PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS AT NUCLEAR FACILITIES IN IN KOREA



Recommended Citation

Jeong-ho Lee, "PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS AT NUCLEAR FACILITIES IN IN KOREA", NAPSNet Special Reports, October 27, 2017, https://nautilus.org/napsnet/napsnet-special-reports/preventive-and-protective-measures-against-insider-threats-at-nuclear-facilities-in-in-korea/

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS AT NUCLEAR FACILITIES IN KOREA

JEONG-HO LEE

OCTOBER 27, 2017

I. INTRODUCTION

In this essay, Jeong-ho Lee describes the steps taken in the Republic of Korea to implement the advice of the International Physical Protection Advisory Service and national nuclear security legislation and policy. The ROK, he concludes, is "working on developing a national framework against insider threats. It includes revising legal requirements, improving access control and contraband detection procedures to vital areas, and enhancing the nuclear security culture."

Jeong-ho Lee is Researcher, Korea Institute of Nuclear Non-proliferation and Control

Paper prepared for Workshop *Reducing Risk of Nuclear Terrorism and Spent Fuel Vulnerability in East Asia* co-sponsored by Nautilus Institute and Research Center for the Abolition of Nuclear Weapons, Nagasaki University, Nagasaki, January 20-22, 2017

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Banner image: lifting device for spent fuel transport container, from here

II. NAPSNET SPECIAL REPORT BY JEONG-HO LEE

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS AT NUCLEAR FACILITIES IN KOREA

OCTOBER 27, 2017

Table of Contents

1. Introduction

2. Insider Threats

3. Current and Improved Measures against Insider Threats

4. Conclusions

Figures and Tables

Figure 1. Nuclear Facilities in Korea

Figure 2. Population around Nuclear Sites

Figure 3. Legal Framework for Nuclear Security

Figure 4. Categories of Insiders

Figure 5. Preventive and Protective Measures against Insider Threats

Figure 6. A Conceptual Model for Nuclear Security

Figure 7. Result of Nuclear Security Awareness Survey

Figure 8. Vital Area Identification Process

Table 1. Measures against Insider Threats

Abstract

A series of tragic events raised world-wide fear of nuclear terrorism. The September 11, 2001 attacks in the USA revealed how terrorist groups could actually target a nuclear power plant. Such unforgettable events raised international attention for the need to strengthen nuclear security. As a result, the United Nation introduced the “International Convention for the Suppression of Acts of Nuclear Terrorism.” The IAEA also adapted the “Amendment to the Convention on the Physical Protection of Nuclear Material” in 2005. As well, world leaders presented their ideas to combat nuclear terrorism during a series of Nuclear Security Summits.

At this point, what answer we can give to the question, “Have we done enough?” A security guard was killed and his access card was reported stolen at Tihange nuclear power plant in Belgium in 2016. Also, In November 2015, Belgian police discovered that the terror cell that carried out the Paris attacks used a secret video camera to monitor an official at nuclear research sites with a wide range of nuclear and radiological materials. Terrorists seemed interested in making use of employees at nuclear facilities. Another incident that we should consider is the Germanwings incident in 2015. A copilot, who suffered from depression, crashed an airplane to the Alps Mountains while a captain left the cockpit for a moment. It is not a nuclear security event. However it is a reminder of what can happen when employees at nuclear facilities are connected in some way to a nuclear terrorist attack. Both these incidents require us to take closer look at our nuclear facilities.

When Korea took the International Physical Protection Advisory Service (IPPAS) mission in 2014, the IPPAS team advised the Korean government to develop a national framework for preventive and protective measures against insider threats. Our original focus was on threats from outside nuclear facilities rather than inside. Matthew Bunn and Scott D. Sagan pointed out that low-consequence facilities such as in the diamond industry or gambling industry consider insider threats more seriously than such high-consequence facilities such as nuclear power plants.

As the IPPAS team advised, we are working on developing a national framework against insider threats. It includes revising legal requirements, improving access control and contraband detection procedures to vital areas, and enhancing the nuclear security culture. In this paper, we would like to introduce our efforts to establish effective preventive and protective measures against insider threats.

1 Introduction

1.1 Nuclear Facilities in Korea

South Korea is heavily depends on nuclear energy. Thirty percent of the country’s electricity is generated by twenty four nuclear power plants. The nation also possesses a research reactor that is crucial for the production of radioactive isotopes for cancer diagnosis and treatments. When t temporarily ceased production in 2005, hospitals experienced a supply crisis.

