CURRENT STATUS OF THE INSIDER THREAT IN THE NUCLEAR INSTALLATIONS IN THE ROK

Recommended Citation

Yongsoo Hwang, "CURRENT STATUS OF THE INSIDER THREAT IN THE NUCLEAR INSTALLATIONS IN THE ROK", NAPSNet Special Reports, September 29, 2017, https://nautilus.org/napsnet/napsnet-special-reports/current-status-of-the-insider-threat-in-the-nuclear-installations-in-the-rok/

YONGSOO HWANG

SEPTEMBER 29, 2017

In this essay, Yongsoo Hwang concludes that the “proper measures to prepare for the insider threat are not yet fully introduced for many countries. In fact it is not easy to detect, delay, and respond to

insider threats in a timely manner… Nonetheless, iterative approaches throughout planning, drills, and assessment are essential to set up the practical measures to mitigate the insider threat in the nuclear installation."

Yongsoo Hwang is Principal Researcher, Korea Atomic Energy Research Institute, Republic of Korea

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

Banner image: dry cask manufacture, from author

II. NAPSNET SPECIAL REPORT BY YONGSOO HWANG

CURRENT STATUS OF THE INSIDER THREAT IN THE NUCLEAR INSTALLATIONS IN THE ROK

SEPTEMBER 29, 2017

Summary

Since 911 and the adoption of the IAEA INFCIR225/Rev5, all the nuclear energy system companies have paid deep attention to secure the safe operation of the facilities against natural and man-made threats along with some hybrid events in combination of the both man-made and natural events. However, even though many good practical measures have been implemented against terrorist attacks such as the air craft kidnapping and collision to the nuclear installation and the missile attacks by sub-nation terrorist groups, still the proper measures to prepare for the insider threat are not yet fully introduced for many countries. In fact it is not easy to detect, delay, and respond to insider threats in a timely manner. In many cases it might be difficult to determine who would act as a potential people for the insider threat in reality. Nonetheless, iterative approaches throughout planning, drills, and assessment are essential to set up the practical measures to mitigate the insider threat in the nuclear installation.

Current Status

Even though the nuclear regulatory authority in the Republic of Korea has worked hard to tighten the nuclear security measures for the all nuclear installation in its territory, there as yet is no solid legal basis against insider threats in Korea. But the International Physical Protection Advisory Service (IPPAS) recommendation from IAEA in 2014 stipulated the need for prevention and preparedness against insider threats. In the report IAEA specifically defined the insider as people who have authority to access the nuclear installation and nuclear materials and have a certain intention to do sabotage and to initiate the illegal transfer of nuclear materials or to assist the intrusion of outside intruders. The IAEA emphasized the importance of proper mechanisms against insider threat in its report.

As mentioned before even though the comprehensive legal system to mitigate the insider threat is not yet fully developed in the ROK, certain critical achievements have been accomplished. The acts and the associated decrees and notices for the atomic energy safety and protection and

preparedness against emergencies in the nuclear installation define the key factors. Especially in the NSSC Notice for the Physical Protection, Article 2014-83 stipulates the key definitions for mitigation of insider threats. All key definitions in Korean regulatory systems are given as follows:

(1) Insider Threat Actors: Those who have authority to access sensitive information over nuclear materials and nuclear installation and have intention to illegal acts and to assist the outside malicious actors

(2) Adversaries: Those who plan and implement malicious actions. The adversaries might be either insiders or outsiders

(3) Malicious Actions: The attempts to create illegal intentional transfer of nuclear material, sabotages, and similar actions

(4) Illegal Transfer: The actions to receive, possess, use, alter, transport, dispose of, and diversify nuclear materials without any legal right

(5) Direct Sabotage: The actions to release nuclear and radioactive materials and their radiation using the external energy sources such as explosives and incendiary bombs.

(6) Indirect Sabotage: The actions to release nuclear and radioactive materials and their radiation using the latent energy sources such as heat and pressure. In such a case, the potential actors do not have to access the places for the application and storage of nuclear and radioactive materials. Malicious actors try to attack the safety related structures and systems or to disrupt the normal activities of key operators to achieve the mission success.

(7) Potential Malicious Actors: Those who work as special mission staffs such as physical protection managers, nuclear material management managers, security staffs, administrative workers, building management staffs, maintenance staffs or high ranking staff members have potential for the malicious actions later on. In addition those who work for the supply companies, emergency staff members at the fire stations and the emergency preparedness teams, inspectors and sub-contractors having the authority to access the installations and materials for malicious actions later on.

