On the Software Reliability Modeling for Digital I&C PSA

Seung-Cheol Jang
Korea Atomic Energy Research Institute, Daedeok-Daero 989-111, Yuseong-Gu, Daejeon, 34057, Korea
Corresponding author: scjang@kaeri.re.kr

1. Introduction

According to the ISO/IEC standard[1], the software (SW) is defined as "all or part of the programs, procedures, rules and related documentation of an information processing system" and includes executable SW as well as related SW, firmware, documentation (e.g., requirements, design, user manuals, etc.) and data. Although SW reliability modeling in Probabilistic Safety Assessment(PSA) is an unresolved issue, there is a common consensus on the philosophical aspects of SW failures and the use of probabilistic models as follows[2]: 1) SW fails, 2) The occurrence of SW failures can be treated stochistically, 3) Using SW failure rates and probabilities is meaningful, and 4) SW failure rates and probabilities may be included in the reliability model of the digital system.

To quantify SW failure rate/failure probability, many approaches are presented, such as reliability growth model and rule-based method[3], Bayesian Belief Network(BBN) method([4],[5],[6]), test-based approach ([7],[8]), SW metric-based method[9], context-based SW risk model(CSRM) approach([10],[11]), and advantages and disadvantages of these methods are reviewed in various literature[12].

However, many SW reliability assessment methods presented in these academic literatures do not apply to the actual PSA of the nuclear industry for many reasons. Rather, it uses an engineering judgment approach and is classified as four categories, based on arguments and grounds - screenig-out, use of screening values, expert judgment and engineering judgment based on operational experience[13]. For example, in the PSA model, SW reliability is considered in a way that is difficult to justify, such as no occurrance of SW failure (by a groundless claim that contribution to SW failures is trivial or there is no practical way to assess SW probability of failure), using screening values based on SIL(Safe Integrity Level) levels, and giving 10% of hardware failures, and so on. Simply speaking, safety-critical SW reliability in the PSA model is judged to depend on engineering judgement that is still difficult to justify.

In this paper, authors discuss more rational modeling background, logic and method for the safety-required SW reliability in digital I&C PSA. In particular, the paper provides a Bayesian statistical formulation with a safety-critical SW reliability model of the digitalized nuclear power plant, and also illustrates a result of evaluation results by simple bounding approach.

2. Concern of SW Failure in the Viewpoint of PSA

2.1 Terminology and Mechanism of the SW Failure

First, it is very important to distinguish between SW faults and failures, together with the definitions associated with SW reliability assessment. In this paper, as defined in IAEA NP-T-1.5[14] and NP-T-3.27[15], SW failure is 'the result of the activation of a fault by a triggering event', and the triggering event is defined as 'a specific event or operating condition that causes structures, systems, or components (SSC) to fail due to a latent fault'. SW Fault is a 'defective state' of a system or SW that is caused by an error, simply speaking, the error is a cause of the fault. Examples of SW errors include mistakes (human errors) or defects (design errors), and the extent of SW errors that are the cause of the defects includes all processes and operating conditions during the SW life cycle. As shown in the figure below, SW failure is an event that a potential fault not detected so far is activated by a trigger condition or mechanism that occurs in randomness during the SW life. In short, it is worth noting the difference between a fault being a state and a failure being an event, which is the basis for stochastic handling of SW reliability with random occurrence of trigger conditions.

In addition, the ultimate concern for SW reliability in the PSA is to assess the probability of failure of the final target system due to SW failure, as shown in the figure below. In general, the effects of SW failures result in the final target system, propagating to internal, interconnected, or dependent systems. However, the safety requirement SW of nuclear power plants is implemented with various fail-safe design concepts, such as failure detection techniques, and may not result in the target system failure depending on the detection capacity of SW failures and the success of the fail-safe design in the failure event.

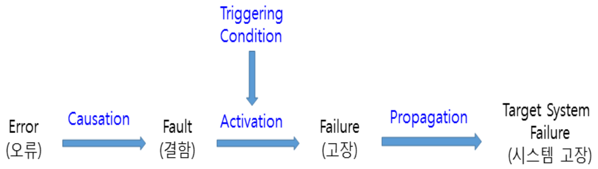

Fig. 1 Relationship among SW error, fault and failure [15]

2.2 Nature of the SW Failure

First, HW is subject to random failures due to manufacturing defects, ageing, wear or environmental effects. Because of these characteristics, failure data of HW components can be used in conjunction with an operational profile for assessing the reliability of a system consisting of several HW components.

SW, on the other hand, is not a consideration for aging, so if using perfect SW, it will operate indefinitely and accurately. SW failures are associated with errors (causes of potential faults) that are addressed in the SW development phase, and are highly systematic because replications of fault-triggering conditions (combination of inputs and software internal states) cause the same SW failure.

