models and FTA method are adopted in this article to estimate the failure probability of the lubricating oil warning system.

The remainder of this article is organized as follows: Section "Key concepts of imprecise probability theory" reviews several key concepts of imprecise probability theory. The new FTA method based on imprecise probability is proposed in section "Imprecise reliability model–based FTA." In section "FTA for lubricating oil warning system," the new method is applied to lubricating oil warning system to show the effectiveness of the new method; discussion and a brief comparison with Bayesian inference model and interval analysis method are made at the end of this section. The conclusion and future studies are summarized in section "Conclusion and remarks."

Key concepts of imprecise probability theory

Basic definitions of imprecise probability theory

The models and methodologies of imprecise probability theory are based on the behavioral interpretation. The basic idea relating to the behavioral interpretation is the concept of a gamble, while the probabilistic models of imprecise probability theory are the lower and upper previsions of these gambles. Three fundamental principles are constructed on the basis of subjective rationality. The basic definitions are given here, and more detailed information is available in Walley.[8]

Definition 1. A gamble X is a bounded real-valued function defined on possibility space Ω; it can be regarded as an uncertain reward whose value depends on the uncertain state $\omega_i \in \Omega$, $i = 1, \ldots, n$. If you accept gamble X, then some time later the true state ω_i will be revealed, and you will receive the reward $X(\omega_i)$ in units of utility.[8,16]

Definition 2. A lower prevision $\underline{P}(X)$ is a bounded real-valued function defined on a gamble X; it can be treated as a supremum buying price for a person to buy gamble X. While an upper prevision is a bounded real-valued function defined on a gamble X, which can be regarded as an infimum selling price for a person to sell gamble X. It should be noted that the lower and upper previsions should be correlative for they are determined under same amount of information.

Definition 3. Avoiding sure loss means that any predictable sure loss is unacceptable. Consider a gamble X, $\underline{P}(X)$ is the supremum buying price for you to buy gamble X; obviously, $G(X) = X - \underline{P}(X)$ is the profit via buying gamble X. If you have to make decisions on various gambles, in order to make the profit and avoid sure loss, $\sup_{\omega \in \Omega} \sum_{i=1}^{n} G(X_i(\omega)) \geqslant 0$, which means there is at least one outcome, which gives the net gain of any n gambles.[16]

Definition 4. We define coherence indirectly from the definition of incoherence. Suppose there are several gambles, $X_1, \ldots, X_n$, and X_0 is a certain linear combination of these gambles. According to Walley,[8] incoherence means that the specified buying prices $\underline{P}(X_i)$, $i = 1, \ldots, n$, effectively implying a buying price for the gamble X_0, are higher than its specified price $\underline{P}(X_0)$. According to the principle of coherence, the lower probability $\underline{P}(X)$ is coherent, if and only if when for any $n \geqslant 1$, $m \geqslant 0$, $\sup_{\omega \in \Omega} [\sum_{i=1}^{n} G(X_i(\omega)) - mG(X_0)] \geqslant 0$.

Besides, natural extension can be regarded as a mathematical model to deduce new assessments upon relatively known information. It has several forms and

each of them has pros and cons in the context of specific applications. The use of proper form can substantially facilitate the inference and computation of the previsions. Please refer to Utkin and Kozine[17] for more detailed information.

Redefinitions of imprecise probability theory in reliability theory

A particular case of gambles is considered for which the reward can be either 0 or 1, in units of utility.[15] The 0–1 valued gamble identified with an event X can be written as follows

$$X(\omega) = \begin{cases} 1, & \text{if } \omega \in X \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

A lower prevision $\underline{M}(X)$ can be interpreted as the maximum price you are willing to pay for buying the 0–1 valued gamble X, while the upper prevision $\overline{M}(X)$ can be interpreted as the minimum price you are willing to sell the gamble. The upper prevision can be written as $\overline{M}(X) = 1 - \underline{M}(X^c)$ since X, X^c are complementary, and the lower and upper previsions are quantified under same amount of information. $\Delta = \overline{M}(X) - \underline{M}(X)$ is called the imprecision for event X. When $\underline{M}(X) = \overline{M}(X)$ for all events X, imprecise probability degenerates into precise probability, so precise probability is one of the special cases of imprecise probability. A relative straightforward interpretation of an interval $[\underline{M}(X), \overline{M}(X)]$ is all possible values for precise probability $M(X)$, which has not been able to exclude. Also, there is a subjective interpretation of imprecise probability underlying Bayesian statistics where $M(X)$ is the "fair price" for a bet on an event X, loosely speaking such that you consider that the £$M(X)$ is the fair price for a bet that pays £1 if event X occurs and nothing otherwise.[7,8] Formally, this reward is given in units of utility instead of pounds to avoid the influence of personal attitude toward risk. Generalizing this to imprecise probability theory, $\underline{M}(X)$ is the maximum price for one to buy the bet, while $\overline{M}(X)$ is the minimum price for one to sell the bet. In imprecise reliability theory, $M(X)$ can represent a certain reliability measure, while $[\underline{M}(X), \overline{M}(X)]$ is the range of this reliability measure defined by one's own knowledge.

Application of natural extension in reliability theory

Consider a system consisting of n components, assume x_i is the time-to-failure (TTF) or other reliability measures of the i component, and there are m_i assessments or judgments related to the i component. Suppose that all assessments can be described with the form of mathematical expectations $\mathrm{M}(\varphi_{ij}(x_i))$, $j = 1, 2, \ldots, m_i$, where $\varphi_{ij}(x_i)$ is a function of the basic gamble x_i corresponding to the j assessment for this component. According to Barlow and Proschan,[18] the system lifetime can be uniquely determined by component lifetimes. Let $X = (x_1, x_2, \ldots, x_n)$, then there is a function $g(X)$ of the components' lifetimes, which can characterize the system reliability behavior. Here, functions $g(X)$ and $\varphi_{ij}(x_i)$ can also be regarded as gambles.

