A New Physical Protection System Design and Evaluation Process

Heoksoon Lim [a*], Myungsu Kim [a], Yeongkyoung Bae [a], Janghwan Na [a]
[a]*70, 1312 beon-gil, Yuseong-daero, Yuseong-gu, Daejeon, 305-343, KOREA*
[*]*Corresponding author: lhs6169@khnp.co.kr*

1. Introduction

Since the attack on the World Trade Center on September 11, 2001, the security-related budget has been rapidly increased in the United States in order to enhance physical protection level of nuclear facilities. Furthermore, International Atomic Energy Agency (IAEA) had established security-related department and has been strengthening security measures against possible sabotage. IAEA enforces the recommendations for the physical protection of NPPs in the INFCIRC/ 225/Rev.5 [1] to the member states and U.S. NRC also enforces the similar requirements in 10 CFR 73.55. Thus, in order to let Korean NPPs meet the new requirements in INFCIRC/225/Rev.5 or U.S. NRC requirements, Korea nuclear licensee should develop or establish appropriate physical protection system (PPS) design methods for the physical protection of the operating NPPs and new NPPs. KHNP is doing the project of "Development of APR1400 Physical Protection System Design (2012~ 2015, KHNP/KAERI /KEPCO E&C)". This paper describes overview of a physical protection system (PPS) design and evaluation for an advanced nuclear power plant.

2. Physical Protection System Design Methodology

The two main design considerations for a PPS are the prevention of (1) onsite sabotage of material resulting in radiological release and (2) theft of nuclear and/or radioactive material. So, this methodology, which was development by Sandia National Laboratories for Department of Energy (DOE), focuses on nuclear facility security and utilizes approaches consistent with standards, recommendation and guidance. This section describes the overview of entire design, evaluation process, design consideration, and system effectiveness.

2.1 Define PPS Requirements

Design of a PPS begins with defining system requirements (see figure 1). The requirements establish the basis for how PPS should perform. This step involves facility characterization, target identification, and threat identification

- Facility characterization: as part of characterization, the designer should obtain information on the physical layout of a facility, operation and mission of a site, and information regarding security and safeguard policies and procedures. Characterization information can come from sources such as facility drawings, site tours, as well as interviews with staff and management.

- Target identification: Understanding what the site is protecting is essential to an effective system. The analyst must understand the configuration of material, when stored or in use at a facility, as well as material consequence values, material locations, amount and composition.

- Threat definition: The characterization of the threat an important notion with a wide impact. The threat influences the design of a PPS and, therefore, the analysis outcome. Designing a PPS without a specific threat strategy in mind could potentially place a facility's infrastructure, material and personnel at risk.

This design and analysis process, emphasizing determination, design and evaluation, is illustrated in Fig.1

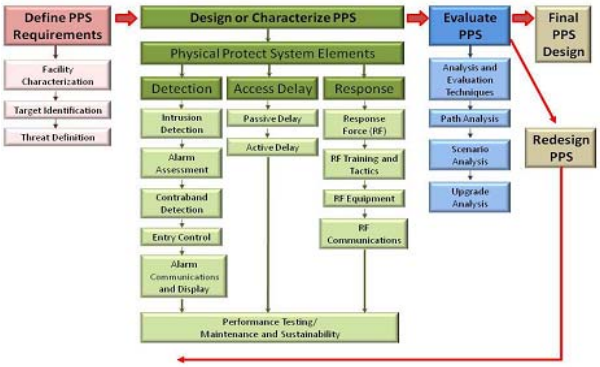

Fig. 1. Overview of performance-Based Design and Evaluation Process

2.2 Design of a Physical Protection System

The purpose of a PPS is to prevent an adversary from successful completion of a malevolent action through the use of assessed detection, delay, and response. All three functions are equally important, and all must be present for an effective system. An important design goal is to ensure detection as early as possible, followed by sufficient delay to allow a timely response by the response force.

- Detection assessment: A detection design goal is to have uniform and balanced detection around the entire length of the perimeter. Normally, a minimum of two continuous lines of detection is used in high security systems. Better performance can be achieved by selecting different and complementary sensors for the multiple lines of detection, e.g., microwave and active infrared within an isolation zone. Proven, mature technologies can provide a high probability of detection, but require consideration of multiple design criteria including terrain features, environmental conditions, and false alarm rates/nuisance alarm rates; design vulnerabilities; installation factors; and integration with other technologies and systems.

