Uncertain random fault tree analysis based on cloud security protection framework

Changyou Guo[1, 2, 3]*, Xuefeng Zheng[1, 2], Jianjun Liu[3]

[1]*School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China*

[2]*Beijing Key Laboratory of Knowledge Engineering for Materials Science, Beijing, China*

[3]*Department of Computer Science, Dezhou University, Dezhou, China*

Received 1 March 2014, www.cmnt.lv

Abstract

Based on uncertainty theory and chance theory, this paper proposes a method that constructs and analyses fault tree. The fault tree is constructed based on logical relations between bottom events. Fault rate of bottom event would be characterized as random variable if it is obtained from historical data, it would be characterized as uncertain variable if it has no statistical data but is obtained from expert's subjective judgment. The chance that top event occurs is an uncertain random variable. The minimal cut set of fault tree is obtained by Boolean algebra method and at same time, the simplest standard disjunction expression of top event is obtained. This paper also constructs hybrid simulation algorithm to calculate the chance that top event occurs. At last validity of this method is confirmed by taking cloud security protection framework risk fault tree as example.

Keywords: Fault tree, Chance theory, Uncertain random variable, Cloud Computing, Cloud security

1 Introduction

Fault tree is a special inverted treelike logic graph, it consists of logical gate symbols and event symbols. Logical gates mean relationships between events. A fault tree describes an accident model and interprets the relations between malfunctions of components and observed symptoms with gate. Fault tree analysis is important to predict reliability for complex and large scaled system. It is a logical and diagrammatic method to evaluate the probability of an accident resulting from sequences and combinations of faults and failure events. Since fault tree analysis was developed in 1962 at Bell Telephone Laboratories in USA [1], it has been extensively used in many fields such as semi conductor industry, man-machine system, flexible manufacturing systems, nuclear power plants transmission pipelines, chemical industries and LNG terminal emergency shut down systems [3-7].

The conventional fault tree analysis based on probabilistic approach has been used extensively in the past, but still has the following problems.

(1) Fault tree analysis is carried on at early designed stage of system, so it is difficult to estimate precise failure rates or failure probabilities of individual components or failure events.

(2) New components are usually used or new events occur in practical system, historical data that is used in probabilistic approach cannot be obtained.

(3) In a highly automated system, people are still the key component. Human component is responsible for 20%-90% of the failures in many systems. It is very difficult to be characterized as probability [2].

Since fuzzy set theory (FST) developed by Zadeh [8] in 1965, many researchers tried to apply it to solve the above problems. Paper [1] applied the fuzzy sets theory to model the fuzzy system structure, proposed the new procedure to calculate the system reliability and a new importance index of basic events. It overcame shortcoming, which probability was difficult to be evaluated precisely in traditional fault tree analysis, it was a simple and effective fault tree analysis method. Paper [2] was suitable for situations which both probabilistic and fuzzy evaluations were necessary. Instead of directly estimating failure probability, the fuzzy failure rate was used to characterize the failure occurrence of system events involving imprecise information such as human errors. Paper [9, 10] analysed that how probability of top event is calculated by using triangle fuzzy number, trapezoidal fuzzy number, LR fuzzy number, normal fuzzy number as chance that bottom event occurs. Paper [11-13] applied fuzzy fault tree analysis to many fields such as nuclear reactor, aerospace, petrochemical industry, pipelines and so on.

Because fuzzy measure does not obey the law of truth conservation and is inconsistent with the law of excluded middle and the law of contradiction [14], the above fuzzy fault tree analysis methods lost their correct theory foundation.

* ***Corresponding author*** e-mail guochangyouustb@139.com

When historical data are not available to estimate a probability distribution, we have to invite some domain experts to evaluate their belief degree that each event will occur. Since human beings usually overweight unlikely events, the belief degree may have much larger variance than the real frequency. Perhaps some people think that the belief degree is subjective probability. However, paper [20] showed that it is inappropriate because probability theory may lead to counterintuitive results in this case. In order to deal with this phenomena, uncertainty theory was founded by [15] in 2007 and refined by [18] in 2010. Nowadays uncertainty theory has become a branch of mathematics for modelling human uncertainty, and have been developed and applied widely to operational research, risk analysis, reliability, comprehensive evaluation, portfolio selection, etc. [16, 17, 19, 14, 23-25].

In many cases, uncertainty and randomness simultaneously appear in a complex system. For example, some quantities have no samples while others have samples enough to determine probability distributions. In order to describe this phenomenon, the concepts of uncertain random variable and chance measure were pioneered by Liu in 2012 [14]. Chance theory begins with uncertain variable and chance measure, and is a mathematical methodology composed of uncertainty theory and probability theory.

Wen [26] recently proposed uncertain random fault tree analysis, she led uncertain random measure into Boolean system. But in this paper, fault rate of bottom event would be characterized as random variable indirectly if it is obtained from reliable historical data otherwise it would be characterized as uncertain variable. The chance that top event occurs is an uncertain random variable and is presented with simple formula.