Important Features of the Insider Threat

The malicious insiders can have the following authorities and abilities to create the threat:

(1) Comprehensive and partly authorities to access the proper installations, systems, components and instruments,

(2) Authorities to operate installations and to control man-power at site,

(3) Ability to understand the layouts of installations, transportation mechanisms, physical protection, safety and security systems and the other sensitive information,

(4) Technical capabilities and good experiences, and

(5) Authorities and abilities to use instruments, systems, weapons, and explosives at the event of a malicious action.

Preparing and Mitigating the Insider Threat

The proper mechanisms to prevent the insider threat in advance and to mitigate its consequence in a

timely manner should it eventuate are totally different from those against external sabotage. The key two principles for the insider threat management are to a) prevent the event as much as possible and b), to detect in a timely manner when such has happened. To convert these two principles into the practical action plan, the following items should be considered as having the top priority:

(1) To exclude the potential insider threat malicious actors who have intention to enter the nuclear installations,

(2) To screen out malicious actors among people who enter the nuclear installations,

(3) To minimize the chance for a malicious action.

(4) To detect, deter, and respond a malicious action in a timely manner, and

(5) To mitigate a risk by a malicious action.

For the five items described above, the following action plan is required:

(1) Development of personnel security programs: These programs are essentials to eliminate the potential risk actors stipulated in the items (1) and (2).

(2) Authorizing the entry permits

(3) Systematic periodic background check-up

(4) Training for nuclear security culture and all other security issues

(5) Comprehensive control over the visitors

(6) Introduction of Human Reliability Program (HRP)

(7) Creating Physical Security Systems: These systems comprised of detection, delay, and response to reduce the possibility of successful malicious actions and require the following sub-systems:

(a) Entrance blockage systems such as physical barriers

(b) Intrusion detection systems

(c) Detection systems for dangerous goods

(d) Record management systems for all visitors and staff members

(e) Routine surveillance systems

(f) Security guards

(g) Emergency preparedness plans

(8) Material Control and Accountability Systems: These systems are effective to mitigate the malicious actions listed as items (3) and (4) from the insiders. Transparent and well organized operation of MC&A systems and minimization of storage spots for the nuclear materials act as practical measure to prevent the insider threat in the real installation.

Approach to Mitigating the Insider Threat

The most important action to prevent the insider threat is to introduce a tightened security check-up system. The ROK which is confronted with the constant threat from the DPRK has implemented the thorough national security check-up system at the stage of recruiting new employees for important government operated entities. However, the lack of the comprehensive periodic security re-check-up when staff members join the entities creates another concern to prevent the any attempt for the insider threat. At nuclear power plants, the pre-recruitment security check-up is comprehensive and solid. But these days to identify the proper credible operators are not an easy mission because of the nature of the operator's duties. But to overcome the difficulty KHNP, the regulatory body and the power company, would like to implement the following principles:

(1) To prevent any possibility of insider threat, thorough security check-up is fully implemented for all new staff members at the stage of recruitment.

(a) To identify all potential malicious actors the new staff members are required to pass through the *official security check-up at the stage of the recruitment*.

(b) *During the recruitment processes, intensive interviews and aptitude tests are to be implemented for all applicants*. Those who will be hired and the staff members for the potential sub-contractors are to be cross-checked by the employers for their general features, credibility and good reputation by all means.

(2) To screen out potential malicious actors from the existing staff members, the following step is to be implemented

(*a) Comprehensive periodic security check-up and the introduction of better working environment:* The following up security check-up for every five year is essential to screen out the potential malicious actors. In addition to enhance job satisfaction for all key staff members, the better working environment, the systematic on job training, effective fringe benefit systems are to be implemented along with a solid program to minimize the discontentment from staff members.

(3) Periodic training to disseminate the nuclear security culture

(a) Initial phase training: This is the course for the newly recruited staff members covering personal security enhancement measures, information security management, physical security management and the other matters if any along with general procedures to enter and retry from the working spots inside the nuclear installation and the special accompany processes with other staff members to perform a specific mission. It also covers the list of all banned goods for staff members at the facility and the proper reporting mechanisms for all security related issues.

(b) Training to acquire a pass to enter a vital area: Those staff members who will get the authorization to enter a vital area and to access the nuclear materials and sensitive information are to pass this training course covering information security management, physical protection measures on special nuclear materials, detailed reporting and confirming measures on these issues, penalties against any action to violate security procedures.

(c) Annual training over physical protection and nuclear security awareness: Those who possess the authority to access a vital area and a nuclear material handling area should take a special course over the physical protection. All others are to attend the annual training course covering the policy and processes on the physical protection, good examples on the recent nuclear security related incidents, natures and lessons of any accidents related with physical protection

if any, characteristics of natures in physical security threats and the general procedures over the security matters.

(d) Job Shift/Retirement Training: Those who are free from the missions related to a vital area and nuclear material management and about to retire are to take a special training course covering hand-out of all passes, special education not to release special information learned from the nuclear installation, and writing up a special memo of intent swearing the will to observe all security procedures even after the retirement.

