MODULE 5: FACILITY CHARACTERIZATION
Briefing Overview

• A security system must accomplish its objectives either by deterrence or a combination of:
  • Detection
  • Delay
  • Response
• There is a balance between the use of hardware and the use of guards
• A well designed system provides protection-in-depth, minimizes failures, and exhibits balanced protection
3 Step Process

1. Define System Objectives
   - What are we protecting?
   - Who are we protecting it from?
   - What technology tools do we have to protect it?
   - What controls/procedures do we have to protect it?
   - What path will the adversary follow?

2. Design/Characterize System
   - When will security neutralize threat?

3. Evaluate System
Facility Characterization

• Requires the investigation of anything that impacts the performance of the MPC&A system

• This includes:
  - Site information
  - Physical protection system (PPS) components
  - Material Control & Accounting Systems
  - Information Sources
    • Documentation
    • Open sources
    • Site survey
    • Test data
    • Military and police
Facility Characterization

Types of information to collect:

- Physical conditions
- Facility operations
- Facility policies and procedures
- Insider access/authority/knowledge and insider groups
- Regulatory requirements
- Safety considerations
- Legal issues
- Organizational protection goals and objectives
- Others?
Physical Conditions

- Site boundaries, fences, barriers
- Topography, weather, and environment
- Building construction materials for walls, ceilings, floors, doors, windows, etc.
- Areas and rooms
- Access points
- Heating, ventilation, air conditioning
- Communication paths and types
- Power distribution system
- Environmentally controlled areas
- Locations of nuclear materials and vulnerable equipment
- Locations of non-target, hazardous material
Facility operations

Operational Activities

- Products and processes
- Operational hours
- Number, types, and locations of employees
- Visitors and vendors
- Access management

On-site location and movement of materials

- Shipping and receiving process
- Intra-site movements/convoy
- Internal processes
- Tracking mechanisms
Characterize The System

1. Physical *Protection* is a collection of integrated components specifically designed to allow response forces to detect penetration and respond to it.
   • Physical Protection has a presence at every level of the site

2. Material *Control* is a collection of integrated components and procedures designed to control the location and use of nuclear materials through containment and surveillance
   • Material Control is present at the vault through the protected area

3. Material *Accounting* provides a complete, accurate, and timely record of the nuclear material inventory and tools used to calculate the inventory
Security System Goals

**Design Strategies**

1. **Deter the adversary**
   - Implement a system that potential adversaries perceive as too difficult to defeat and thus do not attack
   - Deterrence is difficult to quantify or measure
   - Not all adversaries can be deterred

2. **Defeat the adversary**
   - Required functions: detection, delay, response
     - Integrated as a system
   - Recommended design approach and the one used in design of systems protecting critical assets
Security Protection Goals

Relationship between Risk and Time

• Probability of a security system’s chance for success increases the longer it takes the adversary to complete their mission.

• Goal of a system should be to integrate detection and delay with response times and capabilities.
## Physical Protection

### Integrated System Components

<table>
<thead>
<tr>
<th>DETECTION</th>
<th>DELAY</th>
<th>RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Intrusion Sensing</td>
<td>- Passive Barriers</td>
<td>- Guards, Response Force (RF)</td>
</tr>
<tr>
<td>- Exterior Sensors</td>
<td>- Active Barriers</td>
<td>- Interruption</td>
</tr>
<tr>
<td>- Interior Sensors</td>
<td></td>
<td>- Communication to RF</td>
</tr>
<tr>
<td>- Contraband Detection</td>
<td></td>
<td>- Deployment of RF</td>
</tr>
<tr>
<td>- Entry Control</td>
<td></td>
<td>- Neutralization</td>
</tr>
<tr>
<td>- Alarm Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Alarm Communication &amp; Display</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Integration

Adversary Task Time

Total MPC&A Response Time

Detection

Response Force Time

Adversary Begins Task

Adversary Completes Task

Adversary Begins Task

Adversary Completes Task
Detection

- Objective is to sense covert / overt adversary action
- Initiate alarm, report, and display alarm
- Assess information and judge validity
  - Detection without assessment is not considered detection
Protection Elements: Detection

Performance Metrics are broken into 2 categories:

1. Function (Probability of detection $P_D$)
   - Probability of sensor alarm ($P_S$)
   - Probability of alarm communication ($P_{AC}$)