The chance that overall system's top event occurs is calculated by using hybrid simulation technology. Finally, feasibility and validity of this method is confirmed by taking the cloud security protection framework risk fault tree as example.

Cloud Computing is a new concept in recent years, and a newly computing model is proposed. Cloud computing is the development of distributed computing, parallel computing and grid computing [27]. The goal of cloud computing is to simplify the computing and storage for like public water and electricity, the user can be convenient to use these resources only could be connected to network, and to pay by the volume that they used. Cloud computing is usually have a distributed infrastructure, and can carry on real-time monitoring of the distributed system, in order to achieve the efficient usage of it [28]. The computing make computers act on the cloud and the computer makes parallel computing technology into people's life [29]. Users service themselves relying on some internet information resources, which lie on some nodes, such as computing resources, software resources, data resources and management resources. This service model emphasize the demand driven, user dominant, on-demand services, no centralized control and users don't care where the server. The parallel computing and virtualization technology has become the core support technology after the concept of cloud computing was put forward. There are existing two means of cloud computing [30]: one aspect is describes the infrastructure, which used to construct applications and the role equivalents to the PC operating system: the other aspect is describes cloud computing applications based on the infrastructure.

The main concern of cloud computing is the safety issue according to latest survey of IDC. Therefore, the security of user data will be the key factor decided cloud computing for enterprise applications [31]. Survey of Gartner in 2009 showed that more than 70% of the respondents in the actual deployment of cloud computing is security and privacy issues [32]. Cloud computing characterized by dynamic services as the main technical, flexible "service contract" as the core business characteristics, is undergoing significant changes. This change has brought huge impact for the information security field.

There have been more and more foreign standards organization started to develop cloud computing and safety standards, in order to enhance the interoperability and security, reduce duplication of investment or reinvent, some organizations such as ITU-TSG17 team [33] launched the cloud computing standard work. In addition, some specially group, such as cloud computing security alliance also has made certain progress in cloud computing security standardization. In the domestic IT industry, all kinds of cloud computing security products and solutions appear. For example, Sun Microsystems released open source cloud computing security tools for Amazon's EC2, S3, and virtual private cloud platform to provide security protection.

2 Preliminary

2.1 UNCERTAINTY THEORY

Definition 1 ([15]) Let Γ be a nonempty set, τ a σ-algebra over Γ, and M an uncertain measure, M meets the conditions: (1)M{Γ} = 1; (2)M{Λ} +M{Λ^c} = 1 for any event Λ; (3)M{$\bigcup_{i=1}^{\infty} \Lambda_i$} ≤ $\sum_{i=1}^{\infty}$ M{Λ_i} for every countable sequence of events {Λi}. Then the triplet (Γ, τ,M) is called an uncertainty space.

Definition 2 ([15]) An uncertain variable is a measurable function from an uncertainty space (Γ,τ,M) to the set of real numbers, i.e., for any Borel set B of real numbers, the set

$$\{\xi \in B\}=\{r\in\Gamma|\xi(r)\in B\} \quad (1)$$

is an event.

Definition 3 ([15]) The uncertainty distribution Φ of an uncertain variable ξ is defined by

$$\Phi(x) = M\{\xi \le x\} \tag{2}$$

for any real number x.

Definition 4 ([15]) An uncertain variable ξ is called linear if it has a linear uncertainty distribution

$$\Phi(x) = \begin{cases} 0, if x \le a; \\ (x-a)/(b-a), if a \le x \le b \\ 1, if x \le b \end{cases} \tag{3}$$

denoted by L(a,b) where a and b are real numbers with a < b(figure 1).

Definition 5 ([15]) An uncertain variable ξ is called zigzag if it has a zigzag uncertainty distribution

$$\Phi(x) = \begin{cases} 0, if x \le a; \\ (x-a)/2(b-a), if a \le x \le b \\ (x+c\text{-}2b)/2(c-b), if b \le x \le c \\ 1, if x \ge c \end{cases} \tag{4}$$

denoted by Z(a, b,c) where a, b, c are real numbers with a < b < c (figure 2).