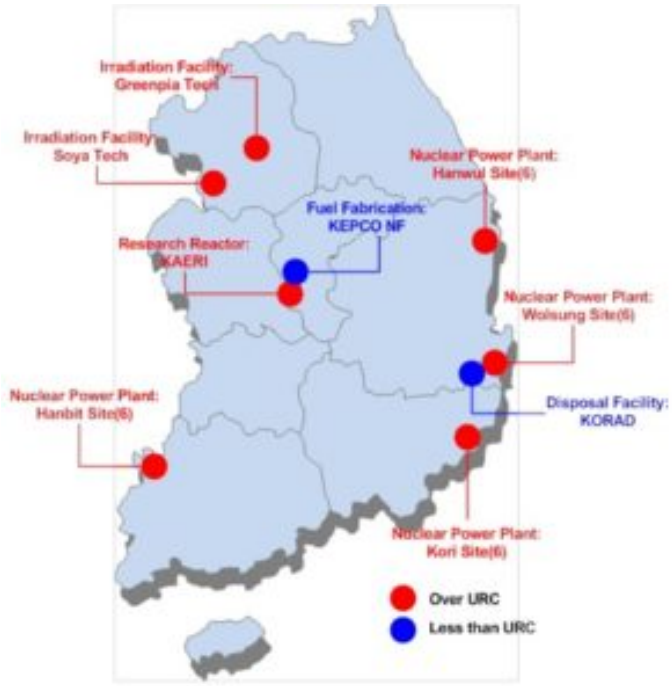


Figure 1. Nuclear Facilities in Korea

1.2 Radiological Consequence

Nuclear Facilities have become more controversial since the Fukushima Nuclear Power Plant accident in 2011. After five years, concerns over nuclear safety have not abated. The issue highlighted in 2016 when the biggest earthquake in Korean history struck one of country's nuclear sites in Kyung-ju. What makes the situation even worse is that nuclear power plants in Korea are located near populated areas. The Kori site itself (where six reactors are in operation, one in preparation, one under construction, two more under contemplation) has around 3.4 million residing within 30km. The Wolsung site also has around 1.3 million people living within 30km of the facility. In addition, a research reactor located in the middle of the fifth biggest city in Korea--with 0.3 million people located within a 10 km area.

The meaning of these population figures becomes more apparent by pointing out how less than 0.2 million people were evacuated from within a 20km area surrounding the Fukushima site.

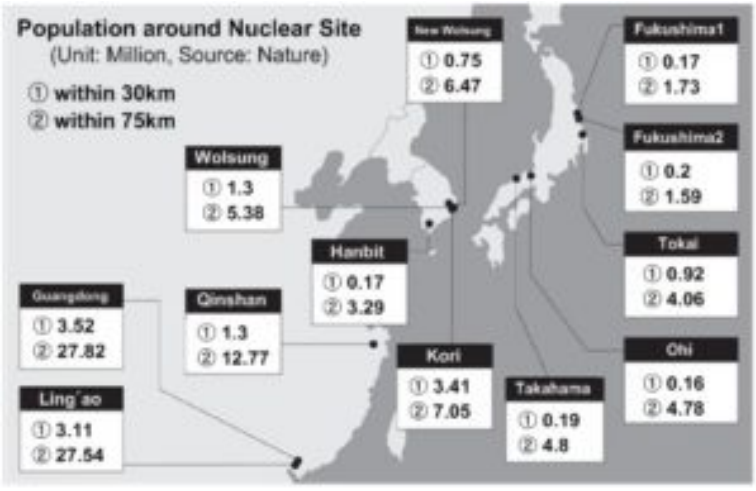


Figure 2. Population around Nuclear Sites

1.3 Legal Framework for Nuclear Security

Korea has strong legal framework to protect nuclear facilities against sabotage, as well as unauthorized removal of material. Three legislative acts regulate security at nuclear facilities. These include: the National Intelligence Service Act, the Act on Physical Protection and Radiation Emergency, and the United Defense Act. The National Intelligence Service Act and the United Defense Act are applied to not only nuclear facilities but also all national security target facilities including certain government buildings, military bases, and thermal power plants. The Unified Defense Act defines procedures to designate national security target facilities and requirements to prepare for war. The act outlines the government's role rather than operator. The National Intelligence Service Act prescribes a variety of regulations for operations of national security target facilities in peace time. Some of these regulations include employee trustworthiness requirements and information confidentiality obligation. The Act on Physical Protection and Radiation Emergency regulates specifically nuclear facilities. It is based on IAEA's recommendations. It mandates that the government set up a design basis threat for nuclear facilities; and outline the responsibility of operators to implement security requirement based on that design basis threat. These acts take broad range of threats ranging from insider threats to those beyond the design basis threat into account.

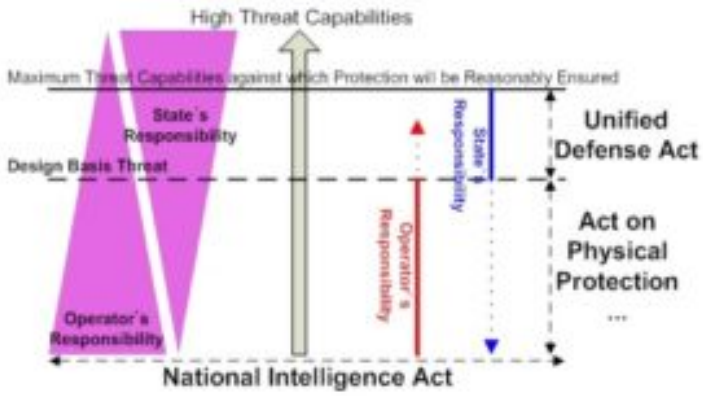


Figure 3. Legal Framework for Nuclear Security

Preventive and protective measures against insider threats described in the IAEA implementing guide (Nuclear Security Series No. 8) encompass such topics as trustworthiness assessments, escort and surveillance, confidentiality, and quality assurance. However, none of those acts outlined clearly define what insider threats are, nor do they clarify the relation between insider threats and those measures. As a result, when we took IPPAS mission in 2014, The IPPAS team advised us to develop a national framework against insider threats. In this paper, we would like to share our work by reviewing our legal system and implementation status regarding insider threats, as well as our efforts to improve them.

