Research on Reliability Analysis Method Based on Dynamic Fault Tree

Han Chen, Ling Chen* and Yongfa Zhang

College of Nuclear Science and Technology Naval University of Engineering, Wuhan, China

*Corresponding author: ling_chen@nue.edu.cn

Abstract. Due to the development of digital technology, digital I&C systems have replaced analog I&C systems and become the mainstream I&C systems for nuclear power plants and marine nuclear power plants. However, there is still a lack of effective and recognized analysis methods for the reliability analysis of digital I&C systems. Based on the commonly used dynamic fault tree analysis method for dynamic system reliability analysis, this paper uses Markov transition matrix to achieve quantitative analysis. Reliability analysis of the digital I&C system, through the improved dynamic fault tree analysis method, provides an effective analysis method for the reliability analysis of the digital I&C system.

1. Introduction

Compared with the traditional analog I&C system, the digital I&C system has the characteristics of high safety and high reliability. Therefore, since Honeywell launched the first digital I&C system, nuclear power plants and marine nuclear power plants in various countries are gradually using digital I&C systems instead of analog I&C systems. The digital I&C system is a dynamic system with multiple dynamic characteristics such as time characteristics. As a result, the traditional PSA analysis method can’t effectively analyze the reliability of the digital I&C system. In order to better verify the reliability of the digital I&C system, the dynamic PSA method began to receive attention in the probabilistic safety assessment of nuclear power plants in the 1980s [1, 2]. Due to many reasons such as knowledge blockade in the field of digital I&C systems, our country started late, and the research on its reliability analysis is relatively new. Therefore, it is necessary to conduct in-depth research on the reliability analysis of the digital I&C system, and propose a relatively valuable reliability analysis method.

2. Dynamic fault tree analysis method

The dynamic fault tree method is based on the traditional fault tree analysis method, adding a series of theoretical analysis methods of dynamic logic gates. The added dynamic logic gates mainly include: priority AND gates, sequence correlation gates, etc. The added dynamic logic gates enable the dynamic fault tree to have the ability to handle the dynamic characteristics of the dynamic system that the traditional fault tree does not have. But at the same time, due to the introduction of dynamic logic gates, the dynamic fault tree has certain difficulties in quantitative calculation compared with the traditional fault tree method. Therefore, in the reliability analysis of dynamic systems, the dynamic fault tree method is usually combined with other methods.
2.1. **Priority AND gate**

Priority AND gates are similar to AND gates. The difference lies in the sequence of events. Only when they occur in order can the fault occur. Figure 1 shows the priority AND gate and its Markov model. The state "1" represents the occurrence of a fault, and the state "0" means normal operation.

![Figure 1. Priority AND gate and its Markov transition diagram](image1)

2.2. **Function trigger gate**

Function trigger gate is a kind of dynamic logic gate, which is mainly used to describe a series of cascading failures caused by a certain failure. Since it has no output, its basic logic is shown in Figure 2. Once A fault occurs, it will inevitably lead to a series of faults such as B, C, D..., so there is no need to consider its calculation problems, that is, it does not need to consider its Markov transition diagram.

![Figure 2. Function trigger gate](image2)

2.3. **Sequence related gates**

Sequence-related gates are similar to priority AND gates. In fact, priority AND gates is one kind of special sequence-related gates. The difference between sequence-related gates and priority AND gates is that sequence-related gates have more basic faults, that is, when a series of B, C, D, etc. The occurrence of fault A will only occur when the faults occur in a certain order. As the number of faults increases, the calculation difficulty of sequence-related gates is also greatly increased. The complexity of the Markov transition diagram increases exponentially with the increase of faults, so the sequence is related Gate is the biggest difficulty in quantitative calculation in dynamic fault tree. Its model and Markov transition diagram are shown in Figures 3 and 4.
2.4. **Spare parts door**