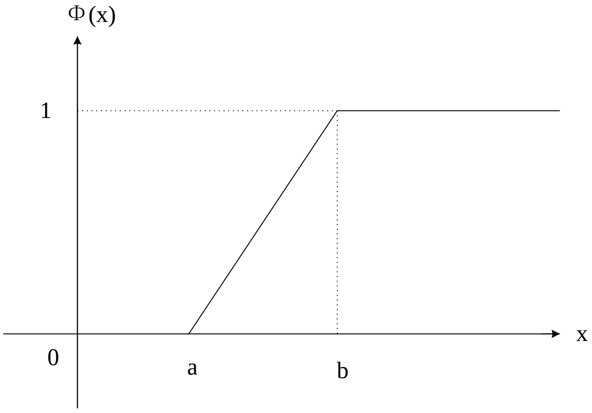

FIGURE 1 Linear Uncertainty Distribution

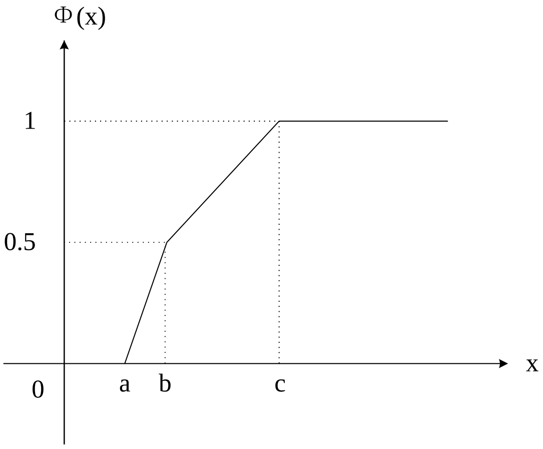

FIGURE 2 Zigzag Uncertainty Distribution

Definition 6 ([15]) An uncertain variable ξ is called normal if it has a normal uncertainty distribution

$$\Phi(x) = (1 + \exp(\frac{\pi(e-x)}{\sigma\sqrt{3}}))\text{-}1 \text{ , } x \text{ Є} R \tag{5}$$

denoted by N(e, σ) where e and σ are real numbers with $\sigma > 0$(figure 3).

Definition 7 ([15]) Let ξ be an uncertain variable. Then the expected value of ξ is defined by

$$E[\xi] = \int_0^{+\infty} M\{\xi \ge r\}\,dr - \int_{-\infty}^{0} M\{\xi \le r\}dr$$

provided that at least one of the two integrals is finite.

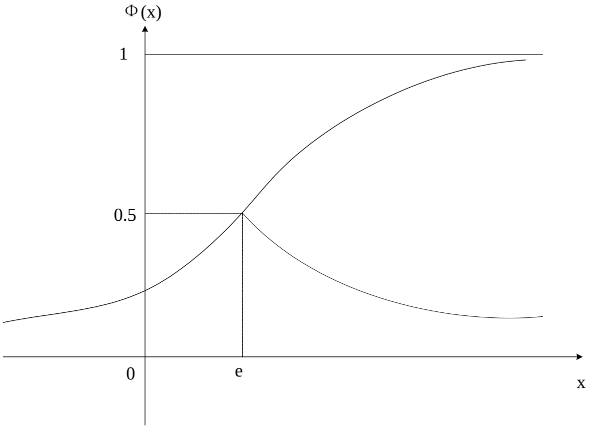

FIGURE 3 Normal Uncertainty Distribution

2.2 CHANCE THEORY

Definition 8 ([14]) An uncertain random variable is a function ξ from a probability space (Ω,A,Pr) to a collection of uncertain variables such that

$$M\{\xi(\omega) \in B\} \tag{6}$$

is a measurable function of ω for any Borel set B of real numbers.

Definition 9 ([14]) Let f: $\Re$ n $\to$ $\Re$ be a measurable function, and ξ1, ξ2,…, ξn are uncertain random variables on the probability space (Ω,A,Pr). Then ξ= f(ξ1, ξ2,…, ξn) is an uncertain random variable defined by

$$\xi(\omega) = f(\xi1(\omega), \xi2(\omega), \ldots, \xi n(\omega)). \tag{7}$$

Definition 10 ([14]) Let ξ be an uncertain random variable, and let B be a borel set of real numbers. then the chance measure of uncertain random event $\xi \in B$ is defined by

$$Ch\{\xi\, B\} = \int_0^1 \Pr\{\omega \in \Omega | M\{\xi(\omega) \in B\} \ge r\}dr. \tag{8}$$

Definition 11 ([14]) Let ξ be an uncertain random variable. Then its chance distribution is defined by

$$\Phi(x) = Ch\{\xi \le x\} \tag{9}$$

for any x$\in \Re$.

Theorem 1 ([14]) Let η_1, η_2,…, η_m be independent random variable with probability distributions ψ_1, ψ_2,..., ψ_m, and let τ_1, τ_2,…, τ_n be independent uncertain variables with uncertainty distributions γ_1, γ_2,..., γ_n, respectively.

Then the uncertain random variable $\xi= f(\eta_1, \eta_2,\dots, \eta_m, \tau_1, \tau_2,\dots, \tau_n)$ has a chance distribution $\phi(x)= \int_{\Re m} F(x;y_1,y_2,\dots.y_m), \ d\Psi_1(y_1)d\Psi_2(y_2),\dots,d\Psi_m(y_m)$, where $F(x;y_1,y_2,\dots,y_m)$ is determined by its inverse function $F^{-1}(\alpha;y_1,y_2,\dots,y_m)=f(y_1,y_2,\dots,y_m,\gamma_1^{-1}(\alpha),\gamma_2^{-1}(\alpha)\dots,\gamma_n^{-1}(\alpha))$ provide that $f(\eta_1, \eta_2, \dots, \eta_m, \tau_1, \tau_2, \dots, \tau_n)$ is a strictly increasing function with respect to $\tau_1,\tau_2,\dots,\tau_n$.