2 Insider Threats

2.1 Characteristics of Insider Threats

Dealing with an insider threat is challenging due to that individual's intrinsic characteristics--namely authority and knowledge. An insider can bypass physical protection measures, detection, as well as delay and response measures. Even though prevention and protection measures against insider threats are prepared, those measures often conflict with privacy or labor issues. To make matter worse, it is difficult for security managers to evaluate their limited measures by performance test. Such characteristics of insider threats are well explained in IAEA documents.

An analogy between an insider threat and cancer in the human body can be made. As cancer cells

are difficult to distinguish from normal cells before specific symptom appears, insiders in the guise of general employees can undertake malicious actions before anyone realizes. It is difficult to detect insider threats. Even if a threat is detected, response in a timely manner is another issue. Conventional detection, delay, and response measures of a physical protection system cannot be applied against insider threats.

Another challenging problem is “unintended insiders.” As cyber attack techniques become more sophisticated, anyone can unknowingly become an insider threat. Business assistants with a thumb drive might involuntarily be a passive insider providing valuable information from their business support system to an adversary. Maintenance workers for safety systems with a laptop computer could also breach security without being aware of their actions.

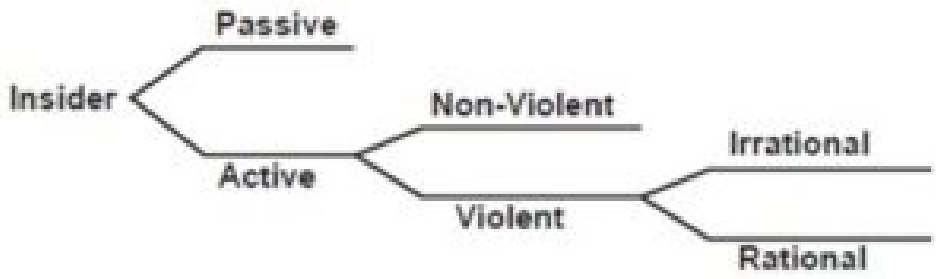


Figure 4. Categories of Insiders

2.2 Insider Threat Diagnostics

Deliberating on the characteristics of insider threats gives some insights on to create preventive measures. These measures include:

- Preventive measures in the first priority
- Protective measures ensuring on-the-spot and immediate response in the worst cases
- Prescriptive based approaches rather than performance based ones

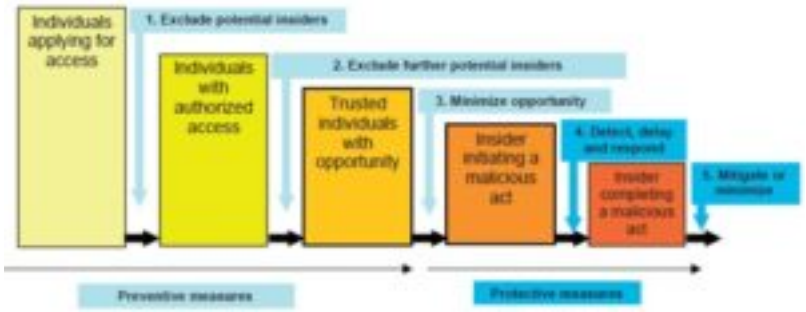


Figure 5. Preventive and Protective Measures against Insider Threats.

Considering the difficulty in responding to an insider threat, best way to deal with potential dangers is to prevent them from happening in advance. While we have planned implement the IPPAS mission’s recommendation, we have already reviewed current practices from all of nuclear operators. This review showed that preventive measures have already been implemented at power plants. However, the preventive measures are not well integrated because their legal basis does not specifically pertain to nuclear security.

Vital areas are also a major concern. A vital area is defined as an area inside a protected area

containing equipment, systems or devices, or nuclear materials which could directly or indirectly lead to high radiological consequences. Vital areas are potential sabotage targets for an insider Proper identification of personnel in these areas is an essential step in securing any facility. For instance, escorts and access controls are important measures for detection. Escorts are also a means for initial response during an emergency. Identifying optimum vital areas helps to implement those measures effectively.

