# 7. Introduction to the Design of Physical Protection Systems

**Abstract.** Detection, delay, and response are required functions of an effective physical protection system (PPS). The total time for detection and response must be less than the time remaining (delay) for the adversary to complete his task after the first sensing. An effective PPS has several specific characteristics. A well-designed system provides defense in depth, exhibits balanced protection, and minimizes the consequence of component failures. 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.

## 7.1 Introduction

<table>
<thead>
<tr>
<th>Definition of a System</th>
<th>A system may be defined as a collection of components or elements designed to achieve an objective according to a plan. The designer of any system must have the system’s ultimate objective in mind.</th>
</tr>
</thead>
</table>
| Objective: Prevent Theft and Sabotage | The objective of a physical protection system (PPS) is to prevent radiological sabotage and/or theft of nuclear materials present within the facility (INFCIRC/225/Rev.5, para.32.1).

A PPS accomplishes its objectives by either deterrence or a combination of detection, delay, and response. The system functions of detection, delay, and response and their interaction will be discussed in this session. More details will be presented in the next few sessions.

### Course Map of Detection, Delay, and Response Sections

- **Detection Sections:**
  7. Intrusion Detection Sensors
  8. Entry Control
  9. Contraband Detection
  10. Alarm Assessment
  11. Alarm Communication and Display

- **Delay Sections:**
  12. Access Delay

- **Response Sections:**
  13. Response

| Balancing Technology with Response Force | The system functions of detection and delay can be accomplished by the use of either technology and/or guards. Response is handled by the response force who also use technology. There is always a balance between the use of technology and the use of people. Facility conditions and applications affect the preferred choice. For detection and delay, the role of hardware and technology will be emphasized in the lecture sessions and the role of response force and procedures will be discussed primarily in the subgroup sessions. |
7.2 PPS Functions

<table>
<thead>
<tr>
<th>Deterrence vs. Defeat</th>
<th>Theft and sabotage of the facility may be prevented in two ways: by deterring the adversary or by defeating the adversary.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deterrence Cannot Be Measured</td>
<td>Deterrence occurs by implementing a physical protection system that is perceived by potential adversaries as too difficult to defeat; it makes the facility an unattractive target. INFCIRC/225 Rev. 5, (para, 4.2.3.63.16) states that “Sanctions against the unauthorized removal of nuclear material and against sabotage are important to an effective State system of physical protection should be part of the State’s legislative or regulatory system.” Sanctions may deter an adversary from illegal actions. The problem with deterrence is that it is impossible to measure or guarantee. It would be a mistake to assume that simply because an adversary has not challenged a system, the system is effective in either deterring or adequately stopping an adversary attack.</td>
</tr>
<tr>
<td>Defeating the Adversary</td>
<td>Defeating the adversary refers to the actions taken by the response force to prevent an adversary from accomplishing his goal after he actually begins a malicious act against a facility.</td>
</tr>
<tr>
<td>Primary PPS Functions</td>
<td>It is essential to consider the system functions in detail, because a thorough understanding of these functions and the measure of effectiveness of each is required to evaluate the system. The primary PPS functions are</td>
</tr>
<tr>
<td>Detection</td>
<td>• Intrusion sensing,</td>
</tr>
<tr>
<td></td>
<td>• Alarm communication, and</td>
</tr>
<tr>
<td></td>
<td>• Alarm assessment.</td>
</tr>
<tr>
<td>Delay</td>
<td></td>
</tr>
<tr>
<td>Response</td>
<td>• Interruption:</td>
</tr>
<tr>
<td></td>
<td>– Communication</td>
</tr>
<tr>
<td></td>
<td>– Deployment</td>
</tr>
<tr>
<td></td>
<td>• Neutralization</td>
</tr>
</tbody>
</table>

7.2.1 Performance Considerations

Factors Affecting Performance

Performance of the technology elements contributing to the functions of detection, delay, and response will vary based on numerous factors:

• The component design
• Unit to unit differences in a specific component, due to manufacturing inconsistencies
7. Design of Physical Protection Systems

- Installation
- Maintenance
- Environmental factors influencing component operation
- The specific adversary threat
- Specific tactics used by an adversary

7.2.2 Detection

Definition of Detection

Detection is the discovery of an adversary action. It includes sensing of covert or overt actions. In order to discover an adversary action, the following events need to occur:

- A sensor reacts to an abnormal occurrence and initiates an alarm.
- The information from the sensor and assessment subsystems is reported and displayed.
- A person assesses the information and judges the alarm to be valid or invalid. If assessed to be a nuisance alarm, detection of an adversary has not occurred. Furthermore, a sensor alarm without assessment is not considered detection.

