Security Effectiveness Review (SER)

Irene Kouprianova, Security Analyst, Institute of Physics & Power Engineering,
Bondarenko sq 1, Obninsk, 249020 Russia
tel. 7-08439-98164

David Ek, Security Analyst, Sandia National Labs,
P.O. Box 5800-0759
Alb, NM 87185
tel. 505-845-9891

Michele Bergman, U.S. IPPE Project Team Lead, Lawrence Livermore Lab,
P.O. Box 808, L-503
Livermore, CA 94551
tel. 925-423-6075

Roger Showalter, U.S. Team Physical Protection Coordinator,
Sandia Nation Labs,
P.O. Box 5800-0762
Alb, NM 87185
tel. 505-844-5657

Abstract

As part of the on-going DOE/Russian MPC&A activities at the Institute of Physics and Power Engineering (IPPE) and in order to provide a basis for planning MPC&A enhancements, an expedient method to review the effectiveness of the MPC&A system has been adopted. These reviews involve the identification of appropriate and cost-effective enhancements of facilities at IPPE. This effort requires a process that is thorough but far less intensive than a traditional vulnerability assessment. The SER results in a quick assessment of current and needed enhancements. The process requires preparation and coordination between US and Russian analysts before, during, and after information gathering at the facilities in order that the analysis is accurate, effective, and mutually agreeable. The goal of this paper is to discuss the SER process, including the objectives, time scale, and lessons learned at IPPE.

Introduction

Background

SERs have been conducted as a part of the on-going DOE-Institute of Physics and Power Engineering (IPPE) MPC&A cooperation in order to provide a basis for planning MPC&A enhancements at IPPE facilities with nuclear material. The primary goal of the SER is to quickly identify appropriate initial upgrades to the MPC&A system. An SER differs from a detailed Vulnerability Assessment (VA) in several ways. The SER is

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.

intended to be a cursory overview of the current material protection, control and accounting system and focuses on identifying immediate upgrades. As a result, some of the analysis is qualitative rather than quantitative. When quantified, the delays and detection probabilities and response times are based upon the subjective opinion of the analyst rather than performance test data. Finally, the threats assumed for the SER include only a limited set of insiders and a pre-defined worst-case outsider.

Experience in carrying out SER

Once a facility has been identified as containing material of the appropriate attractiveness, an SER is initiated as a joint US-Russian effort.

Steps of U.S. and IPPE communications

The first step of an SER is to establish a communication channel to permit the flow of information. Generally, information is passed by E_mail, with the joint team sharing information gathered by the Russian SER participant. Typical information includes the following:

- Building drawings and schematics
- Identification of the types and amounts of material
- The location of material
- A list of insider categories to be considered
- The flow of material within the facility, and
- Any previous VA results

Once the information has been communicated, the Russian participant arranges a joint data-collection visit. Arrangements are made to gather the necessary information for the SER by visiting the facility and interviewing knowledgeable facility employees and potential insider groups. The visit may last from two days to one week depending on the size and complexity of the facility. The information gathered will include:

- NM attributes (type, form, weight, category and others)
- NM handling, transfers (receiving/delivery)
- Access Control procedures and equipment
- Key Control
- Sensors
- Alarm Assessment
- Barriers
- Response Tactics, Numbers and Times
- Number of employees with facility access
- Access and Authorities of Insider categories
- Emergency procedures
- Visitor access, and
- Potential theft scenarios for insider and outsider adversaries.

Difference in U.S. and Russian Analysis Methodologies

The general U.S. methodology for conducting a VA [1] comprises a well structured description of the nuclear material facility, the possible threat to and security system of the facility, and the authorities of persons working with NM. The VA includes a process of quantitatively evaluating the effectiveness of a Physical Protection System (PPS). A VA is conducted whenever change is made to a facility or its Security System, whenever a new building is planned, and/or whenever there is a change in the attractiveness of potential targets. VA procedures include definition of a security state and the characteristics of the PPS. In the U.S., the VA methodology uses a standard risk equation. DOE determines the level of risk which is acceptable.

