Proceedings of the Korean Nuclear Society Autumn Meeting
Taejon, Korea, October 2000

Development of a Vulnerability Assessment Program for Domestic Use

Hyun-Chul Lee, Jin Soo An, In-Koo Hwang, Eun Ho Kwack

Korea Atomic Energy Research Institute
P.O.Box 105, Yusong,
Taejon, Korea, 305-600

Abstract

The physical protection system (PPS) design process includes the vulnerability assessment phase to validate the performance of the designed PPS. The direct evaluation of a PPS consisting of a lot of detection, delay and response elements, requires a large amount of resources (time, manpower, cost, and so on) thus it is an impractical approach in most cases. However, an appropriately developed vulnerability assessment program demands less resources for the PPS design evaluation and provides useful information on PPS improvement. This paper describes the functional requirements, technical considerations, development plan, and conceptual design of a vulnerability assessment program for Korean PPSs.

1. Introduction

Since the 1970s, the IAEA has announced the INFCIRC/225 series[1] and IAEA-TECDOC-967[2] to call upon the Member States to strengthen their physical protection systems against illegal transfer, theft, and sabotage by various adversaries. In addition, each Member State has the responsibility of implementation and maintenance of physical protection systems in its country.

As the power demand in Korea is increasing and new nuclear power plants will be continuously constructed, the number of nuclear facilities and the amount of materials are expected to increase. The importance of physical protection system design and evaluation will be further emphasized because the number of targets which an adversary can attack will increase.

Physical protection system evaluation plays a role in verification and validation of a designed or implemented physical protection system. The evaluation is carried out on the basis of threat definition, target definition and selected performance criteria. Two approaches can be suggested to evaluate a given physical protection system. One is a field test and another is software-based vulnerability assessment. A field test performed in a real or mock-up facility usually requires a large volume of resources, such as manpower, time, tools and/or equipment, etc. while a software-based performance test demands less or little resources. In

addition, it is not practical to try to get perfect performance data of the all elements of the physical protection systems from the field test because there are many combinations of threats and protective elements. A software-based vulnerability assessment is a better method for generating design alternatives or recommending modifications than a field test. To get exact performance data of elements in the physical protection systems or to verify and validate the performance of a physical protection system in a real situation, a field test would be better than software. Both of the two approaches are eventually necessary to evaluate physical protection systems.

KAERI has launched a project including the development of vulnerability assessment software for applying it to analyze domestic physical protection systems. This paper describes the results of the beginning phase for software development, including the functional requirements and conceptual framework of the software.

2. Functional Requirements

The development of functional requirements could start from how to use the software or how to analyze the vulnerability of a physical protection system. At first, vulnerability assessment needs assumptions on adversary strength because a physical protection system is aimed to ensure some level of protection capability against diverse adversary capabilities. There would be many attributes of adversary power, and the definitions of them could result in a Design Basis Threat (DBT). Thus, vulnerability assessment software must have a specific port for DBT input. The port should be sophisticated because the DBT has various attributes for its own flexible characteristic.

To identify the target to be protected or assessed, vulnerability assessment software is also able to configure a real or designed physical protection system in terms of an electronic form that the computer can understand. A consistent procedure for modeling a postulated or existent physical protection system should be provided to guarantee that the result of the procedure never produces differences with the analysts. Completeness as well as consistency should be emphasized in physical protection system modeling. The physical protection system is composed of many components, equipment, subsystems and guarding. Each element would be tightly linked together to play its own role in the provision of protection power. Every element identified or designed as parts of a physical protection system should be revealed and considered in the sequence of vulnerability assessment.

As vulnerability assessment software should know the effect of a specified DBT and the target configuration on a physical protection system so as to utilize them in the course of vulnerability analysis, a data set in which the effect is already defined is necessary. The effect rests on the combination of DBT and the element of the configuration. Thus, a large scale of data would be provided so the software could have an easy and efficient means for data storing and manipulation.

Vulnerability assessment software is used to evaluate on a computer the performance of a physical protection system against adversary power. Performance evaluation is the main activity that the software should have to do and needs to consider how to analyze the physical protection system and draw meaningful results. Probabilistic approaches are appropriate for the system analysis. Well-known time-domain criteria such as the Probability of Interruption (PI), Time Remaining after Interruption (TRI), and Critical Detection Point (CDP) will be incorporated. In addition, a cost-benefit analysis and alternatives generation based on its results shall be considered in the software so that a physical protection system achieves its goal in an efficient way. It is desirable to make the evaluation method as clear and explicit as possible because well-defined evaluation processes can be easily coded.