Suppose that partial information about components is represented as the form of the lower and upper expectations $\underline{a}_{ij} = \underline{\mathrm{M}}(\varphi_{ij}(x_i))$ and $\overline{a}_{ij} = \overline{\mathrm{M}}(\varphi_{ij}(x_i))$, respectively. Actually, many reliability measures can be expressed in the form of mathematical expectations as follows

$$R(t) = P(X > t) = \int_{R^+} I_{[t,+\infty]}(X)\rho(X)\mathrm{d}X = \mathrm{E}\left(I_{[t,+\infty]}(X)\right) \tag{2}$$

$$F(t) = P(X \leqslant t) = \int_{R^+} I_{[0,t]}(X)\rho(X)\mathrm{d}X = \mathrm{E}\left(I_{[0,t]}(X)\right) \tag{3}$$

$$\mathrm{MTTF} = \int_{R^+} X\rho(X)\mathrm{d}X = \mathrm{E}(X) \tag{4}$$

$$\text{Residual TTF} = \mathrm{E}\left(I_{[z,+\infty]}(X - t)\middle| I_{[t,+\infty]}(X)\right) \tag{5}$$

$$\text{Residual MTTF} = \mathrm{E}\left(X - t\middle| I_{[t,+\infty]}(X)\right) \tag{6}$$

In order to compute other reliability measures, natural extension is adopted to construct reliability models. In this case, the natural extension in primal form can be rewritten as[17]

$$\underline{\mathrm{M}}(g)\left(\overline{\mathrm{M}}(g)\right) = \min_{\mathrm{P}}\left(\max_{\mathrm{P}}\right) \int_{\mathrm{R}_+^n} g(X)\rho(X)\mathrm{d}X \tag{7}$$

subject to

$$\begin{aligned} &\rho(X) \geqslant 0, \quad \int_{\mathrm{R}_+^n} \rho(X)\mathrm{d}X = 1 \\ &\underline{a}_{ij} \leqslant \int_{\mathrm{R}_+^n} \varphi_{ij}(x_i)\rho(X)\mathrm{d}X \leqslant \overline{a}_{ij}, \quad i \leqslant n,\ j \leqslant m_i \end{aligned} \tag{8}$$

where the set P is all possible n-dimensional density functions $\{\rho(X)\}$ satisfying constraint conditions. Imprecise probability assumes that only partial information about the reliability of the system and its components is available; obviously; the partial information can be thought as evidence reducing the range of set P. If we have no information about the components' behavior, the set P is very large, and it will shrink as the information increases. If the components are independent, $\rho(X)$ can be written as

$$\rho(X) = \rho(x_1) \times \rho(x_2) \times \cdots \times \rho(x_n) \tag{9}$$

This primal form can be used in some cases; however, it has infinitely many variables, and it can hardly be solved directly. Kuznetsov applied the duality

theorem of linear programming[19] in equations (7) and (8) and generated a new form, that is, Kuznetsov's form,[17,20] which has finite variables and is easy to compute. To make it easier to follow, we introduce the duality theorem first.

The duality theorem in linear programming[19] can be written as

$$\begin{cases} \min\ z = \mathrm{C}^{\mathrm{T}}X \\ \mathrm{A}X \geqslant \mathrm{b} \\ X \geqslant 0 \end{cases} \xrightarrow{\text{from the primal problem to the dual one}} \begin{cases} \max\ w = \mathrm{b}^{\mathrm{T}}Y \\ \mathrm{A}^{\mathrm{T}}Y \leqslant \mathrm{C} \\ Y \geqslant 0 \end{cases} \tag{10}$$

It should be noted that the duality theorem can be applied only for the discrete cases.[17,20] Therefore, we first transfer the primal form into discrete one. X is divided into N parts, which is shown in Figure 1; as N goes to infinity, the following equation can be established approximately

$$\int_a^b \rho(X)\mathrm{d}X = \sum_{K=1}^{N} \rho(X^{(K)})\Delta X_K \tag{11}$$

$$\int_a^b g(X)\rho(X)\mathrm{d}X = \sum_{K=1}^{N} g(X^{(K)})\rho(X^{(K)})\Delta X_K \tag{12}$$

Equations (7) and (8) can be translated as[17]

$$\underline{\mathrm{M}}(g)\left(\overline{\mathrm{M}}(g)\right) = \inf_{\mathrm{P}}\left(\sup_{\mathrm{P}}\right) \sum_{K=1}^{N} g(X^{(K)})\rho(X^{(K)})\Delta X_K \tag{13}$$

subject to

$$\rho(X^{(K)}) \geqslant 0,\quad \sum_{K=1}^{N} \rho(X^{(K)})\Delta X_K = 1$$

$$\underline{a}_{ij} \leqslant \sum_{K=1}^{N} \varphi_{ij}(x_i^{k_i})\rho(X^{(K)})\Delta X_K \leqslant \overline{a}_{ij},\quad i \leqslant n,\ j \leqslant m_i \tag{14}$$

According to the duality theorem, equations (13) and (14) can be rewritten as[17]

$$\underline{\mathrm{M}}(g) = \sup_{c,\,c_{ij},\,d_{ij}} \left\{ c + \sum_{i=1}^{n}\sum_{j=1}^{m_i} (c_{ij}\underline{a}_{ij} - d_{ij}\overline{a}_{ij}) \right\} \tag{15}$$

subject to

$$c + \sum_{i=1}^{n}\sum_{j=1}^{m_i} (c_{ij} - d_{ij})\varphi_{ij}(x_i) \leqslant g(X) \tag{16}$$

and

$$\overline{\mathrm{M}}(g) = \inf_{c,\,c_{ij},\,d_{ij}} \left\{ c + \sum_{i=1}^{n}\sum_{j=1}^{m_i} (c_{ij}\overline{a}_{ij} - d_{ij}\underline{a}_{ij}) \right\} \tag{17}$$

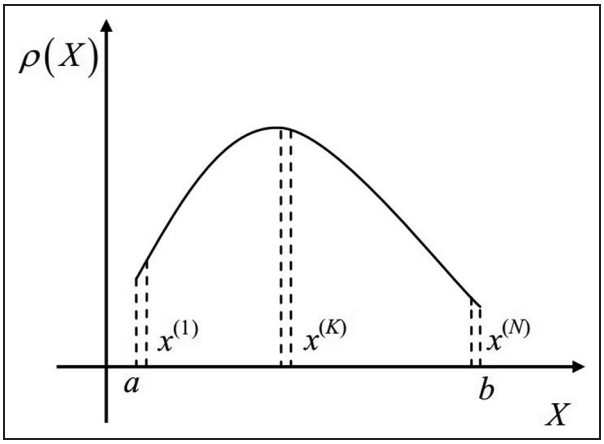

Figure 1. Discretization of continuous interval.

subject to

$$c + \sum_{i=1}^{n}\sum_{j=1}^{m_i} (c_{ij} - d_{ij})\varphi_{ij}(x_i) \leqslant g(X) \tag{18}$$

where c, c_{ij} and d_{ij} are optimization variables; c corresponds to the constraint $\sum_{K=1}^{N} \rho(X^{(K)})\Delta X_K = 1$, c_{ij} corresponds to the constraint $\sum_{K=1}^{N} \varphi_{ij}(x_i^{k_i})\rho(X^{(K)})\Delta X_K \leqslant \overline{a}_{ij}$ and d_{ij} corresponds to the constraint $\sum_{K=1}^{N} \varphi_{ij}(x_i^{k_i})\rho(X^{(K)})\Delta X_K \geqslant \underline{a}_{ij}$.