However, these fault triggering conditions occur often at random. This may be the case, for example, where a SW failure can be triggered by a random HW function degradation or failure. Also, IAEA NP-T-3.27 [15] states that a failure of SW may occur over time for several reasons:

① SW operates as required, but under certain conditions it does not work as expected due to misanalysis at the requirements definition stage.

② SW operates as required, but the operating environment may change due to improvements in plant equipment or operating procedures.

③ If the SW remains a potential design error that has been improperly designed and not detected by verification and verification (V&V), etc., performed prior to the operational service, these errors will cause SW failures throughout the operational life of the SW.

In most cases, SW cannot be perfectly demonstrated that due to its complexity, it is not affected by any of the above three mechanisms. Thus, there is uncertainty about possible residual faults in SW, which increases concerns about common cause failures (CCFs) in systems that use common or similar SW. However, SW-based systems cannot easily break down into components, and the interdependencies of SW components cannot be easily identified or modelled, so modeling SW reliability in a traditional PSA model approach is by no means a small matter.

3. A Formulation for Evaluating SW Reliability

This section proposes a Bayesian statistical model for evaluating practical nuclear SW reliability that can reflect the characteristics of safety-critical SW, with consideration of the technical limitations associated with the safety-critical SW reliability assessment as mentioned in the previous sections.

First, as shown in Fig. 2, the overall operating environment of SW is represented by Ω (which corresponds to the sample space), and it consists of a set of the mutually exclusive and collectively exhaustive(MECE) events (E_i, $i = 1,2,...,n$; $E_i \cap E_j = \varnothing$, $i \neq j$; $\Omega = \cup E_i$). Here, the E_i can be regarded as a triggering condition that can cause SW failures in the SW operating environment, and it can consist of, for example, not only normal operation, but also all abnormalities involving the failure or deterioration of the HW that makes up the digital system. In addition, θ_i is referred to as a set of SW failure events that operate in the E_i environment, they are also a set of MECE events, and then $\Theta = \cup \theta_i$, similarly.

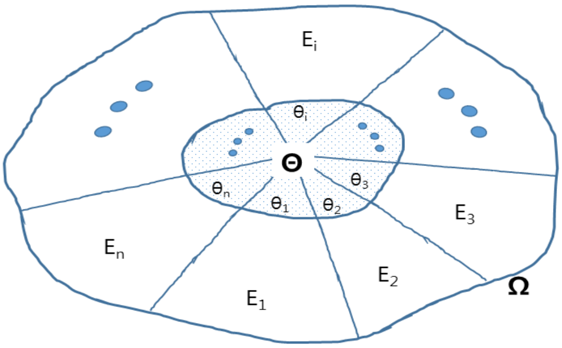

Fig. 2 Relationship between SW failure events and operation environments

Although information about the overall SW reliability (i.e., Θ) is often available, such as the screening values for SILs ([16],[17]), however, it is rarely directly available for SW reliability depending on all operating environments of each SW. Nevertheless, the PSA model requires the results of SW relability analses for all operating environments that can be encountered during the SW life cycle. Thus, the overall SW failure probability can be expressed in the following formula.

$$P(\Theta) = \sum_{i=1}^{n} P(\theta_i) = \sum_{i=1}^{n} P(\Theta \cap E_i) = \sum_{i=1}^{n} P(E_i) \cdot P(\Theta|E_i),$$

$$,\text{for } P(E_i) > 0 \qquad (1)$$

In general, it is difficult to verify SW integrity in abnormal conditions considering all HW-SW interactions (HSIs), even though integrity of the safety-critical SW may be guaranteed under normal operation conditions[8]. For example, simply assume that E_1 is normal and E_2 is abnormal (n=2). $P(\Theta|E_1)$ is close to zero (i.e., SW integrity is guaranteed)[8], based on many test-based fault injection experiments. $P(\Theta|E_2)$ is very different depending on the situation in E_2. E_2 may have a variety of abnormalities that can become trigger conditions of SW faults, and even though data for SW reliability assessment can be obtained using a fault injection experiments for E_2 situation, it is not easy to ensure if it is due to actual SW failure. For example, a problem in the memory area where SW scripts are stored will cause SW failures, but a failure in the memory area where operational data is stored is not technically a SW failure. In addition, the question of whether fault-injection experiments on E_2 can ensure the appropriate situation for the assessment of $P(\Theta|E_2)$ remains. $P(E_i)$ can be estimated as a time fraction for the digital system operating environment.

