Cyber Security Evaluation for Nuclear I&C Systems Corresponding to V-Model

Jiye Jeong , Gyunyoung Heo*
Department of Nuclear Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si,
Gyeonggi-do 17104, Republic of Korea
**Corresponding author: gheo@khu.ac.kr*

1. Introduction

Transition from conventional analog technology to advanced digital technology is a global trend and the instrumentation and control (I&C) devices of nuclear power plants (NPPs) are changing from analog devices to digital devices due to advances in digital technology and obsolescence of analog equipment.

However, the digital technology has some challenges such as proven reliability, common cause failure (CCF), and cyber security for nuclear I&C systems even though the digital system has several channels redundantly.

In the early days of digitization of nuclear I&C systems, since the systems generally has used disconnected network from the outside, it would be safe from cyber-attacks. However, in 2010, there was a cyberattack on the Iranian nuclear facility, which named 'Stuxnet'. In India, the control system of Kudankulam NPP was infected with a malware called 'DTrack', and one out of two was shut down last year [1][2]. Moreover, the increase in cyber-attacks targeting industrial control system (ICS) and the introduction of digital systems in nuclear facilities mean that cyber security is no more outside safety issue, which is of utmost importance due to the characteristic of nuclear facilities handling radiation [2]. Hence, the cyber security of digital I&C systems has been focused nowadays.

According to the report from the Carnegie Mellon University Software Engineering Institute, 70% of security vulnerabilities is possible to occur during the design process [3]. Also, the Microsoft Corporation has discovered that the security vulnerability is reduced by more than 50% when the Security Development Lifecycle (SDL) is applied from the software development stage [4].

Therefore, it is worth investigating the applicability of the analyzed control items of cyber security of NPPs on the stage of each software life cycle, so called V-model in this paper.

2. Software Life Cycle according to V-Model

The embedded system, a combination of hardware and software has increased the complexity of software in order to embody the safety-related demands, and the importance of software is increasing as most mission-critical functions are carried out by software [5]. So, safety-related software of nuclear I&C systems should be required for verification and validation (V&V) process to improve safety and reliability. The V&V process is the process of checking that a software system meets specification and that it fulfills its intended purpose. And it is known to improve software quality. For that reason, Korea Institute of Nuclear Safety (KINS) has stipulated that V&V activities should be conducted independently with regard to Institute of Electrical and Electronics Engineers (IEEE) 1012, and the V-model has been selected as one method of V&V process. Figure 1 showed V-model of digital I&C systems for Korean NPPs considering software development life cycle of IEEE 1012.

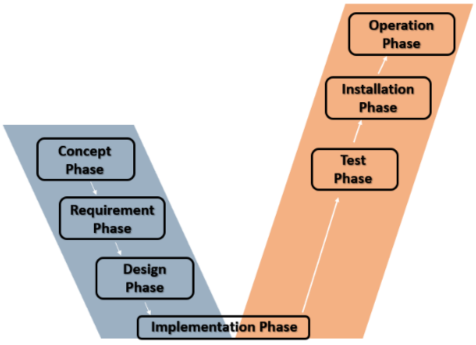


Figure 1. V-model of nuclear I&C systems

The 2016 version of IEEE 1012 recommended that the V&V process should be done in all system, software and hardware with life cycle. The summary of V&V activities in each phase of V-model for nuclear I&C systems was described in Table 1.

Table 1. Summary of V&V activities of V-model

Phase	Description
Concept	Define the features, constraints and goals with the users.
Requirement	Define how the systems work by identifying input data, processing contents and output data.
Design	Logically determine how to perform the function defined in previous phase. From this phase, the V&V process should be divided into hardware and software.
Implementation	Draw for outline and assembly in detail, and purchase components for hardware. Coding for the control and monitoring software.
Testing	This step is to improve the completeness by finding out errors and whether the developed system meets the requirements. The test range should begin with small and gradually widens such as unit tests, module tests and integrated system tests.
Installation	After installing the system in the field, check that there is no abnormality by test run.
Operation & Maintenance	This period is after commercial operation and the longest in the software life cycle. If the systems should be revised, the previous phases must be implemented.