- Delay: Delay elements are effective only if they occur after detection and assessment. Delay before detection serves no purpose because the adversary can take a long time to breach protection elements without fear of detection. Each defensive layer must have balanced delay, meaning it would take an adversary the same amount of time to breach a wall, a door, or an isolation zone. Security layers that are not balanced allow an adversary to exploit the weakest delay elements and bypass the strongest delay elements in the adversary path.

- Response: An effective response is defined as a sufficient number of response force personnel deploying at an appropriate location in a timely manner to stop, or interrupt, the adversary's progress. This timely response relies on early detection, assessment, and sufficient delay to allow the response force to interrupt the adversary. The response force must maintain situational awareness during their response in order to perceive and interpret events as they unfold so that they can forecast potential near-term events and respond accordingly. Proper situational awareness helps the response force become mentally and/or physically prepared to stop the adversary's progress. A response force should have more personnel, be better equipped, and be better trained than the DBT in order to successfully neutralize an attack.

2.3 Evaluation of PPS Design

The evaluation process typically uses computerized assessment tools to assess competing timelines or the effectiveness of the response force against a specific threat. Depending on the level of analysis rigor required, several assessment options are available to the PPS designer. For instance, if the designer is interested solely in determining the weakest path, a path analysis tool will suffice. If the designer is interested only in determining the effectiveness of the response force in relation to its weapon set, procedures, and tactics, then a Force-on-Force tool is appropriate. The use of multiple tools is recommended for reliability and confidence in analysis results. In addition, it is important to maintain and use performance estimates consistently across all tools. For example, analysis results cannot be compared if the RFT input differs in each tool.

Results are provided as system effectiveness in the context of risk, how effective is a facility's detection, delay and response systems in protecting target material against an attack by a specific threat. The facility owner or manager then judges whether the resultant level of risk is acceptable or if improvements must be made. For example, because of the economic and political consequences of a successful attack, the facility owner or manager might adopt an acceptability risk metric of less than 0.2 for conditional risk, based on joint team discussions and agreements. Table 1 provides an example of risk descriptors given the risk value calculated in the analysis. This table describes the PPS requirements for the associated risk value.

Table 1. Risk measure for Physical Protection System

Risk Descriptor	Quantitative Value	Requirements for PPS
Low Risk	< 0.2	PPS deemed effective, improvements not required
Moderate Risk	0.2 to 0.35	Improvements to be recommended for PPS
High Risk	> 0.35	Specific PPS upgrades and/or consequence mitigation features required to reduce risk level

2.4 Integrated Security Plan

The Security Plan includes physical security, training, and qualification of security personnel, safeguards contingency plans, and these together describe a comprehensive physical security program for an advanced NPP design. The Security Plan addresses how regulatory requirements in each of these three areas are met for an advanced NPP design.

The Security Plan also describes measures that are taken to meet regulatory performance objectives to ensure that the overall level of system performance provides high assurance of the protection against the established Design Basis Threat (DBT) of radiological sabotage.

3. Conclusions

It found that a new physical protection system (PPS) design and evaluation. KHNP is doing the project of Physical Protection System design according to U.S. NRC requirements and IAEA requirements in INFCIRC /225 /Rev.5 and will complete by 7.31, 2015 for development of APR1400 Physical Protection System. After completing this project, the results of project are expected to apply new NPPs.

Acknowledgement

This work was support by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) grant funded by the Korea government(Ministry of Trade, Industry & Energy) (No.2012T1002011558)

REFERENCES

[1] Garcia, Mary Lynn. 2001. The Design and Evaluation of Physical Protection Systems.
[2] Garcia, Mary Lynn. 2006. Vulnerability Assessment of Physical Protection Systems.
[3] IAEA (International Atomic Energy Agency). 2002. Handbook on the Physical Protection of Nuclear Facilities, IAEA-TECdoc-1276, Vienna.
[4] IAEA (International Atomic Energy Agency). 2011. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225 /Revision 5), Nuclear Security Series No. 13, Vienna.
[5] Woo-Sik Jung, Integrated Physical Protection System Design of Nuclear Power Plants in Korea
[6] NRC (U.S. Nuclear Regulatory Commission). 2013. Implementation Guidance for 10 CFR Part 73, Washington, DC: US Government Printing Office.