PHYSICAL PROTECTION SYSTEM DESIGN AND EVALUATION

James D. Williams

Sandia National Laboratories
Albuquerque, NM USA

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

19980407 066

This is a reprint of a paper intended for presentation at a scientific meeting. Because of the provisional nature of its content and since changes of substance or detail may have to be made before publication, the preprint is made available on the understanding that it will not cited in the literature or in any way be reproduced in its present form. The view expressed and the statements made remain the responsibility of the named author(s); the views do not necessarily reflect those of the government of the designating Member State(s) or of the designating organization(s). In particular, neither the IAEA nor any other organization or body sponsoring this meeting can be held responsible for any material reproduced in this reprint.
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
PHYSICAL PROTECTION SYSTEM DESIGN AND EVALUATION

ABSTRACT

The design of an effective physical protection system (PPS) includes the determination of the PPS objectives, the initial design of a PPS, the evaluation of the design, and probably, the redesign or refinement of the system. To develop the objectives, the designer must begin by gathering information about facility operation and conditions, such as a comprehensive description of the facility, operating conditions, and the physical protection requirements. The designer then needs to define the threat. This involves considering factors about potential adversaries: class of adversary, adversary's capabilities, and range of adversary's tactics. Next, the designer should identify targets. Determination of whether or not the materials being protected are attractive targets is based mainly on the ease or difficulty of acquisition and desirability of the material. The designer now knows the objectives of the PPS, that is, "what to protect against whom." The next step is to design the system by determining how best to combine such elements as fences, vaults, sensors and assessment devices, entry control devices, communication devices, procedures, and protective force personnel to meet the objectives of the system. Once a PPS is designed, it must be analyzed and evaluated to ensure it meets the PPS objectives. Evaluation must allow for features working together to ensure protection rather than regarding each feature separately. Due to the complexity of the protection systems, an evaluation usually requires modeling techniques. If any vulnerabilities are found, the initial system must be redesigned to correct the vulnerabilities and a reevaluation conducted. After the system is installed, the threat and system parameters may change with time. If they do, the analysis must be performed periodically to ensure the system objectives are still being met.

1. INTRODUCTION

Sandia National Laboratories has performed many evaluations and upgrades of nuclear facilities in the United States and abroad. A methodology for accomplishing these evaluations and upgrades has evolved. This methodology has been developed into courses used for technology transfer and training.

The transfer of physical protection technology by the US Department of Energy (DOE) to the international community has been an ongoing activity for many years. When the United States passed the Nuclear Non-Proliferation Act of 1978, it committed the DOE to transfer current physical protection technology to member states of the International Atomic Energy Agency (IAEA). Since that time, Sandia National Laboratories, the DOE lead laboratory in physical protection, has provided training courses in the systematic design of physical protection systems (PPS). One such course, the International Training Course (ITC) on the Physical Protection of Nuclear Facilities and Materials is sponsored by the Department of Energy International Safeguards Division, the IAEA, and the Department of State. Since 1978, 12 three- and four-week classes have been conducted by Sandia for these sponsors. One- and two-week adaptations of this course have been developed for other customers, and since 1994, more than a dozen of these abbreviated courses have been presented in the Russian language to participants from the Baltic States, the Russian Federation, and the Newly Independent States (NIS).

These courses have been presented in support of the Department of Energy Nuclear Material Protection, Control and Accounting (MPC&A) program. The shorter adaptation of the ITC is intended to inform the participants of the systematic approach to physical protection, analysis, and system design used in the United States to guard nuclear facilities against the threats of radiological sabotage and theft of nuclear material.

The PPS methodology consists of three major steps.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the US Department of Energy under Contract DE-AC04-94AL85000.
(a) Determine PPS objectives—First, study the existing facility or facility plans to learn all of the operations, conditions, and important physical features that affect the PPS. Then conduct a detailed study of the range of adversaries that the PPS must successfully counter. Finally, to complete the determination of objectives, identify the most important areas or materials that must be protected from the adversary.

(b) Design a PPS—Either identify the existing physical protection elements for potential upgrading or design a new protection system.

(c) Evaluate the PPS design—Given the information about the facility, threat, targets, and PPS, use accepted analysis techniques to obtain a measure of the protection system's effectiveness. Redesign and reanalysis may be required if the measure of effectiveness is not satisfactory.

