RESEARCH on RISK MONITOR QUANTIFICATION METHOD BASED on BINARY DeCISION DIAGRAMS

Bing Zhang[1], Ming Wang[2]

[1]*Tower B, CNPEC Building at No. 18 Baolong 3rd Rd, Longgang District, Shenzhen City Guangdong Province People's Republic of China, 518172,xiaohan1123@163.com*
[2]*Tower B, CNPEC Building at No. 18 Baolong 3rd Rd, Longgang District, Shenzhen City Guangdong Province People's Republic of China, 518172,wangming25436@163.com*

ABSTRACT

The Risk Monitor (RM) is a core tool for real-time nuclear power plant risk assessment and has been widely applied in the safety operation management of such facilities. Calculation accuracy and speed are crucial for real-time risk assessment. This paper proposes a quantification method for the Risk Monitor based on Binary Decision Diagrams (BDD). Case studies show that the BDD-based method achieves similar accuracy to the third-order approximation while significantly reducing computational load and improving efficiency. This method can be applied to both the recalculation method and the cut-set method in risk monitors.

Keywords: Risk Monitor, Binary Decision Diagrams, Risk Assessment

I. INTRODUCTION

The Risk Monitor (RM) is a core tool for real-time risk assessment in nuclear power plants, widely adopted in safety and operational management. It relies on Probabilistic Safety Assessment (PSA) techniques to monitor changes in system and equipment status, rapidly quantifying key risk indicators such as Core Damage Frequency (CDF) and Incremental Core Damage Probability (ICDP). This provides a scientific basis for risk management and operational activities, ensuring safe and efficient plant operation. At present, mature risk monitor products have been successfully developed and deployed internationally, forming a complete technical system and application norms. However, the complexity of nuclear power plant systems poses significant challenges for real-time risk assessment. Risk models are typically large fault trees with thousands of logical gates, evolving in real-time with plant configuration changes due to equipment startups, shutdowns, and maintenance. The stringent real-time requirements of risk monitors make the development of fast computational engines as a bottleneck. Traditional algorithms, such as first-order and higher-order approximations, are widely used but face limitations in computational efficiency and accuracy when dealing with large-scale real-time fault trees. These limitations hinder the ability to meet the real-time risk assessment needs of complex nuclear power plant conditions.

To address these challenges, this paper proposes a risk monitor quantification method based on Binary Decision Diagrams (BDDs). This method leverages the strengths of BDDs in logical representation and efficient computation to optimize the minimal cut sets of real-time risk models, thereby enhancing computational performance. The research findings provide innovative ideas and technical support for developing computational engines for nuclear power plant risk monitors, improving safety operation level and risk control capabilities.

II. REAL-TIME RISK MODEL CONSTRUCTION and QUANTIFICATION

The quantification process of real-time risk models can be divided into two main parts: updating the real-time risk model and quantification. The quantification methods commonly include the recalculation method and the cut-set method, as detailed in Figure 1.