From a technical point of view, we developed a vital area identification methodology based on a probabilistic safety assessment. We implemented a computer program called VIPEX (Vital area Identification Package EXpert), based on this methodology. The test was carried out in July of 2015 to identifying vital areas of APR1400--which is the recent nuclear reactor model in Korea. We decide to re-identifying vital areas with VIPEX for all nuclear reactors in Korea, including both in operation and under construction.

Along with reviewing preventive measures, we looked closely at protective measures against insider threats. We found some improvements required to access control points and contraband detection procedures at facilities. Mostly, we are revising escort requirements for accessing vital areas. We revised trustworthiness requirements to authorize unescorted access to vital areas. Also, we extended roles and responsibilities of persons with unescorted access right including discovery of insider threats and on-the-spot and immediate response to them.

We should approach an insider threat problem in a prescriptive manner. It is difficult to come up with performance criteria against insider threats. Since a conventional time line analysis is not quite suitable for insider threats (from detecting to responding against and insider attack). Insiders with authority and knowledge are able to take malicious actions as fast as possible or as slow as possible in order to avoid detection. Delaying measures are not effective to stop malicious actions since insiders have access rights. Finally, we conclude that preventive and protective measures against insider threats should be prescriptive regulatory requirements.

3. Current and Improved Measures against Insider Threats

Let’s look closely into current measures that we are implementing against insider threats in Korea. As mentioned before, we cannot find any definition regarding insider threats in our legal framework. However, most of measures stated in the IAEA implementing guide are already in use. In this section, we are going to review those measures currently implemented according to IAEA guidelines. This paper will also outline current assessment measures, including ways to improve them.

3.1 Preventive measures

3.1.1 Identity verification

Korea has a strong system for identity verification. According to the Residential Registration Act, the Korean government assigns a residential identification number to every citizen and collects personal information from biometric information--including a facial image and fingerprints. The government also issues a residential registration identification card to every citizen over 18 year old. Even though this system has sometimes caused social controversy, it is an effective system.

When he or she authorizes access to its facilities for their employees or contracted workers, a nuclear operator makes use of this governmental identification apparatus. A nuclear operator can request government issued identification such as an identification card or a residential registration document from an applicant. Then a nuclear operator can then ask local police to verify those documents and to provide a criminal background check on an applicant--according to National

Intelligence Act. A nuclear operator can also collect fingerprints for later verification.

3.1.2 Trustworthiness assessment

Several laws are in place to assessing trustworthiness. The National Intelligence Act dictates trustworthiness requirements when a nuclear operator hires new personnel. According to the act, a nuclear operator must conduct a background check for every applicant. The police provide criminal records for crimes defined in the decree. It is impossible for an applicant to gain employment if he or she has a criminal past. In addition, a nuclear operator is required to conduct medical and psychological examinations of every applicant, carried out under contract by an independent medical and psychiatric health hospital.

The Nuclear Supervision Act attempts to prevent corruption in the nuclear industry. This act requires police to present an employee new criminal records (depending on the severity of the crime) to his or her employer. Another requirement is that upper management should declare their yearly financial records; and that employees undergo health examinations every year. Moreover, according to Nuclear Safety Act requires drug and mental health tests for employees those who carry out safety critical jobs including reactor operators on a regular basis. All this information can be a tool for helping to recognize abnormalities and assess job qualification.

3.1.3 Escort and surveillance

The Physical Protection Act and Nuclear Safety Act regulate the use of escorts and surveillance. The Physical Protection Act focuses on access control to protective and vital areas. The Nuclear Safety Act concerns work supervision.

The Physical Protection Act requires facilities to have two types of access rights (as recommended in INFCIRC/225). One type is for unescorted access and the other escorted. The unescorted type grants access rights to nuclear operators, their employees, and the employees of their contractors working at the facility. Along with nuclear operators, their major contractors included government owned engineering and maintenance companies. Therefore, these workers had their security background checks carried out as described previous sections.

The Nuclear Safety Act requires that facilities designate a work supervisor to oversee temporary and unskilled workers who have not completed a security background check.

Escort and surveillance are measures that we are particularly interested in. A work supervisor is a main source of surveillance and an initial response resource for vital areas. We conduct close reviews of regulations and procedures to grant an unescorted access right and responsibilities. We determined three points for improvement: access granting procedures, qualification requirements, and the roles and responsibilities for those granted unescorted access.

The first area of improvement focuses on access requirements. In order to access vital areas in a nuclear facility, there are complicated as well overlapped procedures are taken into account depending on the type of regulation (as outlined in the Physical Protection and Nuclear Safety Act). One example is to grant access rights to a vital area. Workers to access vital areas are required to apply for work permit and access permit separately. Another example is record keeping requirement. Security regulation requires keeping access records to vital areas. Also, safety regulation requires keeping ingress and egress records with radiation dose level. Those record keeping requirements are compatible.

The next point of improvement involves the qualification requirements for unescorted access.

Trustworthiness standards are quite solid and strict for employees hired by a nuclear operator and its major contractors. However, the standards for others are not. Small contractors are not regulated under the National Intelligence Act. Trustworthiness of a worker for those small contractors is assessed when he or she applies for access rights to a nuclear facility. We find out that the qualification requirements for these workers are quite different depending on the type of operator. We need come up with minimum regulatory requirement for granting unescorted access. This seems a simple task, however it is not. We are still working on this matter.

