

# **Physical Protection Systems: Concepts, Analysis, and Practice in the ET Classroom**

Guillermo Rico  
[gurico@nmsu.edu](mailto:gurico@nmsu.edu)

and

Jeffrey S. Beasley  
[jbeasley@nmsu.edu](mailto:jbeasley@nmsu.edu)

Department of Engineering Technology  
New Mexico State University  
Las Cruces, NM 88003

## **Abstract**

In 1997, the departments of Engineering Technology and Criminal Justice jointly developed and established the Security Technology minor for CJ and ET majors. This program was one of the results of a grant supported by the FBI and the Department of Justice.

Students pursuing this minor take courses from both departments and receive adequate preparation for understanding basic concepts, hardware, and procedures in the security technology field that would allow them to increase the possibility of obtaining employment in this growing field.

One of the courses required for the minor, Analysis of Physical Protection Systems, is an offspring of a course offered by security staff at Sandia Laboratories. Originally, Sandia used this course to train security personnel in nuclear facilities. In time, it evolved into a general course for the protection of all kinds of facilities such as government agencies, laboratories, research institutions, and manufacturing facilities.

The purpose of this paper is to describe the contents and interdisciplinary focus of this course: Objectives, basic concepts, sensor devices, electronic equipment, assessment techniques, response to intrusion, and examples of hands-on experience in the laboratory.

## **Introduction**

In 1978, Sandia Laboratories was commissioned by the Department of Energy to conduct the International Training Course on Physical Protection of Nuclear Facilities and Materials. Years later, Sandia also developed a training course on physical security for general facilities based on the same basic principles. In 2000, Mary Lynn Garcia, who had been heading the Sandia training courses, wrote the book "The Design and Evaluation of Physical Protection Systems," published by Butterworth-Heinemann in 2001. We adopted the book for our ET 456 class, Analysis of Physical Security Systems. The book replaced the Sandia manual we had been using for three years.

In this course, the underlying principles encompass a process in which the goal is to design a physical protection system (PPS) in three broad steps: (1) determine security system objectives, (2) design the system, and (3) analyze and evaluate the system.

In order to establish the objectives of the PPS, a detailed study of the facility is essential for identifying probable targets. Characterization of facility operations and conditions requires developing a thorough description of the facility using available documentation and blueprints. Any existing protection

features need to be identified and characterized. As a consequence of facility characterization, identification of targets will naturally follow, and with this, a threat definition can be established including types of probable adversaries.

With physical protection objectives established, the next step is to design the PPS by combining security technology elements, personnel, communications, and procedures to devise a comprehensive protection system that provides three main functions: detection, delay, and response. *Detection* is the discovery of an adversary action which must be followed by an assessment of the alarm to verify whether there is an actual intrusion. *Delay* is the function of slowing down adversary progress during an intrusion to give the guards more time to respond. *Response* is the actions taken by the response force to prevent adversary success; it includes proper communications and protected deployment to the point where interruption of the adversary is to take place.

Finally, the system needs to be analyzed and evaluated in order to determine whether the protection system is effective or needs to be improved. This can be done by simply checking if all the protection features are in place and working properly. However, a true high-performance system can only be achieved by doing more sophisticated qualitative and quantitative analyses based on measurable levels of performance. This is normally done through specialized software that takes into account diverse parameters and yields a numeric result of performance level.

The purpose of this paper is to briefly describe the three PPS functions and how they are approached in the Engineering Technology classroom in an interdisciplinary environment that combines electronics, sensor technology, video, and procedures to establish an effective protection system.

## **PPS Functions: Detection, Delay, and Response**

An effective physical protection system integrates people, equipment, and procedures for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. Depending on the assets and possible targets in the facility, a probable type of adversary may be identified. Adversaries can be categorized into three main groups: outsiders, insiders, and outsiders working in collusion with insiders. *Outsiders* include terrorists, criminals, extremists, and hackers. An *insider* is considered anyone with knowledge of operations in the facility and who has unescorted access to security areas and sensitive information. An outsider that operates with insider assistance represents a great challenge for the security system since the insider can move around the facility without raising suspicion and can choose the best time to act. Regardless of these possibilities, the PPS must respond to the challenge and prevent an attack by bringing into effect its three main functions: detection, delay, and response.