Example 1 ([14]) Let $\eta_1,\eta_2,\dots,\eta_m$ be independent random variables with probability distributions $\Psi_1,\Psi_2,\dots,\Psi_m$, and let $\tau_1,\tau_2,\dots,\tau_n$ be independent uncertain variables with uncertainty distributions $\gamma_1,\gamma_2,\dots,\gamma_n$ respectively.

Then the minimum $\xi=\eta_1\wedge\eta_2\wedge\dots\eta_m\wedge\tau_1\wedge\tau_2\wedge\dots\wedge\tau_n$ is an uncertain random variable whose chance distribution is

$$\Phi(x)=\Psi(x)+\gamma(x)-\Psi(x)\gamma(x), \tag{10}$$

where ψ is the probability distribution of $\eta_1,\eta_2,\dots,\eta_m$ determined by

$$\Psi(x) = 1-(1-\Psi_1(x))(1-\Psi_2(x))\dots(1-\Psi_m(x)) \tag{11}$$

and γ is the uncertainty distribution of $\tau_1 \wedge \tau_1 \wedge \dots \tau_n$ determined by

$$\gamma(x) = \gamma_1(x) \vee \gamma_2(x) \vee \dots \gamma_n(x). \tag{12}$$

Example 2 ([14]) Let $\eta_1,\eta_2,\dots,\eta_m$ be independent random variables with probability distributions $\Psi_1,\Psi_2,\dots,\Psi_m$, $\tau_1,\tau_2,\dots,\tau_n$ be independent uncertain variables with uncertainty distributions $\gamma_1,\gamma_2,\dots,\gamma_n$ respectively. Then the maximum $\xi = \eta_1 \vee \eta_2 \vee \dots \eta_m \vee \tau_1 \vee \tau_2 \vee \dots \vee \tau_n$ is an uncertain random variable whose chance distribution is

$$\Phi(x) = \Psi(x)\gamma(x), \tag{13}$$

where Ψ is the probability distribution of $\eta_1 \vee \eta_2 \vee \dots \eta_m$ determined by

$$\Psi(x) = \Psi_1(x)\Psi_2(x)\dots\Psi_m(x) \tag{14}$$

and γ is the uncertainty distribution of $\tau_1 \vee \tau_2 \vee \dots \vee \tau_n$ determined by

$$\gamma(x) = \gamma_1(x) \wedge \gamma_2(x) \wedge \dots \wedge \gamma_n(x). \tag{15}$$

2.3 BASIC KNOWLEDGE ABOUT FAULT TREE

Cut set: a set of components whose failure interrupts all connections between input and output ends and thus causes an entire system to fail.

Minimal cut set: the smallest combination of components, which will cause the systems failure if they all fail.

Path set: a set of components whose success will make the system successful.

Minimal path set: the smallest combination of components whose success will make the system successful.

There are three methods to obtain minimal cut set of fault tree, Boolean algebra method, ling-row method and structural method. Because Boolean algebra method is simple and effective, it is used in the following analysis.

There are usually three steps to calculate the minimum cut sets by Boolean algebra method.

Step 1. Boolean expressions of top event about fault tree is established. Each layer of events is instead of last layer of events from top event. At last, the top event is instead of all bottom events.

Step 2. The Boolean expression is converted into standard disjunction expression.

Step 3. The standard disjunction expression is simplified to the simplest standard disjunction expression by logic operation rules in Boolean algebra.

3 Uncertain random fault tree analysis

We shall analyse system risk by using fault tree, so three risk definitions will be illustrated as follows.

Definition 12 ([14]) Assume that a system contains uncertain factors $\xi_1, \xi_2, \dots, \xi_n$, and has a loss function f. Then the risk index is $risk = M\{f(\xi_1, \xi_2, \dots, \xi_n) \ge 0\}$.

Definition 13 ([14]) Assume that a system contains random factors $\xi_1, \xi_2, \dots, \xi_n$, and has a loss function f. Then the risk index is $risk = \Pr\{f(\xi_1, \xi_2, \dots, \xi_n) \ge 0\}$.

Definition 14 ([14]) Assume that a system contains uncertain random factors $\xi_1, \xi_2, \dots, \xi_n$, and has a loss function f. Then the risk index is $risk = \mathrm{Ch}\{f(\xi_1, \xi_2, \dots, \xi_n) \ge 0\}$.

For the implementation of uncertain random fault tree analysis for complex system (risk analysis), a systematic methodology is developed and given as follows:

Step 1. System modelling and planning. Identify the problem, carry out the preliminary analysis, gather the data and plan for the solution steps.

Step 2. Risk identification. Identify the top event and the sub-events as well as potential failure-consequence scenarios.

