Cyber Security Considerations for Technologies Intended in the Future SMR

Yoon Ki Choi *, Kyung Jin Lee , Yeon Jun Choo and Kiwhan Chung
FNC Technology Co. Ltd., 13, Heungdeok 1-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 16954, Republic of Korea
**Corresponding author: cyk12@fnctech.com*

1. Introduction

Currently, computers and I&C (Instrumentation and Control) systems in nuclear power plants have been operated independently and in a closed network due to safety issues. However, small modular reactors (SMRs) are considering incorporating autonomous operation, remote control, load-following operation, modularization and network connectivity beyond the usual power plant characteristics in order to reduce operational costs and to expand flexibility [1].

Operational costs may be reduced by optimizing the number of operators through autonomous operation and remote control. In addition, a flexible operation is possible through load-following operation, and economic feasibility can be secured through modularization [2, 3].

However, new technologies considered for SMR may introduce cyber security vulnerabilities stemming from the additional connectivity to the external networks and the unregulated supply chain market that will be available to the SMR supply chain. Therefore, establishing the regulatory requirements for the SMR operation must be established before deployment.

In this study, considerations are derived by analyzing the cyber security vulnerability problems of new technologies expected to be applied to SMR through case studies in the current industry.

2. Cyber Security Vulnerabilities Present in the New Technologies for SMR

This section reviewed cyber security vulnerabilities that may arise when introducing SMR's new technologies based on case studies applied to the current industries.

2.1 Autonomous Operation

SMR may be composed of a number of reactor modules. Each module is independently or integrally managed. The latest SMR design considers introducing autonomous operation to control multiple reactor modules reliably and reduce the operator's burden [4]. In order to introduce autonomous operation in nuclear power plants, cyber security problems that may arise from these should be considered.

Future vehicles such as self-driving cars and connected cars electronically control a number of vehicle functions for the convenience and safety of drivers and passengers. Examples of autonomous operation applied to the industry include self-driving cars and smart factories. In other words, automotive cyber security is becoming increasingly important because it is based on wireless sensor transmission and reception. Various cyber security vulnerability cases have been reported, including a demonstration of the "Jeep Cherokee" hacking in 2015, a paper on the hacking of vehicle's unlocking in 2013, and the discovery of Hyundai Motor's BlueLink vulnerability in 2017 [4].

Smart factories are connected to ICT in various processes, so process data is collected in real-time, analyzed, and controlled by themselves. In other words, since smart factories are also networked, vulnerabilities have been found in their cyber security network. A well-known example is the "Stuxnet" incident. Stuxnet is a worm virus discovered in June 2010 that infects programmable logic controller (PLC) used to program the equipment, changing the behavior of the equipment. It infected Iran's uranium enrichment facilities, and its existence became widely known.

Analyzing the cases of self-driving cars and smart factories applied to the industry, autonomous operation seems to have cyber security vulnerabilities regarding networks.

2.2 Remote Control Incorporated for SMR Operation

Remote control and support may be considered to optimize the number of operators present to improve the economic feasibility of the SMR operation [5].

The remote control is possible when safety and security are already established in manned SMR operations. The remote control can efficiently distribute roles and improve operational safety and security when multiple units are located on a single site or nearby sites and are necessary for the real-time load-following operation. However, it is still exposed to cyber security problems caused by vulnerabilities within the wired and wireless communication used for remote control access.

Among the current industrial technologies, drone control is an area where the importance of cyber security due to wired and wireless communication is emerging. Security threats to drones can be classified into wireless signal attacks between drones and controllers, attacks using security problems in wireless communication protocols such as Wi-Fi, and attacks taking advantage of drone software vulnerabilities [6].

A wireless signal attack is an attack through spoofing or jamming that deceives or interrupts an RF signal or GPS signal between a drone and a controller. Wireless communication protocol attacks take advantage of known security issues in wireless communication protocols, such as unencrypted Wi-Fi signal snipping, WEP vulnerabilities, WPA/WPA2 authentication

encryption hijacking through pre-attack, communication failure of normal users, and DoS.

The software attack mounted on the drone is an attack that can take control of the drone as well as privacy information stored in the drone due to internal unencrypted data theft attacks (such as photo and video leakage) and malicious code injection attacks.

