Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 18-19, 2017

Review of Technical Issues in Reliability Analysis of Digital Instrumentation and Control Systems in Nuclear Power Plants

Man Cheol Kim*, Seung Hoon Chae, Jae Sun Ha
School of Energy Systems Engineering, Chung-Ang University, 84 Heuksek-ro, Dongjak-gu, Seoul, Korea
**Corresponding author: charleskim@cau.ac.kr*

1. Introduction

The trend of nuclear I&C systems has been moving from conventional analog technology to advanced digital technology. This is mainly due to the recent rapid advances in digital technology and the problem of the obsolescence of analog components. Therefore, verification of the safety of digital technology is a global issue, and the absence of established methods for a reliability analysis of digital I&C systems in NPPs is regarded as a bottleneck for a risk-informed technical framework.

Even though various new safety issues are continuously arising as digital technology is introduced to NPPs, several issues are considered to be more important in the viewpoint of reliability analysis of digital I&C systems in NPPs. Some of such issues are (1) software reliability, (2) fault coverage, and (3) human reliability in advanced digital-based main control rooms (MCRs).[1] Even though many sophisticated modeling methods such as dynamic reliability analysis methods are proposed and investigated, it seems that research activities in reliability analysis of digital I&C systems in NPPs are mainly based on conventional static fault tree analysis, so that the modeling can be compatible with the conventional modeling framework of probabilistic safety assessment (PSA).

2. Software Reliability

One of the most controversial factors in a digital I&C PSA is the software reliability, which is defined as the probability of failure-free software operation for a specified period of time in a specified environment. Because the same software is used in redundant channels, software failures may affect multiple redundant channels. For this reason, software failure is modeled as a common cause failure (CCF) in digital I&C PSA.

It is generally known that software reliability growth models (SRGMs) cannot be applied to safety-critical software such as those used in digital I&C systems in NPPs. This is mainly because of the lack of software failure data in such highly reliable systems. By applying the two most widely known SRGMs, Kim et al.[2] found that there are possibilities that SRGMs may be applied to highly reliable safety-critical software, but limitations of SGRMs need to be carefully considered. Some of the identified limitations are the high sensitivity of the software reliability to the software failure data and the lack of sufficient failure data.

Kang et al.[3] proposed the input-profile-based software failure probability quantification. The main idea behind the proposed method is the consideration of discrete nature of digital systems and the calculated limits in variations of plant parameters due to being physical quantities in the real world. It was found that a finite number of test cases can be sufficient to demonstrate the high reliability of the safety-critical software.

Kim [4] identified two different viewpoints for software failures during the operation of a digital I&C system or a statistical software test. In one viewpoint, software failures are viewed with respect to system operation. In the other viewpoint, the software failures are viewed with respect to the system input. The mathematical relation between the failure probability density functions corresponding to the two viewpoints are derived and identified.

3. Fault Coverage

Fault coverage is defined as the probability that a system properly processes an occurring fault in the system. One of the important advantages of digital I&C systems is self-diagnosis features, by which the digital I&C systems continuously monitors the integrity of itself. The importance of fault coverage can be found by the fact that fault coverage is the measure for the effectiveness of self-diagnosis features for detecting and properly processing various component failures.

For the purpose of estimating the fault coverage of digital I&C systems, an experimental approach based on fault injection experiments is considered as most promising. In such fault injection experiments, a fault is intentionally inserted into a digital I&C system, and whether the inserted fault is properly detected or not is observed. After repeating such experiments for a lot of times, the experimental results are statistically analyzed to obtain an estimate of the fault coverage of a digital I&C system.

For the purpose of systemically performing faults injection experiments, Kim and Lee [5] identified important factors in fault injection experiments that affect the fault coverage of digital I&C systems. Those important factors consist of four system-related factors and four fault-related factors. The identified important factors are expected to provide a framework for systemically analyzing the results of different fault injection experiments in estimating the fault coverage of digital I&C systems.

Recently, attention is also given to more detailed information on the process of executing binary codes under the existence of injected faults. Kim [6] argued that it is important to clearly identify when, where, and how a fault injected into a digital I&C system affects the execution of the binary codes and results in discrepancies compared to the case of fault-free execution.

4. Human Reliability in Digitalized MCR

The introduction of digital technology to MCRs may have both positive and negative effects on the performance of human operators. Positive effects include crew performance enhancement, workload reduction, changes in crew structure and communication. Negative effects include new types of human errors, reduction of primary task performance, failure to recognize important information under high workload.