Imprecise reliability model–based FTA

Basic assumptions

The following assumptions are given for imprecise reliability model–based FTA:

1. The states of events are crisp: occurrence or nonoccurrence. However, the event state is uncertain at a given future instant.[4]
2. Assessments coming from experts or engineers are expressed in the form of the upper and lower expectations.

General imprecise reliability models for top event

Consider a minimum cut consisting of n basic events, suppose x_i is the state of the ith basic event, and there are m_i assessments related to the ith basic event. Assessments for basic events are represented as $\underline{a}_{ij} = \underline{\mathrm{M}}(\varphi_{ij}(x_i))$ and $\overline{a}_{ij} = \overline{\mathrm{M}}(\varphi_{ij}(x_i))$, where $\varphi_{ij}(x_i)$ is a function of state variable x_i corresponding to the j judgment or assessment for this basic event and $j = 1, 2, \ldots, m_i$. Imprecise reliability model of the ith basic event can be expressed as a set of m_i available upper and lower expectations

$$\mathrm{M}_i = \left\langle \underline{\mathrm{E}}_{ij}, \overline{\mathrm{E}}_{ij}, f_{ij}(X_i), j = 1, 2, \ldots, m_i \right\rangle \tag{19}$$

Our aim is to analyze the reliability and safety of the top event, suppose $\Phi(X)$ characterizes the state of the top event, which can be uniquely determined by all

basic events. Let $X = (x_1, x_2, \ldots, x_n)$, imprecise reliability model for the top event can be conducted as

$$\mathrm{M} = \left\langle \underline{\mathrm{E}}, \overline{\mathrm{E}}, h(g(X)) \right\rangle = \wedge_{i=1}^{n} \mathrm{M}_i = \wedge_{i=1}^{n} \left(\wedge_{j=1}^{m_i} \mathrm{M}_{ij} \right) \tag{20}$$

Here, the symbol $\wedge_{i=1}^{n}$ means that all models M_i are simultaneously used to obtain M.

In order to compute the aforementioned model, the natural extension in theory of imprecise probability is adopted, which can be regarded as a transformation of the component imprecise models to the system model, that is

$$\underline{\mathrm{M}}(g)\left(\overline{\mathrm{M}}(g)\right) = \min_{\mathrm{P}} (\max_{\mathrm{P}}) \int_{\mathrm{R}_+^n} h(g(X))\rho(X)\mathrm{d}X \tag{21}$$

subject to

$$\rho(X) \geqslant 0, \quad \int_{\mathrm{R}_+^n} \rho(X)\mathrm{d}X = 1 \tag{22}$$

$$\underline{a}_{ij} \leqslant \int_{\mathrm{R}_+^n} \varphi_{ij}(x_i)\rho(X)\mathrm{d}X \leqslant \overline{a}_{ij}, i \leqslant n, j \leqslant m_i$$

As mentioned earlier, the primal form of a natural extension is appropriate for some cases, especially when there are few components and relative assessments, as well as indeterminate independent relationship. However, if the number of judgments, $\sum_{i=1}^{n} m_i$, and the number of basic events, n, are large, imprecise reliability model has infinite variables, and it can hardly be solved.[5] Therefore, simplified algorithms for approximate solutions to such optimization problems must be developed. There are many ways to simplify imprecise reliability model, that is, integrate homogeneous assessments to reduce the dimensionality of $\sum_{i=1}^{n} m_i$, and decompose the whole system into several subsystems to reduce the number of n and so on. Using fault tree, system safety analysis can be resolved to qualitative and quantitative analyses of its minimum cut sets and path sets, and thus, it reduced the complexity of the imprecise reliability model to some extent.

Imprecise reliability model on basic of Boolean function

Suppose the basic event has two states, fails and functioning, and x_i is the state variable of the basic event. The state for x_i can be expressed as

$$x_i = \begin{cases} 1, & \text{if the component } i \text{ fails} \\ 0, & \text{if the component } i \text{ is functioning} \end{cases} \tag{23}$$

The state of the top event can be quantified via the basic events' states, that is

$$\Phi = \Phi(X), X = x_1, x_2, \ldots, x_n \tag{24}$$

where $\Phi(X)$ is system structure function characterizing the state of the system, which is a Boolean function.[15] System structure function $\Phi(X)$ and failure probability $F_s(t)$ of "and gate" can be expressed as

$$\begin{aligned} \Phi(X) &= \bigcap_{i=1}^{n} x_i \\ \Phi(X) &= \prod_{i=1}^{n} x_i, x_i \in [0,1] \end{aligned} \tag{25}$$

$$F_s(t) = E(\Phi(X)) = E\left(\prod_{i=1}^{n} x_i \right) \tag{26}$$

System structure function $\Phi(X)$ and failure probability $F_s(t)$ of "or gate" can be expressed as

$$\begin{aligned} \Phi(X) &= \bigcup_{i=1}^{n} x_i \\ \Phi(X) &= 1 - \prod_{i=1}^{n} (1 - x_i), \quad s_i \in [0,1] \end{aligned} \tag{27}$$

$$F_s(t) = E(\Phi(X)) = E\left(1 - \prod_{i=1}^{n} (1 - x_i) \right) \tag{28}$$

Consider a minimum cut with n basic events, we will use the following designations:

m_i the number of assessments of the ith basic event, $i = 1, 2, \ldots, n$.
m_{ij} the jth assessment of the ith basic event, $j = 1, 2, \ldots, m_i$.
$\varphi_{ij}(x_i)$ a function of the ith basic event corresponding to the jth assessment.