Reporting functions shall be provided in the software. The description of a given physical protection system, defined domestic DBT, analysis mode and results based on the criteria shall be shown on a computer and documented. An IAEA document, INFCIRC/225 rev.4, suggests the general requirements for physical protection system configuration. The software would compare those requirements with a given physical protection system configuration and provide the comparison results and recommendations. Showing the results and iterative runs with any modification of the given elements in the physical protection system provides easy verification of effectiveness of an alternative system as well as a rapid search mechanism when large changes on the system are attempted.

Figure 1. shows the relationship between DBT, target configuration, evaluation module, reporting and data set. As shown, the data set has three support links to the target configuration, internal evaluation mechanism, and reporting because the data set is used to transform the input configuration into an electronic format, provide the evaluation modules with an appropriate value and criteria, and look for recommendations and alternatives.

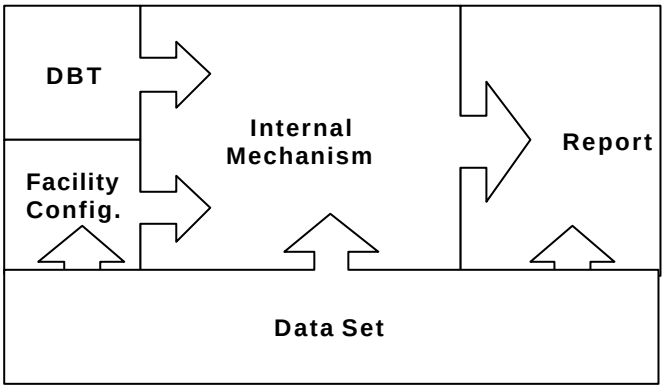

Figure 1. Relationship between the elements of the Vulnerability Assessment Software

3. Technical Consideration

As to the functional requirements mentioned above, several further technical considerations have been applied. As frequent usage of the data set is expected, we decided to adopt a DataBase (DB) to efficiently support the demand of data retrieval and modification in a computer. The data set required by vulnerability assessment software can be divided into smaller sets according to data attributes. For instance, there can be a data set for things sensing illegal entrance, things to delay intruders, and so on. This downsizing is expected to give a clear view on the data set and convenient data management through a consistent access method. The configuration DB corresponding to target information, the barrier DB to equipment for delay, the detector DB to sensors or monitors, and the guard DB to the guarding system were identified.

With the reviews of various sources for performance data of the elements, KAERI and a security company are planning to carry out a series of field tests to judge the performance data of the elements belonging to domestic physical protection systems. The gathered data will be stored into the database according to its attributes by the software in order to keep an updated history and consistently reflect the effect of new data values.

In spite of the fact that the public does not use the software, its user interface shall be designed with a consideration of usability. As the software has many components integrated with each other and infrequent use of the software is anticipated contrary to general-purpose software, an improperly designed user interface will make users confused so slips or mistakes could occur. A simple and consistent process shall be provided through a usability analysis.

The cost-benefit analysis function shall be incorporated in the software to suggest alternative physical protection system designs or modifications for security enhancement. If the performance of a physical protection system does not reach an appropriate pre-defined level, the software shall provide efficient alternatives that demand low cost and a sufficient margin to threat.

4. Conceptual Design

Through functional requirements and considerations, we framed the construct of the vulnerability assessment software as Figure 2. This conceptual design reflects the integration requirements between the database and execution module, the configuration requirements of the plant and DBT, data update requirements, and reporting requirements.

This conceptual design does not show the user interface of the vulnerability assessment program. Many users have pointed out the user interface of the software as a big problem. They complain the difficulties on plant configuration, protection elements configuration, analysis mode selection, lack of useful analysis functions, and result interpretation while they use a vulnerability assessment software. We will focus on user-friendly data input supports and interpretation assistance.