Step 3. Fault tree construction. Find failure logic and build up a fault tree using the bottom events.

Step 4. Bottom events classification. Fault rate of bottom event would be characterized as random variable if it is obtained from historical data, otherwise it would be characterized as uncertain variable.

Step 5. Expression of top event simplification and obtainment. The expression is converted and simplified into the simplest standard disjunction expression and minimal cut set is obtained by Boolean algebra.

Step 6. Expression of top event conversion. The simplest standard disjunction expression is converted into another one based on variable type and Theorem 1.

Step 7. System risk calculation. The chance that top event (system risk) occurs is calculated by hybrid simulation algorithm.

Step 8. Risk management and control. analyse the results, monitor and review the process and propose countermeasures.

4 Uncertain random fault tree analysis application

The priority problem of cloud computing security needed to solve are these: establish a comprehensive cloud computing security model according threats, and actively carry out various key technology research. But in the long run, the security and privacy protection of user data needs is the core problem that is unable to avoid. The important security objectives of cloud users are the data security and privacy protection services.

A cloud security model is put forward through the research on data security in cloud computing security mechanism. As shown in Figure 4:

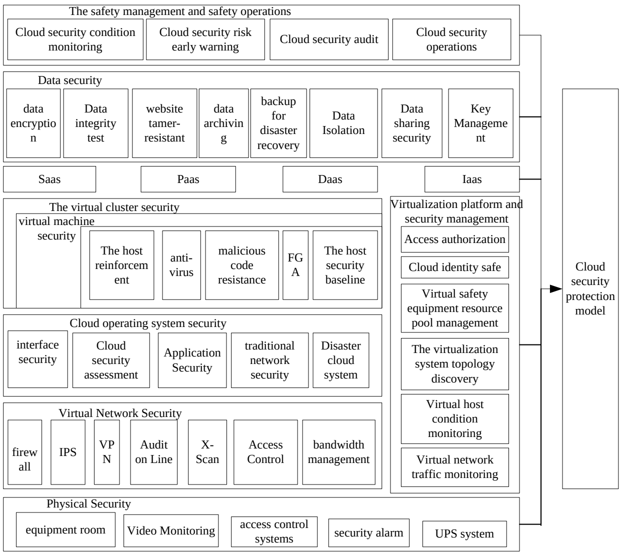
The safety management and safety operations
Cloud security condition monitoring
Cloud security risk early warning
Cloud security audit
Cloud security operations
Data security
data encryption
Data integrity test
website tamer-resistant
data archiving
backup for disaster recovery
Data Isolation
Data sharing security
Key Management
Saas
Paas
Daas
Iaas
The virtual cluster security
virtual machine security
The host reinforcement
anti-virus
malicious code resistance
FGA
The host security baseline
Virtualization platform and security management
Access authorization
Cloud identity safe
Virtual safety equipment resource pool management
The virtualization system topology discovery
Virtual host condition monitoring
Virtual network traffic monitoring
Cloud operating system security
interface security
Cloud security assessment
Application Security
traditional network security
Disaster cloud system
Virtual Network Security
firewall
IPS
VPN
Audit on Line
X-Scan
Access Control
bandwidth management
Physical Security
equipment room
Video Monitoring
access control systems
security alarm
UPS system
Cloud security protection model

FIGURE 4 A Cloud Security Framework

Figure 4 mainly includes physical security, virtual network security, cloud operating system security, virtual cluster security, SaaS/PaaS/IaaS security, data security, safety management and safety operational and so on. In fact, cloud computing is introduced into the virtualization technology, and changed the service way, but did not overthrow the traditional safe mode.

Many risk factors that affect cloud security protection system include trusted access control, cipher text retrieval and processing, data exists and reusability, data privacy, virtual security technology and so on [34-37]. The chances that some factors occur are obtained from historical data, so they are random, others have no historical statistical data but are obtained from questionnaire to experts, so they are uncertain. Therefore, this paper applies UR-FTA to cloud security protection framework risk analysis.

Step 1. System modelling and planning. This paper analyses cloud security protection framework from two aspects of internal risk and external risk, internal risk includes identity and security, data security and host security; external risk includes security audit, risk early warning, security condition monitoring and security resource management. It also analyses the characters of all factors and gathers the data and plans for the solution steps.

Step 2. Risk identification. Identify the top event and the sub-events as well as potential failure-consequence scenarios.

Step 3. Fault tree construction. The logical relationship between events is analysed and the fault tree is constructed, it is shown in Figure 5. In the figure, the top event E represents the entire cloud security protection framework risk, intermediate events B and C represent respectively external risks and internal risks in the framework, the bottom events 1, 2, 3 and 4 respectively security audit, risk early warning, security condition monitoring and security resource management, the bottom events 5, 6, 7 represent respectively identity and security, data security and host security. The logical relationships between them are shown in figure 5.