Suppose partial information of a basic event can be expressed in the form of the upper and lower expectations. That is, $\underline{a}_{ij} \leqslant E(\varphi_{ij}(x_i)) \leqslant \overline{a}_{ij}$, the imprecise reliability model for the ith basic event can be expressed as

$$\mathrm{M}_i = \left\langle \underline{a}_{ij}, \overline{a}_{ij}, \varphi_{ij}(x_i), j = 1, 2, \ldots, m_i \right\rangle \tag{29}$$

Imprecise reliability model for the kth minimum cut can be given by

$$\begin{aligned} \mathrm{M} &= \left\langle \underline{P}, \overline{P}, \Phi(X) \right\rangle = \wedge_{i=1}^{p} \mathrm{M}(C_i) \\ &= \wedge_{j=1}^{m_i} \left\langle \underline{a}_{ij}, \overline{a}_{ij}, \varphi_{ij}(x_i), j = 1, 2, \ldots, m_i \right\rangle \end{aligned} \tag{30}$$

Suppose there are p minimum cut sets of the top event, $C_1, C_2, \ldots, C_k, \ldots, C_p$, the failure probability of the top event can be calculated using imprecise reliability model. The imprecise reliability model of the top event under the case of the minimum cuts has nonempty intersections and can be expressed as

$$\mathrm{M} = \left\langle \sum_{k=1}^{p} \underline{P}_k, \sum_{k=1}^{p} \overline{P}_k \right\rangle \tag{31}$$

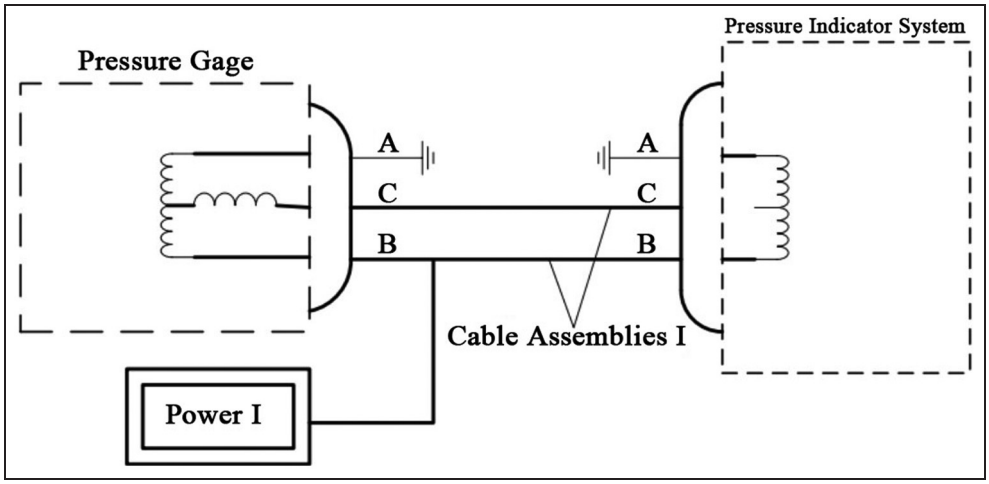

Figure 2. Schematic diagram of pressure indicator system.

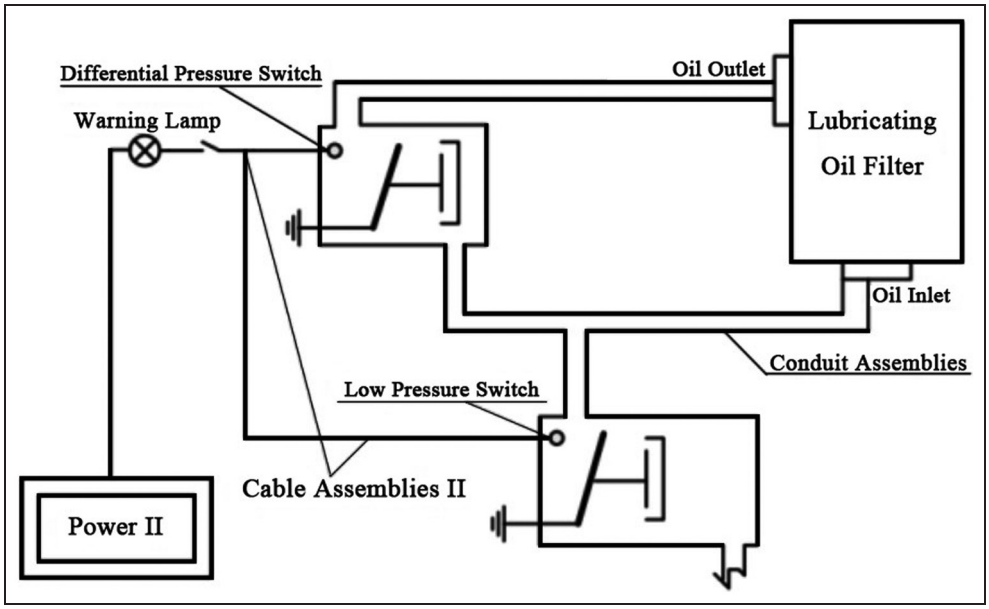

Figure 3. Schematic diagram of pressure alarm system.

The imprecise reliability model of the top event under the case of the minimum cuts has intersections and can be shown as

$$\mathrm{M} = \left\langle \underline{P}_1 + \sum_{k=2}^{p} (1-\overline{P}_1)\cdots(1-\overline{P}_{k-1})\underline{P}_k, \overline{P}_1 + \sum_{k=2}^{p} (1-\underline{P}_1)\cdots(1-\underline{P}_{k-1})\overline{P}_k \right\rangle \quad (32)$$

FTA for lubricating oil warning system

Lubricating oil system transports sufficient clean lubricating oil to every rotatable part of the engine when they are in a continuous working state, minimizes friction and wear between machine joint surfaces and also takes away fricative heat and sundries. Shortage of oil supply will damage engine and affect the safety of the aircraft. Therefore, lubricating oil pressure warning system is very important for ensuring the safety of aircrafts. Lubricating oil warning system consists of pressure indicating system and pressure alarm system. Pressure indicating system monitors oil pressure with a pressure sensor that can translate pressure into electrical signals accepted by pressure gage where the driver can read and pressure alarm system can signal an alarm to the driver when the pressure is below the index value.[15]

Schematic diagrams of pressure indicating system and pressure alarm system are shown in Figures 2 and 3, respectively.

