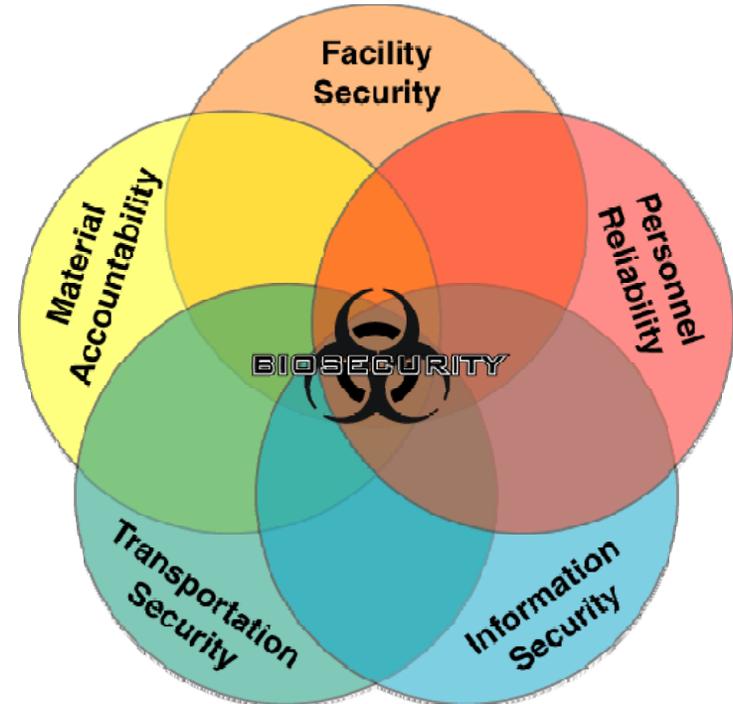

Principles of Design for a Physical Security System for Bioscience Laboratories

**International Biological Threat Reduction Department
Sandia National Laboratories
October 07, 2007**

**Physical Security for Bioscience Laboratories
ABSA pre-conference course**

Biosecurity System

- **Biosecurity system components**
 - **Physical security**
 - Personnel security
 - Material handling and control measures
 - Transport security
 - Information security
 - Program management practices
- Each component implemented based on results of risk assessment
- In general, biosecurity for
 - Moderate risk focuses on the insider
 - High risk focuses on both the insider and the outsider



How Physical Security Supports Laboratory Biosafety



- **Laboratory biosecurity supports the laboratory biosafety agenda of preventing disease in people, animals, and plants and minimizing the risk of worker injury**
 - **Limits the number of individuals who may be exposed to the hazards**
 - **Limits access to those who are professionally qualified and properly trained to be there**
 - **Access control procedures and records can be used to support investigations of laboratory safety or security incidents.**