The last point is to clarify the roles and responsibilities for those who have unescorted access rights. It is a regulatory requirement for those who have unescorted access rights to escort those who have escorted access rights. Those who have unescorted access rights are the main resource of surveillance and can initial a response when their charge encages in suspicious activities. Their roles and responsibilities require clarification. Also, we revised access grant procedure to include obtaining escort's agreement on the roles and responsibilities.

3.1.4 Security awareness

Nuclear security depends highly on the human factor. Security awareness for every employee in a nuclear facility is fundamental. Based on this understanding, it is policy to regulate a nuclear operator's security training and exercise according to the Physical Protection Act.

In the case of security training, all employers and employees nuclear at a facility should receive regular training. There are two types of training: one for physical protection workers, including security managers and guards, and the other is for everyone else. Physical protection workers are persons who have dedicated roles and responsibilities in a facility security plan. Those persons should be trained and qualified based on security training programs provided by the International Nuclear Nonproliferation and Security Academy (INSA) every year. The remaining personnel should be trained by a nuclear operator each year. Training courses provide education concerning a variety of topics, such as: the nuclear security culture, legal framework, threat assessments, physical protection system design and implementation, and contingency plans.

Security exercises should be performed at least three times per year. One of three exercises should be a force on force exercise and assessed by a regulatory body. These exercises are designed to test a contingency plan of a facility based on a design basis threat. Even though they are conducted with a limited number of facility personnel, exercises, especially force on force, indirectly but greatly help to enhance security awareness.

A survey examining nuclear security awareness is carried out on a yearly basis in order to evaluate the effectiveness of a facilities nuclear security policy. We developed a conceptual model to help prepare a security awareness survey. We designed a questionnaire for use in a survey based on a conceptual model and the IAEA's implementing guide on the nuclear security culture. Each year we conduct a survey on nuclear security awareness and organize a focus group interview with facility personnel in order to improve current nuclear security implementation.

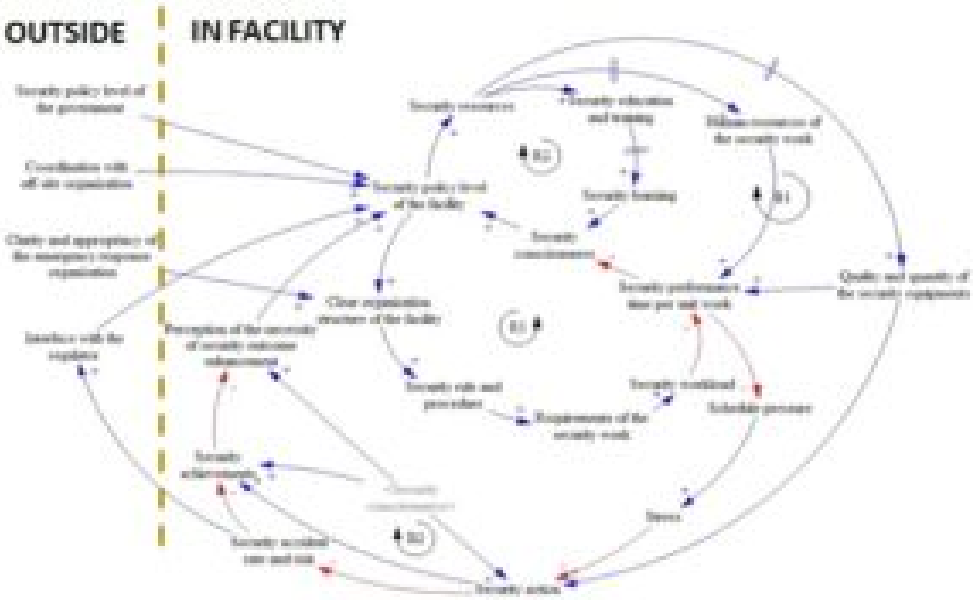


Figure 6. A Conceptual Model for Nuclear Security

A survey questionnaire consists of four parts: beliefs and attitudes, management system, leadership behavior, and employee behavior. We derived the awareness index from the answers on the questionnaire. Each part of the questionnaire has a different proportion reflected to the index, based on relations in the conceptual model. We have conducted surveys since 2010 and the results are shown in Figure 7. It is worth noticing that awareness indexes notably increased in 2012 and 2014. In 2012, security training and exercises were mandated--according to Physical Protection Act. In 2014, INSA was established and started to operate. The IPPAS mission was also carried out. We assume that those events had a positive effect on security awareness.



Figure 7. Awareness Survey Results

The Physical Protection Act requires regular analysis on a facility's security plan. According to this requirement, an operator must review its current security implementation including measures against an insider threat. During the inspection process, we provide an overview the results from an operator's review. An operator performs several drills including a contingency response. Operators must also monitor the actions of its employees when they receive suspicious e-mails. An operator conducts one form of cyber security drills by sending out an e-mail looking suspicious to their employees and monitors receivers' reactions whether they open, delete, or report it to a cyber security team.