2.3 Load-Following Operation

Efforts have been made worldwide to introduce load-following operation functions to improve economic feasibility in the new SMR design. Load-following operation refers to an operation method that adjusts the electrical power of a generator in response to fluctuations in demand or power supply requests in the power system. Domestic nuclear power plants are not operating load-following due to nuclear fuel performance and safety [7].

There are two types of load-following operation: planned load-following and frequency control. The planned load-following operation changes the electrical power according to a predetermined plan. Frequency control operation maintains a planned grid frequency by adjusting power supply according to real-time power demand, also called an automatic frequency control (AFC).

For a nuclear power plant to perform AFC operations, it must receive control signals from its external power management system (EMS). Key functions of EMS are dispatch scheduling, state estimation, and monitoring and control of the subsystem. To perform an AFC operation for SMR, a network connection with the EMS is necessarily required.

The Korean domestic power system control system is operated as a closed network, so communication security is most likely guaranteed. Nevertheless, in 2015, there was a case in Ukraine where malicious code was distributed to the internal network of power plants due to cyber attacks, resulting in massive power outages [8].

2.4 Supply Chain

With the rapid development of the information society, all activities during the entire life cycle, such as product development, production, sales, and maintenance, in the ICT and general industries can be said to be intertwined with various supply chains. Since the 2000s, related policies and technical preparations are already being actively discussed worldwide under the leadership of the United States. Supply chain cyber security has already emerged as a big topic in the ICT field. Advanced and gen III+ reactors, including SMR, are being studied to apply various digital technologies with the goal of autonomous operation based on remote control using digital I&C. Many advantages are highlighted through this. However, it should be noted that the expanded digital footprint increases the cyber attack surface, subsequently increasing cyber security risk. In particular, unlike on-site assembly of power plants, the modular construction method, a unique characteristic of SMR, poses a problem: the threat from attacks on the nuclear power plant I&C supply chain becomes easier.

Entering the 2000s, supply chain attacks have been reported in various industries, including the ICT sector. These supply chain attacks have recently been perpetrated regardless of fields and targets. One of the representative examples of supply chain attacks is the malicious code attack by unknown hackers on SolarWinds' Orion products which provides network management solutions in the United States. Supply chain cyber attacks have a variety of methods, procedures, and targets using vectors such as software, hardware, and firmware. An investigation into these types of supply chain cyber attack patterns is well introduced through the MITRE report [9].

The development and application of a management system to protect the supply chain from these cyber attacks have been most actively carried out in the United States. The US cyber security Framework (CSF) reflects supply chain risks in the cyber security Framework [10, 11], a federal agency information security guideline previously developed to respond to supply chain attacks. The cyber security framework presented by the US NIST is a kind of security management that guides operators of major national infrastructures (government facilities, transportation, defense, energy, etc.) to recognize cyber threat situations and respond appropriately. Recently, NIST has emphasized the importance of C-SCRM (Cyber Supply Chain Risk Management) through CSF v2.0 [12]. C-SCRM is a process for managing the supply chain from cyber threats. It includes all activities during the life cycle (from R&D to disposal) of all ICT products and services, including assets managed by the institution. The above activities are divided into four stages: 1) creation of a basis for risk (frame, context setting for risk-based decision-making), 2) risk assessment, 3) response to the determined risk and 4) continuous risk monitoring.

Another supply chain security management system is the ISO/IEC 27036 standard. This standard presents security requirements and guidelines required for suppliers.

Another ISO/IEC 20243's O-TTPS (Open Trusted Technology Provider Standard - Mitigating maliciously tainted and counterfeit products) is another ISO standard related to supply chain cyber security. O-TTPS is a standard the OTTF (Open Trusted Technology Forum) developed. It is an open standard for global supply chain security and integrity enhancement of commercial ICT products and services. ISO/IEC 20243 consists of two parts; a set of guidelines, requirements, and recommendations addressing specific threats to the integrity of hardware and software COTS ICT products throughout the product lifecycle and procedure

evaluators can utilize when conducting conformity assessment for the essential requirements of O-TTPS.

3. Cyber Security Considerations

This section derived the following considerations to respond to the potential cyber security vulnerabilities described in Section 2.

