PHYSICAL PROTECTION SYSTEM DESIGN AND EVALUATION

JAMES D. WILLIAMS
SANDIA NATIONAL LABORATORIES

ABSTRACT

The design of an effective physical protection system includes the determination of the physical protection system objectives, the initial design of a physical protection system, the evaluation of the design ,and probably, and 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 physical protection system, 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 elements, procedures, communication devices, and protective forces personnel to meet the objectives of the system. Once a physical protection system 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 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.

This paper reviews the physical protection system design and methodology mentioned above. Examples of the steps required and a brief introduction to some of the technologies used in modern physical protections system are given.

Introduction

The transfer of physical protection technology by 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 DOE to transferring current physical protection technology to member states of the IAEA. Since that time, Sandia National Laboratories 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 International Atomic Energy Agency, 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 for the Baltic States, the Russian Federation and the Newly Independent States.

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 attendees 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. Sandia National Laboratories has performed many evaluations and upgrades of nuclear facilities in the United States and abroad. Sandia Laboratories, the lead DOE laboratory in physical protection, has established a methodology for accomplishing these evaluations and upgrades. This physical protection system methodology consists of three major steps.

1. 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 physical protection system. 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.

2. Design a physical protection system—Either identify the existing physical protection elements for potential upgrading or design a new protection system.

3. 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 system effectiveness is unsatisfactory.

No attempt is made during the training courses to cover the physical protection of nuclear materials while they are being transported from one site to another. However, the same basic principles apply. This very general treatment of PPSs is presented so that the participants will understand how this aspect of nuclear safeguards complements nuclear MC&A. This design and analysis process that emphasizes "determine, design, and evaluate" is illustrated in Figure 1.

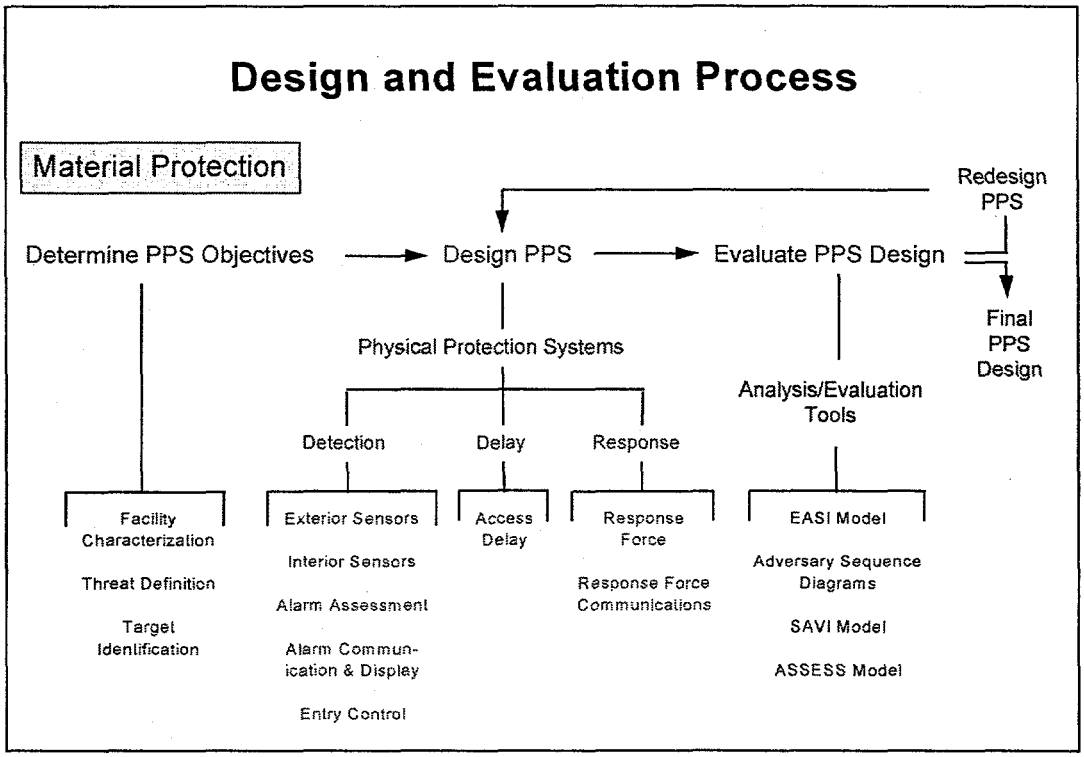

Figure 1. Design and analysis process

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 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 physical protection system, 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, procedures, communication devices, 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.