2. Time
   - Alarm Signal Communication Time ($T_{AC}$)

Diagram:
- Alarm Sensor
- Control Box
- Network
- Server
- Central Alarm Station
- Assessment System
Protection Elements: Detection

- Nuisance Alarms and sensitivity of sensors can reduce $P_D$
- $P_D$ for a sensor depends on:
  - Sensor hardware design
  - Installation conditions
  - Sensitivity setting
  - Weather conditions (exterior sensors)
  - Maintained condition
  - Target (adversary) size and speed
Protection Elements: Assessment

• Performance measures (Function & Time)
  - Probability of assessment $P_A$
    - Probability of video signal ($P_V$)
    - Probability of correct assessment ($P_A$)
    - Alarm assessment time ($T_A$)
    - Communication time ($T_{AC}$)
    - Nuisance alarm rate (NAR)

• High NARs increase probability of incorrect assessment

• A long time delay between sensor alarm and assessment lowers $P_D$

$$H_{FOV} = \frac{W_1 D}{FL}$$
Protection Elements: Delay

• Installing delay upgrades can increase the adversary task time.

• Features of a good barrier system
  • Provides delay **immediately** after detection
  • Exhibits balanced design; no weak links
  • Uses delay-in depth (requiring different tools/skills)
  • Maximized at the target area
  • Delay features are present 100% of time or take compensatory measures
  • Design a penalty into parts
Protection Elements: Delay Metrics

- Performance measures (Function & Time
  - Time to penetrate or bypass barriers
  - Time to travel across areas
- Delay must occur after detection
  - Delay before detection is deterrence
- Can be composed of
  - Passive Barriers
  - Active Barriers
  - Response ( Interruption)
  - Traversal time
Protection Elements: Response

• Determine types of response
  - Number of responders
  - Response times
  - Rules of engagement
  - Roles and trained capabilities
  - Weapons, equipment, vehicles
  - Tactics, strategies, and access

• Response force initial locations and deployment positions

• Review response procedures

• Review assessment, communication, and deployment times
Protection Elements: Response

**Response Posture**

- Two types of response used to counter attempted unauthorized removal (theft) of nuclear material or act of sabotage
  - **Interruption**
    - Stopping the progress of the adversary by the response force
  - **Neutralization**
    - Rendering the adversary actions and plans ineffective

\[
\text{Probability of Interruption} \times \text{Probability of Neutralization} = \text{System Effectiveness}
\]
**Goals & Performance Metrics**

- The role of an immediate response force is to:
  1. Intermpt adversary progression of attack
  2. Neutralize adversary team or render the adversary ineffective

*The time it takes to accomplish this metric should be less than the total adversary task time*

---

**Interruption** is a measure of detection, communication, delay, and response functions.

**Neutralization** is a measure of response success, given arrival.

---

**Diagram:**
- **Adversary Task Time**
- **Total MPC&A Response Time**
- **Detection**
- **Assessment Time**
- **Response Force Time**
- **Adversary Begins Task**
- **Adversary Completes Task**
- **Alarm Signal**
- **Assessment of Alarm**
- **Communication of Alarm to Response Force**
- **Deployment Preparation Time for Response Forces**
- **Deploy and Traverse Times for Response Forces**
- **Total PPS Response Time**
Tools For Managing Time

**DETECTION**
- Exterior/Interior Sensors
- Contraband Detection
- Alarm Assessment
- Alarm Communication & Display

**DELAY**
- Passive Barriers
- Active Barriers
- Response Forces
- Traversal Time

**RESPONSE**
- Response Force (RF)
- Interruption
  - Communication to RF
  - Deployment of RF
- Neutralization

---

**Diagram: Time Management**
- **Begin Action**
- **Adversary Task Time**
- **Time Remaining After Detection (Delay)**
- **PPS Response Time**
- **Detection Time**
- **Alarm Assessed**
- **Response Force Time For Interruption**
- **Time Remaining After Interruption For Neutralization**
Target Characterization

- Target Identification
- Threat Definition

What do we protect?

What are we protecting against?
- Theft
- Reputation of the facility
- Sabotage

How to protect the targets
- Design/Characterize PPS
1. Security Characterization defines the tools that are available to:
   • Detect the adversary
   • Assess the adversary
   • Delay the adversary timeline to allow
   • A response to the adversary that will:
     1. Interrupt adversary progression
     2. Eventually lead to neutralization

2. Total time for detection and response must be less than adversary task time