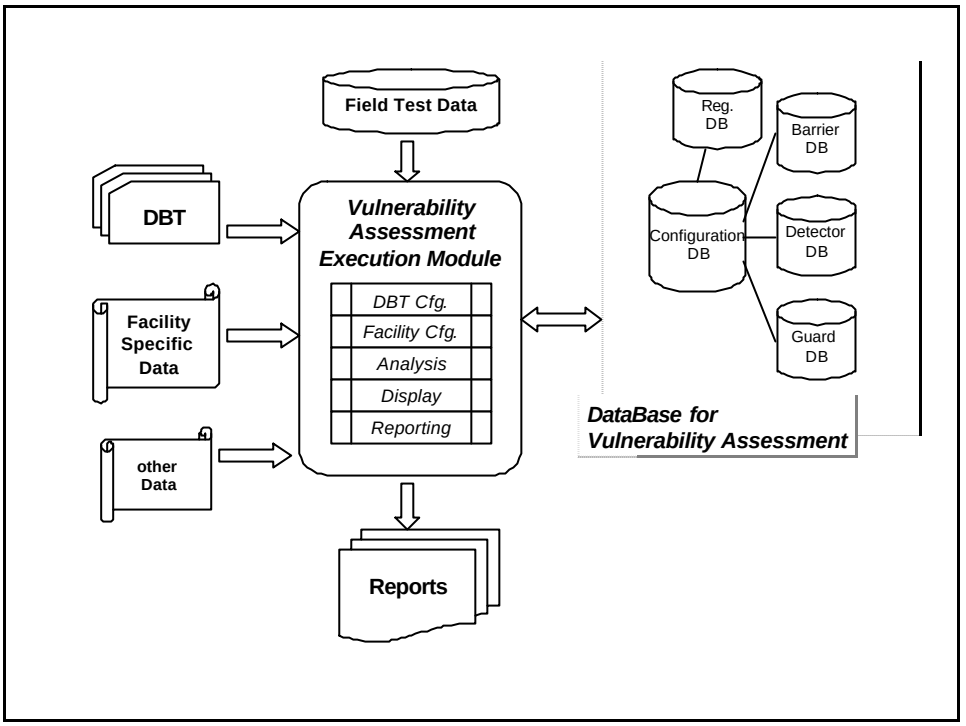

Figure 2. Conceptual Framework of the Vulnerability Assessment Software

4. Development Plan

In 1999, KAERI developed vulnerability assessment software, PIGSAM(Probability of Interruption Generator with Sensitivity Analysis Module)[3] which is based on the EASI model[4]. This software, even though it supports a one-path-level analysis, also has functions to show the effect on the Probability of Interruption (PI) in the case that an element is improved. KAERI also carried out a preliminary vulnerability assessment with respect to a hypothetical physical protection system induced from domestic nuclear power plants for the purpose of defining the software functional requirements mentioned above.

To acquire the performance data of elements which are used in domestic physical protection systems, a series of field tests was planned and the tests will begin this year.

After the sequence of development activities, we will investigate the probability of standardization of the physical protection system to enhance maintenance capability and provide easy management.

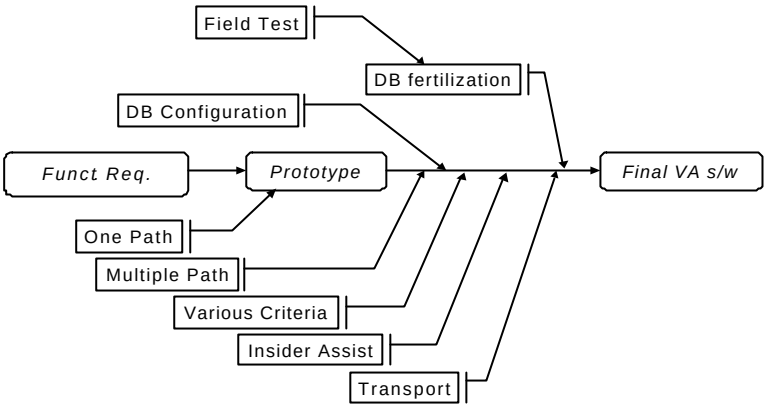

Figure 3. Sequence of the Development Process

5. Acknowlodgement

This study is sponsored by the long-term project on nuclear research and development of the Korean Ministry of Science and Technology.

6. References

[1] IAEA, “The Physical Protection of Nuclear Material”, INFCIRC/225/Rev.4, 1999.

[2] IAEA, “Guidance and considerations for Implementation of INFCIRC 225/Rev.3”, IAEA-TECDOC-967, 1997.

[3] SNL, “Physical Protection System Design Methodology Workshop”, Sep., 1996.

[4] KAERI, “Design Basis Threat and Vulnerability Assessment of Physical Protection System”, KAERI/TR-1560/2000, 2000.