Nuclear Cyber Security Issues and Policy Recommendations

Cheol-Kwon Lee [a*], Dong-Young Lee [a], Na-Young Lee [b], Young-Soo Hwang [b]
[a]*Korea Atomic Energy Research Institute, Daejeon, Republic of Korea*
[b]*Korea Institute of Nuclear Nonproliferation and Control , Republic of Korea*
[*]Corresponding author: cklee1@kaeri.re.kr

1. Introduction

Last December, the design information of KHNP nuclear power plants was seized by hacking groups that called themselves the 'nuclear opposition groups', which caused public anxiety about nuclear facilities, including nuclear power plants. Then this incident decorated the headline news of all domestic media and the group is still working to discredit the credibility for nuclear power plants.

Cyber security has already become an issue in all aspects of society, in particular, financial and information industries. The cyber-attack against computer systems causes the loss of function which brings about the big economic loss, and it becomes a national-wide issue. In recent days the cyber threat has occurred in the national critical infrastructure around the world.

In the nuclear industry, while discussing responses to various threats against nuclear facilities since 2006, cyber-terrorism was also discussed. But at that time, cyber-attacks against control networks in nuclear facilities were not seriously considered because those networks were isolated from the Internet thoroughly and it was evaluated that cyber penetration would not be possible.

However Stuxnet worm virus which attacked Iran's nuclear facilities confirmed that the cyber security problem could occur even in other nuclear facilities. The facilities were isolated from the Internet. The virus attacked through an infected USB. This attack is now being called APT (advanced persistent threat), a malicious cyber threat. After the cyber incident, we began to discuss the topic of NPP cyber security.

It is very difficult to predict whether or when or how the cyber-attack will be occurred, which is a characteristic of cyber-attack. They could be always detected only after when an incident had occurred.

This paper summarizes the report, “Nuclear Cyber Security Issues and Policy Recommendations” by issue committee in the Korea Nuclear Society, which reviewed the cyber security framework for nuclear facilities in the Republic of Korea being established to prevent nuclear facilities from cyber-attacks and to respond systematically [1]. As a result this paper proposes several comments to improve the security and furthermore safety of nuclear facilities

2. Characteristics of nuclear cyber security

In the 2000s legacy nuclear power plant instrumentation and control(I&C) systems which were based on analog technologies, have rapidly been upgraded to the digitalized ones and now most of the nuclear power plants in Korea are being operated with digital technology. Therefore nuclear cyber security is addressed to be a key issue for supplying a stable power to the state as well as ensuring the public safety.

While typical cyber-attacks are appeared in the form of functional loss of the Internet or data/information takeover, cyber-attacks on industrial plants can lead to malfunction of the systems. In particular a malfunction of the safety-related core systems in nuclear facilities can cause the leakage of radioactive materials, and it can cause more serious incidents when cyber-attacks and physical attacks are combined.

The scope of nuclear cyber security covers all the following digital devices and systems, but not limited to;

1) safety-related digital devices and I&C,
2) computer servers in security system and emergency preparedness systems,
3) built-in digital devices of major components,
4) testing and analysis equipment, etc.

These are similar with those of industrial control systems but there are many things that need to be considered when applying cyber security technologies due to the unique characteristics of nuclear safety.

The control networks of NPPs are designed normally in a closed network and do not have any connection to the Internet. Also, in principle, it is being operated in 365 days for 24 hours a day and employs the proprietary communication protocols for each system and the embedded operating system designed and fabricated only for the purposes to be used in the specific system. Because of this, it is difficult to employ a general-purpose security solution, and it is not possible to update the security patch of the operating system on-line.

Consequently, if the nuclear facility is infected it is difficult to prevent the system from inside spread and propagation to other systems. However common IT measures or existing general corresponding measures developed for industrial control systems can not be used directly in nuclear facilities. Therefore nuclear specific security systems and solutions should be developed as soon as possible.

3. Status of nuclear cyber security response system

In 2001 Korea enacted a law (Act on the Protection of Information and Communications Infrastructure), which was to establish measures to protect a critical information and communication infrastructure and enforcement. The purpose of the law is to bring the stability of the country and people's lives through the stable operation of a critical infrastructure.

Nuclear facilities has been designated as a critical information and communication infrastructure in February 2011, and a system that can respond to cyber incidents has been established through a critical information and communication infrastructure protection scheme (as shown in figure2).