### **The Detection Function**

Detection is the discovery of an adversary action. It includes sensing of covert or overt intrusion activities. The following is a typical detection sequence:

1. A sensor reacts to a stimulus and initiates an alarm.
2. The information from the sensor is reported and displayed.
3. A person assesses the information and judges the alarm to be valid or invalid. (Note: detection without assessment is not considered detection.)

An increasing number of exterior and interior sensors for intrusion detection are in the market today. They are designed to respond to specific stimuli and are classified according to whether they are active or passive, covert or visible, volumetric or line detection, line-of-sight or terrain following, and according to application modes. Some are associated with fences, others are buried, and others are freestanding such as infrared sensors and video motion detectors. All sensors are susceptible of generating invalid alarms, called nuisance alarms, which are caused by anything other than an intrusion. Invalid alarms caused by faulty equipment are called false alarms. Some sensors are of the type called dual

technology because they respond to two different stimuli thereby reducing the probability of generating nuisance alarms.

In interior environments, detection of moving objects or persons plays a very important role in physical security. Most common types are infrared and microwave sensors. For detection of entry through doors or windows, the most common types are electromechanical sensors such as magnetic switches and vibration detectors. Protection of large metallic objects is commonly done through proximity sensors where the metallic object itself becomes part of the detection system.

Assessment of alarms is normally done with video cameras strategically located around the facility and aimed to probable targets. Additionally, video cameras can also be effectively used as motion sensors, in which case they are called video motion detectors, or VMDs. They can only be used as sensors, however, in places where there is no movement of objects or persons, such as in storage rooms or vaults.

*Entry control* is also included in the detection function. It allows the entry and movement of authorized persons and materials and detects any attempt of unauthorized entry. There are many different technologies for entry control of personnel, but in essence, an entry control system verifies if the person trying to gain access into a facility is in reality who they claim they are. This is based on whether the person has a valid credential, or knows a valid personal identification number, or possesses the proper unique physical characteristic that matches the one on record. In other words, verification is done based on what you have, what you know, or what you are. Examples of credentials include photo ID badge, magnetic card, bar code card, and proximity card, with the last one being among the most secure credential systems these days.

In increasing use recently, *biometric* identification systems make use of unique physical characteristics such as fingerprints, hand geometry, retinal pattern, speech recognition, and handwriting. Fingerprinting has been in use for many years and is considered one of the most reliable means of distinguishing one individual from another. With modern technology based on image processing and pattern recognition, automatic fingerprinting is now a common means for entry control. Another example of advanced technology is the retinal scan device, which recognizes the unique pattern of blood vessels in the retina of the eye.

### **The Delay Function**

This function provides elements of delay that slow down adversary progress. Delaying an adversary is an effective means of giving the response force adequate time to respond and interrupt the adversary. Delay elements are normally barriers in the form of fences, barbed concertina tape (BTC), reinforced walls and doors, cages around storage bins, heavy duty roll-up doors, to mention a few. Overall PPS effectiveness can be increased by placing sensors at delay points, preferably in a way that delay takes place right after detection to improve the assessment function. Delay before detection can only be a deterrent and not an effective measure because it does not provide additional time to respond to the adversary. Delay elements outside the facility, such as big boulders, trees and shrubbery, could force adversaries to change or abandon their tactic.

Conventional construction is relatively weak for a highly motivated and well-trained attacker. Chain-link fences can only stop small vehicles but are totally ineffective against medium and large trucks. However, if an adversary encounters a series of progressively more difficult barriers, he will be forced to carry heavier equipment and tools that will contribute to increase the delay time. In any event, the most cost-effective means of improving the delay provided by a chain-link fence against climbing is to add a roll of BTC to the outriggers.

Other forms of delay elements include reinforced concrete walls, special doors and windows, reinforced roofs and floors, and dispensable barriers. *Dispensable barriers* are those that are deployed only when necessary, that is, during an attack. They are normally foams or other chemical products that can delay or even totally immobilize an intruder. Due to their high cost, they are more appropriate to use near the asset to be protected, preferably in a closed area to contain the collateral contamination and reduce the clean up task.

