Methodology for Evaluating the Software Reliability of Digital Instrumentation and Control Systems

Jeongil Seo and Seung Jun Lee
Ulsan National Institute of Science and Technology: 50 UNIST-gil, Ulju-gun, Ulsan, 44919, Republic of Korea
jeongil.seo@unist.ac.kr

1. Introduction

Recent nuclear power plants (NPPs) have been developed and operated by replacing old analog systems with digital systems. Especially, Republic of Korea is using the digitized Reactor Protection System (RPS) since Hanul units 5, 6 and Shingori units 3, 4. In order to secure the safety of the modern NPPs, the reliability of digital Instrumentation and Control (I&C) system must be analyzed. Its reliability should be analyzed using a method other than the reliability analysis method of the analog system, because this system has inherent characteristics; failure coverage, self-diagnosis and software reliability. Through this study, we propose a method to evaluate the software reliability of digital I&C system of NPP, which can contribute to confirm safety of digital system in other fields as well as NPP.

2. Methods and Results

In order to evaluate the safety of a nuclear power plant, it is necessary to examine the Probabilistic Safety Assessment (PSA) model of the system. In this process, we can see which part of the PSA model the digital I&C system affects. The risk of NPP, such as a Core Damage Frequency (CDF), occurs when an initial event occurs and an Mitigation System, the system consists of analog systems and digital I&C systems, fails. Among the various systems, digital I&C system's analysis of PSA model is important because it has inherent characteristics.

2.1 PSA Model of digital I&C system

According to PSA Model made by Korea Atomic Energy Research Institute (KAERI), fault tree of digital I&C can be expressed by following figure [1].

Since the digital I&C system has a self-diagnosis function, Failure Coverage as well as System Failure must be considered. For example, to make processor fail to generate trip signal, processor should fail to calculate trip condition and watch dog timer (WDT) should fail to reset processor. To make the WDT fails to perform its function, the WDT should fail and the WDT should not be able to detect the failure by self-diagnosis. The self-diagnosis occurs when all system failures occur, such as hardware failure, software failure, network failure, human error failure, and so on. To quantitatively evaluate the probability of a software failure, the reliability of the hardware-operating system-software integrated systems as well as the software logic must be evaluated.

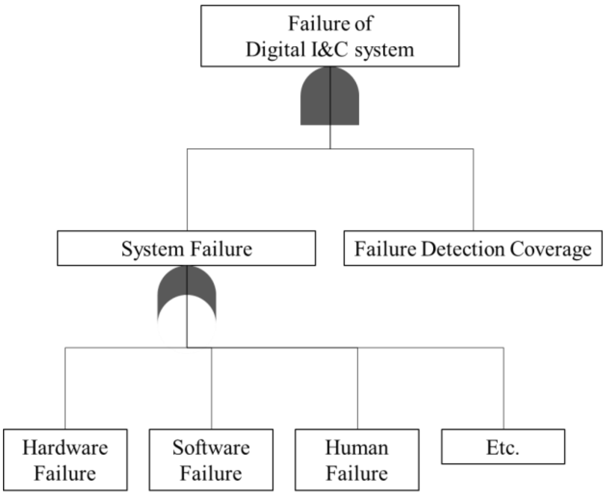

Fig. 1. Fault tree of digital I&C PSA model

2.2 Software reliability evaluation method of digital I&C system

There are two ways to evaluate software reliability like below figure and both are necessary. The first method is to make sure that when you input all possible combinations of inputs into the software, it produces a normal output. It is a good way to evaluate the software logic. The second method is to collectively check the function of the software as well as the related systems in a fully integrated form. To do this, we should set up a test environment that is as close as possible to the actual operating environment and consider scenarios based on probabilistic safety assessment. For example, if RPS can generate trip signal using pressurizer low pressure parameter during Loss Of Coolant Accident (LOCA), the integrated system is reliable. Especially it is necessary to perform integration tests in environments where hardware, operating system, and software are considered.

