Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 19-20, 2022

A State-of-Art of Supply Chain Control Regulation to Digital Commercial Grade Item for Cyber Security of Nuclear Facility

Seunghoon Park [*], Chae-Chang Lee, Poe il Park, and Kookheui Kwon
Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseongdaero, Daejeon, Republic of Korea
[*]Corresponding author: shpark@kinac.re.kr

1. Introduction

Digital system delivered to nuclear facilities have been considered in terms of quality control and safety. In December, 2020, the federal agency computer network penetration incident occurred through an attack on the SolarWinds (network monitoring solution) supply chain by Russian presumed hackers.

Although KINAC/RS-015 [8] specifies cybersecurity requirements for digital items introduced into nuclear facilities, cybersecurity verification measures for digital commercial products are insufficient. In order to respond to increasing cyber threats and supply chain attacks, it is necessary to verify the security of digital commercial products introduced to domestic nuclear facilities and control the supply chain.

In this study, it is intended to derive legal/administrative/institutional improvements for supply chain control of general standard items through the trend and analysis of the regulatory status of supply chain control and security verification of digital commercial graded items introduced to nuclear facilities.

2. Methods and Results

2.1 Supply chain control regulation of 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. Unauthorized production, tampering, theft, insertion of malicious software and hardware into the supply chain; Designate supply chain risk factors such as 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 as shown in Fig. 1.

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.

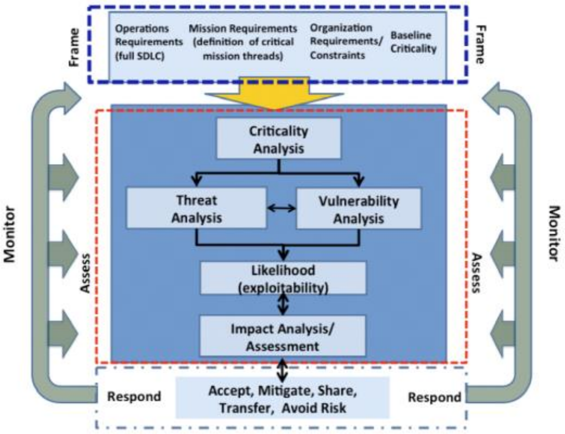
Frame
Operations Requirements (full SDLC)
Mission Requirements (definition of critical mission threads)
Organization Requirements/ Constraints
Baseline Criticality
Frame
Monitor
Assess
Criticality Analysis
Threat Analysis
Vulnerability Analysis
Likelihood (exploitability)
Impact Analysis/ Assessment
Assess
Monitor
Respond
Accept, Mitigate, Share, Transfer, Avoid Risk
Respond

Fig. 1. ICT SCRM risk process

2.2 International supply chain control regulation of nuclear facility

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. To provide high assurance that the integrity of systems and services is 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 dialogue between plant operators and regulators when dealing with procurement issues provides a common technical basis. However, this document does not include supply chain control in terms of cyber security.

2.3 Domestic supply chain control regulation of nuclear facility

Domestic nuclear equipment quality assurance inspection, supplier inspection verifies that equipment that meets the technical standards for quality assurance for the safety of nuclear equipment is introduced [5].

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.) [6].

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 [7].

In terms of cyber security, for critical digital asset, 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) [8].

3. 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. Security aspects are not taken into account. Domestic nuclear facilities have stipulated to perform general standard quality verification when converting items produced according to general industrial standards to safety grade items, but this is a guideline to verify product safety. Since digital commercial goods are also analyzed as information systems under the Radioactive Disaster Prevention Act, it is necessary to introduce a supply chain control plan suitable for the introduction of digital commercial goods to prevent electronic infringement on the information systems of 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.