Optimization of Test Cases for Experimental Reliability Evaluation of Digital Reactor Protection System

Jeongil Seo[a]* and Seung Jun Lee[a]

[a] Ulsan National Institute of Science and Technology (UNIST), Ulsan, Republic of Korea

Abstract: Software reliability to evaluate the safety of digital I&C systems was assumed as extremely low or zero. The probability of Software Failure can be evaluated by two specific tests. This work is a part of the project to quantitatively evaluate the software reliability of digital RPS; Software Logic Exhaustive Test and Hardware-Software Integrated Test. This research offers experimental importance during the reliability evaluation to obtain approximate reliability with limited test cases. On the other word, test cases with low importance, which means that the test cases occur rarely, can be screened out according to the results of this research.

Keywords: Optimization of Test Case, Hardware Software Integrated Environment, FMEA, PRA, Software Reliability

1. INTRODUCTION

It is necessary to understand digital systems and evaluate the reliability of software because of the recent trend of digitalization of instrumentation and control (I & C) systems in a nuclear power plants. Especially in case of Republic of Korea, digital Reactor Protection System (RPS) has been used since Hanul units 5, 6 and Shingori units 3, 4; however, there is no exact way to evaluate the reliability of highly reliable software, which is integrated with related hardware and operating system (OS) like RPS. Until now, RPS software reliability was assumed as extremely low or zero; for example, IEC61226 categorized the probability of a dangerous failure on demand of the safety function into four Safety Integrity Level (SIL) and assume that RPS software failure probability per demand as SIL 4, which means that the probability is between 10E-4 to 10E-5.

The reliability of software affects not only the reliability of the digital I & C system but also the risks of nuclear power plants, so quantitative evaluation is needed. However, conducting an exhaustive test of software logic and hardware-software integrated systems to evaluate this software reliability requires a lot of money and time. This research suggests that when performing a hardware-software integrated test, there is no need to perform test cases with a certain level of importance or less. The certain level can be proposed through Failure Modes and Effects Analysis (FMEA) of the software-related hardware.

2. BACKGROUNDS

Optimization of the test case is needed to evaluate software reliability that affects the safety of a nuclear power plant. In order to evaluate the safety of nuclear reactors, the Probabilistic Risk Assessment (PRA) model of the system should be reviewed as shown below, and Level 1 PRA is used to quantify the Core Damage Frequency (CDF). This CDF can be expressed as the probability that Mitigation System will fail when Initiating Event occurs. The Mitigation System is composed of various system such as Digital I & C system. Especially Failure of Digital I & C occurs when the system fails, and Failure Detection fails due to the failure of the self-diagnosis function. Because the system fails because of hardware, software, network, human failures, and so on, quantification of each failure rate is important.

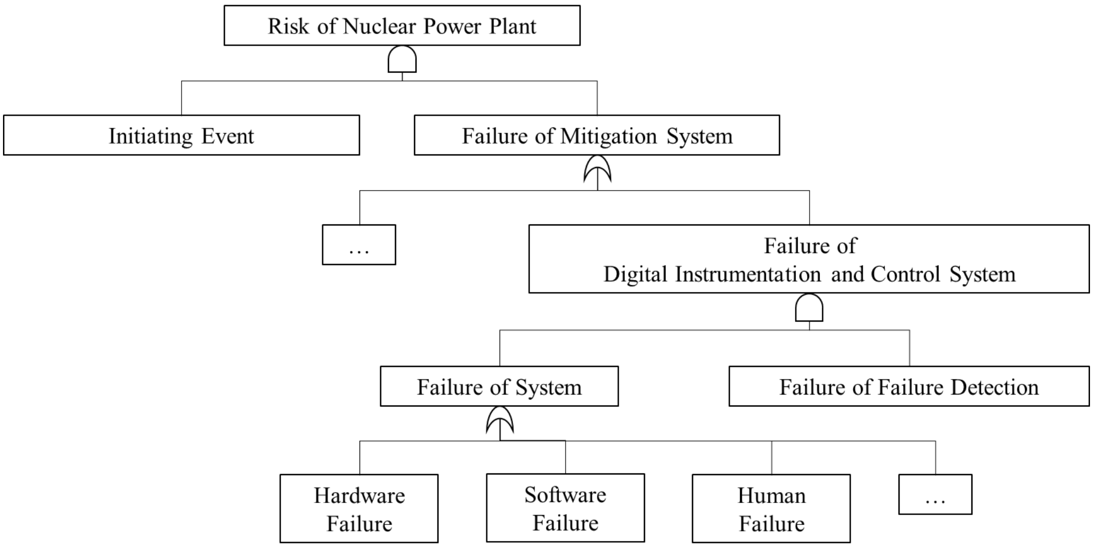
Risk of Nuclear Power Plant
Initiating Event
Failure of Mitigation System
…
Failure of
Digital Instrumentation and Control System
Failure of System
Failure of Failure Detection
Hardware
Failure
Software
Failure
Human
Failure
…