To date, the protection strategy in Russia has been based mainly on security measures and safeguards against outsider and administrative measures for personnel. The protection standards are not always well coordinated between the protective forces and the operational personnel. A secondary role was assigned to nuclear enterprises in determination of threats. These departmental standards did not require a quantitative VA of a facility as a whole.

Difficulties/Obstacles

Following the U.S. methodology, two detailed Vulnerability Assessments and three SERs were performed for facilities of different types at IPPE. A number of difficulties were encountered during the performance of these SERs.

Database:

Among the main difficulties encountered in adopting the U.S. methodology is the lack of a verified database of quantitative information on detection and delay values for different Russian protection elements. During the SER, this lack of database resulted in a difference of opinion between U.S. and Russian representatives on the quantitative values to assume for protection elements.

MVD force tactics:

Information concerning MVD tactics is considered sensitive, and is not even shared with the Russian participant in the SER. Therefore, detailed information for these types of activities cannot be gathered, and the SER team is limited to their own judgment for response tactics and effectiveness.

Emergency/Abnormal Situation Procedures:

The emergency procedures are developed for actual emergencies, but do not incorporate procedures to protect against adversary actions, such as a theft attempt masked by a fire drill or real evacuation. Further, well-developed procedures on how to control the personnel during the complicated inventory process do not exist.

Requirements:

The SER process was hindered most of all by the lack of a written requirement for a vulnerability analysis. Each facility usually determined for itself the form and scope of reports to the Ministry on the effectiveness of its security system.

Classification:

Currently, there is no well-defined process for establishing the sensitivity of information with the exception of "national security" information. Every facility may assign information as "sensitive" or "confidential" and, as a result, there are no available descriptions of the effectiveness of physical protection systems that are collected in a single report. Therefore, information access is limited in a non-uniform manner to foreign nationals including the U.S. Laboratory co-workers.

Communication:

Since the U.S. and Russia have two different conceptual approaches for facility protection, communication can be easily misunderstood. In the former USSR, the protection concept focused on preventing penetration of an outsider adversary. To this end, very strong protected perimeters surround Russian nuclear facilities; however, the reliability of the employees of the facility is assumed to be high since they must adhere to strict requirements to work with nuclear material at the facility. The U.S. on the other hand pursues a layered approach to physical security to protect against both outsider and insider adversaries, since they consider all employees to be potential insiders.

Analysis of existing system and effectiveness assessment

The objective of a protection and material control and accounting system is to:

- Detect adversary actions
- Communicate the detection to the assessment personnel
- Provide positive assessment of detection
- Communicate assessment to response forces
- Delay the adversary long enough for assessment, communications, and response force to arrive
- Successfully respond to the alarm
- Defeat the adversary

If the system fails to achieve any one of these steps, it will fail the protection goal.

System Characterization

In order to assess the effectiveness of a system in meeting the above objectives, the following must be investigated:

- Control of access into the protected area, inner area, and vaults. Access control limits insider movements, and detects outsider penetration.

- Detection of adversaries through sensors or human observation
- The barriers and their effectiveness against adversaries, and
- Control of material through procedures, human or electronic observation, and physical barriers.

Analysis

Once the protection system is understood, the effectiveness of this system in protecting the targets against pre-defined adversaries can be evaluated. The analysts will *estimate* the effectiveness with which the access and material control system will defeat efforts of insiders to execute theft for any scenarios hypothesized given the insider access, authorities and privileges; the analysts will *estimate* the effectiveness of the detection system at providing assessed detection of outside adversaries for potential paths, and compare the *estimated* time attributed to the barriers to the *expected* response force times. Further, the analysts will attempt to estimate any problems the response team might encounter trying to interrupt and neutralize the adversary, given the limited understanding of response tactics.

