



Physical Security

John A. Milloy

Security Systems and Technology Center

February 4, 2004



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.





Elements of a Physical Security System

- **Security system design**
- **Graded protection**
- **Perimeter demarcation**
- **Structural hardening**
- **Access control**
- **Intrusion detection**
- **Response force**
- **Physical security procedures**
- **System performance testing**

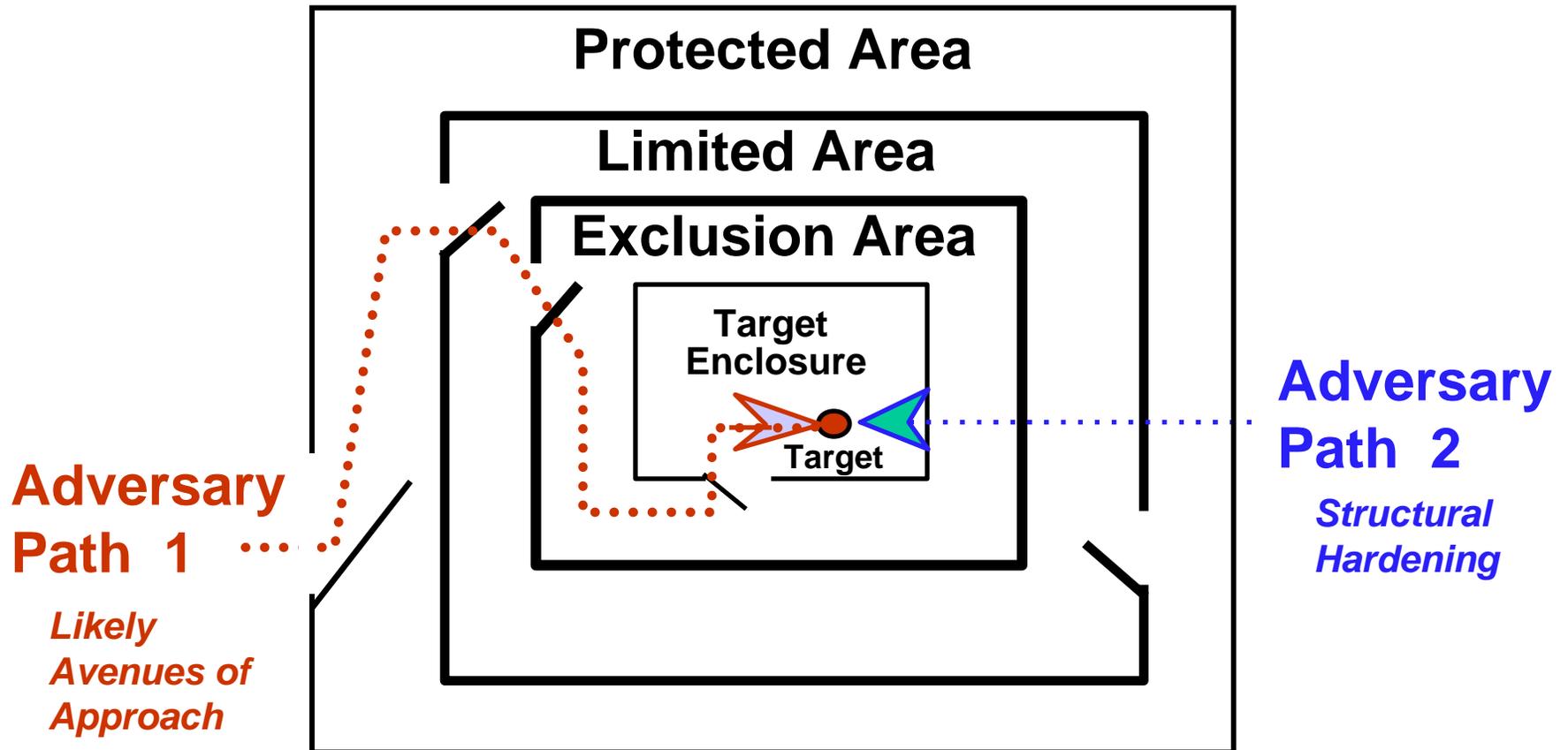


Security System Design Basis





Graded (Concentric) Approach





Concentric Layers of Security

- **Property Protection Areas**

- **Low consequence assets**

- Grounds
- Public access offices
- Warehouses
- Garages, ...