In our preliminary study, there are two cases that will make serious damage to the engine. One is that the inlet pressure exceeds the specialized range; meanwhile,

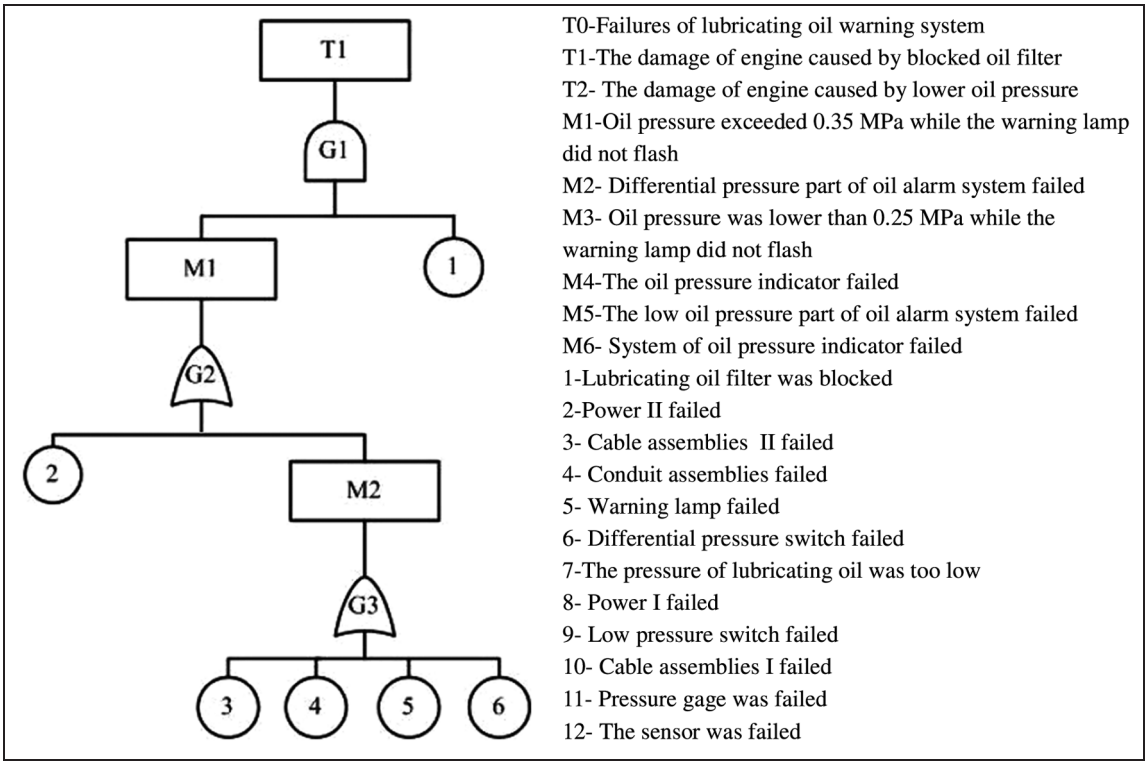

Figure 4. FTA of lubricating oil pressure indicating system and alarming system caused by blocked filter.

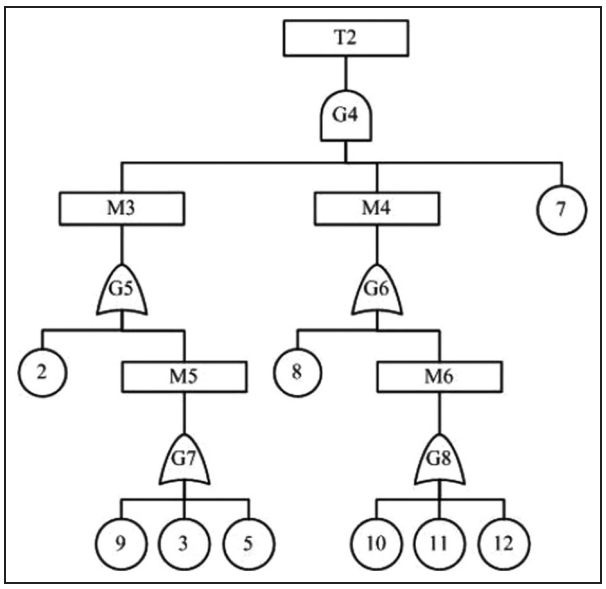

Figure 5. FTA of lubricating oil pressure indicating system and alarming system caused by low oil pressure.

pressure indicator system does not give any indicator and pressure alarm system does not give an alarm. The other is that lubricating oil filter is blocked.[15] In this article, these two cases will be taken as the top events, and FTA, as well as quantitative analysis, will be given based on the imprecise reliability models.

The fault trees for oil pressure system, oil alarm system and the whole lubricating warning system are given in Figures 4–6, respectively.

It should be noted that the working environment of the aircraft is very complicated, and the performance of an aircraft is affected by many kinds of uncertainties. In engineering practices, sufficient data to quantify uncertainties by probability theory are not easy to satisfy, so the reasonable quantification of these uncertain aspects should be performed based on subjective information. The components' failure probabilities of lubricating warning system before 500 flight hours are obtained by consulting two experts in this article. They can provide an interval or a rough range according to their knowledge about these components rather than the precise value. Partial information of lubricating oil warning system from the two experts is shown in Table 1.

As can be seen in Table 1, some judgments from the two experts are consistent, and some are conflicting. These judgments should be fused in order to minimize, if not completely eliminate, the conflict. Conjunction rule and unanimity rule proposed by Kozine and Filimonov[16] are adopted for handling these conflicts; the fusion results are shown in the last column of Table 1.

FTA of engine's damage caused by blocked oil filter

When the oil filter is blocked and alarm system gives no warning, unfiltered oil will flow to bearings, which will block the nozzles. Take this case as the top event; fault tree of this example is given in Figure 4; in order to reduce the computational burden, Fussell–Vesely