For assessment of the physical protection system and its risk against outside adversaries, the analysts use following equation [**3**]:

Conditional Risk = Consequences * (1 – $P_{effectiveness}$)
Probability (P) of PPS effectiveness = $P_{timely\ detection} * P_{neutralization}$

The tools utilized to assist in the analysis include the ASSESS software.

A time line diagram shows (**Figure 1**) the delay values and probability of detection for every step of a path.

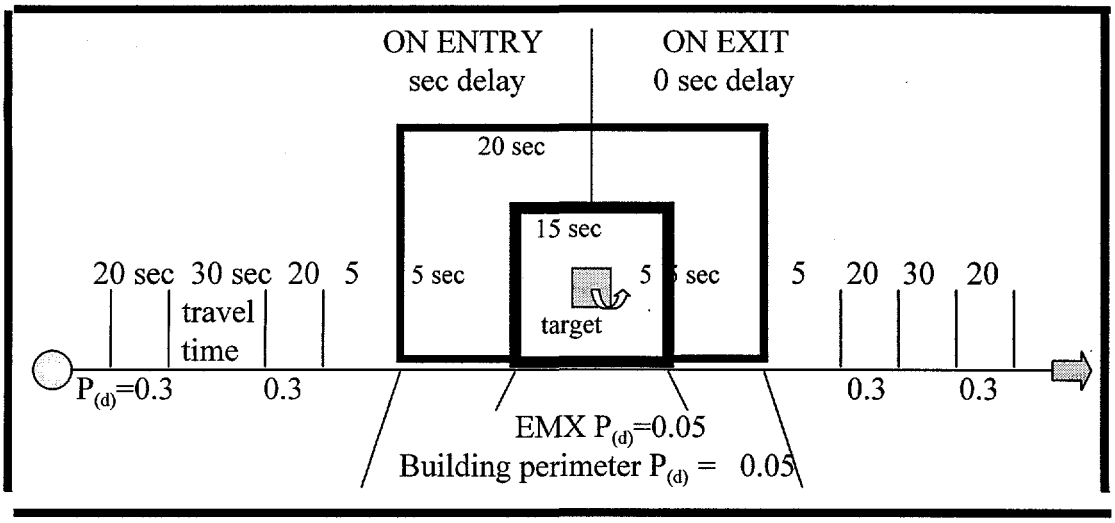

FIGURE 1. Delay time diagram

Figure 2 represents the estimated probability of interruption, neutralization, and risk for an analysis.

Path through Emergency Exit for day and for night time. (Response time is 60 sec)

Time	P(i)	P(n)	Risk
Day	75	80	32
Night	52	70	51

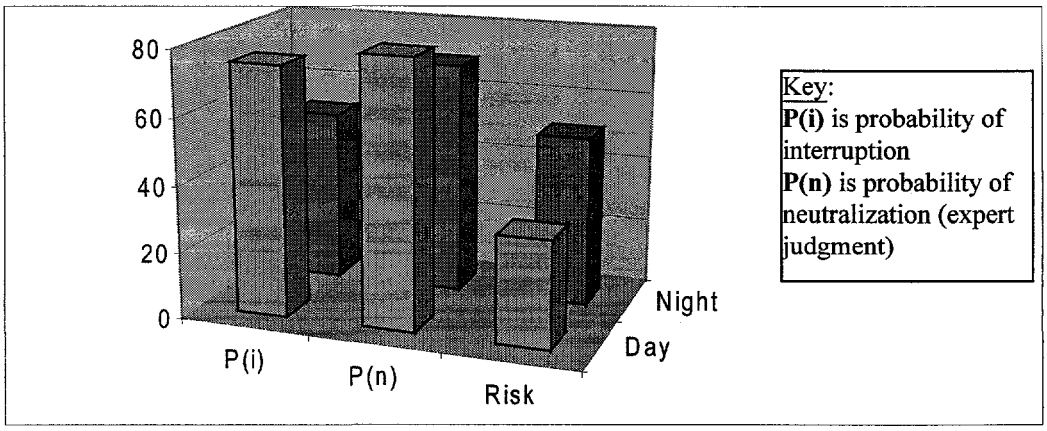

FIGURE 2. Risk for outsider adversary scenarios against the current system

The ASSESS program could be used to model upgrades effectiveness. Due to difficulties mentioned before, the analysts' experience must be used for the probability of neutralization and sometimes for the probability of interruption values.