3.1.5 Confidentiality (Security of Information)

Confidentiality requirements are defined in the National Intelligence Act. According to the Act, a nuclear operator must classify information into four categories. Information related to physical protection is usually categorized as confidential. Confidential information can only be accessed by authorized personnel. There are strict requirements for exchanging confidential information. For example, it is forbidden to exchange such material on public internet.

Due to a series of cyber security events, concerns over electronic information have grown. The most notable incident happened in December of 2014. At that time, a cyber terrorist called “Who Am I” released internal memos and design documents from nuclear power plants. Even though this material did not affect plant safety, this event stimulated public concern not only over nuclear security but also nuclear safety. After this incident, a reorganization of cyber security was made. The first change occurred when enterprise networks for nuclear operators were separated from public internet. Next, regulatory requirements for accessing business and plant control networks by operators were revised under the Physical Protection Act. Under these new revisions, operators must strictly control devices such as thumb drives and laptop computers that can access business as well as control networks. In addition, operators must now monitor data transmission using public or business networks. Moreover, we are developing a methodology to identify critical digital assets. This methodology is similar to how we identify vital areas in a facility using probabilistic risk assessment (PRA). We produce a sabotage logic model from the PRA model and then calculate candidates for vital areas. During this process we break down gates in the fault tree or event tree of the PRA model into systems. Then, we map those systems to actual areas in a facility. This process will be explained in a later section. Using this process we hope to derive critical digital assets by mapping systems into their dependent digital systems.

3.1.6 Quality assurance

3.1.7 Employee satisfaction

Employee satisfaction is managed according to two laws. One is for employees of an operator--regulated under the Worker Participation Act. The other is for employees of private contractors—regulated under the Small and Medium Sized Business Promotion Act. An operator must organize a grievance committee to resolve demands and complaints. Most of operators have an anonymous bulletin board system. An Operator at large facility, such as a nuclear power plant, should establish a growth committee to deal with contractor issues. The Ministry of Labor regulates these activities. How to regulate those activities from security point of view is still in doubt.

3.1.8 Physical compartmentalization of areas

The physical compartmentalization of areas is carried out by developing a methodology for vital area identification using PRA and VIPEX software based. We donated VIPEX software to IAEA in 2010. We tentatively applied the methodology to our recent nuclear reactor model called APR1400 in 2015. From 2016, we have gone through a regulatory review to re-identify vital areas of nuclear power plants in both operation and under construction. We are going to finish re-identification by 2018.

Our method is to build a sabotage logic model based on PRA models. In order to build a sabotage logic model, an internal PRA model should be modified with additional events and policy assumptions. Additional events should be considered, but not in the internal PRA model. The internal PRA model is a group of events that can cause core damage. However, a sabotage logic model is a group of events that can cause high radiological consequence (HRC) by malicious acts. Even though

a facility has radiological material inventories that can cause HRC, a sabotage event to the inventories is not an in internal PRA model since it did not case core damage. PRA models are built from a safety perspective not a security perspective. For instance, a malicious act to water tanks and cable trays are not in a PRA models. Those events should be added to an internal] a PRA model.

In addition, policy assumption should be considered when deriving a sabotage logic model. In order to prevent an HRC during a contingency response, it is important to decide as to whether or not random failures of the safety systems should be counted. Those policy considerations should be made and applied to a sabotage logic model.

Next, area information is required to build a sabotage logic model. Fire or flood PRA models anticipate the effects of fire or flood in a certain area in a facility. Hence, those PRA models have area information. We make use of area information to build a sabotage logic model.

After building a sabotage logic model, we have to consider the threat capability. In this step, we consider the number of vital areas that the threat is capable of destroying or disabling. Suppose the design basis threat is assessed to be capable of sabotaging four areas. This means we have to consider a target set with four area elements whose destruction by the threat can cause HRC. We are able to carry out this process using VIPEX.

The next step is to calculate a minimum cut set consisting of the number of area elements specified by the threat capability with a calculation engine called FTREX (Fault Tree Reliability Evaluation eXpert). The final step is to produce a prevention set. The target set is an attack sequences by adversaries that causes HRC. On the other hand, a prevention set is the lists of areas to prevent HRC due to sabotage. The prevention set is derived by applying De Morgan’s law to a target set.