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. Nongovernment 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.

Target Identification

Target identification is the process of identifying specific areas or components to be protected to prevent undesirable consequences. There are three steps for identifying targets. The first step is to specify undesirable consequences. For this paper, theft of special nuclear material and radiological sabotage are the undesirable consequences to be addressed. Next, a technique for identifying target must be selected and then applied to identify areas or components to be protected. The manual listing of target techniques can be used for theft of localized items. For simple facilities, it can also be used for theft of material-in-process and sabotage of critical components. When the facility is too complex for a manual identification of targets, a more rigorous identification technique may be used. Vital Area Identification is a structured approach based on logic diagrams called fault trees to identify critical components for the prevention of radioactive release caused by sabotage. The locations of the critical components are called vital areas. The basic steps of the approach are applicable to any nuclear facility. They include

determining (1) what level of radioactive release constitutes a hazard, (2) the sources of radioactive material at the facility, (3) the operating states of the facility, (4) how the material can be released from the sources, (5) the system failures required for release to occur, and (6) the location of the components that must fail for release to occur. This detailed information is used to develop or modify existing sabotage fault trees. The sabotage fault trees can then be analyzed to yield the vital areas to be protected.

Design of a Physical Protection System

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 the adversary to complete his 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 the procedures of the facility. Security, safety, and operational objectives must be accomplished together at all times.

Exterior Intrusion Sensors

The integration of individual sensors into a perimeter sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the perimeter 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 for 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 sensors. An effective perimeter sensor system provides a continuous line of detection using multiple lines of complementary sensors located in an isolated clear zone. Topography, vegetation, wildlife, background noise, climate and weather, and soil conditions and pavement all affect the performance of exterior sensors. Using alarm priority schemes can reduce the nuisance alarm rate. The designer of the perimeter sensor system must also consider its interaction with the video assessment system and the access delay system.

Interior Intrusion Sensors

Interior intrusion sensors can also be active or passive, covert or visible, or volumetric or line detectors. Their performance is discussed in terms of probability of detection, nuisance alarm rate, and vulnerability to defeat. The application classes discussed include boundary penetration sensors, interior motion sensors, and proximity sensors. Various sensor technologies can be applied to achieve protection-in-depth: at the boundary, within the room, and at the object to be protected. The designer of a good interior intrusion detection system considers the operational, physical, and environmental characteristics of the facility. Also, the designer should be familiar with the sensors that are available, how the sensors interact with the intruder and the environment, and the physical principles of operation for each sensor. The interior sensor system must support a balanced PPS.

Alarm Assessment

Alarm assessment can be accomplished by closed-circuit television coverage of each sensor sector displayed at a local alarm station in combination with the protective force (guards) in towers and roving patrols, or by guards only. The assessment system is composed of several cameras at remote sensor areas, a display monitor at the local end, and various transmission, switching, and recording systems. The

major components include (1) the camera and lens to convert the image of the physical scene into an electrical signal, (2) the lighting system to illuminate the alarm location evenly with enough intensity for the camera and lens, (3) the transmission system to connect the remote cameras to the local video monitors so that no undesirable effects are introduced to the video signal, (4) a synchronization system to ensure that switchings are recording, clean, and free of vertical roll, (5) video switching equipment to connect multiple video signals from cameras with monitors and video recorders, (6) video recording system to produce a record of an event, (7) video monitors to convert a signal to a visual scene on the output display, and (8) video controller to interface between the alarm sensor system and the alarm assessment system. The video assessment system must be designed as a component of the total intrusion detection system. Interactions between the video system, intrusion sensors, and display system must always be considered.

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. Although annunciator panels are easy to understand and maintain, they can be expensive, require a large amount of physical space for a large number of zones, and display only a limited amount of information. 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 work station. An alarm communication system is an integrated system of people, procedures, and equipment, and must be designed with the specific needs and resources of the site in mind.

Entry 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 entry control is to detect the unauthorized removal of nuclear material on persons, in packages, or in vehicles leaving a protected area. An effective entry control system cannot be easily bypassed, allows observation by the protective force (guards), protects guards, accommodates peak loads, performs personnel and material control, blocks passage until personnel and material control are done, is under surveillance by the central alarm station, provides secondary inspection for those who cannot pass the automated inspection, and is designed for both entry and exit.