Spare parts doors are divided into cold, hot and warm spare parts doors. The feature of spare parts doors lies in the consideration of the status of spare parts. Cold spare parts doors are different from warm spare parts doors and hot spare parts doors. In normal operation, the spare parts of cold spare parts doors are in shutdown state, namely In the absence of failure in A, the failures of B, C and D are not considered. When the warm spare parts door and the hot spare parts door are in operation, the spare parts are also in operation. The difference is that the spare parts of the warm spare parts door are in the low power operation state, and the spare parts of the hot spare parts door are in the normal power operation state, and their failure probability is different. The cold spare parts door model and its Markov transition diagram are shown in Figure 5. The warm spare parts door and the hot spare parts door can be represented by the same model and Markov transition diagram, as shown in Figure 6. The main difference between the hot spare part door and the warm spare part door model is that $\lambda_B$ and $\lambda_C$ are equal in the hot spare part door, while $\lambda_B$ and $\lambda_C$ are different in the warm spare part door, and $\lambda_B$ is usually greater than $\lambda_C$. 

---

**Figure 3.** Sequence related gate

**Figure 4.** Sequential correlation gate Markov model
3. Solution of dynamic logic gate

There is no recognized and reliable method for the quantitative calculation of dynamic logic gates now. This paper uses the Markov model method to convert the difficult-to-calculate dynamic logic gates into a probability matrix that can be solved. Its application has been recognized in other fields. The credibility is high.

The dynamic logic gate adopts the same processing method as the traditional fault tree in the qualitative analysis. The difference from the traditional fault tree reliability analysis lies in the quantitative analysis part. When the dynamic fault tree is quantitatively analyzed, the matrix equation is often used to analyze the Markov model is used for processing, and the failure parameters of the dynamic subtree are obtained, and the dynamic fault tree is simplified to the traditional fault tree for analysis. This section will introduce the quantitative solution method of dynamic subtree on the above-mentioned dynamic logic gate.

3.1. Quantitative analysis of priority AND gate (considering repairability)

Analyze the Markov model of the priority AND gate, and get the transition probability matrix as follows:
Define the steady-state probability of each state in the priority AND gate (that is, the probability of being in that state in normal operation) as $\pi_{00}, \pi_{01}, \pi_{10}, \pi_{11}$, then the stable probability and probability transition matrix of each state should have the following equations to hold \[3\].

\[
\begin{pmatrix}
\pi_{00} & \pi_{10} & \pi_{01} & \pi_{11}
\end{pmatrix}
\begin{pmatrix}
A_1
\end{pmatrix}
\begin{pmatrix}
\pi_{00} \\
\pi_{10} \\
\pi_{01} \\
\pi_{11}
\end{pmatrix}
\begin{pmatrix}
\pi_{00} \\
\pi_{10} \\
\pi_{01} \\
\pi_{11}
\end{pmatrix} = \begin{pmatrix}
\pi_{00} + \pi_{10} + \pi_{01} + \pi_{11} = 1
\end{pmatrix}
\]

(2)

Expand the matrix equation to get:

\[
\begin{align*}
\pi_{10} \mu_A + \pi_{01} \mu_B - \pi_{00} (\lambda_A + \lambda_B) &= 0 \\
\pi_{00} \lambda_A + \pi_{11} \mu_B - \pi_{10} (\mu_A + \lambda_B) &= 0 \\
\pi_{00} \mu_B + \pi_{11} \mu_A - \pi_{01} \mu_B &= 0 \\
\pi_{10} \lambda_B - \pi_{11} (\mu_A + \mu_B) &= 0 \\
\pi_{00} + \pi_{10} + \pi_{01} + \pi_{11} &= 1
\end{align*}
\]

(3)

Solving this equation can get:

\[
\pi_{11} = \frac{\lambda_A \lambda_B \mu_B}{\mu_A^2 \mu_B + \mu_A \lambda_B \mu_B + \mu_B \lambda_A \mu_B + \mu_A^2 \lambda_B + \mu_B^2 \lambda_A + \mu_A \lambda_B^2 + \mu_B \lambda_A^2 + \lambda_A \lambda_B + \lambda_A \lambda_B \mu_B}
\]

(4)

Through the quantitative analysis of the priority AND gate, the probability solution formula of the top event in the dynamic subtree containing the priority AND gate is obtained. This formula can be used to solve the dynamic subtree containing the priority AND gate in the later fault tree analysis of the specific dynamic system. Regard the entire dynamic subtree as an event to participate in the quantitative analysis of the fault tree, so as to solve the problem that the dynamic fault tree is difficult to quantitatively analyze, and minimize the impact on the final result of the quantitative analysis.