(4) Implementation of Human Reliability Program (HRP)

(a) This HRP covers all the spectrum of activities from the employer to tighten the security measures for all staff members throughout the consistent comprehensive medical check-up, monitoring managers, and security awareness check-up. To accomplish this mission, all managers are required to perform the so-called human reliability management programs for their staff members to prevent any potential abnormal actions by their team staff members. The basic job actions under the control of the HRP are as follows:

- Job missions to manage, protect, and transport the Category I nuclear material

- Job missions taken by nuclear reactor operators

- Job missions which creates a big impact over physical protection

(b) Medical check-up: All newly recruited staff members are to pass through medical check-up to find out any potential problem over the psychiatric issues and the drug problems. It is consist of the general check-up, drug tests, and mental disorder screening

(c) Non-regular management by higher ranking staff members: The managers are responsible for frequent and non-regular check-up to monitor their team staff members over severe alcohol and drug dependency, mental and physical weakness deteriorating normal performance, clear mental disorder rated with the mental control difficulty, melancholy, sudden and mental disruption, severe stress and its side effects, bullying and physical violence against neighboring staff members, irresponsible mission accomplishment and intentional determination problems, and intentional violation against safety, security, and physical protection related with activities in the operation of nuclear installations.

Practical Implementation

To prevent the malicious actions by insiders the following measures are to be implemented at all nuclear installations:

(1) Producing official passes & badges

All staff members and workers from sub-contractors and official visitors should bear appropriate passes/badges which clear state the authority level to access specific buildings and sites by color and code. The photos and the other information to clearly identify all members are required for any pass/badge.

(2) Wearing official passes/badges: All the workers and visitors at nuclear installations are to wear ID on their chests clearing showing the clear photo of each individual. When there is significant alteration over the outlook of each member such as the change of hair style, wearing glasses and other distinct alteration, the existing ID is to be replaced immediately for the security check-up. Or

any damaged ID’s should be replaced by the appropriate security office.

(3) Record keeping for official passes/badges: All the relevant records should be managed by the responsible offices. The key information such as the ID number, the date of issuance, the bearer’s name and department, and the date of termination of the ID should be permanently recorded. Also, all the information on the lost badges/passes should be recorded. To prevent malicious reuse of all lost ID’s the appropriate measures are to be implemented comprehensively by all related departments. Upon the notification of the lost event the proper information is to be shared among security officers including the chief of the security guards. The list of all lost events, recording log-inn to the management system and the limiting the re-issuance of the ID’s for the frequent losers are implemented for the security enhancement.

(4) Class of official passes/badges: The passes/badges are authorized to specific accessing staff members to the facilities. Those who clear security check-up are free to access the sensitive information and installations. The number of staff members accessing a vital area and special nuclear materials is minimized. Also, the time zone to access a vital area and special nuclear materials are well under the control of the security office.

(5) Visitor access

All the visitors whose background information is fully checked are to be admitted to the installations. The qualified visitors who individually access the installations are to be fully escorted by appropriate staff members. Those appropriate staff members guiding the visitors are to observe the following procedures:

(a) The guiding staff member is to be familiar with all detailed steps to accompany a visitor.

(b) The guiding staff member is to be well known a visiting destination and its security nature and the stored nuclear materials.

(c) The guiding staff member is to be familiar with the visitor’s intention, the mission that the visitor plans to accomplish during the facility visit, and to immediately recognize any abnormal action by a visitor during the campaign.

(d) The guiding staff member is to follow the assigned routes to reach the destination spot inside the installation.

(e) The guiding staff member is to discuss the matter pre-approved by the manager with a visitor.

(f) The guiding staff member is not to visit any unauthorized building and site with a visitor.

(g) The guiding staff member is to obey all appropriate security regulations, and

(h) The guiding staff member is responsible for immediate reporting to the security guards in case of any emergency.

(6) Security concern by staff members during the presence of a visitor

(a) All staff members are to pay attention to the possession of the passes/badges of visitors.

(b) All staff members are to pay attention to the presence of a guiding staff member for a visitor.

(c) All staff members are to pay attention to the strange will of a visitor regarding an unauthorized area and information

.(7) MA&C

To minimize the illegal acquisition and transfer of nuclear materials, comprehensive material accounting and control is essential along with thorough monitoring of storage of materials at designated spots.

(8) Operation management

The appropriate management of job missions at a vital area and the nuclear material management spots are practical ways to reduce the insider threat. During the pre-review of the job mission, the time span, the work content, and the assigned staff members are clearly reviewed. This mission also contributes to minimize human errors.