- **Limited Areas**

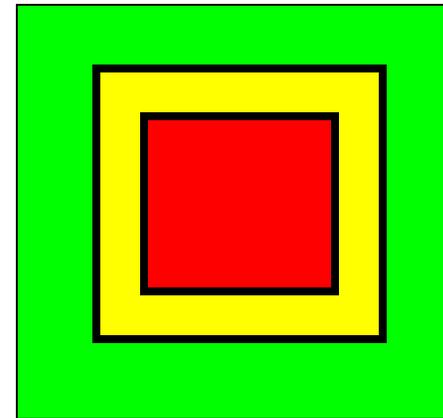
- **Moderate consequence assets**

- Laboratories
- Sensitive or administration offices
- Hallways surrounding Exclusion Areas, ...

- **Exclusion Areas**

- **High consequence assets**

- High containment laboratories
- Computer network hubs, ...





Property Protection - Perimeter

- **Fences**
 - **Mark the boundaries of your property**
 - **Announce your intention to protect the property**
 - **No Trespassing!**
 - **Discourage people from strolling onto your property**
 - **Elicit strong statement of intent from intruder**
 - **Cannot “accidentally” climb an 8-foot fence**



Property Protection - Perimeter





Property Protection - Perimeter

- **Fences**
 - **Mark the boundaries of your property**
 - **Announce your intention to protect the property**
 - **No Trespassing!**
 - **Discourage people from strolling onto your property**
 - **Elicit strong statement of intent from intruder**
 - **Cannot “accidentally” climb an 8-foot fence**
 - **Terrain features can also serve the purpose**
 - **Cliffs and water**
 - **Can be designed as vehicle barriers**



Property Protection - Perimeter





Limited Area - Structural Hardening

- **Increases adversary task time after detection**
 - **Allows response force to get into position to contain the adversary or prevent malevolent action**
 - **Is a factor in determining likely avenues of approach**
- **Passive Nature**
 - **Robust construction**
 - **Penetration makes lots of noise**
 - **Requires heavy tools and equipment**
 - **Minimal penetrations (doors, windows, ducts, vents, etc.)**
 - **Building complexity**
 - **Concentric shells**
 - **Long path times and devious routes**
- **Balanced strength (no vault door on a cardboard box)**
 - **Windows and doors as strong as adjacent walls**



Limited Area - Structural Hardening





Access Control

- Access control ensures that only authorized individuals are allowed into certain areas
- Increasingly strict controls as you move toward assets of highest consequence
 - Unique credential
 - Grants access to specific areas by specific personnel
 - Can be easily and quickly changed or revoked
 - Unique knowledge or physical characteristic
 - Assures that the person who presents the credential is the person to whom that the credential is issued
- Limited Areas
 - Requires unique credential for access
 - Electronic key card
 - Controlled key
- Exclusion Areas
 - Requires unique credential and unique knowledge for access
 - Electronic key card and keypad or biometric device
 - Controlled key and second individual to verify identity
- Electronic systems record and time-stamp valid transactions