3. Cyber Security Measures with V-model

In this section, the cyber security of nuclear I&C systems was screened out, grouped, and itemized along with the V-model.

Frist of all, by referring IEEE 1012 (2016) with the Korean regulation on cyber security for nuclear facilities, KINAC/RS-015, cyber security activities were defined at each phase of the V-model described in Table 2 [6]. Moreover, compared to SDOE(Secure Development and Operational Environment) activities, which are requested by KINS RG-8.13, definition of cyber security activities of V-model satisfied requirements.

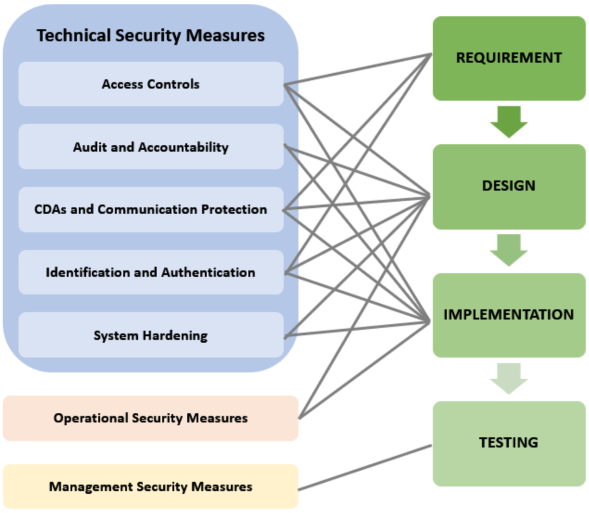
Table 2. Cyber security activities at each phase of V-model

Phase	Cyber security activities	SDOE activities
Concept	Identify security targets and security requirements, and develop an in-depth protection strategy from cyber security risks.	Establish a safe operating environment by evaluating potential sensitivity and identifying obstacles.
Requirement	Develop cyber security activities plans by finding the vulnerabilities of hardware, software, network and environment.	Defining functional performance requirements and system configuration for SDOE.
Design	Begin the cyber security design of hardware, software and network. It is necessary to understand the difference between safety features and security features. Create environment for cyber security to carry out cyber security policies described in the previous phase.	Physical and logical approaches to system functions, use of safety system services, and control of data communication with other systems should be addressed.
Implementation	Implement the cyber security for hardware and software by using the authorized tools. Remove the unsafe or unnecessary features of systems.	Identification of undocumented code or features. Also, check the effect of these functions on the safety and reliability of the safety system.
Testing	Testing of cyber security such as unit test or penetration test is conducted along with safety impact assessment. Verify that all cyber security requirements are met.	Tests to identify unauthorized pathways and ensure system integrity.
Installation	Establish a specific level of cyber security for the place where installed and make sure the system work well.	
Operation & Maintenance	Audit and evaluate the cyber security periodically as described in cyber security plans. Evaluate the impact of design changes on secure operating environment.	Hardware and software configuration management and maintenance of design characteristics.

According to KINAC/RS-015, after the critical digital assets (CDAs) identified and analyzed, it is proposed to take 101 (one-hundred one) security measures, which are technical security measures, operational security measures and management security measures. The fifty cyber security measures were selected, which could directly affect system design. The others were mostly related to policies or periodic activities of audit or secure operation environment during development of systems. Moreover, during installation phase and operation & maintenance phase, the activities of cyber security were not related to develop the cyber security systems.

The selected fifty measures were connected to V-model of software development life cycle shown as Figure 2. Figure 2 were based on the relationship between the control items of KINAC/RS-015 and the cyber security activities defined in Table 2. According to Figure 2, the technical security measures accounted for the largest portion, and most of the cyber security activities should be finished before test phase. This means that it is possible to occur cyber threats and it is necessary to be conducted audit and evaluation strongly during the requirement, design and implementation phase.

