Development of a Methodology for Quantifying the Amount of Additional S/W V&V Processes: When Cyber Security Techniques are Applied to NPP I&C Systems

Chanyoung Lee, Poong Hyun Seong*

[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, Republic of Korea*
**phseong@kaist.ac.kr*

INTRODUCTION

Digital Instrumentation and Control (DI&C) systems have been developed and installed in Nuclear Power Plants (NPPs). This introduction of DI&C has brought up a new issue of cyber security. Actually, NPP DI&C systems are physically isolated from external networks, and thus NPPs are regarded as safe from external cyber-attack. Consequently, cyber security has received less attention than other safety problems have. However, continuous cyber-attack attempts against NPPs signify that NPPs are as susceptible to cyber-attack as other safety critical infrastructure, and so public perception of cyber security for NPPs has been changing [1].

To deal with the cyber security issues in the nuclear industry, several regulatory documents such as RG 5.71 and RS-015 were published. These documents include cyber security plans and comprehensive sets of security techniques. However, there are still difficulties when it comes to deciding which security techniques are needed and to defining appropriate requirements for security techniques [2]. Therefore, in order to provide useful information on the application of security techniques, efficient and quantitative methods for verifying security techniques are needed for the nuclear industry. In addition, considering the fact that safety is a top priority in the nuclear industry, methodology for verifying security techniques should go in the direction of maximizing the synergy between security and safety [3], so that both aspects of security performance and effect on safety should be reflected.

For the verification of security performance aspect, several conceptual methodologies were proposed [4]. However, although the verification of the adverse effect of the security techniques on the safety is essential, there has been no research or guide for the verification process in the nuclear industry. Considering the fact that security techniques were not considered when the existing digital I&C systems were designed, it is important to verify not only the aspect of security performance, but also, the aspect of effect on safety of target systems in S/W V&V processes [1]. Therefore, in this study, it is aimed to develop a method to quantitatively measure the degree of effects of security techniques on the S/W V&V processes, so that it can be used for the developing an efficient V&V processes covering both aspects of security performance and effect on safety.

ANALYSIS OF THE IMPACT OF APPLICATION OF SECURITY TECHNIQUES ON V&V PROCESSES

The degree of adverse effects of the security techniques on the system should be verified in the Software V & V process. In addition, depending on the cases, additional efforts should be made to reduce its size or to find alternative alternatives [2]. A major concern of Software V & V process is to manage software faults to reduce the software failure probability (SFP) below a reasonable level. When software modules are hard to be tested directly, estimation has been based on the qualitative approach using the verification and validation (V&V) level with the assumption that the current state of software exhibits low-level complexity [5]. However, if security techniques are applied, the complexity level cannot be assumed as low-level as before. According to researches which confirmed the relationship between S/W complexity and the amount of S/W faults, if the complexity of software increases due to the application of security techniques, this can lead to an increase in SFP [6], [7]. In this study, the amount of additional effort required for recovering the increased SFP to the previous value is defined as an indicator of the amount of impact of security techniques on S/W V&V processes.

For the analysis of the impact of application of security techniques on increase of SFP, an integrated approach including two kinds of models is adopted. 1st model estimates the number of residual S/W faults using the degree of V&V quality [8], and 2nd model estimates the SFP using the number of residual faults [9]. In this study sub-processes which can be affected by the application of the security techniques have been identified as follows.

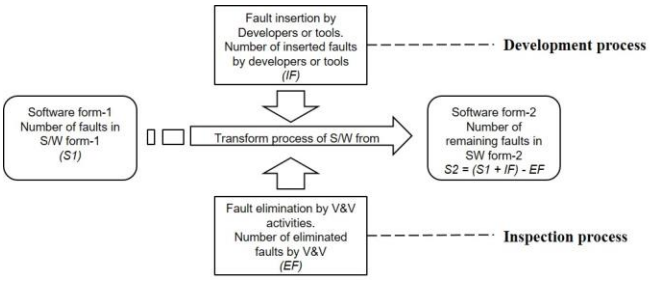

Fig. 1. A fault insertion/elimination scheme in the SW development phase [8]

- Development process: As the system-size and the system-complexity increase, the number of inserted faults increases.
- Inspection process: As the system becomes more complex, the number of eliminated faults decreases [10].

As the number of residual faults can be obtained by the faults inserted minus the faults removed, it leads to an increase in the number of residual faults when software become large and complex.

QUANTIFICATION OF THE IMPACT OF APPLICATION OF SECURITY TECHNIQUES ON V&V PROCESSES

The adopted models, introduced in the previous chapter, suggested a method for calculating SFP using various inputs from development processes and inspection processes. Since estimating the number of eliminated faults during the inspection processes is not clear among the inputs from inspection processes, the probability of fault elimination was fixed as 0.9. This value was estimated by the I&C experts [8]. However, in this study, based on the fact that the more complicated the software is, the harder inspection process is, a technique for calculating complexity called *Cyclomatic Complexity* is applied to determining complexity level [11]. In addition, based on the assumption that the more difficult in inspection process, the more difficult it is to correct faults, the probabilities of faults elimination are assigned according to complexity level. The values are summarized in Table 1.

Table I. Estimated probability of faults elimination

Complexity Level	Low	Moderate	High	Very-High
	0.9	0.8	0.7	0.6

The probability of faults elimination at the low-level case is assigned the estimated value in the adopted model. In addition, the other values are assumed in this study reflecting the fact that the probability of faults elimination decreases when the complexity level increases. However, these values can be changed depending on the used hardware, software and system state. Further researches are needed for more acceptable values.

