Transactions of the Korean Nuclear Society Autumn Meeting
PyeongChang, Korea, October 30-31, 2008

Physical Protection System (PPS) Design Processing and Test Bed Design for testing a PPS

Jounghoon Lee*, Jung-Soo Kim, Jae-Kwang Kim
Korea Institute of Nuclear Nonproliferation and Control, 119 Munji-Ro, Yuseong-Gu, Daejeon, Korea
**Corresponding author: jhlee@kinac.re.kr*

1. Introduction

The potential of a malicious act involving nuclear or other radioactive materials is a continuing worldwide threat. Existing data indicates that when nuclear or other radioactive materials are left uncontrolled or in unauthorized circulation, they become vulnerable to theft [1]. Under these circumstances, the Korean government has enacted a new law protecting nuclear facilities and materials. However, in Korea, there is little experience in designing, testing, and analyzing a physical protection system (PPS) for the protection of nuclear facilities and materials. In this paper, we will discuss the PPS design method and its influence on Korean PPS design methods.

2. Physical protection system design method

In this section, the method used to design a PPS is described. This method was developed by Sandia national laboratories. Figure 1 shows a PPS design and evaluation process outlined.

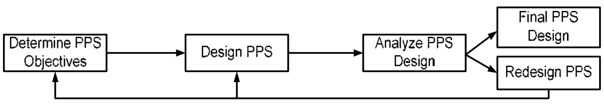

Fig. 1. Design and evaluation process outline

2.1 Determine PPS objectives

The first step in the development of a PPS design is to determine the objectives of the PPS. To formulate these objectives, the designer must understand a facility's operations and conditions, define the threat, and identify the targets.

Facility operations and conditions that characterize a facility include: the location of the site boundary, building location, building interior floor plans, and access points. A description of the activities taking place within the facility is also required, as well as identification of any existing physical protection features.

Next, a threat definition for the facility must be made. Information about an adversary's tactics and capabilities must be collected. Adversaries can be separated into three classes: outsiders, insiders, and outsiders in collusion with insiders. For each class of adversary, a full range of tactics should be considers such as: deceit, force, stealth, or any combination of these. Important capabilities for the adversary include: knowledge of the PPS, level of motivation, any skills that would be useful in the attack, the speed with which the attack is carried out, and ability to carry tools and weapons.

Finally, identifying potential targets with in the facility should be performed. The attractiveness of the target determines the measure and method of protection that will be applied to the facility.

2.2 PPS design

The next step in the process is to determine how best to integrate elements such as fences, sensors, vaults, procedures, communications devices, and protective force personnel into a PPS that can achieve protection objectives. The primary functions of a PPS are detection, delay, and response.

The detection function in a PPS includes exterior and interior intrusion sensors, alarm assessments, entry controls, and the alarm communications and display subsystems all working together. An effective PPS must first detect an intrusion, generate an alarm, and then transmit that alarm to a location for assessment and appropriate response.

The second function of an effective PPS is delay. Slowing an adversary time allows for the desired assessment and response. This delay is effective only if it follows detection. Increase in adversary task time is accomplished by introducing impediments along all possible adversary paths to provide sufficient delay for any suitable response.

The final function of a PPS is response. There are many ways to response to a security event, and these will relate to two important and interrelated factors. The first is the time it takes for the desired response to be placed into effect. The second is the effectiveness of that response.

2.3 PPS design analysis

Analysis of a PPS design begins with a review and thorough understanding of the protection objectives that the designed system must meet. Analysis of a PPS design will either find that the design effectively achieved the protection objectives or else the analysis will identify weakness. Analysis can be performed by two basic methods, required features and performance measures. Required feature analysis simply means that the specified features such as intrusion detection, entry control, access delay, response communications, and protective force exist. However, a PPS design based on required features cannot be expected to lead to a high performance system unless those features are sufficient to ensure adequate levels of protection. More sophisticated analysis and evaluation techniques, based on performance measures of system components, can be used to estimate the effectiveness achieved by a PPS.

2.4 Final design

If the protection objectives are achieved, then the design and analysis process is completed. However, a PPS should be analyzed periodically to ensure that the original protection objectives remain valid and that the protection system continues to meet them.

2.5 Redesign of a PPS

If a PPS is found to be ineffective, vulnerabilities with in the system can be identified. The next step in the design and analysis cycle is to redesign or upgrade the initial protection system in order to correct the noted vulnerabilities. As well, it is possible that a PPS's objectives need to be reevaluated. As the analysis of a redesigned system is performed, the cycle will continue until the results indicate that the PPS has met the protection objectives [2, 3].

3. Test-bed design for testing PPS

Korean nuclear power plants have three levels of borders. One is military line of defense, because Korea is a divided country. Another two borders are under facility's control.

An analysis on the physical protection systems of nuclear power plants is needed, because these borders are designed without a physical protection system concept. The detection and delay systems are especially more vulnerable than the response systems. Actually, six vulnerabilities of detection systems and seven vulnerabilities of delay systems were found out at a periodical inspection during last three years.

We have a plan for making a test-bed. (A test-bed is a platform for experimentation for testing the detection and delay systems.) An existing PPS at an operational facility cannot normally be fully tested as a system. Because direct system tests are not practical, evaluation techniques are based on performance tests of component subsystems. Component performance estimates are combined into system performance estimates by the application of system modeling techniques. Therefore, we will make a test-bed.

Using a test-bed, we can produce a proper PPS for a renewal design basis threat (DBT). Every three years, Korean government must set up a renewal DBT, and facilities should make a PPS according to the DBT. This test bed data can assist the facilities which can not design and analyze the PPS.

Figure 2 shows the schematic design of our test-bed system. This system is 6m wide, 15m in length, and 3m high. It has fences, microwave sensors, infrared ray sensors, and CCTV as similar type of real nuclear facilities. It was designed with PPS design concept.

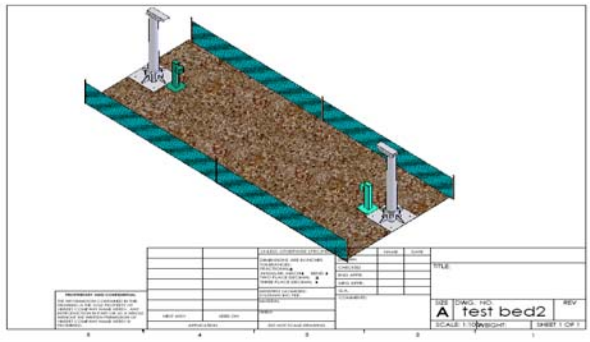

Fig 2. Test-bed system outline

Considering the Korean physical and environmental conditions such as topography, wildlife, background noise, climate and weather, the test-bed system is ready for construction. The construction will be completed at the end of 2008, and it will be operational by 2012.

4. Conclusions

Because of testing PPS, we will set up the test-bed. We expect that it can produce detection probabilities, performance criteria, environment conditions, maintenance methods, and databases. The database from the test-bed test will be used for the whole physical protection system analysis. This data, also, can be used as a criterion for these systems. It can be used at developing inspection equipments, as well, and verifying a design basis threat.

REFERENCES

[1] IAEA, Board of Governors General Conference GOV/2008/35-GC(52)/12, "Nuclear Security Report 2008", 22 August 2008.

[2] Sandia National Laboratories, "Technology Transfer Manual, Exterior Intrusion Detection", 30. September 1999.

[3] Mary Lynn Garcia, "Vulnerability Assessment of Physical Protection Systems", Sandia National Laboratories, 2006.