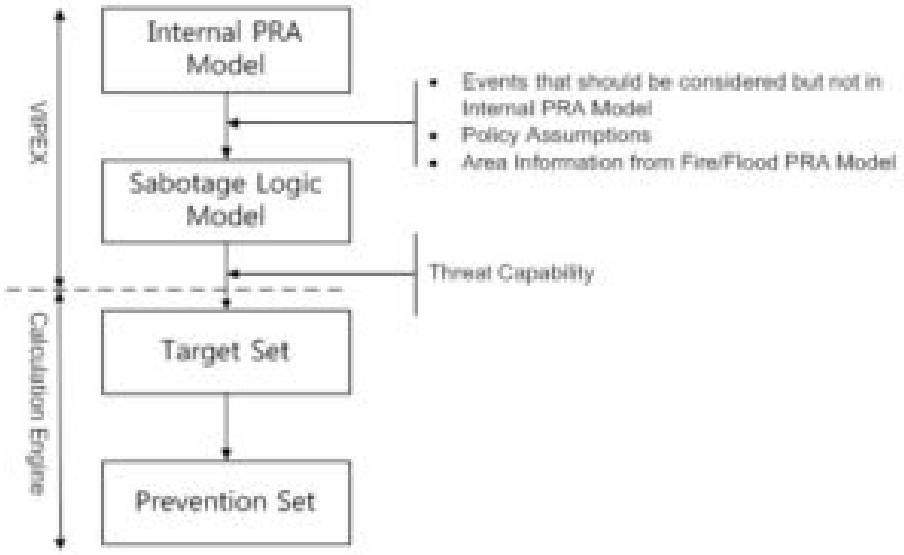


Figure 8. Vital Area Identification Process

In order to control access to vital areas, each vital area has two dedicated access rights: one for unescorted access and the other for escorted access. Each vital area is assigned to a certain division. The division manages access rights for its responsible vital areas.

3.1.9 Compartmentalization of activities

Requirements for compartmentalization of activities lie mostly with the Nuclear Safety Act. In order to carry out a safety analysis at a nuclear power plant, a plant operator must make use of a system called RIMS (RIsk Management System). This system is based on an internal PRA model with

information on safety system. When scheduling works, a work supervisor inputs equipments of the work subject to RIMS. RIMS considers those systems are disabled for the period of works and calculates overall risk probability for core damage. With the help of RIMS, a work supervisor is able to schedule works maintaining risk level. Therefore, the system keeps track of all works to equipments and quantifies a risk level of a certain work considering other concurrent works. A plant manager examines the risk level before he or she can give approval a work permit.

3.1.10 Sanctions

During the inspection process, we reviewed records for reprimand give to employees by operators. We reviewed the severity and frequency of these violations and assessed their level of punishment. We found out that some sanctions were too soft and that the punishment did not prevent repeated violations. Therefore, an administrative order was given to nuclear operators to reinforce their practice of sanctioning rule violators.

3.2 Protective measures

3.2.1 Detection

Detecting a malicious act perpetrated by an insider heavily depends on observation and surveillance. Even though vital areas are monitored by surveillance cameras, this detection equipment alone might not provide enough time for a proper response. Thus, we focus on the roles and responsibilities of persons having unescorted access. Unescorted access rights to vital areas should be granted to persons who are trusted and have qualified knowledge in order to be in that area. Employees are responsible for those persons that they are escorting. If he or she notices some kind of suspicious actions, he or she must report it and, if it is possible, take an initial response.

Another role for those staff members escorting persons is contraband detection. Contraband detection in Korea is mainly carried out at a main gate of a power plant by security guards. It is difficult to deploy security guards in front of every vital area. Our solution is for escort personnel to perform contraband detection on items carried by those persons in their charge. Items brought to vital areas are listed in approved work schedules. Escort personnel are able to perform this based on the list provided.

For contraband detection in front of vital areas, we have revised a regulatory guide for operators to specifically define contraband items. The revised guide categorizes contraband items are into three groups: harmful items, restricted items, and general contrabands. Harmful Items are those that should be reported as soon as they are detected. Examples of these items include firearms, bombs, ammunitions, and radioactive materials. Restricted items are defined as items that should be closely monitored, such as hazardous chemicals and flammable gas, since they can affect the safety and security of a facility. General contraband items, such as nonpowered hand tools, could potential be dangerous; however its effect is not significant. Those contraband items must be declared and approved before they are brought into a facility.

During our review, we realize that these role of Escort personnel is so important that it should be assigned as a formal duty. The duty must be formally granted and mutually agreed when an operator authorizes unescorted access.

3.2.2 Delay

Our improving effort to delay measures against insider threat is mostly related information security. Introducing delays to business networks, plant control networks, stand alone servers and clients for

security and safety systems are our main concern.

Our main goal is to separate business networks and plant control networks from public internet access. Plant control networks were designed to be independent networks. In this case, the connections between them should be limited and monitored.

During the review process, all connections between business networks and plant control networks were reevaluated. We revised a regulatory guide to only allow necessary data to be transmitted from plant control networks to business network via a one way channels. We strictly prohibit any control signal and data transmitted from business networks to plant control networks. We are still analyzing plant control networks on their dependencies. With the analysis results, we will introduce similar regulatory guidelines to plant control networks.

Even though networks are separated, there still remains a sneaker net. A sneaker net is a term used to describing information that is transferred by people carrying thumb drives or laptop computers. To defend against a sneaker net, we introduced physical delays to digital systems such as placing locks on cabinets and stoppers on data ports.