Figure 2. Cyber security measures on V-model


Technical Security Measures
Access Controls
Audit and Accountability
CDAs and Communication Protection
Identification and Authentication
System Hardening
Operational Security Measures
Management Security Measures
REQUIREMENT
DESIGN
IMPLEMENTATION
TESTING

The fifty cyber security measures were composed of forty-five for technical security measures, three for operational security measures and two for management security measures described in Table 3.

Table 3. Selected security measure at each phase of V-model

Class	Control Items	Numbers of sub-items
Technical Security Measures	Access Controls	16
	Audit and Accountability	7
	Critical Digital Asset and Communications Protection	15
	Identification and Authentication	4
	System Hardening	3
Operational Security Measures	System and Information Integrity	3
Management Security Measures	System and Service Acquisition	2

Moreover, each security measures were rated importance according to how much it affects the system of NPP with reference to KINAC/RS-015. Table 4 shows that the level of impact has been evaluated from 1 to 3 depending on the degree of impact: high (score:3), medium (score:2), low (score:1).

Table 4. Level of impact according to phase

Phase	Numbers of cyber security measures	Level of impact
Requirement	4	3.5
Design	26	2.89
Implementation	19	2.76
Testing	1	3.6

In other words, the four technical security measures for requirement phase, twenty-six security measures for design phase, nineteen security measures for implementation phase and two management security measures for testing phase should be conducted to comply with regulatory guidelines. Specially, during the design and implementation phases, the cyber security activities should be carried out critically and traceability of cyber security activities must be guaranteed.

4. Conclusion

The step-by-step cyber security activities along with V-model could reduce the opportunity cost of failures and errors, and it also protects against cyber hacking that could occur during development. Furthermore, the result can help to examine cyber security activities and deliverables. However, it should be considered at the software, hardware and network levels as mentioned in IEEE 1012. This method is an effective for cyber security evaluation of digital I&C systems of NPPs.

Based on the results described in section 3, the impact of cyber threats on each control item with each phase could be evaluated. The level of impact would also represent according to platforms such as PLC(Programmable Logic Controller) or FPGA(Field Programmable Gate Array). In this process, the level of cyber security could be derived according to the architecture design and platforms of I&C systems of NPPs.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP: Ministry of Science, ICT and Future Planning) (No. 2017M2B2B1072806)

REFERENCES

[1] Jinsoo Shin (2017). Cyber Security Evaluation for Nuclear I&C System using Bayes Theorem, KyungHee University

[2] Seungmin Kim, Gyunyoung Heo, Enrico Zio, Jinsoo Shin, Jaegu Song (2019). Study on Cyber Attack Taxonomy for Digital Environment in Nuclear Power Plants. Nuclear Engineering and Technology (NET)

[3] James W. Over (2002 March). Team Software Process for secure Systems Development, Carnegie Mellon University

[4] Microsoft Corporation (2012 May). Microsoft Security Development Lifecycle (SDL) Version 5.2, page 167, Microsoft Corporation

[5] Ki-chang Kim (2011 August). A Case Study on Application for Software Reliability Model to Improve Reliability of the Weapon System. KIISE page 406

[6] Kookheui Kwon (2018 May). Cyber Security for Direct CDA Life-cycle, Korean Nuclear Society Meeting 2019

[7] M.A.Awan, M.Alamger. “Cyber Security for Nuclear Facilities : Role of Regulatory Body”, International Conference on Nuclear Security, 2014

[8] Dalmi Seo, Kijong Cha, Yosoon Shin, ChoongHeui Jeong, Youngmi Kim (2015). Assessment Method of Step-by-step Cyber Security in the Software Development Life Cycle. Korea Institute of Information Security & Cryptology. Vol.25, No.2