Measures of Effectiveness for Detection

The measures of effectiveness for the detection function are

- The probability of sensing an adversary action
- The time required for reporting and assessing the alarm. Probability and time are generally related as shown in Figure 7–1. A sensor activates at time $T_0$. Then at a later time such as $T_1$, $T_2$, or $T_3$, a guard receives information from the sensor and assessment subsystems. If the time delay between when the sensor activates and when the alarm is assessed is short ($T_1$), the probability of detection, $P_D$, will be close to the probability that the sensor will sense the abnormal occurrence, $P_s$. The probability of detection decreases as the time until assessment increases. This is because a timely assessment must be able to verify that an adversary has been in the sensor’s detection area. As time passes, the adversary will have moved on, to another area perhaps with no evidence of his intrusion.
- The frequency of nuisance alarms. A nuisance alarm is defined as an alarm that is not caused by an actual intrusion attempt. Many environmental, technology, operational, and installation factors can lead to nuisance alarms. As nuisance alarm rates increase, the guards will begin to disregard the validity of that sensor and so its effective performance will diminish.
- The probability of an accurate assessment. If the assessment component of detection is degraded, then overall detection performance will suffer.

Detection by People

The guard force or other personnel can provide some detection. Guard force at fixed posts or on patrol may serve a vital role in sensing and
assessing an intrusion. Facility employees may contribute to detection if the two-person rule is used in critical areas.
7.2.2.1 Assessment

Effective Assessment

An effective assessment system provides two types of information associated with detection:

- information about whether the alarm is a valid alarm or a nuisance alarm, and
- details about the cause of the alarm—when, where, what, who, and how many.

![Figure 7–1. Probability of Detection vs. Time Between Sensing and Assessment](image)

7.2.2.2 Entry Control and Contraband Detection

Entry Control Factors

Entry control has two major aspects: 1) allowing entry to authorized personnel and 2) detecting the attempted entry of unauthorized personnel and preventing their entry.

The measures of effective entry control are

- Throughput. The number of authorized personnel allowed access per unit time.
- False accept rate. The rate at which unauthorized persons are allowed entry.
- False reject rate. The rate at which authorized persons are denied entry.

Contraband detection is analogous to entry control, but it is applied to equipment and material instead of people.
7.2.3 Delay

Definition of Delay
Delay is the slowing down of adversary progress so that a timely response can be executed. Delay can be accomplished by passive barriers, locks, and activated delays. The response force can be considered elements of delay if they are in fixed and well-protected positions.

Measuring the Effectiveness of Delay
The measure of delay effectiveness is the time required by the adversary (after detection) to overcome each delay element. Because a response action can only begin after detection has occurred, any delay prior to detection is of no value to the effectiveness of the physical protection.

7.2.4 Response

Definition of Response
The response function consists of the actions taken by the response force to prevent adversary success. Response consists of:

- Deployment—Actions of the response force from the time an alarm communication is received until the force is in position to neutralize the adversary.
- Interruption—A sufficient number of response force personnel deploying at the appropriate location to stop the adversary’s progress.
- Neutralization—The act of gaining physical control of the adversary before his goal is accomplished.

Measuring the Effectiveness of Response
Measures of response effectiveness include metrics for communications, deployment, and neutralization. The effectiveness measures for response communications are:

- Probability of communication to response force
- Time to communicate

Relationship Between Communication Time and Probability
The probability of communication and the time required for communication are related, as shown in Figure 7–2. The time after information is initially transmitted may vary considerably depending on the method of communication. After the initial period, the probability of valid communication begins to increase rapidly. With each successive communication, the probability of correct and current data being communicated is increased.
7. Design of Physical Protection Systems

The effectiveness measures for deployment and neutralization are

- Probability of deployment to adversary location,
- Time to deploy, and
- Response force effectiveness.

7.3 Adversary Task Time vs. PPS

The PPS must perform the functions of detection, delay, and response. The total time for detection and response must be less than the time remaining (delay) for the adversary to complete his task after the first sensing. Figure 7-3 shows the relationships between adversary task time and the time required for the physical protection system to defeat the adversary. The total time required for the adversary to accomplish his goal has been labeled Adversary Task Time. It is dependent upon the delay provided by the physical protection system. The adversary begins his task at some time before the occurrence of the first alarm, labeled on the diagram $T_0$. The adversary task time is shown by a dotted line before this point, because without detection this period of time is indeterminate. Any system delay in the area before the first possible detection has no effect on the physical protection system performance.