Step 4. Bottom events classification. Fault rate of bottom event would be characterized as random variable if it is obtained from historical data, otherwise it would be characterized as uncertain variable. It is shown in Table 1. Security audit, risk early warning, security condition monitoring and security resource management have historical statistical data, so η_1, η_2, η_3, η_4 are random variables with random distributions Ψ_1, Ψ_2, Ψ_3, Ψ_4; and identity and security, data security and host security have no statistical data, so η_5,η_6,η_7 are uncertain variables with uncertain distributions γ_5, γ_6, γ_7.

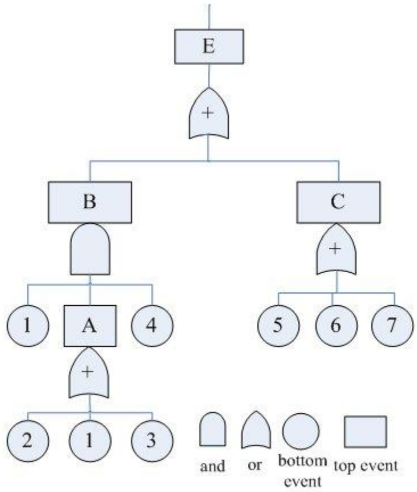

FIGURE 5 Cloud Security Protection Framework Risk Fault Tree

TABLE 1 Chance that Bottom Event Occurs

code	bottom event	chance
η_1	security audit	Ψ_1
η_2	risk early warning	Ψ_2
η_3	security condition monitoring	Ψ3
η_4	security resource management	Ψ4
η_5	identity and security	γ5
η_6	data security	γ6
η_7	host security	γ7

Step 5. Expression of top event obtainment. The risk formula of event B is obtained based on logical relations of bottom events in fault tree

$$B = \text{event1}\wedge(\text{event2}\vee\text{event1}\vee\text{event3})\wedge\text{event4}. \qquad (16)$$

The risk formula of event C is obtained based on logical relations of bottom events in fault tree

$$C = \text{event5}\vee\text{event6}\vee\text{event7}. \qquad (17)$$

So the risk formula of top event E is obtained

$E = \text{event1}\wedge(\text{event2}\vee\text{event1}\vee\text{event3})\wedge\text{event4}\vee\text{event5}\vee\text{event6}\vee\text{event7} = \text{event1}\wedge\text{event4}\wedge\text{event5}\vee\text{event6}\vee\text{event7}$.

The simplest disjunction expression is

$$E = \text{event1}\wedge\text{event4}\vee\text{event5}\vee\text{event6}\vee\text{event7}. \qquad (18)$$

So the minimal cut set of fault tree is {1,4,5,6,7}.The key bottom events of fault tree are 1,4,5,6,7. The equivalent fault tree of original fault tree is shown in figure 6.

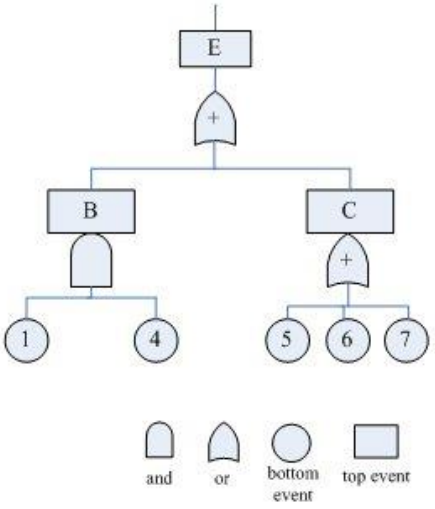

FIGURE 6 Equivalent Fault Tree

Step6. Expression of top event conversion. Because η_1, η_4 are probability variables, the risk formula of event B is obtained based on logical relations of bottom events in equivalent fault tree and two examples of chance theory

$$\Psi_B = 1-(1-\Psi_1)(1-\Psi_4). \qquad (19)$$

Because η_5, η_6, η_7 are uncertain variables, the risk formula of event C is obtained based on logical relations of bottom events in equivalent fault tree and two examples of chance theory

$$\gamma_C = \gamma_5 \wedge \gamma_6 \wedge \gamma_7 . \qquad (20)$$

So the risk formula of top event E is obtained

$$\Phi_E = (1-(1-\Psi_1)(1-\Psi_4))(\gamma_5 \wedge \gamma_6 \wedge \gamma_7). \qquad (21)$$

Step 7. System risk calculation. Suppose that Ψ_1, Ψ_2, Ψ_3, Ψ_4 are random exponential distribution, where $\Psi_1 = \exp(0.8)$, $\Psi_2 = \exp(0.5)$, $\Psi_3 = \exp(0.2)$, $\Psi_4 = \exp(0.4)$; γ_5, γ_6, γ_7 are uncertain normal distribution, where $\gamma_5 = N(0.1,0.01)$, $\gamma_6 = N(0.4,0.02)$, $\gamma_7 = N(0.5,0.01)$. The risk chance can be obtained by hybrid simulation algorithm. The flow chart of algorithm is shown in figure 7.