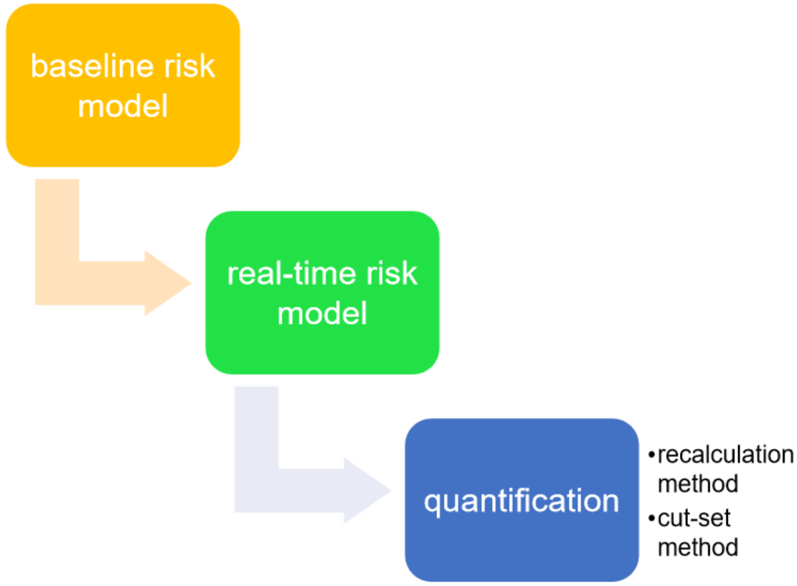

FIGURE 1. Quantification Process of Real-time Risk model

II.A Real-Time Risk Model Update

The real-time risk model is based on a baseline configuration developed using the zero-maintenance and zero-failure configuration of the nuclear power plant. It leverages data interfaces to continuously collect real-time operational status data, such as equipment shutdowns and restarts, from the plant's information monitoring system and main control room logs. These real-time data are dynamically integrated into the baseline risk model, adjusting the failure model parameters of corresponding equipment in real-time to generate a risk model that accurately reflects the current plant configuration. Any change in the plant's configuration status triggers an automatic update mechanism to ensure that the risk assessment results remain highly synchronized with the actual configuration.

II.B Quantification of Real-Time Risk Model

To address the challenge of quickly quantifying large-scale fault trees in real-time risk models, the mainstream methods currently used in the industry include the cut-set method and the recalculation method.

1) Cut-Set Method: This method first pre-calculates the minimum cut sets of the fault tree using top-down or bottom-up approaches. When the plant configuration changes, the relevant basic events within the minimum cut sets are modified. New minimum cut sets are then formed through cut-set absorption methods, followed by quantification using methods such as first-order, second-order, or third-order approximation.

2) Recalculation Method: After each update of the real-time risk model, the recalculation method recalculates the risk model from scratch and outputs new minimum cut sets. Quantification is then performed based on these new minimum cut sets. Although this method ensures computational accuracy, it is time-consuming, posing a challenge for real-time risk monitoring. As a result, improving the efficiency of the recalculation method has become a research hotspot in the industry, with various techniques such as model simplification and cut-set reconstruction being gradually proposed.

Both the cut-set method and the recalculation method require the crucial step of quantifying the minimum cut sets. Traditional quantification methods include first-order, second-order, and third-order approximations. These methods simplify the solution of complex models by truncating higher-order terms in the Taylor expansion of the polynomial, which has been widely applied in the quantification analysis of risk models. However, these methods essentially represent a trade-off between accuracy and efficiency. Ensuring both computational accuracy and speed is particularly challenging in scenarios involving large-scale real-time models, such as those in nuclear power plant risk monitors. Therefore, there is an urgent need to introduce more efficient algorithms, such as BDD-based methods, to break through the bottleneck of traditional methods in terms of computational efficiency and accuracy, achieving efficient and accurate quantification of real-time risk models.

III. RISK MONITOR QUANTIFICATION METHOD BASED on BINARY DECISION DIAGRAMS

In principle, the Binary Decision Diagram (BDD) method can be used for both obtaining minimal cut sets and quantifying them. This paper mainly focuses on the quantification of minimal cut sets. The main principle is to first decompose the minimal cut sets into a BDD tree using Shannon decomposition and then conduct quantification based on the disjointness principle of the BDD tree.

Shannon Decomposition, also known as the Substitution Law for Boolean functions, is based on Boolean algebra principles. It simplifies a complex Boolean function by introducing a variable, breaking it down into two simpler sub-functions. For a Boolean function $F(x_1,x_2,\ldots,x_n)$, selecting a variable as the decomposition variable, according to the value of x_i (0 or 1), can decompose F into:

$$F(x_1,x_2,\ldots,x_n) = x_i \cdot F(x_1,x_2,\ldots,x_i=1,\ldots,x_n) + \overline{x_i} \cdot F(x_1,x_2,\ldots,x_i=0,\ldots,x_n) \tag{1}$$

Where:
$F(x_1,x_2,\ldots,x_i=1,\ldots,x_n)$ represents the Boolean function when x_i is set to 1, called the "positive part."
$F(x_1,x_2,\ldots,x_i=0,\ldots,x_n)$ represents the Boolean function when x_i is set to 0, called the "negative part."