Potential Conflicts between Laboratory Biosafety and Physical Security

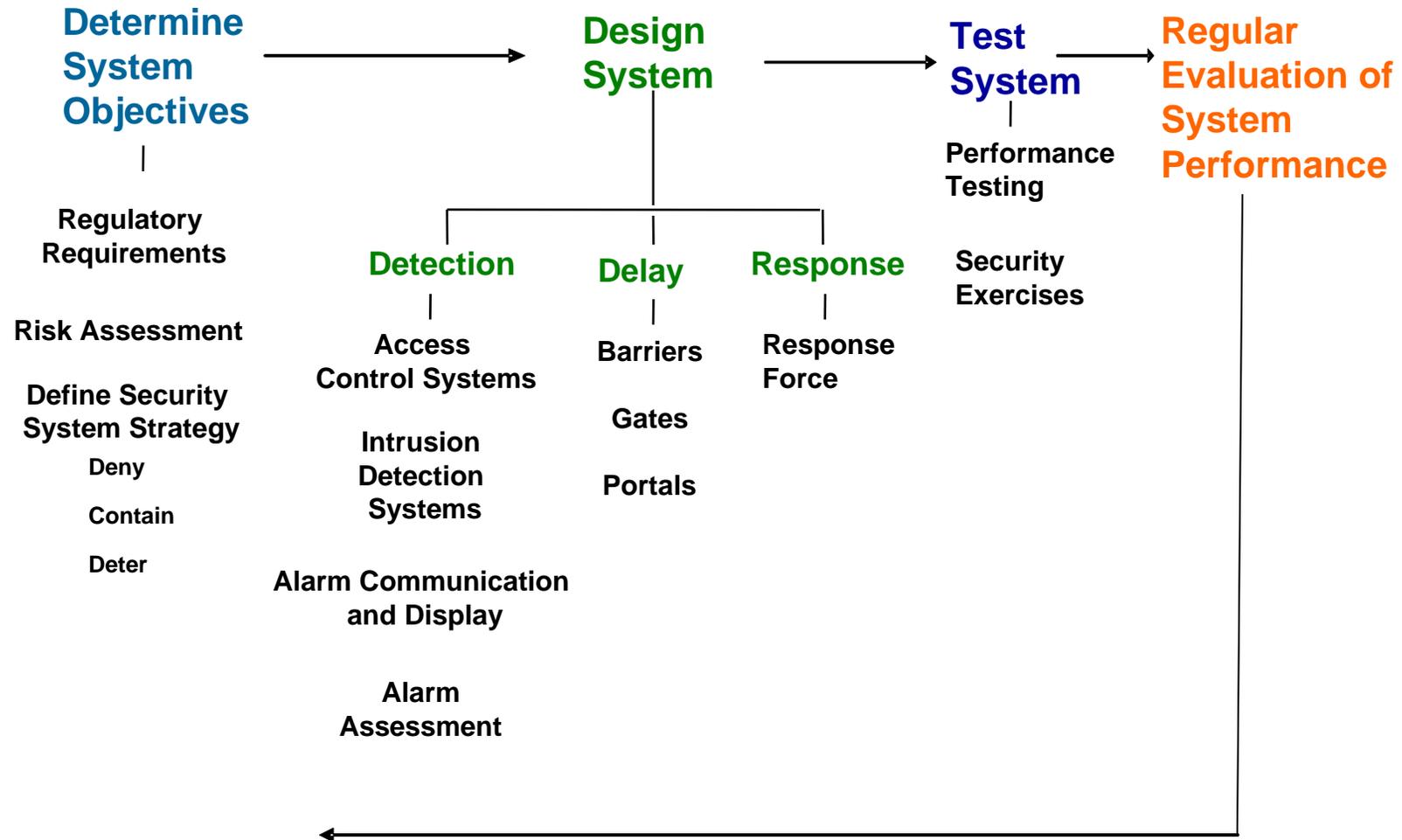
- **Emergency alarm – electronic locks**
 - **Safety – doors fail open**
 - **Security – doors fail secure**

- **Emergency egress**
 - **Safety – move people into the safest location as quickly as possible**
 - **Security – prevent people from moving into or through restricted areas**

- **Keys required inside laboratory areas**
 - **Safety – contamination concern**
 - **Security – multiple layers of access**



Physical Security System



Goal: Achieve desired performance as defined by system objectives
 Method: Low and high technology alternatives usually available

Define System Objectives

- **Management responsible for meeting all international, national, and local regulatory requirements**
 - Biological Weapons Convention
 - UN Security Council Resolution 1540
 - U.S. – Select Agent regulations

- **Risk assessment allows management to decide which scenarios to actively protect against**

