Four Methods for Calculating the Failure Frequency of Digital Systems with Redundancies in Nuclear Power Plants

Man Cheol Kim, Seung-Cheol Jang
Integrated Safety Assessment Division, Korea Atomic Energy Research Institute,
150 Deokjin-dong, Yuseong-gu, Daejeon, 305-353, Korea, charleskim@kaeri.re.kr

1. Introduction

Redundancies have been widely used to increase the reliability of digital systems. An example can be found in the digital control systems (DCSs) in the CANDU-6 nuclear power plants (NPPs). In CANDU-6 NPPs, two DCSs, DCS-X and DCS-Y, receive the same plant data and generate the proper control signals for the plant. Usually, one DCS, say DCS-X, takes the role of a primary controller, i.e. the control signals of DCS-X are used to actually control the plant, and the other DCS, say DCS-Y, takes the role of a hot-standby, i.e. the control signals of DCS-Y are used when DCS-X is unable to provide proper control signals due to a system failure, maintenance of the system and so on. The failure of both DCSs will lead to a complete loss of the plant control signals, which could possibly become an initiating event for a serious accident. The purpose of this paper is to provide a summary of various methods for calculating the expected failure frequency of such digital systems with redundancies that can be used as input data for a probabilistic safety assessment (PSA).

2. Failure Frequency of an Example System

2.1 Four Methods for Calculating System Failure Frequency

From the literature survey, we identify four methods for calculating a system failure frequency. The four methods are summarized in Figure 1.

The method (1) in Figure 1 shows the use of rare-event approximation in calculating a system failure frequency. By using spreadsheet software such as Microsoft Excel^{TM}, the method (1) in Figure 1 can be implemented easily. Even though the method (1) is easy to implement, it only provides an approximation for the system failure frequency.

To calculate the correct system failure frequency, we have to make use of one of the three method, namely methods (2)-(4). The method (2) requires the development of the software modules for Abraham [1] and Shi [2], and the method (3) requires the development of the software modules for KDH88 [3] and Amari [4]. The method (4) requires two software modules, one for the Shannon decomposition and the other for BDDs.

2.2 An Example System

Instead of lengthy explanation, we demonstrate the use of the methods (1)-(3) with an example system. The selected example is the fault tree in Ref.[5]. The example fault tree is shown in Figure 2. In Ref.[5], it is mentioned that the example fault tree admits 12 minimal cut sets (MCSs) of order 2, 0 of order 3 and 21 of order 4. The system failure frequency in the steady-state condition is provided as 2.32×10^{-4} hr^{-1}, and the mean-

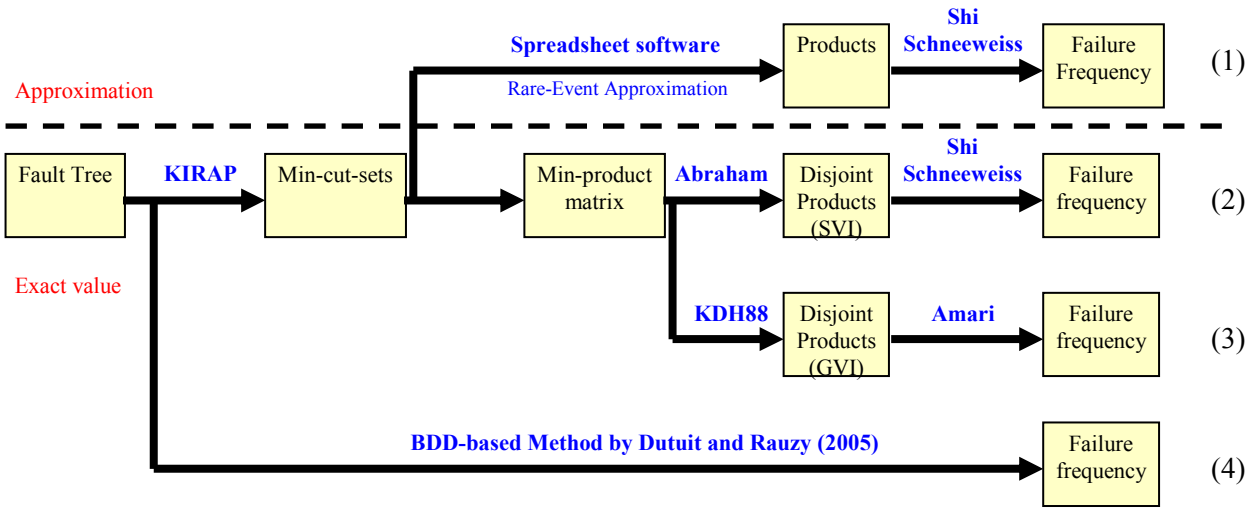

Figure 1 Four procedures for calculating system failure frequency from a fault tree

up-time (MUT), which is the inverse of a system failure frequency in the steady-state condition, is provided as 4312 hours.