This design and analysis process emphasizing determine, design, and evaluate is illustrated in Fig. 1.

2. DETERMINE PHYSICAL PROTECTION SYSTEM OBJECTIVES

The design of an effective PPS includes the determination of the PPS objectives, the initial design of a PPS, the evaluation of the design, and, probably, a redesign or refinement of the system. To develop the objectives, the designer must begin by gathering information about facility operations and conditions, such as a comprehensive description of the facility, operating states, and the physical protection requirements. The designer then needs to define the threat. This involves considering factors about potential adversaries: class of adversary, adversary's capabilities, and range of adversary's tactics. Next, the designer should identify targets. Determination of whether or not nuclear materials are attractive targets is based mainly on the ease or difficulty of acquisition and desirability of the material. The designer now knows the objectives of the PPS, that is, "what to protect against whom." The next step is to design the system by determining how best to combine such elements as fences, vaults, sensors, entry control devices, communication devices, procedures, and protective force personnel to meet the objectives of the system. Once a PPS is designed, it must be analyzed and evaluated to ensure it meets the physical protection objectives. Evaluation must allow for features working together to ensure protection rather than regarding each feature separately. Due to the complexity of protection systems, an evaluation usually requires modeling techniques. If any vulnerabilities are found, the initial system must be redesigned to correct the vulnerabilities and a reevaluation conducted.

2.1. Threat definition

The physical threat to a nuclear facility must be defined as part of determining the objectives of the PPS. A methodology for defining the threat for a specific facility should be developed. The first part of the methodology consists of listing the information needed to define the threat. A list of necessary information might include the type of adversary and possible adversary tactics, potential actions of the adversary, motivations of the adversary, and physical capabilities of the adversary. There are various sources of information on threat. Intelligence sources can provide detailed information about groups which might pose a threat to nuclear facilities. Crime studies which review past and current crimes can provide useful information for characterizing the potential threat. Non-government networks for information exchange, such as meetings of various professional organizations, can provide information on the assessment of threat. With electronic databases, current published literature can provide extensive information concerning threat. The threat information can then be tabulated and summarized so that adversaries can be ranked in order of their threat potential to a specific facility. The result is valuable information for the designer of the PPS.
2.2. Target identification

Target identification is the process of identifying specific areas or components to be protected to prevent undesirable consequences. Theft of special nuclear material and radiological sabotage are the undesirable consequences to be considered at most nuclear sites.

3. DESIGN OF A PHYSICAL PROTECTION SYSTEM

3.1. Physical protection system

Detection, delay, and response are all required functions of an effective PPS. These functions must be performed in order and within a length of time that is less than the time required for adversaries to complete their task. An effective PPS has several specific characteristics. A well-designed system provides protection-in-depth, minimizes the consequence of component failures, and exhibits balanced protection. In addition, a design process based on performance criteria rather than feature criteria will select elements and procedures according to the contribution they make to overall system performance. The procedures of a PPS must be compatible with security, safety, and operational procedures of the site.

3.2. Exterior and interior intrusion sensors

The integration of individual sensors into a sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the system with a balanced and integrated PPS. Sensor performance is described by the following characteristics: probability of detection, nuisance alarm rate, and vulnerability to defeat. The methods of classification of exterior sensors used in this session include passive or active; covert or visible; line of sight or terrain-following; volumetric or line detection; and application—either buried-line, fence-associated, or freestanding for exterior sensors. The classification methods for interior sensors are similar to those for exterior sensors and their applications are boundary penetration, motion, or proximity detection. The designer of the sensor system must also consider its interaction with the alarm assessment and the access delay systems.

3.3. Alarm assessment

Assessment of alarms can be provided by closed-circuit television coverage of each sensor sector displayed at a local alarm station by video coverage with the help of the protective force (guards) in towers and roving patrols, or by guards only.

