Cyber security guideline for supply chain controls of digital commercial product in nuclear facilities

Seunghoon Park[*], Poe il Park, Kookheui Kwon, and Chae-Chang Lee

Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseongdaero, Daejeon, Republic of Korea

[*]*Corresponding author: shpark@kinac.re.kr*

1. Introduction

According to guideline such as KINAC/RS-015, NRC's RG5.71, and NEI 13-10, supply chain controls of critical digital assets (CDAs) for cybersecurity for nuclear facilities are considered from a principled point of view. In reality, when introducing CDAs, the safety-related supply chain control requirements are applied. Although digital I&C systems apply safety regulatory requirements due to overlapping safety and cybersecurity requirements, CDAs for emergency preparedness and physical protection in a blind spot of the regulations. NEI 13-10 classify the types of CDAs according to functions except for general computer type. In case of digital commercial products, there is a limit to applying the control of the supply chain in current safety and cybersecurity field It is necessary to apply supply chain control operator policies, procedures, and purchase requirements for each SSEP function, or to establish cybersecurity integrated supply chain control requirements. In this study, the cybersecurity regulation guideline for supply chain control considering SSEP (Safety-Security-Emergency Preparedness) function of CDAs.

2. Supply Chain Controls of Digital Commercial Product

2.1 Supply chain control regulation of general cyber security

Supply chain control is mostly about quality of digital commercial grade items. The control regulation about cyber security NIST guide SP 800-161 and "executive order 14082" in U.S. The NIST SP 800-161 is guide for supply chain control State information system and organization. The guideline provides identifying ICT supply chain risks, assessment and mitigation. Designate supply chain risk factors such as unauthorized production, malicious software into the supply chain, poor manufacturing and development practices in the supply chain. In order to management of ICT risks, according to importance, the guide suggest risk determination process frame.

Domestic supply chain control for cyber security, regulatory authority is preparing the guideline of ICT supply chain control system. The guidelines have been developed based on NIST SP 800-161 following 2019 national cyber security strategy promotion national cyber security master plan. However, the concrete guidelines are not yet.

2.2 Regulation of Supply Chain Control for Nuclear Facilities

Regulatory guide 5.71 (RG.5.71) [1] in US provides security regulation guide to Nuclear Regulatory Commission (NRC). The guide describes security controls for cyber threats, risks and vulnerabilities, as well as well-known countermeasures and protection technologies, divided into three categories: technology, operation and management. Designates digital assets that need to be protected from cyberattacks as Critical Digital Assets (CDAs), and provides guidance for addressing potential cybersecurity risks of CDAs by applying an identified set of defense architectures and security controls. In order to provide high assurance for the integrity of systems and services to be maintained during the procurement process, the content of the procurement policy development defining the purpose, scope, roles, responsibilities and management commitments, and the implementation of procurement policies related to supplier security and development lifecycle; Includes development of procedures to facilitate and maintain.

NEI 08-09 [2] highlights the need for procurement from verified suppliers to ensure that items obtained from the supply chain (including software) are procured from trusted sources and that these critical items have traceability and validity, such as compliance certification for Commercial-Off-The-Shelf (COTS).

IAEA [3] provides supply chain control guideline through Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities (IAEA NP-T-3.21) [4]. This document sets out the key procurement functions and current practices for nuclear facilities, helping all managers directly or indirectly involved to ensure the safe operation of nuclear facilities, and communication between plant operators and regulators for dealing with procurement issues provides a common technical basis. However, this document does not include supply chain control in terms of cyber security.

For CDAs, domestic regulatory standard of cyber security of nuclear facility, KINAC/RS-015, provides supply chain control guide which Nuclear operators must prepare and implement measures to maintain integrity and protect against threats in the supply process when introducing essential digital assets (Administrative Security Measures of KINAC/RS-015).