For a fault tree with minimal cut sets ABC and CD, it can be transformed into a BDD tree based on Shannon decomposition, as shown in the Figure 2 and Figure 3. The probability of the top event can be calculated by traversing all paths that lead to 1. The calculation formula is as follows:

$$P = P(A)P(B)P(C) + P(A)\overline{P(B)}P(C)P(D) + \overline{P(A)}P(C)P(D) \tag{2}$$

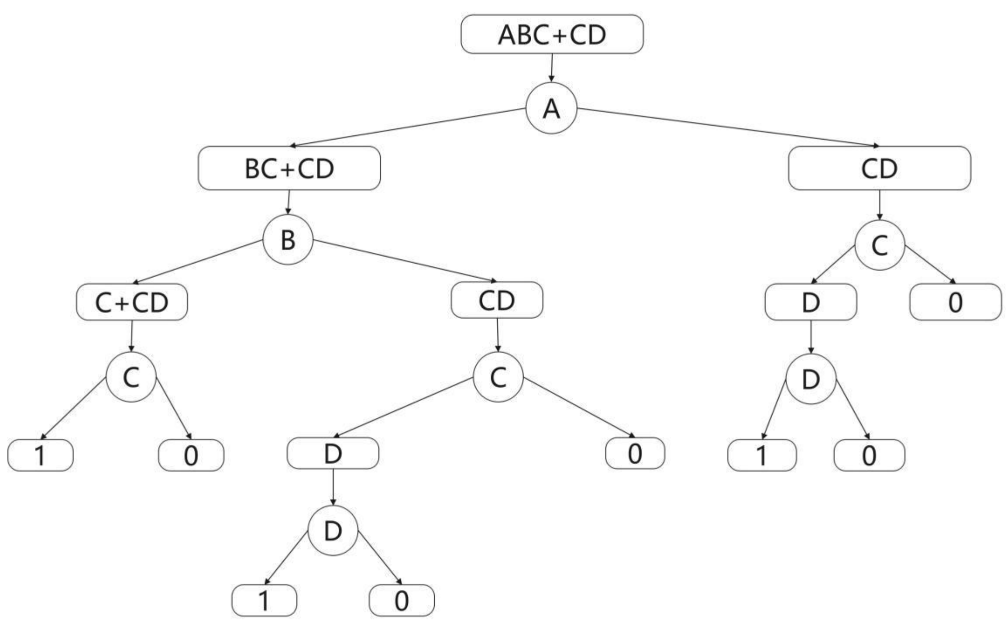

FIGURE 2. Shannon Decomposition

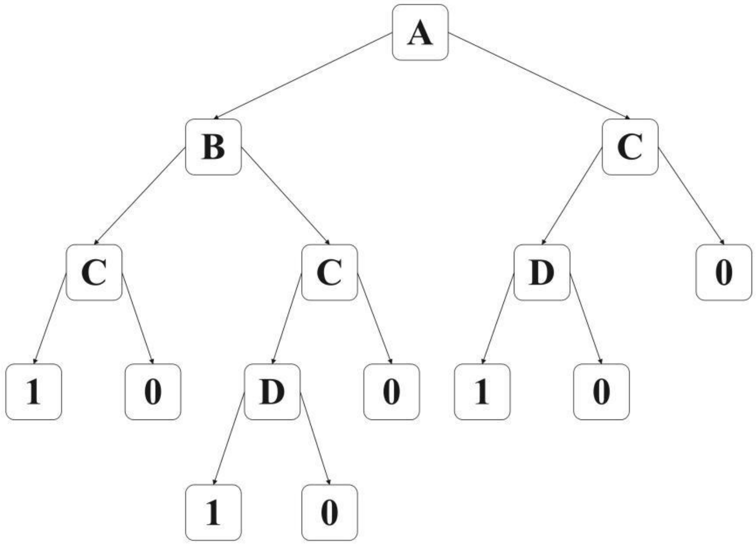

FIGURE 3. BDD Tree

The simplest method for quantifying minimal cut sets is the first-order approximation method. However, its disadvantage is that the result will be overly conservative if there are basic events with high failure probabilities in the cut set. The calculation formula is as follows:

$$P \approx \sum_{i=1}^{k} MCS_i \quad (3)$$

A more accurate method for quantifying minimal cut sets is the third-order approximation method. Its disadvantage is that the calculation is more complex, especially when there are many cut sets. The calculation formula is:

$$P \approx \sum_{i=1}^{k} P(MCS_i) - \sum_{1\le i<j\le k} P(MCS_i \cap MCS_j) + \sum_{1\le i<j<m\le k} P(MCS_i \cap MCS_j \cap MCS_m) \quad (4)$$

It can be seen from the above calculation formulas that the BDD algorithm is much simpler than the third-order approximation and provides an exact solution. It has significant advantages for cases with a large number of minimal cut sets. Particularly in uncertainty analysis calculations, which require thousands of repeated calculations, the computational efficiency will be significantly improved compared with the third-order approximation.

