Cyber-Security Considerations for SMRs to Conduct Load-following Operations in Korea

Kiwhan Chung, Kyung Jin Lee, Yeon Jun Choo, Yoon Ki Choi, Seong Youn Jo[1]

FNC Technology Co. Ltd., 13, Heungdeok 1-ro, Giheung-gu, Yongin-si, Gyeonggi-do, 16954, Korea, kiwhan@fnctech.com, cyk12@fnctech.com, yjchoo@fnctech.com
[1]Korea Institute of Nuclear non-proliferation And Control, 1418, Yusung-Daero, Yuseong-Gu, Daejeon, 34101, Korea, jerry@kinac.re.kr

ABSTRACT

In most countries where nuclear power plants (NPPs) are employed for commercial power generation, the NPPs are used as the baseload power sources. The emergence of SMRs brought up several flexible applications that were not feasible with the current large NPPs, such as multiple energy end-products and other industrial uses. One of the novel opportunities is the option to operate SMRs in the load-following mode and take advantage of the expanded capabilities of the latest SMR design considerations offered in Korea.

Currently, all nuclear power plants in Korea are not conducting load-following operations and only serve to fulfill the base load. They do not respond to the fluctuating demands that may occur daily or seasonally. Therefore, the baseload NPPs do not have to alter the power production level and act independently.

However, if SMRs are utilized as load-following power sources, several issues require operational policies and procedures modification. One area of such change that must be addressed is cyber-security. The SMR integrated control system will likely need to receive frequent control signals from the National Energy Management System (EMS) outside the plant and process the signals to control multiple reactor modules in a coordinated manner to conduct load-following operations. This change will inevitably require an intimate linkage between the power reactor control system and national EMS, as never happened in Korea previously.

In this paper, we address the identification of the potential cyber security issues that may arise during the load-following operation and discuss the cyber security measures and considerations that will protect the SMRs from increased connectivity to off-site.

Introduction

Nuclear power plants in Korea do not conduct load-following operations (LFO) and only serve to fulfill the base load. They do not respond to the fluctuating demands that may occur daily or seasonally. Therefore, the baseload NPPs do not have to alter the power production level or act independently to the varying power demand during the fuel cycles.

In most countries where nuclear power plants (NPPs) are employed for commercial power generation, the NPPs are used as the base load power sources. The recent development in SMR conceptualization brought up several flexible applications that were not feasible with the current large NPPs, such as multiple energy end-products and other industrial uses. One of the novel opportunities is the option to operate SMRs in the load-following mode and take advantage of the expanded capabilities of the latest SMR design considerations offered in Korea.

However, if SMRs are utilized as load-following power sources, several issues require operational policies and procedures modification. One area of such change that must be addressed is cyber-security. To operate in load-following mode, the SMR integrated control system (ICS) will likely need to receive frequent control signals from the national energy management system (EMS) outside the plant and process the signals to control one or more reactor modules in a coordinated manner. This change will inevitably require an intimate linkage between the power reactor control system and the national EMS, as never happened in Korea previously.

In this paper, we address the identification of the potential cyber security issues that may arise during the LFO and discuss the cyber security measures and considerations that will protect the SMRs from increased connectivity to off-site.

Load-Following Operation for Nuclear Power Plants

What is LFO?

LFO is a power plant operational mode that adjusts the electrical power output in response to changes in power demand. There are two types of LFO: One is a planned LFO, and the other one is frequency control operations. Planned LFO alters the power level at a preset time in agreement with EMS to balance the load and supply. The daily and seasonal power demands are met with the scheduling of the power output variation, as the fluctuation can be obtained from operational data.

Frequency control operation alters the power frequency minutely by varying the power supply up to 5% to stabilize the frequency variation that may exist in the power grid for up to several minutes. Frequency control operation is performed by governor-free operation (GFO) and automatic generation control (AGC). The GFO automatically increases or decreases the generator output by the turbine governor in response to the sudden fluctuating frequency. The GFO corresponds to a change in a short cycle of about a few seconds to keep the power grid frequency at a constant target.

AGC is responsible for frequency control beyond GFO control and corresponds to a change cycle of several minutes. Real-time control through AGC is crucial to ensure system stability in power grid systems [1]. AGC controls the power for each generator in consideration of system load and frequency adjustment participation rate by the generator. Each plant must be able to accept AGC control signals from the EMS to participate in frequency control operations. The EMS controls a power generation, transmission, distribution, and information transmission/reception system, including the frequency of the power grid. To perform LFO for the SMR, network connection with the outside system is inevitable.

Current status of LFO for nuclear power plants

In France, LFO technology, including frequency control operation, is already a commercial technology, and many, if not all, nuclear power plants operate effectively in LFO mode. An LFO mode called Mode G was developed for France in 1976, and Mode X was developed in 1990 to improve performance [2].