Step 8. Risk management and control. The risk chance of top event 0.0132 is calculated by hybrid simulation algorithm. The risk chance of this system is small, it illustrates that risk control of this system is perfect.

5 Conclusions

This paper proposes a method that constructs and analyses fault tree based on uncertainty theory and chance theory.

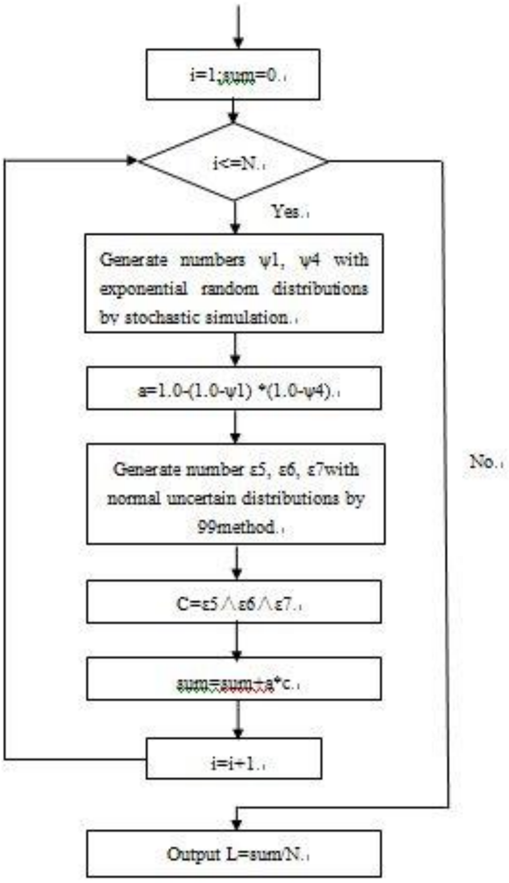
i=1;sum=0.
i<=N.
Yes.
Generate numbers ψ1, ψ4 with exponential random distributions by stochastic simulation.
a=1.0-(1.0-ψ1) *(1.0-ψ4).
Generate number ε5, ε6, ε7with normal uncertain distributions by 99method.
C=ε5∧ε6∧ε7.
sum=sum+a*c.
i=i+1.
No.
Output L=sum/N.

FIGURE 7 Flow Chart of Hybrid Simulation Algorithm

It also constructs hybrid simulation algorithm to calculate the chance that top event occurs. The URFTA methodology has several advantages compared to strictly deterministic FTA method and these are listed as follows.

(1) The proposed method is suitable for situations where probabilistic risk or uncertain risk exists.

(2) The methodology can be properly handled in a consistent manner in a situation with ill-defined, ambiguous information as well as probabilistic data.

(3) By using uncertainty theory and probability theory, the state of each bottom event can be described in a realistic form. The use of chance theory provides more precise descriptions and accurate solutions.

(4) This UR-FTA model is a simple and useful tool to estimate and evaluate risk in complex system.

(5) The methodology has been very versatile and flexible in applications. Therefore, it can easily be applied in other fields related risk analysis problems.

The future work of this study will focus on two directions: from the purely technical point of view, if operational rules between uncertain random variable and uncertain variable or random variable is correctly defined, the methodology will be applied to more complex system in all kinds of fields; from the practical point of view, dependent failures and common cause failures should be analysed in fault tree, the new general hybrid simulation algorithm should be developed to apply in all kinds of fault tree analysis.

Acknowledgments

This work was supported by the Natural Science Foundation of China (No.61163025) and the Project of Beijing Key Laboratory of Knowledge Engineering for Materials Science(No.Z121101002812005).

References

[1] HanSuk Pan, WonYoung Yun 1997 Fault tree analysis with Fuzzy Gates *Computers ind Engng* **33**(3) 569-72

[2] Ching-torng Lin, Mao-jiun J.Wang 1997 Hybrid fault tree analysis using fuzzy sets *Reliability Engineering and system Safety* **58** 205-13

[3] Khan F I, Abbasi S A 2000 Analytical simulation and PROFAT II: a new methodology and a computer automated tool for fault tree analysis in chemical process industries *J.Hazard. Mater* **75** 1-27

[4] Hu W, Starr A G, Leung A Y T 2003 Operational fault diagnosis of manufacturing systems *J. Mater. Process Technol* **133** 108-17

[5] Li H X, Zuo M J 1999 A hybrid approach for identification of root causes and reliability improvement of a die bonding process a case study *Reliab. Eng. Syst.Saf.* **6** 43-8

[6] Sohn S D, Seong P H 2004 Quantitative evaluation of safety critical software testability based on fault tree analysis and entropy *J. Syst. Softw* **73** 351-60

[7] Roy P K, Arti B, Chitra R 2003 Quantitative risk assessment for accidental release of titanium tetrachloride in a titanium sponge production plant *J. Hazard. Mater* **102** 167-86