(9) Operating the inside threat monitoring systems

All physical protection systems such as barriers, intrusion detection, dangerous good detection, entry control and surveillance contribute the reduction of malicious actions by insiders. The comprehensive confirmation by managers during the upgrade, correction, and replacement of critical assets are needed to further prevent the insider threat.

(10) Quality Assurance (QA) over nuclear facilities

The proper QA means the pre-confirmation of plans and management processes over the activities in the nuclear installation. All the needed work procedures, the roles of the assigned workers, and the work scopes are to be set up in advanced and confirmed through the document review. Throughout this arrangement, all the work steps can be clearly confirmed in a timely manner at the site. It acts as the practical mechanism to prevent the potential insider threat actions at each step of the job mission.

Principles to Manage the Insider Threat

To effectively detect, delay and respond against the potential insider threats in the nuclear installations, the following principles should be fully implemented at the site.

(1) Two person co-worker principle

At least two co-workers are at the site to perform a job mission at the nuclear material management site and a vital area. This will significantly reduce the potential for malicious action by one insider and enhance the timely detection of such malicious action.

Multiple workers are to work together at all times and all the members are to fully understand the detailed job missions to identify any malicious action by the other worker in a timely manner. All the proper procedures are to be stipulated so that all the security guards at a vital area follow this principle.

(2) Tracing the work location of assigned workers

Proper sensors are used to monitor the exact locations of assigned workers at a vital area and the nuclear material handling spots. The information from sensors can check whether only authorized workers are at assigned jobs and whether the distance between co-workers are not so far away from

each other to assure the security. It will help alarming in real time so that the security guards can access the reported spot quickly. The entire workers' location records and their entry information are to be stored at the centralized data management system so that when the abnormal accident occurs these data can be used for detailed analysis.

(3) Manager monitoring

Managers monitor the change of action patterns of their team staff members and encourage the proactive actions by their staff members to prevent the potential insider threat. Managers are responsible for checking the duration of a team staff member at a sensitive area and confirming the reason for that action.

(4) Limiting the entrance doors for a vital area

The number of the entry ports for a vital area is to be minimized. All movements of illegal goods and nuclear materials at the entry ports are strictly prohibited by all means.

(5) Operation of inspection equipment for banned and radioactive substances

Proper detection equipment such as X-ray detectors are to be installed at the entry port against malicious actions by actors. The high quality detectors are installed at the exit points for the nuclear material storage facilities. All the passengers to the concerned facilities are to be cleared by the on-site security guards.

(6) Limiting the manipulation of physical protection systems by not assigned staff members

Physical protections systems inside nuclear facilities are vulnerable to the illegal manipulation by malicious insiders. These systems are designed to avoid such a malicious functioning. Whenever these systems are operated by non-assigned insiders the warning signal should be immediately delivered to the central command center. The fiber optics information network system is best suited to avoid any malicious interruption by insiders. The periodic inspection over the sensors and the information networks are essential to prevent the potential disasters. In addition, the comprehensive procedures are to be established so that only authorized staff members access the area with installed physical protection systems.

(7) MA&C

The comprehensive material accountability and control is to be implemented to prevent the illegal transfer of special nuclear materials, sabotage and any potential pre-threatening actions by insiders. All the material management missions are pre-formed by pre-set processes and the time schedule along with all detailed work assigned for all individual staff members.

(8) Management of extra parts

All the extra parts and their storage facilities in a vital area are under the surveillance of security guards. If not insiders can manipulate with malicious will extra sensors and pumps, which will significantly damage proper operation of key safety and security systems in a vital area.

(9) Response to the malicious insiders

Even though it might be practically difficult to identify a passive malicious insider, to mitigate the potential risks all actions over reporting, investigation, prosecuting the insiders, identifying the risk and limiting its consequence is the key to reduce the insider threat.

For the active malicious actors the immediate action plan against any abnormal action is to be fully prepared. For the non-physical actions, the neighboring workers are to be well trained to stop those actions. For physical violence, the neighboring staff members are to be trained to report immediately to the security guards nearby.

These counter-actions should be accomplished with a very short time to mitigate the risk. Also to prevent the illegal transfer of nuclear materials from an installation to the outside, the combined team effort among the security staff members at a facility along with military and police is essential. All measures should be implemented to prevent any movement of sensitive materials from the border of the facility.

The comprehensive emergency preparedness action plan is to be established among all concerned security entities. Then, detailed investigation of any attempted malicious actions will give good lessons to solidify the upgraded security plan.

III. REFERENCES

1) “Preventive and Protective Measures against Insider Threats”, IAEA Nuclear Security Series No. 8, Vienna.

2) INFCIRC/255/Revision5, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities”, IAEA Nuclear Security Series No. 13, Vienna.

3) Insider Analysis, Sandia National Laboratory, 2014

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/current-status-of-the-insider-threat-in-the-nuclear-installations-in-the-rok/

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