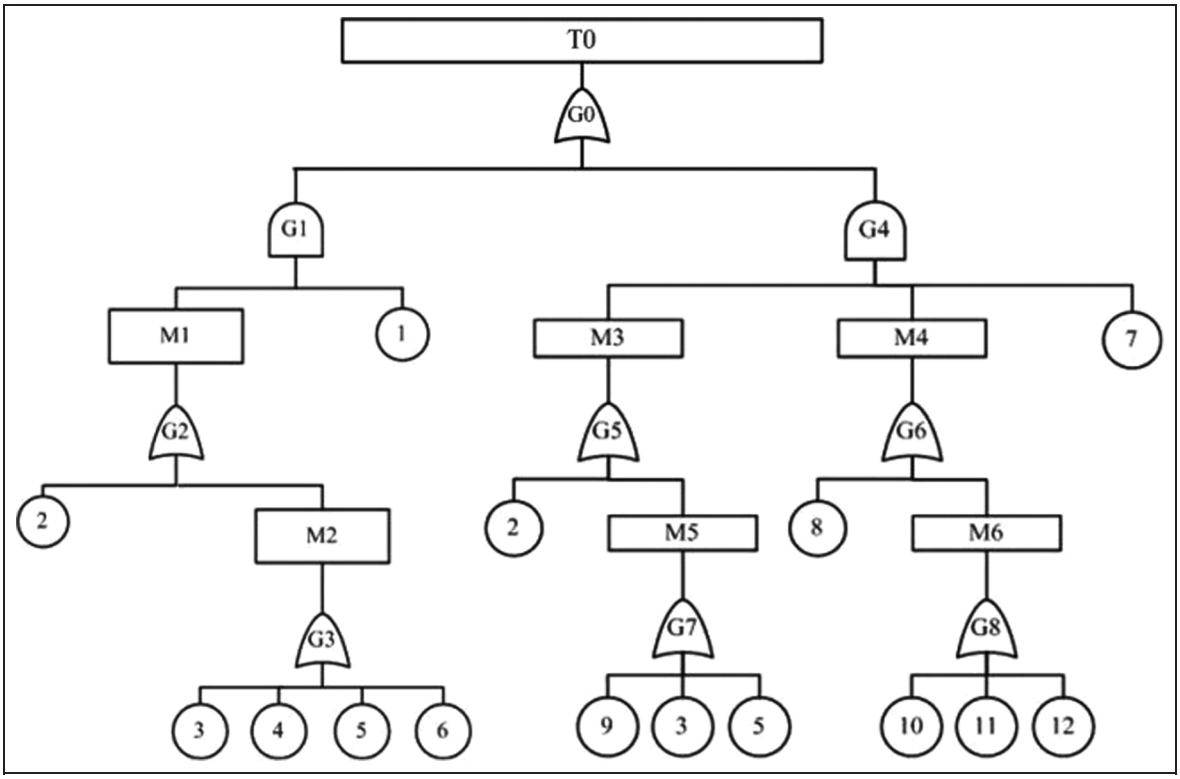

Figure 6. FTA of lubricating oil warning system.

Table 1. Failure probabilities of lubricating oil warning system components before 500 flight hours.

	Expert 1	Expert 2	Fusion results
Lubricating oil filter	$[0.98 \times 10^{-3}, 1.02 \times 10^{-3}]$	$[0.98 \times 10^{-3}, 1.01 \times 10^{-3}]$	$[0.98 \times 10^{-3}, 1.01 \times 10^{-3}]$
Power I		$[1.5 \times 10^{-3}, 1.51 \times 10^{-3}]$	$[1.5 \times 10^{-3}, 1.51 \times 10^{-3}]$
Power II	$[1.48 \times 10^{-3}, 1.49 \times 10^{-3}]$	$[1.5 \times 10^{-3}, 1.51 \times 10^{-3}]$	$[1.48 \times 10^{-3}, 1.51 \times 10^{-3}]$
Cable assemblies I	0.8×10^{-3}		0.8×10^{-3}
Cable assemblies II	0.8×10^{-3}		0.8×10^{-3}
Conduit assemblies	1×10^{-3}		1×10^{-3}
Warning lamp	0.5×10^{-3}	0.5×10^{-3}	0.5×10^{-3}
Differential pressure switch	$[1.2 \times 10^{-3}, 1.21 \times 10^{-3}]$	$[1.13 \times 10^{-3}, 1.25 \times 10^{-3}]$	$[1.2 \times 10^{-3}, 1.21 \times 10^{-3}]$
Pressure of lubricating oil	$[0.99 \times 10^{-3}, 1.01 \times 10^{-3}]$	$[1.0 \times 10^{-3}, 1.02 \times 10^{-3}]$	$[1.0 \times 10^{-3}, 1.01 \times 10^{-3}]$
Low-pressure switch	$[0.99 \times 10^{-3}, 1.02 \times 10^{-3}]$	$[0.89 \times 10^{-3}, 1.12 \times 10^{-3}]$	$[0.99 \times 10^{-3}, 1.02 \times 10^{-3}]$
Pressure gage	$[1.19 \times 10^{-3}, 1.22 \times 10^{-3}]$	$[1.2 \times 10^{-3}, 1.23 \times 10^{-3}]$	$[1.2 \times 10^{-3}, 1.22 \times 10^{-3}]$
Sensor	$[1.2 \times 10^{-3}, 1.25 \times 10^{-3}]$	$[1.26 \times 10^{-3}, 1.3 \times 10^{-3}]$	$[1.2 \times 10^{-3}, 1.3 \times 10^{-3}]$

Table 2. Minimum cuts of blocked filter by Fussell–Vesely.

Steps	1	2	3
	M_1, 7	2, 1 M_2, 1	2, 1 3, 1 4, 1 5, 1 6, 1

theory[15,19] is adopted to calculate the minimum cuts, and the results are shown in Table 2.

According to Table 2, minimum cut sets of this system are

$$\{2,1\},\{3,1\},\{4,1\},\{5,1\},\{6,1\}$$

Considering x_i is the state variable of the basic event, imprecise reliability model for every cut is constructed as

$$\begin{aligned}
&M_{C_{1-1}} = \wedge(M_1, M_2),\ M_1 = \langle 0.98\times10^{-3}, 1.11\times10^{-3}, x_1\rangle,\\
&M_2 = \langle 1.49\times10^{-3}, 1.51\times10^{-3}, x_2\rangle\\
&M_{C_{1-2}} = \wedge(M_1, M_3),\ M_1 = \langle 0.98\times10^{-3}, 1.11\times10^{-3}, x_1\rangle,\\
&M_3 = \langle 0.8\times10^{-3}, 0.8\times10^{-3}, x_3\rangle\\
&M_{C_{1-3}} = \wedge(M_1, M_4),\ M_1 = \langle 0.98\times10^{-3}, 1.11\times10^{-3}, x_1\rangle,\\
&M_4 = \langle 1.0\times10^{-3}, 1.0\times10^{-3}, x_4\rangle\\
&M_{C_{1-4}} = \wedge(M_1, M_5),\ M_1 = \langle 0.98\times10^{-3}, 1.11\times10^{-3}, x_1\rangle,\\
&M_5 = \langle 0.5\times10^{-3}, 0.5\times10^{-3}, x_5\rangle\\
&M_{C_{1-5}} = \wedge(M_1, M_6), M_1 = \langle 0.98\times10^{-3}, 1.11\times10^{-3}, x_1\rangle,\\
&M_6 = \langle 1.2\times10^{-3}, 1.21\times10^{-3}, x_6\rangle
\end{aligned} \tag{33}$$

Table 3. Minimum cuts of low oil pressure by Fussell–Vesely.