3.2. Quantitative analysis of spare parts door

The warm spare parts door in the spare parts door is basically the same as the quantitative analysis process of the priority door considering repairability, and its top event probability can be calculated using formula (4).

Considering the calculation of the probability of the top event of the cold spare parts door, the probability transition matrix is calculated according to its Markov transition diagram as follows:

\[
A_2 = \begin{pmatrix}
1 - \lambda_B & \lambda_B & 0 & 0 \\
\mu_B & 1 - \lambda_C - \mu_B & 0 & \lambda_C \\
\mu_C & 0 & 1 - \mu_C & 0 \\
0 & \mu_C & \mu_B & 1 - \mu_B - \mu_C
\end{pmatrix}
\]

(5)

Define the steady-state probability of each state of the cold spare parts door as $\pi_{00}, \pi_{01}, \pi_{10}, \pi_{11}$, and the following equations can also be established:

\[
\begin{pmatrix}
\pi_{00} \\
\pi_{10} \\
\pi_{01} \\
\pi_{11}
\end{pmatrix}
\begin{pmatrix}
A_2
\end{pmatrix}
\begin{pmatrix}
\pi_{00} \\
\pi_{10} \\
\pi_{01} \\
\pi_{11}
\end{pmatrix} = \begin{pmatrix}
\pi_{00} + \pi_{10} + \pi_{01} + \pi_{11} = 1
\end{pmatrix}
\]

(6)

Expand the matrix equation to get the following equations:
\[ \begin{align*}
\pi_{10}\mu_B + \pi_{01}\mu_C - \pi_{00}\lambda_B &= \pi_{00} \\
\pi_{00}\lambda_B + \pi_{11}\mu_C - \pi_{10}(\mu_B + \lambda_C) &= \pi_{10} \\
\pi_{11}\mu_B - \pi_{01}\mu_C &= \pi_{01} \\
\pi_{10}\lambda_C - \pi_{11}(\mu_C + \mu_B) &= \pi_{11} \\
\pi_{00} + \pi_{01} + \pi_{10} + \pi_{11} &= 1
\end{align*} \] (7)

Solving this equation can get:
\[ \pi_{11} = \frac{\lambda_B\lambda_C\mu_C}{\mu_B^2\mu_C + \mu_B\mu_C^2 + \mu_B\mu_C\lambda_B + \mu_A\mu_B\lambda_C + \mu_C^2\lambda_B + \mu_C\lambda_B\lambda_C + \mu_B\lambda_B\lambda_C} \] (8)

3.3. Quantitative analysis of dynamic fault tree

In the quantitative analysis of the dynamic fault tree, the dynamic subtree of the dynamic fault tree including priority AND gates and spare parts gates can be regarded as a virtual event based on the calculation results in Section 2.1 and 2.2 above. Substituting formulas (4) and (8) into the calculation of the top event probability of the dynamic subtree and regarded it as the occurrence probability of the virtual event, so that the quantitative analysis of the dynamic fault tree is transformed into the quantitative analysis of the traditional fault tree.

4. Application examples

In the reactor instrument and control system, the failure of the emergency shutdown function of the safety-level system is an extremely important part. Among the reasons for the failure of the emergency shutdown function, the failure of the setter processing logic subsystem is the key part. This article takes Westinghouse’s IPS system as the analysis object. This system is mainly used as the instrument control system of the AP600 reactor, and is also basically used as the instrument control system of the AP1000 reactor [4].