Korea's nuclear power plants have not adopted LFO. One historical reason is that most Korean NPPs are of the US designs, where LFO was never rooted. Using the US facilities and the corresponding operational procedures and policies, Korean NPPs were never initially equipped with LFO capabilities. Also, up to the 1990s, Korean electric power usage was mostly satisfied with NPPs supplying the baseload of the power demand.

However, as the Korean economy expanded, the power demand started to resemble the power demand of a more advanced economy. It showed daily and seasonal fluctuations that started to demand the consideration of incorporating LFO for the NPPs. Also, renewable energy sources that are mostly privately owned are allowed to connect to the Korean power grid and have started to contribute enough volume such that the power grid regulators are forced to think about balancing the additional contribution from the renewable by LFO the coal-fired power plants. As the Korean power industry warms up to the LFO, the emergence of SMRs logically carried the discussion to include LFO capabilities to fulfill the perceived gap left by the Korean NPPs performing only the baseload operation.

In Korea, research has been conducted to confirm the LFO capability of existing PWR nuclear power plants by developing driving technology suitable for domestic power demand. Through the study, Mode K, a Korean nuclear power plant LFO technology, was developed, and its applicability was reviewed [3].

Application of LFO for SMRs

It is generally accepted that SMRs provide a promising option to fulfill the need for flexible power generation for various applications [4] without disturbing grid stability. SMRs are deployable either as a single or multi-module plant and offer the possibility to combine nuclear power efficiently with alternative energy sources, including renewable energy sources [5]. The International Energy Agency (IEA) also argues that it should be recommended to accelerate innovation in new reactor designs, which improve the operational flexibility of nuclear power plants to facilitate the integration of growing wind and solar capacity into the electricity system [6] as recently experienced in several countries including Korea.

From a technical point of view, SMRs are better equipped than large power plants for increased operational flexibility for several reasons [5] as follows:

- Small power output: SMR units can support small grids with modest power demand or reinforce large grids by, for example, replacing aging fossil-fired power plants, which are typically small power sources

- Scaled power capacity: in situations where small incremental additions are needed to satisfy slow growth in load demand, an SMR plant is a credible option
- Reduced source term & relatively low thermal output: an individual SMR unit expands the option for siting, which enables closer locations to power customers or even co-location with heat processes that may use the waste heat
- Inherent self-regulation and resilience to external events (e.g., station blackout, loss of heat sink, etc.): many SMR design concepts can substantially contribute to grid stability
- Enhanced availability (i.e., increased capacity factors): an extended operation cycle with significantly shorter intervals between refueling outages
- Non-electrical product streams available (district heating, desalination, hydrogen production, etc.): flexible to transition SMR output among multiple hybrid energy product streams depending on the demand (e.g., electricity production at peak demand times transitioning to other heat processes at low demand times)
- Innovative design and operational features: advanced SMRs may include design specificities such as innovative fuel elements (accident tolerant fuels) or innovative reactivity power control (boron-free designs) that may reduce the core solicitations during load following and thus increase the achievable core power ramps

Cyber Security Concerns for SMR

While there are several promising advantages to operating SMRS, performing the LFO for SMRs requires a network connection with a power grid system outside the plant. For this reason, cyber-security considerations in the following areas need to be reviewed.

- Power grid system
- Network connection: wired and wireless communication
- Autonomous operation: safe autonomous operation when communication means are not available
- Supply Chain: Application of the latest ICT Technology

This section reviewed cyber security vulnerabilities in the above field based on case studies applied to the current industries.

Power grid system

Efforts have been made to incorporate LFO to improve economic feasibility in the new SMR designs. While Korean NPPs are not performing LFO currently, if the SMRs in the Korean energy market are to perform LFO, then a communication channel with EMS must be established and maintained. For the planned LFO, a real-time connection is not necessary; however, a real-time connection is imperative for performing AFC.

For an NPP to perform an AFC operation, it must receive control signals from the EMS. Key functions of EMS are dispatch scheduling, state estimation, and monitoring and control of the subsystem. To perform an AFC operation with SMRs, a real-time network connection with the EMS is required.

The Korean domestic power grid control system is operated as a closed network, so communication security is better protected. However, in 2015, there was a cyber attack in

Ukraine where malicious code was distributed to the internal network of power plants, resulting in massive power outages [7].

Previous studies on cyber-security in electrical grid networks [8] presented various cyber-security threats and security requirements to respond to them, as shown in Table 1.