3. Supply Chain Controls in Nuclear Facilities by SSEP

3.1 Safety and Safety Related Functions

Supplier inspection verifies that equipment that meets the technical standards for quality assurance for the safety of nuclear equipment is introduced. Regulatory authority, i.e. NSSC, inspect designers, manufacturers, and performance verification organizations that supply safety-grade structures, systems, and equipment to power reactors, research reactors, and educational reactors (inspection by Korea Institute of Nuclear Safety, suppliers, etc.). Also, NSSC inspect whether the design, manufacturing, and performance verification activities for safety-rated facilities (structures, systems, and equipment) satisfy the standards for construction permit or operation permit required by the Nuclear Safety Act, and whether the contents of the safety-related facility contract report are appropriate. In NEI 13-10 [10], CDAs with safety and safety-related functions recommend that differential security measures be applied by classifying them as direct and indirect CDAs. Since the safety grade CDA is a development product, it follows the quality-related supply chain control of the safety grade mentioned above. However, in the case of indirect CDA, quality-related supply chain control of the safety grade is followed, but commercial products are also used in the case of PC-type CDA that performs some data processing. Since these PC-type or digital commercial CDAs have been reported to be vulnerable to the latest cyber threats, it is judged that cybersecurity supply chain control in other fields such as IEC-62443 part 4-2 [9] and TTA (Telecommunications Technology Association in Republic of Korea) certification needs to be applied correspondingly.

3.2 Physical Protection and Emergency Preparedness Functions

In NEI 13-10, CDAs with security functions are classified as direct CDAs. CDAs that function as security are not important in quality-related supply chain control in the safety sector. However, from a cybersecurity perspective, CDAs that function as security are exposed to vulnerabilities against the latest cyber threats, and both software and hardware need to apply cybersecurity supply chain control such as IEC-62443 part 4-2, TTA certification. In addition, in the case of security facilities recently introduced, digital commercial products account for the majority, and it is necessary to develop new supply chain control regulatory requirements.

The CDA only supports emergency preparedness (EP) function and does not perform or support any other Safety-Related, Important-to-Safety or Security function. EP CDA is also a recent trend to introduce the latest digital products. In the case of EPs, it is also necessary to develop new supply chain control regulatory requirements

5. Conclusions

Supply chain control in domestic and international information and nuclear fields is mostly about quality, and supply chain control for security is in the initial stage of making specific plans. Nuclear facilities have stipulated to perform general standard quality verification when converting items produced according to general industrial standards to safety and safety-related CDAs, but this is a guideline to verify product safety. Since digital commercial products are also analyzed as information systems under the Radioactive Disaster Prevention Act, it is necessary to introduce a supply chain control guideline suitable for the introduction of digital commercial products to prevent electronic infringement on the information systems of nuclear facilities. Applying supply chain control operator policies, procedures, and purchase requirements shall be necessary for each SSEP functions which are CDAs of digital commercial products. The general cybersecurity standards such as IEC-62443 part 4-2, TTA certification can be applied correspondingly for digital commercial products without special products only for nuclear facilities.

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. 2106012)

REFERENCES

[1] NRC, Cyber Security Programs for Nuclear Facilities (Regulatory Guide 5.71), 2010.

[2] NRC, Addendum 3 to NEI 08-09, Revision 6 Dated April 2010 System and Services Acquisition, 2010.

[3] IAEA, Computer Security at Nuclear Facilities (NSS-17), 2011.

[4] IAEA, Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities (IAEA NP-T-3.21), 2016.

[5] IAEA, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, 1999.

[6] Nuclear Safety Act Enforcement Decree, Article 31 (Quality Assurance Inspection).

[7] Enforcement Decree of the Nuclear Safety Act, Article 31-2 (Inspection of suppliers, etc.).

[8] KINAC, Computer and Information System Security of Nuclear Facility (KINAC/RS-015), 2016.

[9] International Electrotechnical Commission, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (IEC 62443-4-2:2019), 2019

[10] Nuclear Energy Institute, Cyber Security Controls Assessments (NEI 13-10, Rev. 5), 2017