Fig 1. PRA Model of Digital I & C System

The probability of Software Failure can be evaluated by two specific tests. This work is a part of the project to quantitatively evaluate the software reliability of digital RPS. The first part is to evaluate the reliability of applications through exhausted testing using emulator, and the second part is to evaluate the entire software reliability including OS using integrated hardware-software testing environment. The second part considers hardware-software combined tests to represent that the software works reliably under certain environment. The completeness of applications is proved in the first part and the second part proves that complete application logic performs its functions perfectly even in situations where it is installed on the hardware and OS as in real operating situations. Both two experimental methods are necessary for software evaluation and this research is focused on the second part.

While the emulator can examine whole test cases of software logic, the experimental approach cannot handle all of them. Because the testing environment in this work uses actual hardware, there is a limit to shortening the test execution time. For example, there are 25 signal sets for Coincidence Processor (CP), which is one of important hardware components of RPS and the number of test cases considering combination of the signal sets is more than fifty million. To carry out the experiment realistically, we can screen out some test cases with a certain criterion. This research offers experimental importance during the reliability evaluation of digital RPS to obtain approximate reliability with limited test cases. If appropriate criteria can be proposed, this approximate reliability will have a value very similar to the result from the whole test cases.

3. METHODS AND RESULTS

3.1. Methods to Quantify Software Reliability

In order to quantify Software Reliability, a series of processes should be performed as shown below. First, Software Characteristic Analysis is required. In case of Software Logic Exhaustive Test, it is possible to know which variables should be considered according to the characteristics of software and the domain of each variable. The results of the Exhaustive Test' can be obtained by performing test cases considering all the domains of all variables. Hardware-Software Integrated Test should consider the characteristics of the software and its hardware collectively to check the safety of fully integrated system. To this end, a test environment that is as close to the actual operating environment as possible should be set up and scenarios based on PRA should be considered.

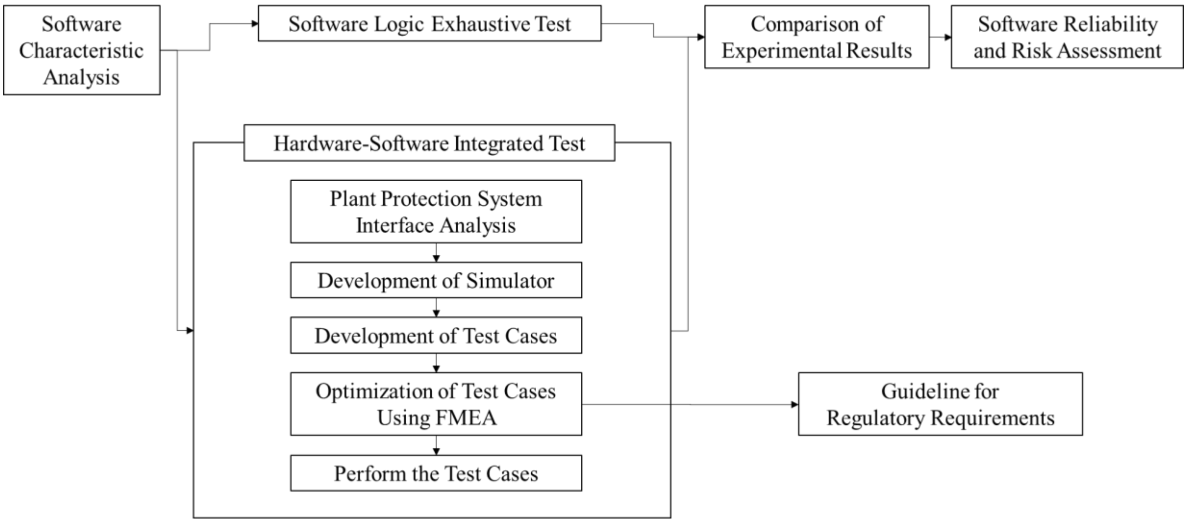
Software Characteristic Analysis
Software Logic Exhaustive Test
Comparison of Experimental Results
Software Reliability and Risk Assessment
Hardware-Software Integrated Test
Plant Protection System Interface Analysis
Development of Simulator
Development of Test Cases
Optimization of Test Cases Using FMEA
Perform the Test Cases
Guideline for Regulatory Requirements