3.1 Supply Chain

In order to derive the supply chain-related considerations of SMR from the cyber security aspect, it should be considered with multi-faceted approaches as follows;

- Regulatory situation current nuclear power plant
- Activities of supply chain cyber security in the ICT field introduced in Section 2.4 above
- Future SMR supply chain environment

Firstly, the preceding regulatory positions related to the supply chain regarding the cyber security for the existing commercial nuclear power plants can be confirmed through RG 5.71 [13] and 1.152 [14] issued by the US NRC. The NRC's RG 5.71 is used as regulatory guidelines to protect digital computers, communication systems, and networks at nuclear facilities from cyber attacks.

RG 1.152 presents standards applied to computers used in safety systems used in nuclear power plants. Unlike RG 5.71, which is a regulatory guideline for responding to malicious behavior, it is a guideline for non-malicious behaviors and approaches that supply chain actors (designers, manufacturers, operators, etc.) must abide by during the life cycle of nuclear power plants.

The IAEA published TECDOC 919 [15], a guideline for managing procurement activities and supply chains to operate and maintain nuclear facilities. In addition, through TECDOC 1169 [16], the IAEA provided detailed methods and practical guidelines to prevent the use and purchase of counterfeit and questionable items that occur in multiple processes and organizations involved in the supply chain.

The existing cyber security regulations of nuclear facilities can be applied to SMR as it is. However, given the design and construction characteristics of SMR, the existing regulations are still insufficient to fundamentally prevent, manage, and respond to various attack points and forms in the supply chain. It is, therefore, necessary to actively introduce and utilize advanced supply chain management measures in the ICT field, such as the countermeasure system for supply chain cyber security in the ICT field described in Section 2.4 (e.g., NIST's CSF's C-SCRM). Establishing a management system throughout the asset lifecycle is necessary based on the physical flow and data flow for digital assets. Furthermore, it is required to present technical standards to support such a management system.

Various technical management methods have been studied and proposed for software attacks with relatively different attack points and patterns than hardware or firmware attacks. A typical example is SBOM (Software Bill Of Materials). SBOM means meta-information representing the components of the software and can be referred to as corresponding to the BOM of the manufacturing industry. This may enable transparent supplier management. As a similar concept, some concepts, such as SPDX(Software package Data Exchange) and ISO/IEC 5230(known as OpenChain), are widely used in the industry.

3.2 Autonomous Operation

Cyber security is becoming more important because self-driving cars and connected cars operate based on AI and wireless sensor transmission and reception. In these future vehicles, various cyber security threats may exist as following

- Real road vehicle-related backend servers
- Using communication channels
- Related to car update procedures
- Unintended human behavior
- External connection of the vehicle
- Data and code Threats
- Potential Vulnerabilities

Therefore, it is necessary to have a system to identify and cope with the above cyber security threats in order to perform the stable and safe driving function of future vehicles.

Smart factories should consider cyber security because production facilities with ICT are connected to the network. In smart factories, various cyber security threats can exist as follows.

- External malicious code
- System self vulnerability
- Unauthorized remote access
- Access to the internal network of unauthorized devices
- Employee's mistake
- Intentional leakage of programs by employees
- Outflow of assets by an unauthorized person

Due to the above cyber security threat, interruption and malfunction of the control program and leakage of confidential industrial assets may occur. Accordingly, it is recommended to establish security standards by referring to IEC 62443 standard to achieve internalization of security in industrial plants. IEC 62443 standard is an international standard for 'Industrial Communication Networks-Network and System Security.' This standard is currently the leading

industrial cyber security standard for all plants, facilities, and systems throughout the industry [17].

3.3 Remote Control

Considerations for preventing cyber security problems and vulnerabilities of wired and wireless communication applied to remote control are securing the reliability of the component supply chain, checking the security of HW and software, and maintaining the integrity of the system by establishing security policies [18].

To maintain the security of hardware and software, constant security updates, falsification, and malicious code response, libraries maintained by reliable third parties, and applying highly secure coding are required [7].

To fundamentally block access from unauthorized users, the system should be operated to allow users to access only the authorized level through proper authentication procedures. Protecting wireless signals that are the basis of communication and transmission data is necessary by securing communication channels.