IV. CASE STUDY and RESULTS

This section presents a case study comparing first-order approximation, third-order approximation, and BDD methods for fault tree quantification, contrasting their results and computational demands.

A top event with four minimal cut sets：ABC, ACD, ABE, and FG is assumed, where A, B, C, D, E, F, and G are independent basic events with probabilities P(A)=0.01, P(B)=0.02, P(C)=0.1, P(D)=0.05, P(E)=0.05, P(F)=0.02, and P(G)=0.02.

IV.A Construction of the BDD Tree

The Shannon decomposition process is illustrated in the Figure 4.
The BDD tree constructed based on this is shown in the Figure 5.

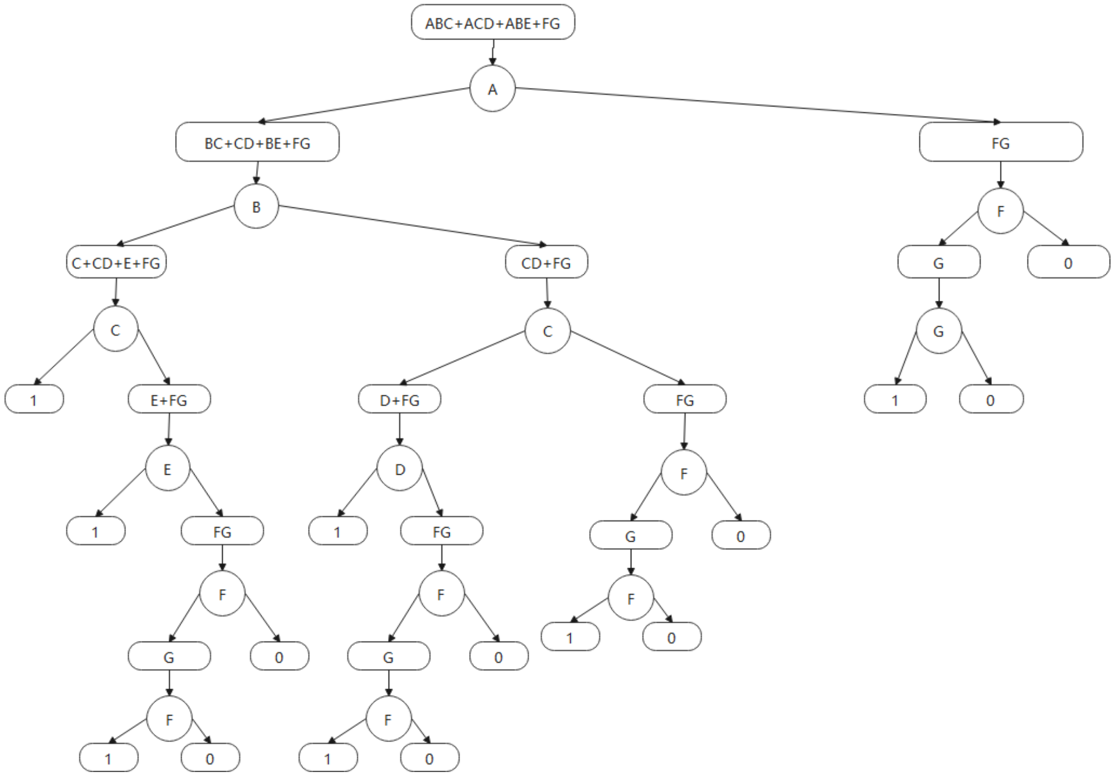

FIGURE 4. Shannon Decomposition Process

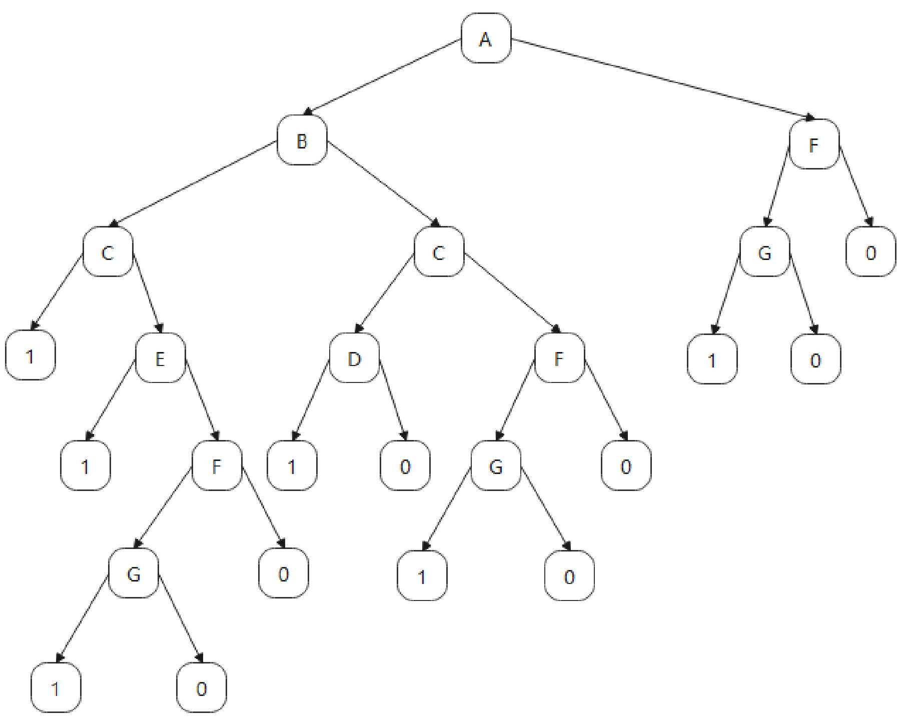

FIGURE 5. BDD Tree for the Case Study

IV.B Quantification Comparison

1）Quantification using RiskSpectrum (RS) Software

Computational complexity: The third-order calculation is carried out according to Eq. (4), and the computational complexity includes:

- ✓ $\sum_{i=1}^{k} P\ (MCS_i\ )$, it includes 7 multiplication operations and 3 addition operations;
- ✓ $\sum_{1\le i<j\le k} P\ (\ MCS_i \cap MCS_j\ )$,it includes 6 logical operations, 2 multiplication operations and 2 addition operations；
- ✓ $\sum_{1\le i<j<m\le k} P\ (\ MCS_i \cap MCS_j \cap MCS_m\ )$, it includes six logical operations.

Adding the two addition/subtraction operations of Eq. (4) itself, the third-order approximation method requires a total of 12 logical operations and 16 addition, subtraction, multiplication and division operations.

Computational Result: Quantification was performed using first-order and third-order approximation methods, with the following results:

TABLE I. Quantification Method and Result

Quantification Method	Result
First-order Approximation	4.8E-4
Third-order Approximation	4.47E-4

2）Using the BDD Algorithm

Computational complexity: According to Figure 5, the failure probability of the top event can be expressed as follow:

$P=P(A)P(B)P(C)+P(A)P(B)\overline{P(C)}P(E)+P(A)P(B)\overline{P(C)}\overline{P(E)}P(F)P(G)+P(A)\overline{P(B)}P(C)P(D)+P(A)\overline{P(B)}\overline{P(C)}P(F)P(G)+\overline{P(A)}P(F)P(G)$. Therefore, the total amount of calculation is 4 simple logical (probability negation) operations and 18 addition/ subtraction/multiplication/division operations.

Computational Result: the failure probability of the top event is:

P=0.01*0.02*0.1+0.01*0.02*0.9*0.05+0.01*0.02*0.9*0.95*0.02*0.02+0.01*0.98*0.1*0.05+0.01*0.98*0.9*0.02*0.02+0.99 *0.02*0.02=（2E-5）+（9E-6）+（6.84E-8）+（4.9E-5）+（3.528E-6）+（3.96E-4）=4.78212E-4.

TABLE II. Quantification Method and Result- BDD

Quantification Method	Result
First-order Approximation	4.80 E-4
Third-order Approximation	4.78 E-4
BDD Algorithm	4.78212E-4

In probabilistic safety analysis, the failure probability of each basic event is a distribution, and it usually requires more than 1,000 samples to obtain a good mean value. When using the BDD algorithm, it is only necessary to replace the failure probability values of each basic event. There is no need to regenerate the BDD tree for each calculation. Since the amount of computation for each sample is greatly reduced, it is expected that the computational efficiency in uncertainty analysis will be significantly improved compared with the third-order approximation.