Lee et al.[7] indicated that the introduction of computerized displays and soft controls in digitalized MCRs may cause new types of human errors, and classified the human errors in soft controls into six types, (1) operation omission, (2) wrong object, (3) wrong operation, (4) mode confusion, (5) inadequate operation, and (6) delayed operation. From the results of soft control task analysis, Jang et al.[8] further divided operation omission into operation selection omission and operation execution omission, and wrong object into wrong screen selection and wrong device selection. As a result, it is proposed that soft control human errors are classified into eight types. For the purpose of assessing human reliability of advanced MCRs with computer-based procedures, soft controls and more effective error recovery features, HuRECA method [9] was proposed by reflecting newly identified design-related influencing factors (DIFs) into the K-HRA framework as performance shaping factors (PSFs).

For the purpose of human factors validation in a digitalized MCR, Ha et al.[10] selected main and complementary measures for six factors considered to be important in human performance evaluation, which are (1) plant performance, (2) personnel task performance, (3) situation awareness, (4) workload, (5) teamwork, (6) anthropometric-physiological factors.

One of the best ways to validate human performance in digitalized MCRs is to collect operator performance data in full-scope simulators. In Korea, experience in collecting and analyzing operator performance data in full-scope simulators have been accumulated, and various research results have been produced based on this experience. Continued efforts need to be provided to the collection of operator performance data in APR-1400 full-scope simulators. Also, human performance in digitalized MCRs needs to be further investigated based on basic researches on human performance measures and correlations among them.

5. Conclusions

This paper provides an overview of the recent research activities on the reliability analysis of digital I&C systems. The research activities include the development of a new safety-critical software reliability analysis method, a fault coverage estimation method based on fault injection experiments, and human reliability and human performance in digitalized MCRs based on operator performance data from full-scope simulators. The complexities of digital I&C systems are very high and our effort to understand such complexities need to be continued.

REFERENCES

[1] H. G. Kang, M. C. Kim, S. J. Lee, H. J, Lee, H. S. Eom, J. G. Choi, S-C, Jang, An Overview of Risk Quantification Issues for Digitalized Nuclear Power Plants using a Static Fault Tree, Nuclear Engineering Technology, vol.41, p. 849, 2009.

[2] M. C. Kim, S-C Jang, J. Ha, Possibilities and Limitations of Applying Software Reliability Growth Models to Safety Critical Software, Nuclear Engineering and Technology, vol.39, p.145, 2007.

[3] H. G. Kang, H, G. Lim, H. J. Lee, M. C. Kim, S-C Jang, Input-Profile-Based Software Failure Probability Quantification for Safety Signal Generation Systems, Reliability Engineering and System Safety, vol.94, p.1542, 2009.

[4] M. C. Kim, Two Viewpoints for Software Failures and Their Relation in Probabilistic Safety Assessment of Digital Instrumentation and Control Systems, Journal of Nuclear Science and Technology, vol.52, p.472, 2015.

[5] M. C. Kim, S. J. Lee, Important Factors Affecting Fault Detection Coverage in Probabilistic Safety Assessment of Digital Instrumentation and Control Systems, Journal of Nuclear Science and Technology, Vol.51, p.809, 2014.

[6] M. C. Kim, Analysis on the Effect of Injected Faults to the Functioning of a Digital System, Transactions of the Korean Nuclear Society 2016 Autumn Meeting, Oct.27-28, 2016, Gyeongju, Korea.

[7] S. J. Lee, J. Kim, S-C Jang, Human Error Mode Identification for NPP Main Control Room Operations Using Soft Controls, Journal of Nuclear Science and Technology, vol.48, p.902, 2011.

[8] I. Jang, A. R. Kim, W. Jung, P. H. Seong, A Framework of Human Reliability Analysis Method Considering Soft Control in Digital Main Control Rooms, Proceedings of the Human Interface and the Management of Information (HIMI 2014), June 22-27, 2014, Heraklion, Greece.

[9] J. Kim, S. J. Lee, S. C. Jang, HuRECA: Human Reliability Evaluator for Computer-based Control Room Actions, Transactions of the Korean Nuclear Society 2011 Autumn Meeting, Oct.27-28, 2011, Gyeongju, Korea.

[10] J. S. Ha, P. H. Seong, M. S. Lee, J. H. Hong, Development of Human Performance Measures for Human Factors Validation in the Advanced MCR of APR-1400, IEEE Transactions on Nuclear Science, vol.54, p.2687, 2007.