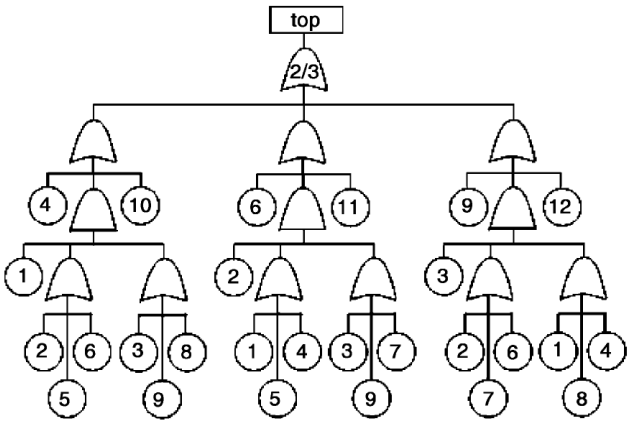

Figure 2 The example fault tree from Ref.[5]

2.3 Calculation Results of Method (1)

To apply the method (1), we first need the minimal cutsets (MCSs) for the example fault tree. The MCSs of the fault tree were generated using KIRAP (KAERI Integrated Reliability Analysis Package) [6]. From the generated MCSs, it could be confirmed that the example fault tree admits 12 minimal cut sets of order 2, 0 of order 3 and 21 of order 4, as mentioned in Ref.[5]. The system failure frequency in the steady-state condition calculated by using the method (1) was calculated to be 2.45×10^{-4} and the MUT was calculated to be 4096 hours. The unavailability of the system was calculated to be 1.02712×10^{-3}. Note that the unavailability and the failure frequency of a system calculated by using the method (1), which is an approximated value by using the rare-event approximation, are always higher than that calculated by using methods (2), (3), or (4), which is the exact value.

2.4 Calculation Results of Method (2)

To implement the method (2), we developed software modules for Abraham [1] and Shi [2] with Mathematica™. The software module for Abraham [1] produced disjoint products with 65 terms. The unavailability and the failure frequency of the system are calculated as 1.01009×10^{-3} and 2.38396×10^{-4}, respectively. One thing that should be noted is that the system failure frequency in the steady-state condition calculated by using the method (4) and that calculated by using the method (2) are different (2.32×10^{-4} v.s. 2.38396×10^{-4}), even though the two results should be the same.

2.5 Calculation Results of Method (3)

To implement the method (3), we developed software modules for KDH88 [3] and Amari [4] with Mathematica™. The software module for KDH88 [3] produced disjoint products with 58 terms. The unavailability and the failure frequency of the system are calculated as 1.01009×10^{-3} and 2.38363×10^{-4}, respectively. We expected that the system failure frequency in the steady-state condition calculated by using the method (3) is same with the system failure frequency in the steady-state condition calculated using the method (2), but it was found that the two results were different (2.38363×10^{-4} v.s. 2.38396×10^{-4}). It will be necessary to find out the cause of this difference between the two results.

3. Conclusions

In this paper, we show how to apply various methods for calculating the expected failure frequency of digital systems with redundancies. Four different methods for calculating the expected failure frequency of a system with redundancies were identified. We also identified necessary software modules for the four methods. Three of the four procedures are actually implemented by using commercial software such as Microsoft Excel™ and KIRAP, or by developing the necessary software modules. An application of the three methods to an example system showed that the three methods can be used to calculate the expected failure frequency of a system with redundancies.

It is concluded that the four methods summarized in this paper can produce mathematically proven solutions for calculating the expected failure frequency of digital control systems with redundancies while considering a somewhat complex dynamic behavior of a combination of the success and failure states of digital control systems.

REFERENCES

[1] J. A. Abraham, An improved algorithm for network reliability, IEEE Transactions on Reliability, Vol.R-28, p.58, 1979.

[2] D. Shi, General formula for calculating the steady-state frequency of system failure, IEEE Transactions on Reliability, Vol.R-30, p.444, 1981.

[3] K. D. Heidtmann, Smaller sums of disjoint products by subproduct inversion, IEEE Transactions on Reliability, Vol.38, p.305, 1989.

[4] S. V. Amari, Generic Rules to Evaluate System-Failure Frequency, IEEE Transactions on Reliability, Vol.49, p.85, 2000.

[5] Y. Dutuit and A. Rauzy, Approximate estimation of system reliability via fault trees, Reliability Engineering and System Safety, Vol.87, p.163, 2005.

[6] S. H. Han, T. W. Kim, K. S. Jeong, and K. J. Yoo, PC workstation-based level 1 PRA code package KIRAP, Reliability Engineering and System Safety, Vol.30, p.313, 1990.