IV.C Discussion

It can be seen from the above research that it is feasible to use the BDD algorithm to solve the failure probability of known minimal cut sets. According to the case study, it can be seen that compared with the third-order approximation method, the BDD algorithm can significantly reduce logical computations, while the computational load of addition/ subtraction/ multiplication/division is basically the same. Based on the calculation theory of the two methods, it can be inferred that the logical computational load of large fault trees will also be greatly reduced, and logical operations are precisely the most time-consuming part. The results show that the BDD algorithm is closer to the third-order approximation, while the first-order approximation method is more conservative. In addition, the structure of the Level 1 probabilistic safety analysis model of nuclear power plants is often rather complex. Using the first-order approximation method to calculate the core damage frequency usually takes several minutes to several hours, and may even exceed 24 hours. If the third-order approximation method is adopted, the calculation time is usually several times that of the first-order approximation method. If it is extended to the Level 2 PSA, the calculation time will be even longer. At this time, the BDD algorithm based on the minimum cut set has significant advantages in terms of calculation accuracy and computational complexity.

Although the BDD algorithm based on the minimum cut set has significant advantages in terms of calculation accuracy and computational complexity, it should be noted that this method is based on the minimum cut set. That is to say, the minimum cut set must be obtained first. For fault trees that have not yet formed the minimum cut set, the minimum cut set needs to be generated first. Moreover, finding the minimum cut set for large fault trees is also a difficulty and requires separate study.

V. CONCLUSION

The BDD algorithm, through its disjointness processing, ensures the precise solution of cut sets. Compared to the third-order approximation method, it significantly reduces the computational load, providing a solution approach for large-scale minimal cut sets. This method can be used for both the rapid cut-set method solution in risk monitors and the quantification calculation in the recalculation method.

This paper primarily demonstrates the feasibility of the BDD method for quantifying minimal cut sets using simple case studies. Compared to the third-order approximation method, the BDD quantification method has significant advantages in both computational accuracy and efficiency. This is especially true in uncertainty analysis, where only data substitution is required, making the computational efficiency more prominent. Building on this approach, quantitative software can be further developed to establish a tool for large-scale minimal cut set quantification.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to the State Key Laboratory of Nuclear Power Safety Technology and Equipment for its relevant support in this research.

REFERENCES

[1] Zhang Chao, Research on Optimization Analysis of Dynamic Fault Tree Based on BDD, Master's thesis, Northwestern Polytechnical University, Xi'an, China. (2004).
[2] Zhang, Min. Research on the Timely Automatic Update Method of Living PSA for Nuclear Power Plants. Doctoral dissertation, Harbin Engineering University, (2019).
[3] Wang J , Wang F , Chen S ,et al.Fault-tree-based instantaneous risk computing core in nuclear power plant risk monitor[J].Annals of Nuclear Energy, 2016, 95(Sep.):35-41.DOI:10.1016/j.anucene.2016.02.024.
[4] Gu, Xiaohui, Jiaqun Wang, Fang Wang, et al. "A Preliminary Study on the Development and Application of Real-Time Risk Models in Risk Monitoring Systems." Chinese Journal of Nuclear Science and Engineering 31, no. 2 (20 11): 180-184, 192.
[5] Reay K A , Andrews J D .A fault tree analysis strategy using binary decision diagrams[J].Reliability Engineering & System Safety, 2002, 78(1):45-56.DOI:10.1016/S0951-8320(02)00107-2.

[6] WU Y C, HU L Q, LI Y Z, et al. Development of third Qinshan nuclear power plant risk monitor［J］. Chinese Journal of Nuclear Science and En- gineering, 2011, 31（1）：68-75.
[7] GU X H, BAO Z L, YU W G, et al. The development and application of real-time monitor at Tianwan nuclear power plant［J］. Chinese Journal of Nuclear Science and Engineering, 2017, 37（4）：691-699
[8] ZHANG Y X, LI Y, LI P F. On application of risk monitor in China and other countries［J］. Shanxi Architecture, 2015, 41（8）：245-247.
[9] GAO W, ZHANG Q F. Development of risk monitor for nuclear power plant［J］. Atomic Energy Science and Technology, 2012, 46（11）：1362- 1367
[10] Sinnamon RM, Andrews JD. Quantitative fault tree analysis using binary decision diagrams. Eur J Automation 1996;30(8).
.