Furthermore, the ultimate concern of the PSA is the probability that the effects of SW failures will result in failure of the final target system, as shown in Fig 1. As mentioned earlier, only a small fraction of the SW failures result in failure of the final target system, due to the implementation of fail-safe design concepts and characteristics of the safety-critical SW. Thus, the failure probability of the final target system due to a safety-critical SW failure can be expressed in the following formula, taking into account the failure probability of the fail-safe design, $k(E_i)$.

$$P(TSF) = \sum_{i=1}^{n} k(E_i) \cdot P(E_i) \cdot P(\Theta|E_i) \qquad (2)$$

4. The Result of Bounding Analysis

To illustrate a simple bounding analysis of target system failure probability from Equation (2), i.e., P(TSF), assume the followings:

- ○ $P(\Theta|E_i)$ is assumed to be a screening value (1E-4) of the conservative SIL-4 level[17].
- ○ $P(E_i)$ is assumed to be the probability of failure of the processor module (4E-6)[18]
- ○ $k(E_i)$ assumes that the fault detection always fails conservatively without the use of engineering judgement for fault detection rate.

Then, the probability of the final target system failure by SW failure is evaluated as a small value not exceeding approximately 1E-9. Of course, $P(\Theta|E_i)$ may use the results of Bayesian update using the fault injection test data or experience data.

5. Conclusions

In this paper, more rational modeling background, logic and method for the safety-required SW reliability in the digital I&C PSA were discussed. In particular, the paper proposes a Bayesian statistical model for evaluating practical nuclear SW reliability that can reflect the characteristics of safety-critical SW, with consideration of the technical limitations associated with the safety-critical SW reliability assessment as well-known previously.

ACKNOWLEDGEMENTS

This work was supported by the Nuclear Research & Development Program of the National Research Foundation of Korea grant, funded by Korean government, Ministry of Science and ICT.

REFERENCES

[1] ISO/IEC, Information Technology: Vocabulary, Standard 2382:2015, ISO/IEC, 2015.

[2] T.-L. Chu, et. al., “Workshop on Philosophical Basis for Incorporating Software Failures in a Probabilistic Risk Assessment,” BNL-90571-2009-IR, Brookhaven National Laboratory, 2009.

[3] G. Dahll, et. al., “Software-Based System Reliability,” Technical Note, NEA/SEN/SIN/WGRISK (2007) 1, WGRISK of OECD/NEA, 2007.

[4] [A. Helminen, 2001] A. Helminen, “Reliability estimation of safety-critical software-based systems using Bayesian networks,” STUKYTO-TR 178, STUK, Helsinki, 2001..

[5] H.-S. Eom, G.-Y. Park, H.-G., Kag and S.-C. Jang, “Reliability Assessment Of A Safety-Critical Software By Using Generalized Bayesian Nets,” Proc. 6th NPIC&HMIT 2009, Knoxville, Tennessee, 2009.

[6] S.C. Jang, et. al., “Development of Integrated Assessment Technology for Risk and Performance, Part 2: Development of the Integrated Digital Risk Assessment Technology for Nuclear Power Plant”, KAERI/RR-3420/2011, KAERI, 2012.

[7] W.D. Jung, et. al., “Development of Site Risk Assessment & Management Technology Including Exterme External Event, Part 4: Development of Advanced Core Technology for Risk Assessment”, KAERI/RR-4225/2016, KAERI, 2017.

[8] KHNP “Evaluation of Human Error Probabilities in Digital Environment and the Reliability of Safety Critical Software(Final Report),” TR A11NJ10, KHNP, 2019

[9] C. Smidts and M. Li, “Preliminary Validation of a Methodology for Assessing Software Quality,” NUREG/CR-6848, U.S.NRC, 2004.

[10] S. Guarro, “Risk-Informed Safety Assurance and Probabilistic Assessment of Mission-Critical Software-Intensive Systems,” NASA Technical Paper AR 07-01; JSC-CN-19704, ASCA, Inc., 2007.

[11] W. Vesely, et. al., “Fault Tree Handbook with Aerospace Applications,” NASA, Washington D.C. 2002.

[12] T.L. Chu, M. Yue, G. Martinez-Guridi and J. Lehner, “Review of Quantitative Software Reliability Methods,” BNL-94047-2010, Brookhaven National Laboratory, 2010.

[13] S. Authen and J-E Holmberg, Reliability Analysis of Digital Systems in a Probabilistic Risk Analysis for Nuclear Power Plants, Nuclear Engineering and Technology, Vol.44, No.5, 2012.

[14] IAEA, “Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants,” IAEA Series No. NP-T-1.5, IAEA, 2009.

[15] IAEA, “Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants,” IAEA Series No. NP-T-3.27, IAEA, 2018.

[16] IEC, “Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions,” IEC61226, International Electrotechnical Commission, 2005.

[17] IEC, “Function Safety of Electrical/Electronic/ Programmable Safety-Related Systems, Part 1: General requirements,” IEC61508-1, International Electrotechnical Commission, 2010.

[18] S.C. Jang and J.W. Kim, “Development of Digital I&C System Unavailability Model for Risk-Informed Application” KAERI, KAERI/TR-7659/2019, 2019.