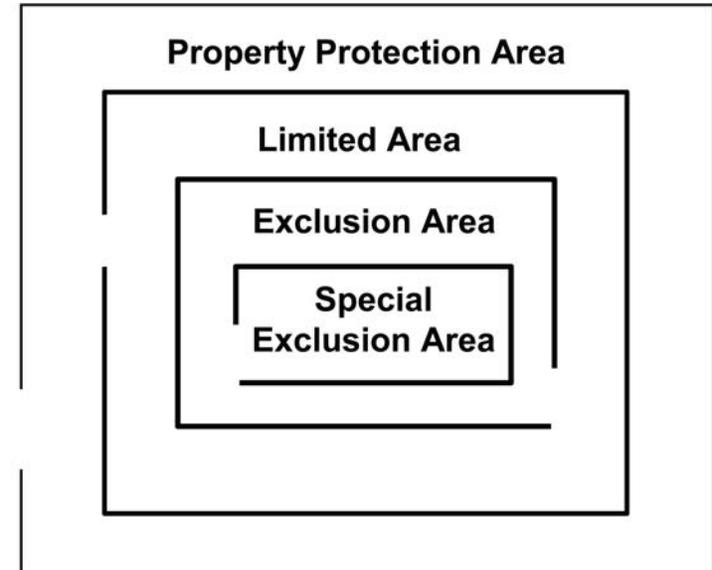
- **Management determines security system strategy:**
 - **Deny: prevent adversary from gaining access to particular pathogen or toxin**
 - **Contain: prevent adversary from leaving facility while in possession of stolen pathogen or toxin**
 - **Deter: discourage adversary from stealing a particular pathogen or toxin by making theft of that agent appear very difficult**

Denial and Containment strategies may only be appropriate when Outsider presents a very high risk

Deterrence generally most appropriate strategy for bioscience facilities because Insiders are typically largest risk

Graded Protection

- **Property Protection Areas**
 - **Low and Very Low Risk Assets**
 - Grounds
 - Public access areas
 - Warehouses
- **Limited Areas**
 - **Moderate Risk Assets**
 - Most bioscience laboratories
 - Administrative offices
 - Hallways adjoining Exclusion Areas
- **Exclusion Areas**
 - **High Risk Assets**
 - Some high containment laboratories
 - Computer network hubs
- **Special Exclusion Areas**
 - **Very High Risk Assets**
 - Extremely valuable intellectual property
 - Dangerous biological agents not found in nature



Property Protection Areas

- **Objective: Announce your intent to protect the property**

- **Perimeters mark the boundaries**
 - **Signs**
 - **Fences**
 - **Elicit strong statement of intent by adversary**
 - **Building walls**
 - **Terrain features**



Limited Access and Exclusion Areas

- **Objective: Provide reasonable assurance that only authorized individuals have access**
- **Limited Access Area requires unique credential for access**
 - Electronic key card or
 - Controlled key
- **Exclusion Area requires unique credential and unique knowledge for access**
 - Electronic key card and keypad or biometric device, or
 - Controlled key and second individual to verify identity
- **Gradations in other elements of physical security**
 - Intrusion detection, alarm assessment, delay, and response



Balanced Protection

- Many unique paths to assets
- System only as effective as weakest path
- Example pathways in bioscience laboratories:
 - Normal entryways
 - Emergency exits
 - Equipment interlocks
 - Double door autoclaves
 - Service elevators
 - Others?



Considerations for Possible Failures in Physical Security System



- **Does risk warrant redundant equipment, such as**
 - **Multiple complementary sensors**
 - **Central Alarm System and Secondary Alarm Stations**

- **Contingency and incident response plans**
 - **Spare parts**
 - **Compensatory measures**
 - **Agreement with local law enforcement**

- **Fail-safe and fail-secure**

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**

Physical Security: Performance Testing and Maintenance



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

Conclusions

- **Physical security system must be carefully designed to ensure that the system:**
 - Is the best allocation of resources
 - Supports, not conflicts with, biosafety
- **Physical security systems should be performance-based**
 - Physical security may be implemented by electronic and/or mechanical means
 - Either must be augmented by people and procedures
- **Physical security is only one aspect of a biosecurity system**
- **Risk Assessment is the key!**