As the complexity of the software increases due to the introduction of security functions, the probability of faults elimination in the inspection process decreases and eventually the number of residual faults and SFP increase. As a result, the degree of increase of SFP due to the application of security techniques can be estimated. The method for estimating SFP is summarized in Fig. 2.

According to Fig.2, there is a S/W test process in which the SFP can be updated by a beta distributed model using the results of test. The following equation used in beta distribution model was used for estimating updated SFP.

$$SFP = \frac{\alpha_{ap}}{\alpha_{ap}+\beta_{ap}+n_{test}} \quad (1)$$

In which, α_{ap} and β_{ap} are the beta distribution parameters which are determined depending on the number of residual faults and the system structure. n_{test} is the number of tests to be performed.

According to beta distribution model, although SFP can be increased due to the increased complexity level, the SFP can be compensated by increasing the amount of tests to be performed. With this regards, the number of additionally required tests for recovering increased SFP is suggested as a quantitative indicator for the impact of application of security techniques on S/W V&V processes.

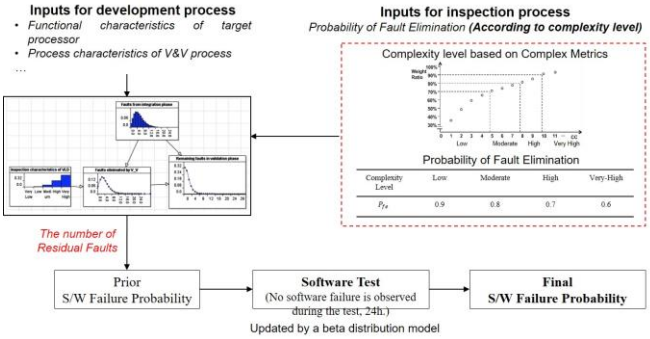

Fig. 2. The process for estimating SFP

SUMMARY AND CONCLUSION

Although the verification of the adverse effect of the security techniques is essential, there has been no research or guide for the verification process in the nuclear industry. A methodology for quantifying the amount of additional V&V processes when security techniques are applied is proposed as a research objective. Based on the analysis of the impact of application of security techniques on V&V process, the adverse effect to be focused is limited to the increase of S/W faults. The impact was quantified as the degree of increase of SFP, and the amount of additional V&V tests for compensating the increased SFP can be obtained. With this regards, the number of additionally required tests is suggested as a quantitative indicator for the impact of application of security techniques on S/W V&V processes.

However, there are some limitations to quantify the additional S/W V&V processes when security techniques are applied. The relationship between complexity level and probability of fault elimination need to be elaborated. In addition to software test process, sub-processes that can compensate for the increased SFP should be investigated.

REFERENCES

1. J. Song, J. Lee, C. Lee, K. Kwon, and D. Lee, "A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants," *Nucl. Eng. Technol.*, vol. 44, no. 8, pp. 919–928, 2012.
2. J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D. Y. Lee, and C. K. Lee, "An analysis of technical security control requirements for digital I&C systems in nuclear power plants," *Nucl. Eng. Technol.*, vol. 45, no. 5, pp. 637–652, 2013.
3. S. Gandhi and J. Kang, "Nuclear safety and nuclear security synergy," *Ann. Nucl. Energy*, vol. 60, pp. 357–361, 2013.
4. J. Shin, H. Son, R. Khalil ur, and G. Heo, "Development of a cyber security risk model using Bayesian networks," *Reliab. Eng. Syst. Saf.*, vol. 134, pp. 208–217, Feb. 2015.
5. S. H. Lee, H. E. Kim, K. S. Son, S. M. Shin, S. J. Lee, and H. G. Kang, "Reliability modeling of safety-critical network communication in a digitalized nuclear power plant," *Reliab. Eng. Syst. Saf.*, vol. 144, pp. 285–295, 2015.
6. D. Cotroneo, R. Natella, and R. Pietrantuono, "Predicting aging-related bugs using software complexity metrics," *Perform. Eval.*, vol. 70, no. 3, pp. 163–178, 2013.
7. M. Nagappan and P. Runeson, "A replicated quantitative analysis of fault distributions in complex software systems," *IEEE Trans. Softw. Eng.*, vol. 33, no. 5, pp. 273–286, 2007.
8. H. S. Eom, G. Y. Park, S. C. Jang, H. S. Son, and H. G. Kang, "V&V-based remaining fault estimation model for safety-critical software of a nuclear power plant," *Ann. Nucl. Energy*, vol. 51, no. December 2016, pp. 38–49, 2013.
9. M. Khalaquzzaman, S. J. Lee, M. C. Kim, and W. Jung, "Estimation of reactor protection system software failure probability considering undetected faults," *Nucl. Eng. Des.*, vol. 280, pp. 201–209, 2014.
10. Y. Shin and L. Williams, "An initial study on the use of execution complexity metrics as indicators of software vulnerabilities," *Proceeding 7th Int. Work. Softw. Eng. Secur. Syst. - SESS '11*, p. 1, 2011.
11. K. Yamashita *et al.*, "Thresholds for Size and Complexity Metrics: A Case Study from the Perspective of Defect Density," *Proc. - 2016 IEEE Int. Conf. Softw. Qual. Reliab. Secur. QRS 2016*, pp. 191–201, 2016.