Steps	1	2	3	4	5
	M_3, M_4, 7	2, M_4, 7 M_5, M_4, 7	2, 8, 7 2, 10, 7 2, 11, 7 2, 12, 7 M_5, M_4, 7	2, 8, 7 2, 10, 7 2, 11, 7 2, 12, 7 9, M_4, 7 3, M_4, 7 5, M_4, 7	2, 8, 7 2, 10, 7 2, 11, 7 2, 12, 7 9, 8, 7 9, 10, 7 9, 11, 7 9, 12, 7 3, 8, 7 3, 10, 7 3, 11, 7 3, 12, 7 5, 8, 7 5, 10, 7 5, 11, 7 5, 12, 7

The failure probability of case 1 is given by

$$\left[\underline{P}(1), \overline{P}(1)\right] = \left[\underline{P}_1 + \sum_{k=2}^{5} (1-\overline{P}_1)\cdots(1-\overline{P}_{k-1})\underline{P}_k, \overline{P}_1 + \sum_{k=2}^{5} (1-\underline{P}_1)\cdots(1-\underline{P}_{k-1})\overline{P}_k\right] = [0, 4.52\times 10^{-3}] \tag{34}$$

FTA of engine's damage caused by low inlet pressure

When both lubricating oil pressure system and oil alarm system failed, and oil pressure is lower than the minimum allowable oil pressure, the engine will fail. Failure tree of this case is given in Figure 5; for case 2, Fussell–Vesely theory is used to determine the minimum cuts, and the analysis results are shown in Table 3; according to Table 3, the minimum cut sets of the system are

$$\{2,8,7\},\{2,10,7\},\{2,11,7\},\{2,12,7\},\{9,8,7\},\{9,10,7\},\{9,11,7\},\{9,12,7\},\{3,8,7\},\{3,10,7\},\{3,11,7\},\{3,12,7\},\{5,8,7\},\{5,10,7\},\{5,11,7\},\{5,12,7\}$$

For case 2, according to equation (6), we have

$$\begin{aligned}
&M_{C_{2-1}} = \wedge(M_2, M_7, M_8),\ M_{C_{2-2}} = \wedge(M_2, M_7, M_{10}),\\
&M_{C_{2-3}} = \wedge(M_2, M_7, M_{11}),\ M_{C_{2-4}} = \wedge(M_2, M_7, M_{12}),\\
&M_{C_{2-5}} = \wedge(M_9, M_7, M_8),\ M_{C_{2-6}} = \wedge(M_9, M_7, M_{10}),\\
&M_{C_{2-7}} = \wedge(M_9, M_7, M_{11}),\ M_{C_{2-8}} = \wedge(M_9, M_7, M_{12}),\\
&M_{C_{2-9}} = \wedge(M_8, M_7, M_5),\ M_{C_{2-10}} = \wedge(M_{10}, M_7, M_5),\\
&M_{C_{2-11}} = \wedge(M_{11}, M_7, M_5),\ M_{C_{2-12}} = \wedge(M_{12}, M_7, M_5),\\
&M_{C_{2-13}} = \wedge(M_3, M_7, M_8),\ M_{C_{2-14}} = \wedge(M_3, M_7, M_{10}),\\
&M_{C_{2-15}} = \wedge(M_3, M_7, M_{11}),\ M_{C_{2-16}} = \wedge(M_3, M_7, M_{12})
\end{aligned} \tag{35}$$

The failure probability of case 2 can be calculated as

$$\left[\underline{P}(2), \overline{P}(2)\right] = \left[\underline{P}_1 + \sum_{k=2}^{16} (1-\overline{P}_1)\cdots(1-\overline{P}_{k-1})\underline{P}_k, \overline{P}_1 + \sum_{k=2}^{16} (1-\underline{P}_1)\cdots(1-\underline{P}_{k-1})\overline{P}_k\right] = [0, 1.949\times 10^{-2}] \tag{36}$$

Safety analysis of the whole system

The fault tree of the whole system is shown in Figure 6, and the minimum cuts of the system are the union of the above two cut sets. The failure probability of the complete system can then be calculated as

$$\begin{aligned}
\left[\underline{P}(S), \overline{P}(S)\right] &= \left[\underline{P}(1) + \underline{P}(2), \overline{P}(1) + \overline{P}(2)\right]\\
&= [0, 2.401\times 10^{-2}]
\end{aligned} \tag{37}$$

Discussion

Although lifetime data used in the above example are a very particular case and they only consider the lower and upper failure probabilities of every basic event, imprecise reliability model allows for a wide variety of possible reliability knowledge representations. Therefore, some of the basic events can be represented by precise reliabilities, and some of them by imprecise reliabilities.[16] The new method's striking characteristic is that it can combine this heterogeneous knowledge into one model without any assumption or very little assumption.

Besides, Bayesian inference model, interval analysis and other non-probabilistic reliability theories[21] can also be used for system safety analysis when lifetime data are lacking. The basic of Bayesian inference model is Bayes' formula[22]

$$\pi(p|x) = \frac{f(x|p)\pi(p)}{\int_{\Theta} f(x|p)\pi(p)\mathrm{d}p} \tag{38}$$

Here, $\pi(p)$ is a precise probability distribution, which is decided by prior knowledge, that is, experts' experience is then translated into a single probability distribution. Note that there may be many probability distributions, which are equally well supported by the prior knowledge; moreover, if experts have little information about the system, $\pi(p)$ is also very difficult to decide. Interval analysis method assumes that parameters related to the structure are independent interval variables,[23] which is $x_i \in [\underline{x_i}, \overline{x_i}]$ and $x_1, \ldots, x_n$ are independent, and computes other reliability measures using interval arithmetic. Actually, as pointed above, it is unreliable to assume that variables are independent unless there is powerful and sufficient evidence to support it. The proposed method in this article does not assume precise probability distributions and the known independent relationship. Therefore, it can be

regarded as an alternative to safety analysis when lifetime data are scarce.