Results

The SER process highlighted weaknesses which were in turn addressed during the upgrades phase of the program. It also helped identify the appropriate upgrades from which costs can be estimated.

Further, as noted in Figure 3, the SER results permitted comparisons of the effectiveness of different physical protection systems of IPPE facilities, and based on this, upgrades of the security and safeguard system for all of IPPE can be planned.

VA Year	Type of Adversary	RFT	P(i)	Category	Risk	Target
1996	Outsider, terrorist, 1 barrier	150 sec	.59	2B	.344	HEU disk
1996	Outsider, terrorist, 2 barriers	180 sec	.60	2B	.354	HEU disk
1997	Outsider, criminal, 1 barrier	60 sec	.98	2B	.055	Fuel elem.
1997	Insider, NM access		.90	2B	.08	Fuel elem.
1997 exp	Outsider, criminal, 1 barrier	180 sec	.30	2B	.572	HEU disk

Key: @exp is expert judgement for P(I)
- for HEU disk the task time is up to 5 sec
- * for fuel element the time task is up to 5 min

*HEU disk is fuel of high enrichment uranium (temporary storage location)
* fuel element is set of disks installed into the tube

FIGURE 3. Risk for BFS facility, database IK/1997. Strategy denial

Overall results - learned lessons

Several lessons were learned during the SER process:

- Close coordination between U.S. and Russian analysts is critical if the SER is to be completed in a timely manner.
- U.S. methodology must be modified to account for lack of quantified performance test data.
- Differences in estimates of equipment and personnel effectiveness must be resolved to determine appropriate upgrades.

Summary

The SER is a fast analysis intended to provide a foundation for immediate upgrades under the MPC&A program. It makes it possible to obtain a reasonable evaluation of the effectiveness of a PPS based upon the analyst's experience, and to propose immediate upgrades.

Furthermore, within it, the importance of modeling the viewpoint and behavior of a possible adversary can be estimated. As a result of the adoption of the SER methodology, the importance of joint participation of various specialists in VAs from our two countries is emphasized [9]. Through the SER, the combined experience of the analysts for the two countries is applied to reach a joint viewpoint for the upgrades. The process divides the responsibility for upgrade identification between the analysts of our two countries, and emphasizes the importance of quantitative assessments.

This work was funded by Department of Energy Non-Proliferation under the MPC&A Program. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-ACO4-94AL85000.

References

[1]. DOE Order 4701 "Vulnerability Assessment"
[2]. NRC publications of the U.S. Department of Energy.
[3]. Physical Security Site Characterization.1997. James Larson, SNL. Department of System Analysis, 5845.
[4]. ASSESS Guide (The Analytic System Software for Evaluation Safeguards and Security) developed for DOE by LLNL and SNL in 1993.
[5]. Description of BFS Facilities, Protection System and Planning of Upgrades. Report under Contract AQ-0115. 1995.
[6]. Results of the Central Storage Inspection for Estimation of NM Physical Protection Necessity. Report under Contract AQ-4492. 1995.
[7]. Preliminary Report of Facility Description, Risk Estimate, and Recommended PP Upgrades for BFS Facility. IPPE, Russia, Obninsk, 1997. C/FGI-MOD.
[8]. Preliminary Report of Facility Description, Risk Estimate, and Recommended PP Upgrades for Central Storage Facility. IPPE, Russia, Obninsk, 1998. C/FGI-MOD.
[9]. Proliferation concerns. National Research Council. Office of International Affairs. Washington, D.C. 1997