Table 1. Cyber-security Threats and Security Requirements in Power Grid Systems

Threats	Requirements
− 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 service − Usage of an unauthorized function − Excessive use of resources.	− Safe local and remote access methods − Setting user access authority by condition − Prevention of leakage of stored personal information and power operation information − Measures to prevent leakage of stored cryptographically important information − Measures to check whether important information stored in devices and systems has been tampered with − Log generation, storage, and transmission plan for accident analysis in case of device infringement − Communication object authentication scheme − Option to provide end-to-end integrity, confidentiality, and non-repudiation according to network structure and service data characteristics in information delivery of application layer service − Network access control plan in connected devices − Ways to mitigate or limit the impact of a DDoS attack − Design of communication data and secure communication protocol's structure considering MAC value field when designing communication protocol − Using secure cryptographic algorithms to provide entity authentication, data integrity, and confidentiality − Protect the system from physical attack

Autonomous operation

SMR may be composed of several 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 [9]. In order to introduce autonomous operation in nuclear power plants, cyber security problems that may arise from these should be considered.

Autonomous operation is a technology that is already being applied in existing industries. And the cyber-security-related issues faced by self-driving cars and smart factories can shed light on potential cyber-security issues the SMRs face.

Currently, self-driving cars and connected cars automatically control several vehicle functions for the convenience and safety of drivers and passengers; however, various cyber security threats exist in these future vehicles [9]. Several 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.

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

Smart factories are connected to ICT in various processes, so process data is collected in real-time, analyzed, and controlled by themselves. Smart factories also have cyber-security vulnerabilities because they are networked. A well-known example is the "Stuxnet" incident. Stuxnet is a worm virus discovered in June 2010 that infects the programmable logic controller (PLC) used to program the equipment, changing the behavior of the equipment. It infected Iran's uranium enrichment facility, which made its existence widely known. Therefore, it is necessary to have a system to identify and cope with the above cyber security threats to perform future vehicles' stable and safe driving functions.

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
- The 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 standards to achieve internalization of security in industrial plants. IEC 62443 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 [10].

Network connection

Network connections used for remote control and support may be considered to minimize the number of operators present to improve the economic feasibility of the SMR operation [11]. 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 real-time LFO. However, it is exposed to cyber security problems caused by vulnerabilities within the wired and wireless communication used for remote control access.

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.

Considerations for preventing cyber security problems and vulnerabilities of wired and wireless communication applied to remote control are to secure the reliability of the component supply chain, check the security of HW and software, and maintain the integrity of the system by establishing security policies [13]. Maintaining hardware and software security requires constant security updates, proactively responding to falsification and malicious codes, using libraries maintained by reliable third parties, and applying highly secure coding [14]. Also, 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.

During remote-control access, the system should be designed to return to a predefined default status when an incomplete control signal occurs so that the system can stop or wait in safe status. 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, encryption algorithms, random number generation, and encryption module are used to increase security in a multi-layer manner [13].

Important SMR data should be protected through encryption and prohibiting access from 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.

Supply Chain

Cyber-security issues for the supply chain have already emerged as a big topic in the ICT field. Advanced and gen III+ reactors, including SMR, are being explored to apply various digital technologies, including digital I&C. Unlike on-site assembly of power plants, the modular construction method, a unique characteristic of SMR, poses potential problems of leaving the digital assets of the SMRs vulnerable to cyber-attacks. It is inevitable that the

expansion of the supply chain increases the surface of cyber-attacks and increases the risk for cyber-security accordingly.

Supply chain cyber-attacks have a variety of methods, procedures, and targets using vectors such as software, hardware, and firmware. 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. An investigation into these types of supply chain cyber-attack patterns is well introduced through the MITRE report [15].

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 on the supply chain risks [16,17] as a federal agency information security guideline previously developed to respond to supply chain attacks. The cyber security framework presented by the US NIST is security management that guides operators of major national infrastructures (government facilities, transportation, defense, energy, etc.) to recognize cyber threats and respond appropriately. Recently, NIST has emphasized the importance of C-SCRM (Cyber Supply Chain Risk Management) through CSF v2.0 [18]. 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 activities consist of four stages: 1) creation of a risk basis (frame, context setting for risk-based decision-making), 2) risk assessment, 3) response to the determined risk, and 4) continuous risk monitoring.

Multi-faceted approaches were considered to derive the supply chain-related considerations of SMR from the cyber security aspect, as follows.

- Regulatory criteria of current nuclear power plant
- Cyber security activities for the supply chain
- Future SMR supply chain environment

The preceding regulatory positions related to the cyber-security issues in the supply chain of the existing commercial nuclear power plants can be confirmed through RG 5.71 [19] and 1.152 [20] 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, a regulatory guideline for responding to malicious behavior, RG 1.152 is a guideline for non-malicious behaviors. It is guidance that supply chain designers, manufacturers, and operators must follow during the life cycle of NPPs.