3.2.3 Response

Responding effectively to insider threats is challenging. The best strategy is to prevent it from happening in the first place. This would include use resources such as escort personnel. These escort personnel would be the first to respond in case of an emergency. As explained before, we are working on the roles and responsibilities of escort personnel and will introduce them into using proper access procedures.

The measures described in the previous sections are listed in Table 1. Emergency situations are not explained in this paper. The IAEA's implanting guide on insider threats mentions the fact that insiders could be members of the emergency response team. However, we have not figured out how to remedy this potential situation.

Table 1. Measures against Insider Threats

Preventive Measures	**Implementation**
Identity verification	□ When issuing access cards - Requesting public identification cards - Asking police for background checks - Collecting fingerprints □ When accessing protected areas - Requesting access cards and fingerprints □ Legal Basis - Residents Registration Act - National Intelligence Act

Trustworthiness assessment	□ Pre-employment checks - Checking past work history, criminal records, medical test, and psychological examinations □ Checks during employment - Requesting financial records for senior managers every year - Performing drug tests and psychological examinations for safety-critical employees every year - Updating employee criminal background checks by police □ Legal Basis - National Intelligence Act / Nuclear Supervision Act / Nuclear Safety Act
Escort and surveillance	□ Escort and surveillance requirements on accessing to protected and vital areas - Access rights: unescorted and escorted access - Escorting and surveilling by personnel authorized for unescorted access □ Legal basis - Physical Protection Act / Nuclear Safety Act
Security awareness	□ Security training and exercise every year - Security training and exercise for security personnel by INSA - Security training program for non-security personnel by operators - Conducting nuclear security awareness survey □ Legal basis - Physical Protection Act
Confidentiality	□ Information Security - Classifying information and managing it according to its classification - Regulating cyber security □ Legal basis - National Intelligence Act / Physical Protection Act
Quality assurance	□ Security inspections and review - By regulatory body and by operators □ Legal basis - National Intelligence Act / Physical Protection Act
Employee satisfaction	□ Employees for nuclear operators - Mandating to establish a grievance committee - Operating anonymous bulletin board system (BBS) □ Contractors - Mandating to establish an accompanied growth committee with contractors □ Legal basis - Worker Participation Act / Small and Medium Sized Business Promotion Act
Physical compartmentalization of areas	□ Vital areas - Regulating operators' vital area identification - Additional security measures on vital areas □ Legal basis - Physical Protection Act
Compartmentalization of activities	□ Work risk management - Analyzing work risk based on PRA model - Managing and scheduling work based on work risk analysis
Sanctions	□ Working on reinforcing sanctions

Detection	□ Intrusion detection sensors and surveillance cameras in vital areas □ Escorts, surveillance, and observation □ Legal basis - Physical Protection Act / Nuclear Safety Act
Protective Measures	**Implementation**
Delay	□ Security doors, equipment locks □ Legal basis - Physical Protection Act / Nuclear Safety Act
Response	□ Report and initial response by escort personnel □ Legal basis - Physical Protection Act
Emergency plans	□ Preparing emergency plans and performing emergency exercise □ Legal basis - Emergency Preparedness Act

Insider threats are particularly challenging due to detection and response limitations. Furthermore, cyber terrorism exasperates a situation since it makes use of unintended insiders. The more we deliberate on insider threats, the closer we can come to solving the problem.

4 Conclusions

The IPPAS mission provided us with a good opportunity to look deeply into this potential problem by developing a national framework for preventive and protective measures against insider threats. We reviewed current measures against insider threats and improved them. Our efforts focused on vital areas. We are re-identifying vital areas with a systematic methodology derived from the PRA. During this process, we re-evaluate current vital areas and a have better understanding of how to protect those areas. In addition, we reviewed current access control implementations and realized the importance of the roles and responsibilities of escort personnel. We revised regulatory guides on procedures for granting access rights and contraband detection. As well, we put much effort on cyber security. We introduce measures such as network separation, data monitoring, and sneaker net prevention.

Are these measures enough? It is difficult to say. It is important to understand that totally removing the potential for an insider threat is impossible. We do not have any other option except reducing the threat, yet not eliminating it entirely. That is the reason why we have to thoroughly implement and improve current measures.

III. REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State’s Nuclear Security Regime, Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, Vienna (2013).

[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).

[3] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[4] Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, Vienna (2011).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, Implementing Guide in preparation (NST021).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities, Implementing Guide in preparation (NST023).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Technical Guidance, IAEA Nuclear Security Series No. 4, Vienna, (2007).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No. 7, Vienna (2008).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, Vienna (2008).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use, and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, Vienna (2009).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, Vienna (2012).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, Vienna (2011).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-Assessment of Nuclear Security Culture in Facilities and Activities That Use Nuclear and/or Radioactive Material, Technical Guidance in preparation (NST026).

[16] KOREA ATOMIC ENERGY RESEARCH INSITUTE, The Application of PSA Techniques to the Vital Area Identification of Nuclear Power Plants, KAERI, Seoul(2004).

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/preventive-and-protective-measures-against-insider-threats-at-nuclear-facilities-in-in-korea/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org