Consideration on Measures against Insiders Threats in ROK

Seungmin Lee [a*], Hobin Yim [a], Yunjeong Hong [a]
[a] *Korea Institute of Nuclear Nonproliferation and Control, 1418 Yuseong-daero, Yuseong-gu, Daejeon, Korea*
[*] *Corresponding author: seungmin@kinac.re.kr*

1. Introduction

The term 'adversary' is used to describe any individuals performing or attempting a malicious act. Adversaries may be insiders or outsiders. The term 'INSIDER' is specially used to describe adversaries with authorized access to a nuclear facility, a transport operation or sensitive information [1]. Insiders are able to take advantage of their access rights and knowledge of a facility to bypass dedicated security measures. They can also threaten cyber security, safety measures, and material control and accountancy (MC&A). Insiders are likely to have the time to plan their actions. In addition, they may work with an external adversary who shares their objectives. Because of these reasons, IAEA published "The Implementing Guide Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8" to help understanding of the Member States.

This paper focus on the current status of the measures to prevent, detect and respond to potential insiders at nuclear facilities in Republic of KOREA. Then the improvement method is derived based on IAEA documents.

2. The Current Status and Improvement Method against the Potential Insiders

In this chapter, the preventive and protective measures against the potential insiders at nuclear facilities, especially nuclear power plants, will be reviewed. Appropriateness of the measures was crosschecked with relevant IAEA documents.

2.1 The current status of the preventive and protective measures against the potential insiders

2.1.1 Background checks

Background checks is required to every person who wants to enter the nuclear facilities. The nuclear facilities are specially designated ones for national security according to the national security laws and regulations. Those laws and regulations defined that background checks who want to enter the nuclear facilities are necessary depending on the specific requirements of each nuclear facility. Background checks is used a measure to guarantee nuclear facility management loyalty, integrity and reliability of employees for national security. However, background checks for nuclear facility employees are generally conducted once for all in entire employment period. More seriously, temporary workers, especially those who are working during the overhaul period, are usually not subject to background checks.

2.1.2 The access control to vital areas

Some of the inspection results for physical protection systems of nuclear facilities, which were drawn by The Korea institute of nuclear nonproliferation and control (KINAC) according to the related laws and regulations, showed that the access control to vital areas was still vulnerable to potential insider threats.

The Security Administrative grants access authority to the vital areas based on the internal regulations. According to the physical protection regulations report, all employees in some nuclear facilities have the access authority to the vital areas due to operational convenience. Results of analyzing the access log, 31.8 % of employees with vital area access permission did not enter the vital areas during the overhaul the busiest access period to vital areas. This result clearly implies that security administrative takes access authority for granted.

In addition, access controls of nuclear facility operators ought to be classified in six categories according to the internal regulations. However, in fact, access to the vital areas with first-categories permission is possible which is not supposed to be. So, the internal regulations are somewhat vulnerable to insider threat.

2.1.3 Cyber security concerns

Cyber security is a specific information security that concerns computer based systems, networks, and digital systems.

A single insider can threat systems with authorized access by harming cyber assets with high safety and/or security importance and sensitive information. Because of these aspects, the nuclear facilities management must pay attention to cyber security to prevent and protect against potential insider threats. However, some employees did not use an authorized memory device. The use of unauthorized memory device with malware can destroy the nuclear facility control system. As the well known example, 'Stuxnet incident' showed why nuclear facilities operators must pay attention to insider cyber security threats for the safety of facilities.

2.2 Comprehensive measures against potential insider threats

The common approach to implementing comprehensive measures against potential insiders is to implement a mixture of preventive and protective measures. The term "preventive measures" is used to describe measures to remove possible insiders and to minimize threat opportunities. And the term "protective measures" is used to describe measures to deter, detect, and delay insiders. Protective measures should be coordinated with overall contingency plans in accordance with corresponding procedures. Fig. 1 illustrates steps for preventive and protective measures against potential insiders.

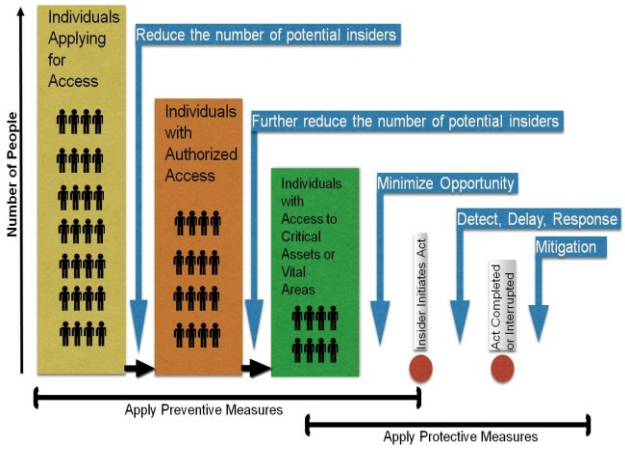

FIG 1. Steps for preventive and protective measures against potential insiders

2.3 Improvement method against Insiders Threats

The design basis threat is an important and commonly used tool to develop nuclear security systems and measures. A State should consider attributes and characteristics of potential insiders and include them in the design basis threat. So, information about insiders was provided for the design basis threat as the start.

Periodic background checks on all employees who work at nuclear facilities have been recommended to the nuclear facility operators. It can be a good measure to prevent potential insiders as already mentioned.

And the improvement of the access permission procedure, such as the list of employees who have access authority, has been proposed. A documented process for authorizing access to nuclear facilities should be implemented because the number of people with authorized access to designated areas should be kept to the minimum necessary. The process should adopt strict need-to-know and need-to-access rules for each facility. Unescorted access of workers is strictly restricted only to the areas that are required to complete assigned task.

The use of process data from facility equipment notified to whom in charge of the process has been suggested. For example, the use of material control and accountancy (MC&A) from facility processes and provision of an alarm system that indicates the unauthorized removal of nuclear material from the material balance could be good measures to deter insiders' attempts.

3. Conclusions

Insiders are able to take advantage of their access rights and knowledge of facilities where they are working or have worked to bypass dedicated security measures. Therefore, insiders can be the most dangerous threats to cyber security, safety measures, and material control and accountancy of nuclear facilities. Preventive and protective measures against the potential insiders in the nuclear facilities are yet insufficient according to the security inspection results. Especially, preventive and protective measures for unauthorized removal of nuclear material by insiders are the weakest area of whole security systems and should be further strengthened. A documented process to authorize and end access to nuclear facilities, nuclear material, systems and/or sensitive information should be established and implemented.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, Vienna (2014).
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, Vienna (2011).