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 the 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 the equipment required. Categories of attack tools and their role in penetrating various perimeter and structural barriers are discussed. 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.

Response Force

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. Effective communication means that the information being transmitted is accurate and timely. The communication system must be protected, and a backup system should exist. Response force communications should provide a way to signal that the guard 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.

Response Force Communications

Response force communications includes the procedures and hardware that allow members of the protective and response forces to communicate with each other. The most common system consists of radios that can operate on low power, are battery operated, and can be handheld. Conventional radio systems can be vulnerable to eavesdropping, transmission of deceptive messages, and jamming. Alternate means of communication must be in place. These might be telephones, intercoms, public address systems, hand signals, sirens, lights, pagers, couriers, computer terminals, flares, duress alarms, smoke, or whistles. In designing a communication system for the response force, specific features must be considered such as cost, complexity, and resistance to: eavesdropping, transmission of deceptive messages, and jamming.

Evaluate the Physical Protection System Design

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. While this section focuses on general evaluation techniques, the following three sections will each present an evaluation technique that uses this principle of timely detection: Estimate of Adversary Sequence Interruption (EASI); Adversary Sequence Diagram (ASD); and Systematic Analysis of Vulnerability to Intrusion (SAVI).

EASI Model

Many computer models have been developed to analyze a PPS. The EASI model, which runs on a PC, is a simple-to-use model that quantitatively illustrates the effect of changing physical protection parameters along a specific path. It uses

detection, delay, response, and communication values to compute the probability of interruption. But, since EASI is a path-level model, it can only analyze one adversary path or scenario at time. Even so, it is able to perform sensitivity analyses and analyze physical protection system interactions and time tradeoffs along that path. The input for the model requires (1) detection and communication inputs as probabilities that the total function will be successful and (2) delay and response inputs as mean times and standard deviations for each element. The output will be the probability of interruption, or the probability of intercepting the adversary before any theft or sabotage occurs. After obtaining the output, any part of the input data can be changed to determine the effect on the output. However, since EASI is a path-level model, it may be necessary to use another model to observe all possible paths to determine which are the most vulnerable.

Adversary Sequence Diagram (ASD)

The adversary sequence diagram graphically models the PPS at a facility. It identifies paths that adversaries can follow to accomplish sabotage or theft. The most vulnerable path can be determined and used to measure the effectiveness of the entire PPS. There are three steps in developing an adversary sequence diagram for a specific site. The first step is to model the facility by separating it into adjacent physical areas. Next, protection layers are defined between the adjacent areas. Each protection layer includes one or more protection elements which are the basic building blocks of a PPS. Examples of protection elements are doors, fences, surfaces, and portals. Finally, path segments between the areas through the protection elements can be drawn. Both entry and exit paths can be modeled.

Systematic Analysis of Vulnerability to Intrusion (SAVI) Model

The SAVI computer code is used to evaluate PPS effectiveness. SAVI determines the most vulnerable path of an adversary sequence diagram as a measure of effectiveness. An analysis using SAVI begins with identifying a target and constructing a site-specific adversary sequence diagram for that target. Next, the characteristics of the threat must be specified. The response force deployment time and delay and detection values for each protection element on the adversary sequence diagram must be defined. All of this information is used as input to the SAVI code. The code calculates the probability of interruption for each path on the adversary sequence diagram. It lists the ten most vulnerable paths and ranks them in order of their vulnerability. The analysis results are also given in the form of graphs and path display. The distribution graph shows the distribution of the probability of interruption for all paths and a specified response force time. The sensitivity graph provides information on the sensitivity of response force time. The vulnerability graph describes the probability of interruption and the time remaining after interruption for the ten most vulnerable paths and a specified response force time. The interpretation of these results can suggest the need for sensitivity analysis of data that has been input to the code, as well as possible PPS upgrades to the most vulnerable paths.

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 would also need to be reevaluated. An analysis of the redesigned system is performed. This cycle continues until the results indicate that the PPS meets the protection objectives.

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. The latest technology to support the design of an effective PPS was presented. 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, such as EASI and SAVI. If the evaluation reveals any vulnerabilities, the initial system design must be redesigned to correct the vulnerabilities and another analysis of the redesigned system is performed.

This work is supported by the U.S. Department of Energy under Contract DE-AC04-94Al85000.