The normal basic operation pattern should be established. During the remote control access, the system should be processed to return to a predefined default status when an incomplete control signal occurs so that the system can safely stop or wait. The operation information and relevant SMR data should be stored securely, and the information transmitted and received should be encrypted to prevent leakage and data falsification during transmission. To execute encryption policies, encryption key management, the encryption algorithm used, random number generation, and encryption module are used to increase security in a multi-layer manner [18].

Important SMR data should be protected through the countermeasures, such as encryption and prohibiting access to unauthorized accounts. Finally, the system should be inspected and recorded in real-time through security logging to monitor abnormalities in the system. The record of the security logging includes user login success/failure, configuration change history, functional performance history, time stamp function, and time synchronization are also useful.

3.4 EMS Network Connections

Load-following operation for a power plant needs to connect with EMS. The EMS consists of a power generation, transmission, distribution, and information transmission/reception system. The following various cyber security threats may exist in each system [19].

- System data and communication data leakage
- Data deletion and destruction of system data
- Tempering and manipulation of communication data
- Operation of the equipment through physical access
- Unauthorized access to the network
- Denial of a conduct
- Usage of an unauthorized function
- Excessive use of resources

4. Conclusions

The autonomous operation, remote control, load-following operation, and modularization are expected to be part of SMR operation and will likely introduce advantages in plant operation and economic feasibility. However, these new technologies will have some potential cyber security vulnerabilities.

As described above, network connection outside the independent network is essential to introduce autonomous operation, remote control, and load-following operation technologies. Therefore, the occurrence of cyber security vulnerabilities due to network connection inevitably occurs. In addition, SMR's modularization technology may also have cyber security vulnerabilities regarding diversified supply chain management.

Therefore, SMR should have a framework to identify and address cyber security threats regarding network connection and supply chain management before establishing the new technologies.

REFERENCES

[1] Advances in Small Modular Reactor Technology Developments, IAEA, 2020.
[2] Kyung-tak Kang, Yeon-jin Lee, SMR Technology Trend Brief, KISTEP, 2022.
[3] World Nuclear Power Market INSIGHT, KEEI, 2022.
[4] An Analysis of Car Hacking Cases and Types of Security Threats in Future Cars, Security News, 2022.
[5] “Advanced Nuclear Technology: Using Technology for Small Modular Reactor Staff Optimization, Improved Effectiveness, and Cost Containment,” EPRI, 2016.
[6] “Cyber Security Guide for Drone,” Korea Internet Security Association, 2020.
[7] “Remote Control System,” Son Jae-beom, Jung Wan-kyun, Yeom Young-il, Advanced Robot System Technology Special Issue, Control, Automation, and System Engineering Journal Vol. 2, 1996.
[7] Load-Following Operation of PWR Plants, KAERI, 1993.
[8] NCCIC/ICS-CERT Incident Alert, Ir-Alert-H-16-043-01, AP Cyber-Attack against Ukrainian Critical Infrastructure, NCCIC
[9] J. F. Miller, Supply Chain Attack Framework and Attack Patterns, MITRE, MTR140021, 2013
[10] NIST, Framework for Improving Critical Infrastructure Cyber security. Version 1.0., 2014
[11] NIST, Framework for Improving Critical Infrastructure Cyber security. Version 1.1, 2018
[12] NIST, NIST Cyber Security Framework 2.0 Concept Paper: Potential Significant Updates to the cyber security Framework, 2023
[13] NRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.

[14] NRC, Regulatory Guide 1.152, Criteria FOR Use OF Computers in Safety Systems of Nuclear Power Plants, 2011.
[15] IAEA, Management of procurement activities in a nuclear installation, IAEA-TECDOC-919, 1996.
[16] IAEA, Managing suspect and counterfeit items in the nuclear industry, IAEA-TECDOC-1169, 2000.
[17] Jungha Jin, Juntae Kim, SangSeon Park, Keunhee Han, A Study on the Security Enhancement of the Industrial Control System through the Application of IEC 62443 Standards, KIPS, 2021.
[18] Overview and Issues of Drone Wireless Communication, Son Seong-hwa, Kang Jin-hyuk, Park Kyung-joon, Information and Communications Magazine, vol 33, 2016.
[19] Pil Sung Woo . Balho H. Kim, Establishment of Cyber Security Countermeasures amenable to the Structure of Power Monitoring & Control Systems, KIEE, 2018.