Fig 2. Flow Chart to Quantify Software Reliability

In order to construct environment for performing Hardware-Software Integrated Test, Simulator considering Plant Protection System Interface should be developed. Since it is not possible to simulate 100% of the hardware used in actual nuclear power plants for software reliability evaluation, some signals should be simulated using the simulator. Although it uses virtual signal, it takes too much time to test all the domains of all software variables because it uses real hardware. This research proposes a criterion for optimizing test cases using FMEA data from Korea Nuclear Instrumentation and Control Systems (KNICS).

3.2. Method to Suggest the Criterion

KNICS is a system, developed in 2008 to provide requirements for the development of NPP I & C System based on Korean equipment, including RPS, ESF-CCS, and so on. Since BP and CP, which are the main parts of RPS, are based on what they actually use for Korean NPP, APR 1400, the Criterion using this FMEA data is reasonable. The RPS in KNICS is composed of four independent channels, each with one independent cabinet. One channel consists of two BP and two CP as shown below. Because the other RPSs are made up of similar systems, these results can be referenced in various other NPPs.

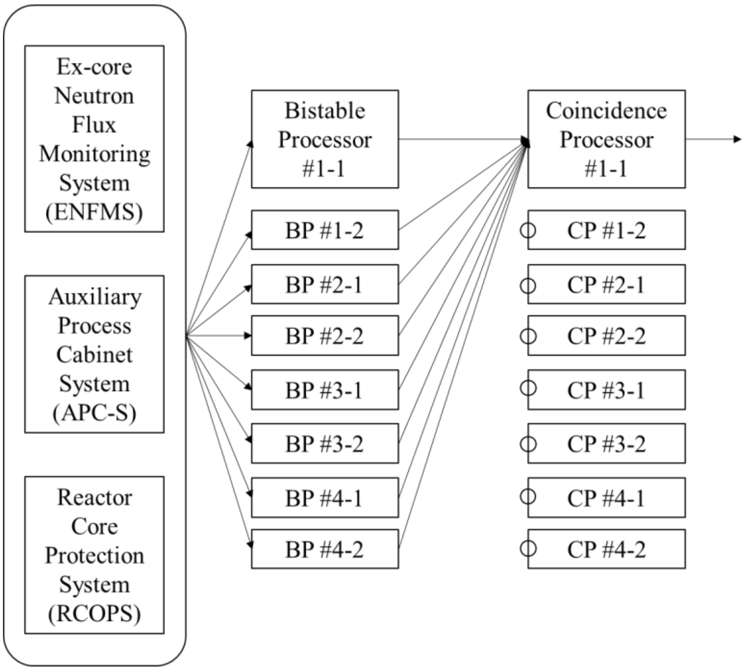
Ex-core Neutron Flux Monitoring System (ENFMS)
Auxiliary Process Cabinet System (APC-S)
Reactor Core Protection System (RCOPS)
Bistable Processor #1-1
BP #1-2
BP #2-1
BP #2-2
BP #3-1
BP #3-2
BP #4-1
BP #4-2
Coincidence Processor #1-1
CP #1-2
CP #2-1
CP #2-2
CP #3-1
CP #3-2
CP #4-1
CP #4-2