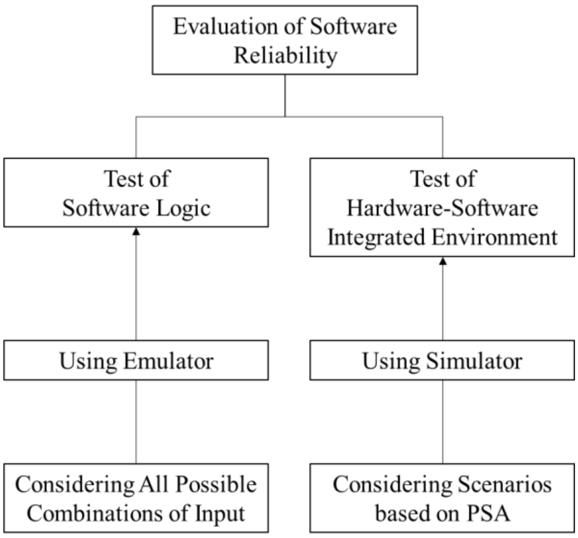
Evaluation of Software Reliability
Test of Software Logic
Test of Hardware-Software Integrated Environment
Using Emulator
Using Simulator
Considering All Possible Combinations of Input
Considering Scenarios based on PSA

Fig. 2. Concept of software reliability evaluation method of digital I&C system

3. Conclusions

Software reliability can be evaluated quantitatively by performing both of the following methods.

- Software Logic Test
- Hardware-Software Integration Test

Reliability of digital I&C system can be evaluated by evaluating system failure rate considering software reliability analysis, hardware reliability analysis, Human Reliability Analysis (HRA), and evaluation of failure detection coverage considering inherent characteristics of digital I&C. In this way, software reliability assessment methodology can secure the safety of digital systems and this methodology can be applied not only to NPPs but also to evaluate the safety of other industries with digital systems.

REFERENCES

[1] S. J. Lee, J. G. Choi, H. G. Kang, S.C. Jang, Reliability assessment method for NPP digital I&C systems considering the effect of automatic periodic tests, Annals of Nuclear Energy Vol. 37, 2010.
[2] T. Aldemir, D. W. Miller, M. P. Stovsky, J. Kirschenbaum, P.Bucci, A. W. Fentiman, and L. T. Mangan, NUREG/CR-6901 U.S. NRC, 2004.
[3] T. Aldemir, M. P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L. A. Mangan, D. W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, and S. A. Arndt, NUREG/CR-6942 U.S. NRC, 2004.
[4] T. Aldemir, S. Guarro, J. Kirschenbaum, D. Mandelli, L. A. Mangan, P. Bucci, M. Yau, B. Johnson, C. Elks, E. Ekici, M. P. Stovsky, D. W. Miller, X. Sun, S. A. Amdt, Q. Nguyen, and J. Dion, NUREG/CR-6985 U.S. NRC, 2004.
[5] T. L. Chu, M. Yue, G. Martinez-Guridi, K. Memick, and J. Lehner, and A. Kuritzky, NUREG/CR-6997 U.S. NRC, 2004.
[6] J. G. Choi, S. J. Lee, H. G. Kang, S. H., Y. J. Lee, and S. C. Jang, Fault Detection Coverage Quantification of Automatic Test Functions of Digital I&C System in NPPs, Nuclear Engineering and Technology VOL. 44, 2012.
[7] H. G. Kang, M. C. Kim, S. J. Lee, H. J. Lee, H. S. Eom, J. G. Choi, and S. C. Jang, An Overview of Risk Quantification Issues of Digitalized Nuclear Power Plants Using Static Fault Tree, Nuclear Engingeering Technology. Vol. 41, 2009.
[8] H. G. Kang and T. Sung, An Analysis of Safety-Critical Digital Systems for Risk-Informed Design, Reliability Engineering and System Safety, vol.78, 2002.
[9] S. J. Lee and W. D. Jung, Evaluation of Fault Detection Coverage of Digital I&C Systems, Korean Nuclear Society, 2013.
[10] S. J. Kim, P. H. Seong, J. S. Lee, M. C. Kim, H. G. Kang, and S. C. Jang, A Method for Evaluating Fault Coverage using Simulated Fault Injection for Digitalized Systems in Nuclear Power Plants, Reliability Engineering and System Safety, Vol. 91, 2006.