## **The Response Function**

The response function consists of the actions taken by the response force to prevent adversary success and includes: responding personnel, contingency planning, communication, and interruption. Responding personnel may include proprietary or contract guards, local and state police, and in some cases federal agencies such as the FBI, DEA, or Customs.

*Contingency planning* is the development of well-documented procedures for identifying potential targets, respond to different threats, interact with outside agencies, and determine what level of force guards can use in different situations. Once potential targets are identified, security personnel can evaluate likely adversary routes and develop tactical plans to address various threats to the facility and to determine guard patrol routes and schedules. Procedures and plans for guard actions in the event of an adversary attack should be well established and practiced through periodic training exercises. If outside agencies are likely to participate in the response, joint training exercises should be planned and executed.

*Communication* is a vital component of the response function since all other system functions depend heavily on proper communication between all responding personnel. Information must be transferred through this network with speed and accuracy. Communication to the response force must contain information about adversary actions and instructions for deployment. The most common means of communication to the response force is through clear-voice radios, normally of the FM (frequency modulation) type. Clear voice means that the signal has not been encrypted or encoded. As a result, however, *eavesdropping* on the part of adversaries is possible through the use of standard receivers or scanners. If an adversary can monitor a conventional radio transmission, they can also transmit *deceptive* messages with a conventional transmitter tuned to the same channel frequency.

Another form of disturbing a radio transmission, known as *jamming*, can be done by inserting an unwanted signal into the channel that can mask a desired signal. If the jamming signal is of sufficient power, it can totally destroy the true signal making it unusable. Periodic jamming exercises should be established to practice procedures to counteract a jamming attack. Alternate means of communication, such as intercoms, public address, or cellular phones must be available at all times and everybody in the response force must know what to do in case of a jamming attack.

One modern technology for counteracting eavesdropping, deception and jamming is the spread-spectrum or frequency-hopping communication system. In this system, the master transmitter makes the other receivers to follow it automatically from channel to channel as the message is transmitted. For any particular receiver in the system, the message is received like any other continuous message. For an intruder, however, the transmission is going to sound like bits and pieces making impossible the intelligibility of the message.

The last segment of the response function is *interruption*, which is defined as the successful arrival in sufficient number of the response force at an appropriate location to confront the adversary. The probability of successful interruption can be enhanced by the use of deployment through known, protected paths. To measure the effectiveness of a PPS, a procedure called *timely detection* can be performed to obtain the probability of interruption based on cumulative delays and probabilities of detection along adversary paths. Timely detection consists in obtaining a cumulative probability of detection at a point in time and place where the remaining adversary time just exceeds the guard response time. In other words, at a point where there is still enough time left for the response force to interrupt the adversaries before their goal is completed.

## **Laboratory Practice in Engineering Technology**

In order for the students to better perceive what physical protection is about, they practice with video cameras and perform field experiments that involve measuring distances and widths and determine camera placement according to the size of the assessment zone.

They also put together an entry control system using high-tech equipment by Hirsch Electronics, a prime provider of security equipment for private and government facilities in the U.S. and abroad. The students get familiar with the operation and wiring of components such as controllers, door lock

operators, keypads, proximity sensors, and line supervisors. Besides wiring the equipment, they also practice with the programming of the controller according to logistic requirements of the system such as operating hours, alarm modes, and entry privileges.

At the end of the semester, students participate in a project where they are given a fictitious facility that can use different levels of improvements. And to verify that improvements will perform as expected, they run a timely detection simulation using a computer program developed by Sandia Laboratories.

## **Conclusion**

In recent years, the world has witnessed an increasing number of terrorist attacks in numerous countries and places. The need for colleges to get involved in the dissemination of new technologies and strategies to counteract these activities is not only desirable but an unquestionable need. The departments of Engineering Technology and Criminal justice have been contributing to this effort through their joint minor in Security Technology and Intelligence Studies for 8 years, and have continually attracted a significant number of students from both departments. Students who graduate with this minor will be better prepared to contribute to efforts aimed at protecting people, facilities and assets.

## **References**

Garcia, Mary Lynn – The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, 2001.

Alexander, George and Dennis Giever – A Security Technology Minor, the Technology Interface, Fall 1997 issue. <http://et.nmsu.edu/~etti/fall97/security/security.html>

Sandia National Laboratories – Physical Protection System Design Course manual, 1999.