Fig 3. Simplified RPS Design of KNICS

Test cases related to hardware with the higher failure rate than the criterion should be performed first through FMEA of the hardware. Test cases that are of lesser importance than the certain level does not need to be tested, because the test cases with lower importance occur rarely. For example, the criterion could be 0.1% of the RPS hardware failure rate. It means that, if the sum of the failure rates of the hardware components involved in one test case is less than 0.1% of the RPS hardware failure rate, the test case is negligible. Because hardware component with high failure rate emits wrong signal more frequently, test case including the hardware component should have high importance. On the other word, test cases with low importance can be screened out because the test cases occur rarely. As for test cases with same importance because of redundant system; for instance, test case of bypassing channel A and test case of bypassing channel B; the results of related cases can be predicted by testing only one case.

3.3. Details of Each RPS Module and FMEA

According to FMEA, the final impact of the various components that make up RPS varies. Among these effects, the part that has the final effect on the system function is analysed and used to present the importance criterion. The components of the RPS, which are largely classified into seven categories, have the following functions and effects.

- Power Module
- Communication Module
- Processor Module (PM)
- Analog Input Module
- Analog Output Module
- Digital Input Module
- Digital Output Module

The Power Module supplies DC 5V to all the control devices attached to the bus module. Up to two Power Modules can be installed, and even if one of the modules fails, redundancy is provided to ensure the normal operation of RPS. According to the FMEA results, the failure of the Power Module does not have a final and effective effect on the system.

Communication Module consists of bus module, Safety Data Network (SDN) Communication Module, Safety Data Link (SDL) Communication Module and SDL communication driver module. In the case of the bus module, the DC 5V output of the Power Module is supplied to all the control devices connected to the bus module, and a bus for transmitting control signals and data signals is provided between the PM and the Input / Output (I / O) module. In the event of a typical failure, the final effect is that all I / O modules, including the PM, are down due to a power outage. The SDN Communication Module transmits and receives data to and from the PM and the external device for SDN communication and transmits the status of the Communication Module to the PM and the user. In case of a typical failure, the final effect is an error in the data transmission function of the SDN communication and a stoppage of the Watchdog Timer.

The PM executes the application program using the input data and transmits / receives data between the I / O module and the Communication Module. The final impact in a typical failure is loss of monitoring capabilities of the PM and loss of device functionality.

The Analog Input Module converts analog signals such as pressure, flow rate, and temperature from the field devices into digital data that can be recognized by the PM. When a failure occurs, the related information is transmitted to the PM and the user. In the event of a typical failure, the final effect is a device outage caused by Power Module failure.

The Analog Output Module receives the output signal from the PM and outputs an analog signal. When a failure occurs, the Analog Output Module transfers the signal to the PM and the user. In the event of a typical failure, the final effect is that certain signals are stuck due to the failure of the associated component, such as a capacitor.

The Digital Input Module receives various inputs and transfers the values to the PM. When a failure occurs, the Digital Input Module delivers the value to the PM and the user. In the event of a typical failure, the final effect is a device outage caused by a power outage.

The Digital Output Module consists of a pulse counter module and a relay output module. The pulse counter module receives the number of revolutions, frequency, voltage, time, etc. from an external device and transfers the count value to the PM. If a failure occurs, it will be delivered to the PM and the user. The relay output module uses the electromagnet to receive the output signal from the PM and output the digital signal. In the event of a typical failure, the final effect is a loss of functionality due to a power outage.

3.4. Results and Analysis

The FMEA data for all components of the KNICS RPS is about 1,000 pages, of which there are about 2,000 effective fault modes that cause problems with the system's functionality. When the failure mode and the final Effects are classified according to the seven types of modules, each module has a certain ratio of effective failure rate as below table.

