Cyber Security for Direct Critical Digital Assets Life-cycle

Kookheui Kwon*, Siwon Kim, Inkyung Kim
Korea Institute of Nuclear nonproliferation And Control, Daejeon, the Republic of Korea
**Corresponding author: vivacita@kinac.re.kr*

1. Introduction

The regulatory standard of cyber security for domestic nuclear facilities (KINAC/RS-015) includes requirements for establishing cyber security system that the licensee should carry out such as roles and responsibilities of cyber security team, identification of Critical Digital Assets (CDAs), Defense-in-Depth protective strategies, implementation of security controls, continuous monitoring and assessment, and an incident response plan. And licensees are implementing cyber security measures gradually to establish the system for the operating nuclear facilities, but some of measures are security requirements to be considered from the development phase of CDAs such as logical access control, log function, security design, security test, configuration management, supply chain control, and acceptance test. Applying the above security measures to CDAs that are already in operation can cause not only design changes and operation delay but also conflicts between safety and security such as affecting system reliability and safety functions. According to U.S. NIST, the cost of eliminating defects or vulnerabilities found during the software operation phase is on average 30 times higher than in the development phase [14]. In addition, according to the domestic design basis threat (DBT), cyber attacks to nuclear facilities could occur in any phase of life-cycle. So cyber security is required not only in the operation phase of CDAs but also in the development and supply period.

Therefore, this paper suggests cyber security activities during the life-cycle including the development phase of CDAs. The regulatory standards of domestic cyber security and lessons learned from review experiences of constructing facilities are referenced, and the IAEA, IEC international guidelines on cyber security of digital I&C, and U.S. NRC Regulatory Guide are cited. Recently, as the NRC endorsed the NEI 13-10 on the graded approach for cyber security measures, this paper focuses on the cyber security activities for Direct CDAs during life-cycle, which many security measures are considered at the development phase [13].

2. Classification of Direct and Non-Direct CDAs

The NEI 13-10 (rev.6), endorsed by the NRC, requires cyber security measures to be phased in as a result of an impact of the CDAs on cyber attacks. It classifies CDAs that is not have an adverse impact on Safety and Security function by the worst consequence of cyber attacks as Non-direct CDAs, and it applies baseline security controls to prevent attack surface. The Non-Direct CDAs are classified into EP, BOP and Indirect CDA in detail according to the functions and consequences, and it is generally required that physical access control, wireless control, communication restriction, media control, configuration management and periodic monitoring of function and security measures as baseline security controls. In particular, Non-Direct CDAs are required only the following activities in place of security design and security test, supply chain control, and acceptance test during the development phase.

- Internal pre-operational testing
- Malicious code scanning when possible
- Calibration / configuration program

Therefore, this paper focuses on security activities of Direct CDAs which affects safety or security function, and Direct CDAs are required more detailed security measures than Non-direct, during life-cycle including the development phase.

Direct CDA	Non-Direct CDA		
Cyber security Activities during development	Indirect	BOP	EP
	- Consideration of Baseline security controls - Internal pre-operational testing - Malicious code scanning when possible - Calibration / configuration program		

Fig. 1. Classification of security activities in development by the NEI 13-10

3. Cyber Security for Direct CDAs Life-cycle

In this section, Cyber security activities during the life-cycle of Direct CDAs are categorized as pre-development, development, and operations, and the activities of each period are described.

3.1 Pre-development Security Activities

In pre-development period, it is necessary to analyze whether it is a CDA and Direct CDA through the evaluation of the function and the consequence on the target system. The CDA should be classified by the security level according to the defense-in-depth strategy and development with effective security requirements

during life-cycle of the system to ensure that the adverse impact on the security level does not lead to the failure of the entire cyber security system considering communication linkage.

Detailed CDA-specific cyber risk assessments can be performed at requirement phase, but risk assessments taking into account the overall CDAs (or Critical Systems) architecture should be performed in advance. Although it is not possible to expect complete and detailed risk assessment results since it is pre-development stage, the results can be utilized in CDA-specific requirements phase. It can be detailed during the development process and used to confirm whether risk has been mitigated through comprehensive assessment before facility operation.

3.2 Security Activities during Development

During the development of CDAs, the following common security activities should be included in the cyber security program and be carried out continuously.

- Configuration Management: Configuration changes including security configuration should be properly controlled and information about configuration changes should be managed in the system configuration management program. Known defects or vulnerabilities should be removed and recorded in accordance with configuration management procedures to enable tracking of change history.

- Integrity Management: Physical and logical access controls should be properly performed and monitored so that only authorized personnel can access them to prevent software and systems from infecting or tampering with malicious code. In addition, only security-proven software, hardware, and development tools should be used and related files should be checked through malware detection software.

- Verification and Validation: The independent V&V for security requirements should be included in the system verification and verification program to ensure that the security requirements are appropriately reflected in the results at each phase. In particular, security testing should be performed as a part of software testing as a dynamic software V&V.

- Security Audit: An independent review of security policy violations such as illegal access, unauthorized device use and appropriateness for implementation of procedures in accordance with the cyber security program should be carried out during the development phase.

The following describes security activities for each phase of development.

3.2.1. Requirement Phase

The risk assessments of the target CDA should be performed taking into account the cyber threats according to the DBT, reference document, and the risk assessment results for the entire CDAs architecture, and it should be analyzed whether security measures are applied to protect vulnerabilities derived from the result. The assessment results include the security measures to be applied to the target CDA, alternative security measures, non-applicable security measures and related grounds. The security requirements according to the assessment results are reflected in the relevant requirements specification of the target CDA.

In particular, a detailed risk assessments is required and justification of use as CDAs and alternate security controls should be made clear for situations in which the pre-developed product was developed without security controls and cannot be verified because the details are not disclosed.