A dynamic fault tree is established with the failure of the setter processing logic subsystem as the top event. Through the analysis of the structure diagram, it can be known that the system includes input and output modules, communication modules and processor modules. Failure of any part will lead to system failure.

The processor module contains a main CPU and a spare CPU element, which runs in the form of hot spare parts, and establishes a dynamic fault tree for the failure of the setter processing logic subsystem as shown in Figure 7.

![Fault Tree of Setter Logic Processing Subsystem](image-url)
For this dynamic fault tree, the method described in section 2 can be used to list the fault subtrees of the part of the dynamic fault tree that contains dynamic logic gates (that is, the part where the processor module fails) separately, and the result of two fault trees is shown in Figure 8.

Figure 8. Main fault tree and dynamic subtree

For the above dynamic fault subtree, since the dynamic logic gates contained in it are hot spare parts gates, the probability of failure of the top event processor module can be obtained by formula (4). In the IPS system, the processor model is 8086 produced by Intel Corporation [5], found its failure rate $\lambda_A = 9.5984 \times 10^{-6}/h$ [6], and its repair rate is set as a constant according to the literature $\mu_A = \mu_B = 0.042/h$ [3]. Substituting equation (4) to obtain the probability of the top event, that is, the failure probability of the processor module is

$$
\pi_{11} = \frac{\lambda_A \lambda_B \mu_B}{(\mu_A^2 \mu_B + \mu_A \mu_B^2 + 2 \mu_A \mu_B \lambda_B + \mu_A \mu_B \lambda_A + \mu_B^2 \lambda_A + \mu_A^2 \lambda_B + \mu_A \lambda_B \lambda_A + \mu_A \lambda_B \lambda_B + \mu_A \lambda_B \mu_B)} = 2.5888 \times 10^{-8} \quad (9)
$$

The failure of the processor module can be used as the basic event in the processed main fault tree, and its failure rate is $\lambda = 2.5888 \times 10^{-8}$, thus converting the calculation of the dynamic fault tree into the calculation of the traditional fault tree.

5. Conclusion
This paper analyzes the dynamic subtrees of the dynamic fault tree separately, and obtains the quantitative analysis method of each dynamic subtree, which helps to improve the credibility of the dynamic system failure analysis.

It should be noted that this article only proposes a feasible method for the quantitative analysis of dynamic fault trees, and at the same time gives a solution formula for quantitative analysis of partial dynamic subtrees. In practical applications, appropriate quantitative analysis methods should be selected based on the actual situation to improve accuracy and reduce the amount of calculation. In the follow-up, it is necessary to calculate the quantitative analysis formulas for different situations of sequence-related doors and summarize their laws. At the same time, consider combining the quantitative analysis method with risk spectrum software to develop a dynamic fault tree analysis program.

References
[1] Yang Jun. Research on reliability analysis methods used in nuclear power plant risk monitoring[D]. Harbin: Harbin Engineering University, 2016.
[2] Chen Peifeng. Research on Dynamic Probabilistic Safety Evaluation Method of Nuclear Power Plant Digital I&C System[D]. Xiamen: Xiamen University, 2014.
[3] Wang Yuchai, Shao Libing, Li Chao, et al. Reliability analysis of fully digital protection system considering dynamic fault characteristics[J]. Electrical Application, 2019, 38(10): 51-59.
[4] Joseph. G. Fougere. Instrumentation and Control System Updatings at Connecticut Yankee. IEEE
Nuclear Science Symposium & Medical Imaging Conference. 1993:1007-1011P

[5] Zhou Haixiang. Research on the structure and reliability of nuclear power plant digital reactor protection system[D]. Harbin Engineering University, 2007.

[6] S.K. KHOBARE, SK. SHRIKHANDE SV, CHANDRA U, et al. Reliability analysis of microcomputer circuit modules and computer based control systems important to safety of nuclear power plants[J]. Reliability Engineering and System Safety, 1998, 59(2): 253-258.