3.4. Alarm communication and display

An alarm communication and display system transmits alarm signals from intrusion detection sensors and displays the information to a security operator for action. A state-of-the-art system uses computer technology and graphics to communicate alarm information to the operator. Characteristics of a good alarm communication system include fast reporting time, supervision of all cables, easy and quick discovery of single-point failures, isolation and control of sensors, and expansion flexibility. The designer of an alarm display system must decide what information to display, how to present the information, how the operator will communicate with the system, and how to arrange the equipment at the operator workstation.
3.5. **Entry/exit control systems**

Entry control systems consist of the hardware and procedures used to verify entry authorization and to detect contraband and special nuclear material. Methods of personnel entry authorization include credentials, personal identification numbers (PINs), and automated personal identity verification. Contraband consists of items such as unauthorized weapons, explosives, and tools. Methods of contraband detection include metal detectors, package searches, and explosives detectors. The purpose of nuclear materials detectors used for exit control is to detect the unauthorized removal of nuclear material on persons, in packages, or in vehicles leaving a protected area.

3.6. **Access delay**

An access delay system integrates protective force guards, passive barriers, and dispensable barriers to maximize the probability that an adversary will be interrupted before accomplishing their task. The role of barriers is simply to increase the adversary task time following detection by introducing impediments along any path the adversary may choose, thus providing the needed time for the response force to arrive and react. Traditional barriers are not likely to delay a group of well-equipped and dedicated adversaries for a significant length of time (several minutes). Barrier penetration time is a function of the attack mode which is governed by equipment required. The use of dispensable barriers offers significant potential for increasing adversary delay. Features of an effective access delay system include detection before delay, balanced design, and delay-in-depth.

3.7. **Response force and response force communication**

Response has been divided into two major parts: (1) interruption, which includes communication and deployment; and (2) neutralization. For interruption to occur, the response force must arrive at the appropriate location to stop the adversary. In order for the response force to arrive on time, effective communication to the response force and successful and timely deployment must occur. The communication system must be protected and a backup system should exist. Response force communications should provide the guard with a way to signal that he is under duress. For successful and timely deployment to occur, the response force must be able to follow a tactical plan, must have been trained in following the tactical plan, and must have practiced specific tactics. The final part of response is neutralization. To neutralize adversary action, the response force must be large enough in number and have the appropriate weapons and equipment. Response force members must be in good physical condition and must be trained and tested on procedures and duties.

4. **EVALUATE THE PHYSICAL PROTECTION SYSTEM DESIGN**

4.1. **Analysis and evaluation techniques**

Detection, delay, and response elements are all important to the analysis and evaluation of a PPS and its effectiveness. For most analysis models, targets and adversary paths (series of actions against a target that result in theft or sabotage) must first be identified. The analyst should then consider the adversary's goal: to complete the path. The delay time or the cumulative probability of detection along a specific path is not satisfactory for evaluating the effectiveness of a PPS along that path. Therefore, the combination of the two (or the principle of "Timely Detection") should be used as a measure of effectiveness. Timely detection focuses on the
probability of interrupting the adversary, that is, detecting the adversary while there is still enough delay time for a response force to respond. But it does not take into account the actual neutralization of the adversary. To truly deduce the effectiveness of a total PPS, consider the most critical path. That is the path with the lowest probability of interruption, so the protection system is really only as effective as its protection of this path. Some modeling programs that use the principle of timely detection include: Estimate of Adversary Sequence Interruption (EASI); Adversary Sequence Diagram (ASD); Systematic Analysis of Vulnerability to Intrusion (SAVI), and Analytic System and Software for Evaluating Safeguards and Security (ASSESS).

5. REDESIGN OF THE PHYSICAL PROTECTION SYSTEM

As mentioned above, the result of the analysis phase is a system vulnerability assessment. If the PPS is found ineffective, vulnerabilities in the system can be identified. The next step in the design and analysis cycle is to redesign or upgrade the initial protection system design to correct the noted vulnerabilities. It is possible that the PPS objectives also need to be reevaluated. As analysis of the redesigned system is performed. This cycle continues until the results indicate that the PPS meets the protection objectives.

6. SUMMARY

A design and analysis procedure together with extensive physical protection technology provide the basis for this paper. The design and analysis procedure consists of three phases: determine, design, and evaluate. The first phase includes the determination of the PPS objectives which involve facility characterization, threat definition, and target identification. A good PPS design provides detection, delay, and response. Analysis of the PPS design begins with a review and understanding of the objectives which the design must meet. Evaluation of the design normally requires the application of modeling techniques. If the evaluation reveals weaknesses, the system is upgraded and another analysis on the redesigned system is performed.
Fig. 1. Design and analysis process