3.2.2. Design & Implementation Phase

According to the security requirements of the requirements specification, the hardware and software of CDA are designed considering technical security measures such as access control, data communication, secure coding and database structure. Administrative and operational security measures should also be considered at the design phase for security during the operation and maintenance of the system and the results of the security design according to the security requirements should be reflected in the design specification.

At the implementation phase, the security design for hardware and software is applied and integrated and the effectiveness of security measures need to be confirmed through additional threat assessments

3.2.3. Test Phase

During the test phase, it is confirmed that the planned security requirements have been properly implemented, and the security effectiveness and impact on safety functions. Test plan should be based on the requirements specification and design specification, and it should be confirmed that there are not known vulnerabilities and malicious codes. The test includes unit, integration, penetration, and malicious user testing.

3.2.4. Installation, Acceptance, and Commissioning Phase

The security test and verification activities of the test phase normally continue to the installation and

commissioning phase, and these activities should be performed in a secure environment in accordance with the licensee's security policy. Supply chain control policies should be properly implemented to ensure integrity in the delivery of the system. In the commissioning process, malicious code should not be infected from outside, and access to illegal changes should be controlled.

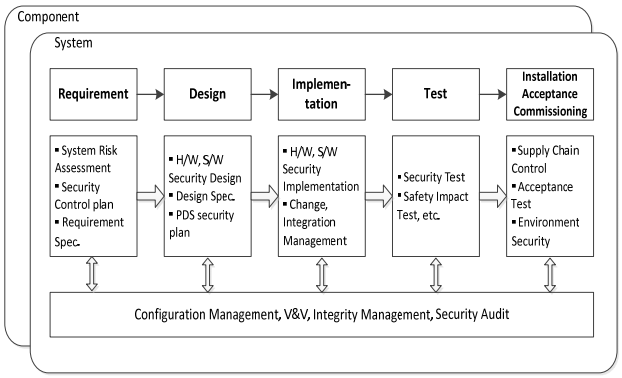

Fig. 2. Cyber security activities of Direct CDAs during development

3.3 Security Activities during Operating

3.3.1. Operation Phase

The ongoing monitoring and effectiveness of cyber security measures should be assessed so that CDAs are continuously protected in accordance with the facility's cyber security plan. System logs, access logs, integrity diagnostic results, and malicious code diagnostic results should be periodically performed as part of security audits. A cyber incident response plan for the CDAs should be prepared, and response and recovery training should be conducted periodically.

3.3.2. Maintenance & Modification Phase

In order to maintain the integrity of the CDA during the maintenance period, limited access should be made to the personnel, media, and communications that have been verified to be secure, and related histories should be maintained and monitored.

In the case of a modification involving a CDA, an assessment of the impact on the overall system security function should be performed and ensure that the security measures are properly followed after the change. During the modification, V&V should be made through the same activities as the security activities during the development period described above.

3.3.3. Retirement Phase

An assessment of the impact on the overall system security function should be carried out before the CDA is retired and the security impacts on the linked systems should be considered. Retirement should be carried out according to the security procedures pursuant to the cyber security plan and sensitive information should be appropriately removed.

4. Conclusions

This paper suggests the cyber security activities during the life-cycle including the development phase of Direct CDAs. The configuration management, V&V, requirements and design specifications, security test, and access control described in this paper are not completely new concepts, but these should be added as security items to the activities already performed as safety activities, or are implemented as the cyber security for operating facilities. The nuclear cyber security should be systematically and effectively applied from the development phase considering the impact on system functions, the limitations on accessing and changing the system and spread of impacts. It is expected that CDAs can be protected through periodic assessments of the monitoring and robustness of implementation these security measures.

ACKNOWLEDGMENTS

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. 1605007)

REFERENCES

[1] KINAC/RS-015, "Cyber Security Regulatory Standard for Nuclear Facilities", KINAC, 2014.
[2] Nuclear Security Series No.17. "Computer Security at Nuclear Facilities", IAEA, 2011
[3] Nuclear Security Technical Guide No.36. "Computer Security of Instrumentation and Control Systems at Nuclear Facilities", IAEA, 2017
[4] International Physical Protection Advisory Service. "IPPAS Mission Report for the Republic of Korea", IAEA, 2014
[5] Draft Nuclear Energy Series. "Engineering and Design Aspects of Computer Security for Instrumentation and Control Systems at Nuclear Power Plants", IAEA, 2017
[6] IEC 62645. "Nuclear Power Plants − Instrumentation and Control Systems − Requirements for Security Programmes for Computer − based Systems", IEC, 2014
[7] DICWG-08. "Common Position on the impact of Cyber Security Features on Digital I&C Safety Systems", OECD NEA, 2012
[8] Vitor M. McCree, Executive Director for Operations. "Security Considerations in New Reactor Construction", U.S. NRC, 2016

[9] Security Guide for Software Development, “Software development security guide for e-government software developers”, KISA, 2017
[10] Regulatory Guide 5.71. “Cyber Security Program for Nuclear Facilities”, U.S. NRC, 2010
[11] Nuclear Energy Series(draft). “Engineering and Design Aspects of Computer Security for I&C systems at Nuclear Power Plants”, IAEA, 2017
[12] IAEA Safety Standards No. SSG-39. “Design of Instrumentation and Control Systems for Nuclear Power Plants”, IAEA, 2016
[13] NEI 13-10(rev.6). “Cyber Security Control Assessments”, NEI, 2017
[14] NIST Planning Report 02-3. “The Economic Impacts of Inadequate Infrastructure for Software Testing”, NIST, 2002
[15] NIST 800-53(rev.2). “Guide to Industrial Control System Security”, NIST, 2015