In the law (Act on measures for the protection of nuclear facilities, etc. and prevention of radiation disasters) of the nuclear facilities, cyber incidents that occurred in nuclear facilities are to be reported immediately to the director of National Intelligence Service (NIS) according to the December 2013 amendments. For a successful nuclear cyber security, the systematic and immediate response through close cooperation between government departments is critical.

4. Recommendations for improving the nuclear cyber security policies

With cyber security of nuclear facilities, it can reduce the possibility of cyber intrusion and minimize damage in the event of cyber incidents by working together between several government departments and the nuclear industry. In order to prevent cyber intrusion and respond to them efficiently, the related systems and legal system to manage the risk should be modified in part as below.

4.1 Maintenance of legal system

Cyber security regulatory framework for the nuclear facilities are being carried out largely on the basis of the 'Act on the protection of information and communications infrastructure', 'Nuclear safety act', and 'Act on measures for the protection of nuclear facilities, etc. and prevention of radiation disasters'.

In February 2011, cyber security checks are being carried out from the various government departments by including nuclear facilities to 'Act on the protection of information and communications infrastructure'. In December 2013, Nuclear Safety and Security Commission was responsible for the cyber security regulations for nuclear facilities as amended by the 'Act on measures for the protection of nuclear facilities, etc. and prevention of radiation disasters'.

Because the scope of regulation of nuclear facilities is not clearly defined between 'Act on the protection of information and communications infrastructure' and 'Act on measures for the protection of nuclear facilities, etc. and prevention of radiation disasters', it is necessary to check the legal system to avoid unnecessary or redundant regulations or regulatory vacuum.

4.2 Target of cyber security in nuclear facilities

The target of cyber security in nuclear facilities was expanded continuously from the safety system to non-safety control and monitoring systems as well as physical protection systems, emergency preparedness systems and other support systems. Furthermore, current trend is to be expanded to a major design information and logging system.

However, the target systems specified in 'Act on measures for the protection of nuclear facilities, etc. and prevention of radiation disasters' are defined as safety systems, security systems, emergency preparedness systems, and support systems, while those in 'Act on the protection of information and communications infrastructure' are whole nuclear facilities. Therefore, the scopes are not identical.

4.3 Application of cyber security technologies during the entire life cycle of nuclear facilities

Cyber security to be applied must be able to ensure safety during the entire life cycle of the target system in order to meet the requirement of 'nuclear safety Act'. By the present 'Act on measures for the protection of nuclear facilities, etc. and prevention of radiation disasters', regulatory commission initiates the security regulation at the time of five months before fuel loading. So, security reviews by the regulatory during the construction phase of a nuclear power plant (design, fabrication, testing and installation, etc.) is omitted.

4.4 Response system against cyber terrorism

Considering the particularities of a nuclear facility and the impact by incident, a cyber crisis management system for nuclear facilities needs to be established separately from industrial control systems.

4.5 Development of prevention-related and response-related technologies against cyber terrorism

In order to strengthen cyber security system, the technology development is needed to respond to the continuously evolving cyber threats. Due to the characteristic of nuclear security, related information is considered confidential, and there is a constraint to the introduction of advanced technologies and the technology cooperation. Nevertheless, the development and application of cyber incident detection technology must be continuously performed, and it is necessary to

ultimately develop an integrated cyber security monitoring and management system.

4.6 Awareness and Training

The KHNP information leakage incident has confirmed that the cyber-attacks on nuclear facilities as well as the insufficient private sector information management can raise people's worries.

Therefore, all operators, regulatory agencies and government-related agencies in nuclear industry should know that cyber security can have serious effects on public safety and it is a critical issue that can have a serious impact on nuclear facilities without physical access

In this sense, cyber security awareness should be spread to people involved a nuclear industry, education and training program should be developed for each level of expertise for cyber security responsibilities

5. Conclusions

Digital technology will be used more widely at the national critical infrastructure including nuclear facilities in the future, and moreover wireless technologies and mobile devices will be soon introduced to nuclear industry. It is therefore anticipated that the rapid advance in digital technology will accelerate the opportunity of hacking these facilities. Now, cyber security has become an essential underlying technology rather than a matter of choice in order to protect the nuclear facilities from cyber-attacks.

Not only the prevention from cyber intrusion is important but also the systematic response and management are required, and these should incorporate the nuclear-specifics. For the public safety and national security, a comprehensive plan for implementation of cyber security technologies as well as R&D activities needs be developed for nuclear facilities.

REFERENCES

[1] Issue committee in Korea Nuclear Society, A report on "Nuclear Cyber Security Issues and Policy Recommendations", 2016.8