Table 1: Ratio of Effective Failure Rate Based on Module Types

Module Types	Ratio of Effective Failure Rate [%]
Power Module	0
Communication Module	0.46
PM	4.11
Analog Input Module	0.09
Analog Output Module	91.5
Digital Input Module	3.61
Digital Output Module (With Rough Assumption)	0.23

The Analog Output Module, which accounts for most of the failure rate (91.5%), eventually provides input to the PM. Digital Input Module with a high failure rate (3.61%) provides a digital input to the PM. All but the Digital Output Module (less than 1%) provide input to the PM.

If there is no problem in the PM and the Digital Output Module, the RPS will operate normally. In other words, problems can occur in the following two situations.

- When the PM fails
- When the Digital Output Module fails even though the PM operates normally

According to the number of PM, a formula can be defined as follows.

$$y = \frac{P(\text{Failure of n PM })\ OR\ \{P(Normal\ operation\ of\ PM)\ AND\ P(Failure\ of\ Digital\ Output\ Module)\}}{The\ total\ failure\ rate\ of\ all\ failure\ modes\ causing\ a\ valid\ final\ impact} \quad (1)$$

It is necessary to analyse the failure modes of the PM and the Digital Output Module in detail. Critical failure modes among various failure types of the PM should be selected. It is a case that there is no detection method among the failure modes in which data transmission / reception with external device is impossible. The percentage of critical failures among PM failure modes is 81.14%.

The Digital Output Module consists of three sub-modules, and they are diverse as below table. Failure rate of Digital Output Module considering its diversity among failure rate of Digital Output Module with rough assumption is 1.94%. It means that the failure rate of PM is dominant to suggest the criterion of test case optimization.

Table 2: Ratio of Effective Failure Rate of Digital Output Module Considering its Diversity

Module Types		Ratio of Effective Failure Rate [%]
Digital Output Module	Sub-module A	26.09
	Sub-module C	69.57
	Sub-module B	4.35

Results of the formula according to the number of PM is as follows.

Table 3: Results of Formula (1) according to n

n	y(n) [%]
1	3.3
2	0.1
3	0.004
…	…

4. CONCLUSION

According to the results of this study, the importance of the test cases with more than 2 PM failures is about 0.1% of the importance of the entire test cases. In other words, it is rare that more than two PMs fail, so this can be used as a criterion to optimize the test case. For example, assuming all PMs can fail, plenty of test cases need to be performed. In the case of using the criterion, only the case where one PM fails can be considered.

Through this research, the importance is given to the experiment so that it is possible to obtain the approximate value of the software reliability only by the specific experiments without experimenting in all test cases. It makes possible to practically evaluate that software works properly on hardware-OS-software combined system. Looking at the progress of this research project, identification of input signal set, test case generation, and Equipment modeling has been completed and test case optimization and equipment setting is in progress. The research will not only save time and resources needed to evaluate software reliability, but also be an important guideline for future regulatory requirements.

Acknowledgements

This work was financially supported by Human Resources Program in Energy Technology (No.20174030201430) of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), funded by the Ministry of Trade Industry and Energy (MOTIE), Republic of Korea.

References

[1] T. Aldemir, D. W. Miller, M. P. Stovsky, J. Kirschenbaum, P.Bucci, A. W. Fentiman, and L. T. Mangan, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments ", NUREG/CR-6901, (2004).
[2] 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, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments", NUREG/CR-6942, (2004).

[3] 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, "A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems", NUREG/CR-6985, (2004).

[4] T. L. Chu, M. Yue, G. Martinez-Guridi, K. Memick, and J. Lehner, and A. Kuritzky, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods", NUREG/CR-6997, (2004).

[5] J. H. Jo, S. J. LEE, and W. D. Jeong, "Fault Analysis of Reactor Protection System Based on FMEA", KAERI/TR-5655, (2014).

[6] C. G. Lee, I. S. Oh, D. H. Kim, J. H. Park, J. H. Shin, and Y. B. Kim, "Requirements for the Development of KNICS Control Systems", KAERI/TR-2737, (2004).

[7] P.V. Varde, J. G. Choi, D. Y. Lee, and J. B. Han, "Reliability Analysis of Protection System of Advanced Pressurized Water Reactor - APR 1400", KARTI/TR-2468, (2003).

[8] 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).

[9] 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.

[10] 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).