It should be noted that the proposed method has some limitations. If the number of judgments $\sum_{i=1}^{n} m_i$ and basic events n are large, natural extension cannot be practically solved due to their extremely large dimensionality, which restricts the application of imprecise calculations to reliability analysis.[5] Besides, since some reliability measures cannot be simply described as forms of expectations and previsions, these models cannot be handled by imprecise probability theory easily. Furthermore, natural extension cannot conveniently express independent relationships.

Conclusion and remarks

The purpose of this study is to introduce a new method to evaluate the failure possibility of complex engineering systems, in which lifetime data are scarce, or the failure probability is extremely small. A new model combining the imprecise reliability theory with FTA is built, and its effectiveness is illustrated in the example of lubricating oil warning system.

The constructed model in the article quantifies uncertainties of basic events via the lower and upper expectations rather than precise probabilities, and it is more convenient for an expert especially when partial information is available.[24] And the imprecision Δ can reflect the amount of experts' information about a basic event where classical reliability theory fails. Furthermore, by comparing several assessments coming from different experts, we can know whether there are conflicts between different experts so that we can adopt some skills to eliminate conflict.[25,26] Using the fault tree, system safety analysis can be resolved to qualitative and quantitative analyses by its minimum cut sets and path sets. Thus, the new model combining imprecise probability theory with FTA can reduce the complexity of system safety analysis as well as imprecise reliability model to some extent.

Note that natural extension with extremely large dimensionality is difficult to be practically solved, and some reliability measures, as well as independent relationships, cannot be simply represented by imprecise probability theory, so future research will focus on simplified algorithms for approximate solutions to imprecise reliability models, together with analytical solutions for some specific types of systems and initial information.

Declaration of conflicting interests

The authors declare that there is no conflict of interest.

Funding

This research was partially supported by the National Natural Science Foundation of China under contract number 51275077 and the National High Technology Research and Development Program of China (863 Program) under contract number 2007AA04Z403.

References

1. Liu J, Yang JB and Wang J. Engineering system safety analysis and synthesis using the fuzzy rule-based evidential reasoning approach. *Qual Reliab Eng Int* 2005; 21: 387–411.
2. Saeed A, Lemos RD and Anderson T. An approach for the risk analysis of safety specifications. In: *Proceedings of the 9th annual conference on computer assurance*, Gaithersburg, MD, 27 June–1 July 1994, pp.209–221. New York: IEEE.
3. Shu MH, Cheng CH and Chang JR. Using intuitionistic fuzzy sets for fault-tree analysis on printed circuit board assembly. *Microelectron Reliab* 2006; 46: 2139–2148.
4. Huang H-Z, Tong X and Zuo MJ. Posbist fault tree analysis of coherent systems. *Reliab Eng Syst Safe* 2004; 84: 141–148.
5. Utkin LV and Coolen FPA. Imprecise reliability: an introductory overview. *Comput Intell Reliab Eng (SCI)* 2007; 40: 261–306.
6. Wang J. A subjective methodology for safety analysis of safety requirements specifications. *IEEE T Fuzzy Syst* 1997; 5: 418–430.
7. Coolen FPA. On the use of imprecise probabilities in reliability. *Qual Reliab Eng Int* 2004; 20: 193–202.
8. Walley P. *Statistical reasoning with imprecise probabilities*. London: Chapman & Hall, 1991.
9. Coolen FPA, Troffaes MCM and Augustin T. Imprecise probability. In: Lovric M (ed.) *International encyclopedia of statistical science*. Berlin and Heidelberg: Springer, 2010, pp.645–648.
10. Tanaka H, Fan LT and Lai FS. Fault-tree analysis by fuzzy probability. *IEEE T Reliab* 1983; 32: 453–457.
11. Soman KP and Misra KB. Fuzzy fault tree analysis using resolution identity and extension principle. *Int J Fuzzy Math* 1993; 1: 193–212.
12. Huang H-Z, Zuo MJ and Sun Z-Q. Bayesian reliability analysis for fuzzy lifetime data. *Fuzzy Set Syst* 2006; 157(12): 1674–1686.
13. Wang J, Yang JB and Sen P. Safety analysis and synthesis using fuzzy sets and evidential reasoning. *Reliab Eng Syst Safe* 1995; 47: 103–118.
14. Utkin LV. A new efficient algorithm for computing the imprecise reliability of monotone systems. *Reliab Eng Syst Safe* 2004; 86: 179–190.
15. Zeng S, Zhao T and Zhang J. *System reliability analysis tutorial*. Beijing, China: Beijing University of Aeronautics and Astronautics Press, 2001.
16. Kozine IO and Filimonov YV. Imprecise reliabilities: experiences and advances. *Reliab Eng Syst Safe* 2000; 67: 75–83.
17. Utkin LV and Kozine IO. Different faces of the natural extension. In: *2nd international symposium on imprecise probabilities and their applications*, Ithaca, NY, 26–29 June 2001. Maastricht: Shaker Publishing.
18. Barlow R and Proschan F. *Statistical theory of reliability and life testing: probability models*. New York: Holt, Rinehart and Winston, 1975.
19. Simmons DM. *Nonlinear programming for operations research* (Prentice Hall International Series in Management). Englewood Cliffs, NJ: Prentice Hall, 1975.

20. Zio E, Librizzi M and Sansavini G. Determining the minimal cut sets and Fussell-Vesely importance measures in binary network systems by simulation. In: Soares CG and Zio E (eds) *Safety and reliability for managing risk*. London: Taylor & Francis Group, 2006, pp.723–729.
21. Ben-Haim Y. A non-probabilistic measure of reliability of linear systems based on expansion of convex models. *Struct Saf* 1995; 17: 91–109.
22. Hamada M, Martz HF, Reese CS, et al. A fully Bayesian approach for combining multilevel failure information in fault tree quantification and optimal follow-on resource allocation. *Reliab Eng Syst Safe* 2004; 86: 297–305.
23. Guo SX, Lv ZZ and Feng YS. A non-probabilistic model of structural reliability based on interval analysis. *Chin J Comput Mech* 2001; 18: 56–60.
24. Aughenbaugh JM and Paredis CJJ. The value of using imprecise probabilities in engineering design. *J Mech Design* 2006; 128: 969–979.
25. Coolen FPA. *Statistical modeling of expert opinions using imprecise probabilities*. PhD Thesis, Eindhoven University of Technology, Eindhoven, 1994.
26. Cooke RM. *Experts in uncertainty*. New York: Oxford University Press, 1991.