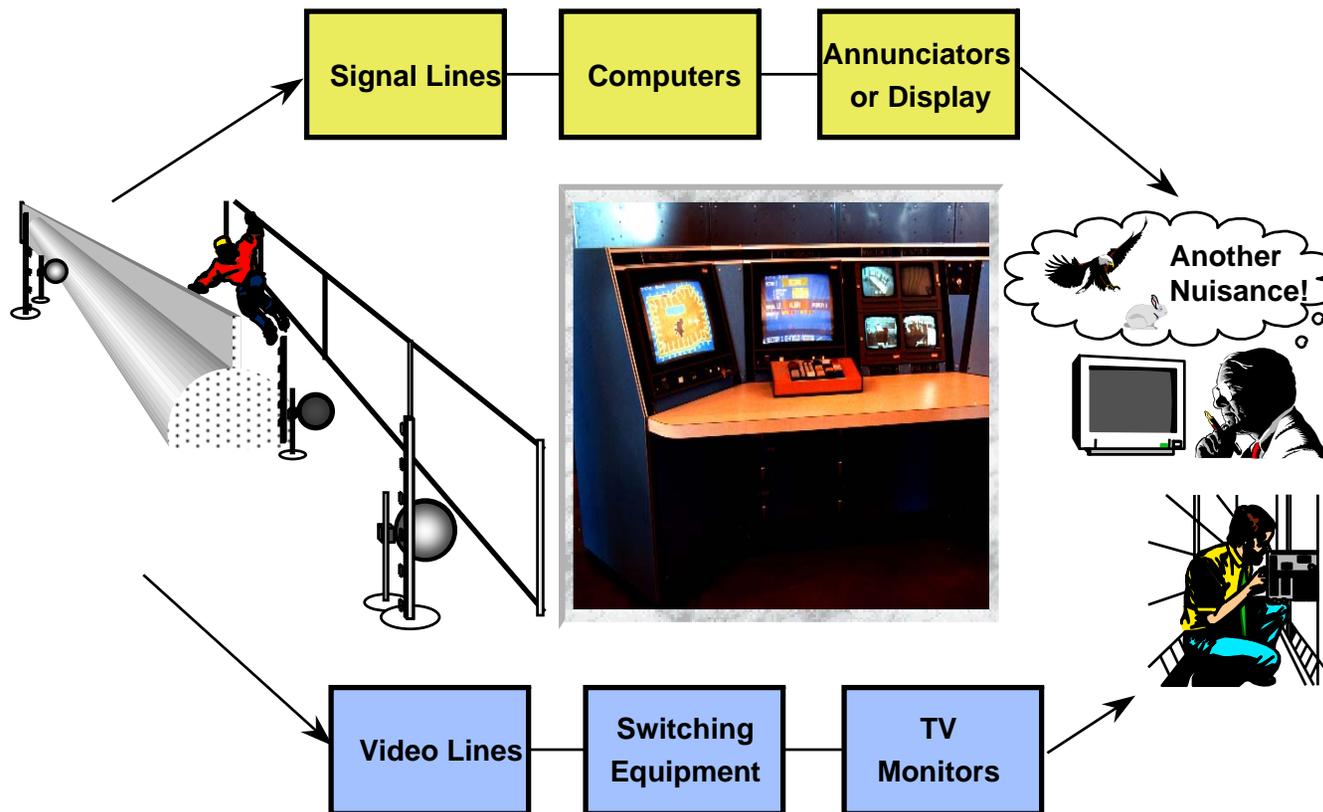
Intrusion Detection

- **Detects a security violation**
 - **Guards**
 - **Electronic sensors**
 - **Balanced magnetic switches (doors)**
 - **Glass break sensors (windows)**
 - **Volumetric motion sensors (rooms)**
 - **Line-of-sight sensors (perimeter)**
- **Assessment**
 - **Validation of violation before response**
 - **Can be direct (guards) or remote (video)**
 - **Direct observation takes time and can put guard in danger**
 - **Video is immediate and focused**
 - **Both require adequate lighting**
 - **Must support visual assessment of alarms**
 - **Must be compatible with video camera sensitivity**
 - **Deters opportunistic adversaries**



Electronic Alarm Communication and Assessment

Security Elements → Alarm Communication → Personnel





Response Forces

- **On-site guard force**
 - **Supports electronic systems:**
 - **Monitors Alarm Communication & Display (AC&D) system**
 - **Assesses electronic alarms at alarm console or at alarm location**
 - **Patrols perimeter and buildings**
 - **Summons and directs local law enforcement**
- **Local law enforcement (police)**
 - **Reinforces on-site guard force**
 - **Responds according to plan when summoned**
 - **Equipped and authorized to confront adversary**



Response Force Requirements

- **Qualification and training**
 - Enforcement responsibilities and skills
 - Equipment familiarity and training
 - Familiarity with facility features and operations
 - Knowledge of restricted area access and biosafety
- **Guard force orders**
 - List specific duties and limits of authority
 - Procedures for response to specific alarm conditions
 - Emergency response procedures
 - Notification list
- **Memorandum of understanding with local law enforcement**
 - Specific instructions and agreements
 - On-site training and orientation



Physical Security Procedures

- **Impose consequences for security violations**
- **Log personnel (including visitor) access to restricted areas including entry and exit times**
- **Establish controls on animal and supply handling**
- **Enforce escort policies**
 - **Visitors**
 - **Maintenance and cleaning personnel**
 - **Delivery personnel**
- **Train personnel on what to do about:**
 - **Unrecognized persons**
 - **Unusual or suspicious activity**



Performance Testing and Maintenance

- **Create security performance test plan and procedures**
- **Schedule periodic testing of hardware**
- **Schedule periodic testing of response force procedures**
- **Document test results**
- **Take corrective action**
 - **Schedule maintenance and repair of hardware**
 - **Corrective training and exercises for guard force**



Summary

- **Physical security may be implemented by electronic or mechanical means**
- **Response forces are required to achieve physical security**
 - **On-site response forces are more important for those systems that are mechanically based**
- **To achieve effective physical security, procedures must be established and enforced**
- **To achieve effective biosecurity, physical security must be supported by:**
 - **Personnel security**
 - **Material control and accountability**
 - **Material transfer security**
 - **Information security**
 - **Program management**