[8] Zadeh L A 1965 Fuzzy sets *Inform. and Control* **8** 338-53

[9] Hua Song, Hong-Yue Zhang, Chan C W 2008 Fuzzy fault tree analysis based on T-S model with application to INS/GPS navigation system *Soft Computing* **3**(9) 21-30

[10] Khan Faisal, Sadiq Rehan, Amyotte Paul, Veitch Brian 2011 Fault and Event Tree Analyses for Process Systems Risk Analysis Uncertainty Handling Formulations *Risk Analysis* **31**(1) 86-107

[11] Chanda R S, Bhattacharjee P K 1998 A reliability approach to transmission expansion planning using fuzzy fault tree model *Electric Power System Research* **45** 101-8

[12] Dong Yuhua, Yu Datao 2005 Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis *Journal of Loss Prevention in the Process Industries* **18** 83-8

[13] Ayhan mentes, Ismail H.Helvacioglu 2011 An application of fuzzy fault tree analysis for spread mooring systems *Ocean Engineering* **38** 285-94

[14] Liu B *Uncertainty Theory* 4th ed. http://orsc.edu.cn/liu/ut.pdf

[15] Liu B 2007 *Uncertainty Theory* 2nd ed. Springer-Verlag,Berlin

[16] Liu B 2009 Some research problems in uncertainty theory *Journal of Uncertain Systems* **3**(1) 3-10

[17] Liu B 2009 *Theory and Practice of Uncertain Programming* 2nd ed., Springer-Verlag, Berlin

[18] Liu B 2010 U*ncertainty Theory: A Branch of Mathematics for Modeling Human Uncertainty* Springer-Verlag, Berlin

[19] Liu B 2010 Uncertain risk analysis and uncertain reliability analysis *Journal of Uncertain Systems* **4**(3) 163-70

[20] Liu B 2012 Why is there a need for uncertainty theory? *Journal of Uncertain Systems* **6**(1) 3-10

[21] Liu B 2001 Fuzzy random chance-constrained programming *IEEE Transactions on Fuzzy Systems* **9**(5) 713-20

[22] Liu B 2001 Fuzzy random dependent-chance programming *IEEE Transactions on Fuzzy Systems* **9**(5) 721-6

[23] Liu J J 2011 Uncertain comprehensive evaluation method *Journal of Information Computational Science* **8**(2) 336-44

[24] Rong L X 2011 Two new uncertainty programming models of inventory with uncertain costs *Journal of Information &Computational Science* **8**(2) 280-8

[25] Yan L M 2009 Optimal portfolio selection models with uncertain returns *Modern Applied Science* **3**(8) 76-81

[26] Meilin Wen, Rui Kang Reliability Analysis in Uncertain Random System http://orsc.edu.cn/online/120419.pdf

[27] Greg B, Padma M, Dennis Q, et al. *Cloud Computing [EB/OL]* http://www.Cloud computing-china.cn

[28] Wang P 2010 *The key technology of cloud computing and application* Beijing: Posts and Telecom Press

[29] Chen K, Zheng W M 2009 Cloud computing: System instances and current research *Journal of Software* **20**(5) 1337−48

[30] John R, James R 2009 *Cloud Computing: Implementation, Management, and Security*

[31] Xia T Z, Li Z 2009 Research on Cloud Computing Based on Deep Analysis to Typical Platforms *cloudcom 2009,beijing, China* 601-8

[32] ITU http://www.itu.int/en/pages/default.aspx

[33] Azanza M P V 2006 HACCP certi_cation of food services in Philippine inter-island passenger vessel *Food Control* **17** 93-101

[34] Goldbach S G, Alban L 2006 A costCbene_t analysis of Salmonella control strategies in Danish pork *production Preventive Veterinary Medicine* **77**(1) 1-14

[35] Fraser R, Souza D Monteiro 2009 A conceptual framework for evaluating the most cost-e_ective intervention along the supply chain to improve food safety *Food Policy* **34** 477-81

[36] Okezie I, Aruoma 2006 The impact of food regulation on the food supply chain *Toxicology* **221** 119-27

Authors	
	Guo Changyou, born in 1976 **Current position, grades:** PhD candidate at the School of Computer and Communication Engineering, University of Science and Technology, Beijing. **Scientific interests:** Access Control, Network Security, Information Security and Cloud Computing Security.
	Zheng Xuefeng, born in 1951 **Current position, grades:** professor and doctoral supervisor in the School of Computer and Communication Engineering, University of Science and Technology Beijing. **His research interest:** Computer Control Systems Development, Computer System Security Analysis, Network Security, Information Security and Distributed Systems Security. He is the senior member of the computer society.
	Liu Jianjun, born in 1976 **Current position, grades:** PhD candidate at the School of Computer and Communication Engineering, University of Science and Technology, Beijing **Scientific interests:** Access Control, Network Security, Information Security and Cloud Computing Security.