The IAEA published TECDOC 919 [21], 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 may be insufficient to fundamentally prevent, manage, and respond to various attack points and forms in the supply chain. Therefore, it is necessary to introduce and utilize supply chain cyber-security countermeasures systems in the ICT field, such as NIST's C-SCM, for future SMRs. 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 a software bill of materials (SBOM). SBOM means meta-information representing the components of the software and can be referred to as corresponding to the BOM of the manufacturing industry. It may enable more transparent supplier management. Similar concepts, such as software package data exchange (SPDX) and ISO/IEC 5230 (also known as OpenChain), are widely used in the industry.

CONCLUSION

Most SMRs deployed by design and economic necessity will likely incorporate LFO capability. While the additional benefits of LFO are clear, the cyber-security policies and procedures necessary for performing LFO are not proposed. Particularly, the cyber-security policies and procedures in several key areas, such as a connection to the external power grid system, a wire or wireless connection for remote-control access, autonomous operation, and the supply chain, will need to be coordinated to present a robust digital system that can withstand the potential cyber-attacks.

These cyber-security issues facing SMRs may not differ greatly from the usual vulnerabilities of complex systems, such as smart factories or self-driving cars; however, the perceived threat to SMRs looms large on the public’s mind, and it would be prudent to exercise cyber-security policies and practices that are already well established in other industries to close the potential vulnerabilities that may exist in operating SMRs. It includes established guidelines set out by national regulatory agencies for protecting supply chain vulnerabilities relevant to cyber-security.

ACKNOWLEDGEMENTS

The Nuclear Safety Research Program supported this work through the Korea Foundation of Nuclear Safety (KoFONS) using the financial resource granted by the Republic of Korea's Nuclear Safety and Security Commission (NSSC). (No. 2205014-0122-SB110)

REFERENCES

[1] J. Jang, “Improved Automatic Generation Control Algorithm for Stabilized Operation of National Power Grid,” Gyongsang National University, 2015.

[2] J. Jang, S. Oh, Y. Koo, J. Lee, and G. Moon, “Load-Following Operation of PWR Plants,” Korea Atomic Energy Research Institute, 1993.
[3] J. Koo, H. Hwang, J. Choi, S. Oh, et al., “The Development of Load-Following Technology in Nuclear Power Plants,” Korea Atomic Energy Research Institute, 1991.
[4] International Atomic Energy Agency, “Small Modular Reactors,” Available: https://www.iaea.org/topics/small-modular-reactors
[5] International Atomic Energy Agency, “Instrumentation and Control Systems for Advanced Small Modular Reactors,” NP-T-3.19, 2017.
[6] International Energy Agency, “Nuclear Power in a Clean Energy System,” 2019.
[7] Cybersecurity & Infrastructure Security Agency, “AP Cyber-Attack against Ukrainian Critical Infrastructure,” Ir-Alert-H-16-043-01, 2021.
[8] P. Woo, and B. Kim, “Establishment of Cyber Security Countermeasures Amenable to the Structure of Power Monitoring & Control Systems,” Korea Institute of Electrical Engineers, 2018.
[9] Security News “An Analysis of Car Hacking Cases and Types of Security Threats in Future Cars, 2022.
[10] J. Jin, J. Kim, S. Park, and K. Han, “A Study on the Security Enhancement of the Industrial Control System through the Application of IEC 62443 Standards,” Korea Information Process Society, 2021.
[11] Electric Power Research Institute, “Advanced Nuclear Technology: Using Technology for Small Modular Reactor Staff Optimization, Improved Effectiveness, and Cost Containment,” 2016.
[12] Korea Internet Security Association, “Cyber Security Guide for Drone,” 2020.
[13] S. Son, J. Kang, K. Park, “Overview and Issues of Drone Wireless Communication,” Information and Communications Magazine, vol 33, 2016.
[14] J. Son, W. Jung, and Y. Yeom, “Remote Control System,” Advanced Robot System Technology Special Issue, Control, Automation, and System Engineering Journal Vol. 2, 1996.
[15] J. Miller, “Supply Chain Attack Framework and Attack Patterns,” MTR140021, 2013.
[16] National Institute of Science & Technology, “Framework for Improving Critical Infrastructure Cyber security,” 2014.
[17] National Institute of Science & Technology, “Framework for Improving Critical Infrastructure Cyber security,” 2018.
[18] National Institute of Science & Technology, “NIST Cyber Security Framework 2.0 Concept Paper: Potential Significant Updates to the Cyber Security Framework,” 2023.
[19] Nuclear Regulatory Commission, Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” 2010.
[20] Nuclear Regulatory Commission, Regulatory Guide 1.152, “Criteria FOR Use OF Computers in Safety Systems of Nuclear Power Plants,” 2011.
[21] International Atomic Energy Agency, “Management of procurement activities in a nuclear installation,” IAEA-TECDOC-919, 1996.