After the first sensing, the alarm information must be reported and assessed to determine if the alarm is valid. The time at which the alarm is assessed to be valid is labeled $T_D$, and at this time the location of the alarm must be communicated to the members of the response force. Further time is then required for the response force to deploy in adequate numbers and with adequate equipment to interrupt and neutralize the adversary actions. The time at which the response force interrupts adversary actions is labeled $T_I$, and adversary task completion time is labeled $T_C$. Clearly, in order for the physical protection system to accomplish its objective, $T_I$ must occur before $T_C$. It is equally clear that the first sensing should occur as early as possible and $T_0$ (as well as $T_D$ and $T_I$) should be as far to the left on the time axis as
7.4 Characteristics

The procedures of the physical protection system must be compatible with the facility procedures. In addition, all of the hardware elements of the system must be installed, maintained, and operated properly. Security, safety, and operational objectives must be accomplished at all times. A well-engineered PPS has the following characteristics:

- defense in depth
- balanced protection
- high reliability

7.4.1 Defense in Depth

INFCIRC/225 Rev. 5 para. 4.2.5.23.45 states that “State requirements for physical protection should be based on the concept of defense in depth for preventive and protective measures. The concept of physical protection requires a designed mixture of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout).”

Adversaries Should Face a Variety of Protective Devices

Defense in depth is a design concept in which an adversary should be required to avoid or defeat several protective devices in sequence. For example, an adversary might have to penetrate three separate barriers before gaining entry to a reactor control room. The times to penetrate each of these

---

1 A concept used to design physical protection systems that require an adversary to overcome or circumvent multiple obstacles, either similar or diverse, in order to achieve his objective. INFCIRC/225 para. 2.3
7. Design of Physical Protection Systems

barriers may not necessarily be equal, and the effectiveness of each may be quite different, but each will require a separate and distinct act by the adversary as he moves along his path. The effect produced on the adversary by a system that provides defense in depth will be to:

- increase uncertainty about the system to the adversary
- require additional tools and more extensive preparations prior to attacking the system
- create additional steps where the adversary may fail or abort the mission.

7.4.2 Balanced Protection

Effective Elements Span Entire PPS
Balanced protection implies that no matter when, where, or how an adversary attempts to accomplish his goal, he will encounter effective elements of the physical protection system. Consider, for example, the barrier surface that surrounds a reactor control room. This surface may consist of:

- walls, floors, and ceilings of several types
- doors of several types; equipment hatches in floors and ceilings
- heating, ventilating, and air conditioning openings with grilles.

7.4.3 High Reliability

Know Potential Causes
A complex system will experience some component failures during its lifetime. Causes of component failures in a PPS are numerous and can range from environmental factors (which may be expected) to adversary actions beyond the scope of the threat used in the system design.

Prepare Contingency Plans
Although it is important to know the cause of component failure to restore the system to normal operation, it is more important that contingency plans are implemented so the system can continue to operate. Requiring portions of these contingency plans to be carried out automatically (so that redundant equipment automatically takes over the function of disabled equipment) may be highly desirable in some cases. Some component failures may require aid from sources outside of the facility in order to minimize the impact of the failure.

Structural or Safety Requirements Affect Balance of PPS
For a completely balanced system, the minimum time to penetrate each of these barriers would be equal, and the minimum probability of detecting penetration of each of these barriers should be equal. However, complete balance is probably not possible or desirable. Certain elements, such as walls, may be extremely resistant to penetration, not because of physical protection requirements, but because of structural or safety requirements. Door, hatch, and grille delays may be considerably less than wall delays and still be adequate. There is no advantage in over-designing by, for example, installing a costly vault door that would take several minutes to penetrate with explosives, if the wall were plasterboard that could be penetrated in a
Features designed to protect against one form of threat should not be eliminated because they overprotect against another threat. The objective should be to provide adequate protection against all design basis threats on all possible paths and to maintain a balance with other considerations, such as cost, safety, or structural integrity.

Detection, delay, and response are required functions of an effective physical protection system. In order to design an effective physical protection system, these functions must be combined in a proper space and time relationship. These security functions must be performed in sequence and within a length of time that is less than the time required for the adversary to complete his tasks.

The performance measures for these functions are:

**Detection**
- Probability of sensor alarm
- Time for communication and assessment
- Frequency of nuisance alarms
- The probability of an accurate assessment

**Delay**
- Time to defeat obstacles

**Response**
- Probability of accurate communication to response force
- Time to communicate
- Probability of deployment to adversary location
- Time to deploy
- Response force effectiveness in neutralizing the adversary

Some potential adversaries may be deterred from attacking a facility because it is protected by an apparently effective physical protection system. The deterrence function of a physical protection system is difficult to measure, and reliance on successful deterrence can be risky; thus it is considered a secondary function and is not discussed further in this course.