



Physical Security for Bioscience Laboratories

Biosecurity Inspector Training

**Staten Serums Institut
31 August – 2 September 2009**

www.biosecurity.sandia.gov

SAND No. 2009-5485C

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.





Principles of Design



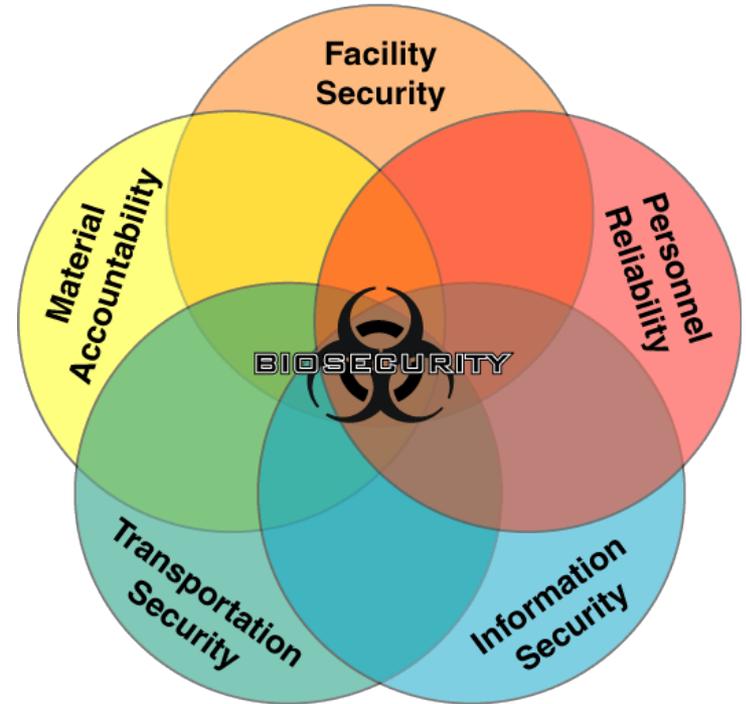
Laboratory Biosecurity

- **Biosecurity System**
 - Not limited to theft and deliberate misuse of biological agents
 - Assessment based methodology
 - **Can be applied to other important laboratory assets**
 - Computers
 - Laboratory notebooks and notes
 - **Can be applied to other malicious actions**
 - Sabotage
 - Theft of other assets
- **As a minimum, every laboratory biosecurity system should consider strategies to minimize the risk**
 - Theft and deliberate misuse of dangerous biological agents



Biosecurity System

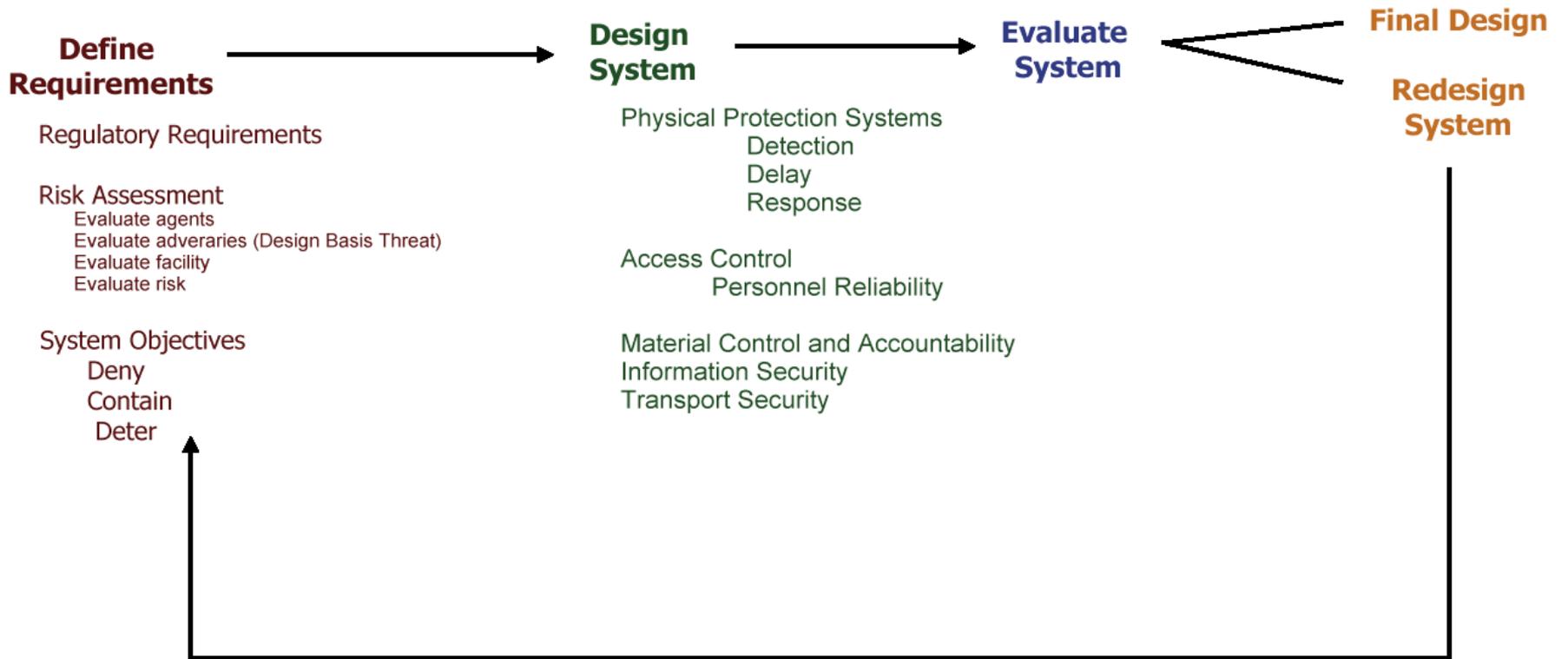
- **Biosecurity system components**
 - **Physical security**
 - Personnel security
 - Material handling and control measures
 - Transport security
 - Information security
 - Program management practices
- **Each component implemented based on results of risk assessment**
- **In general, biosecurity for**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

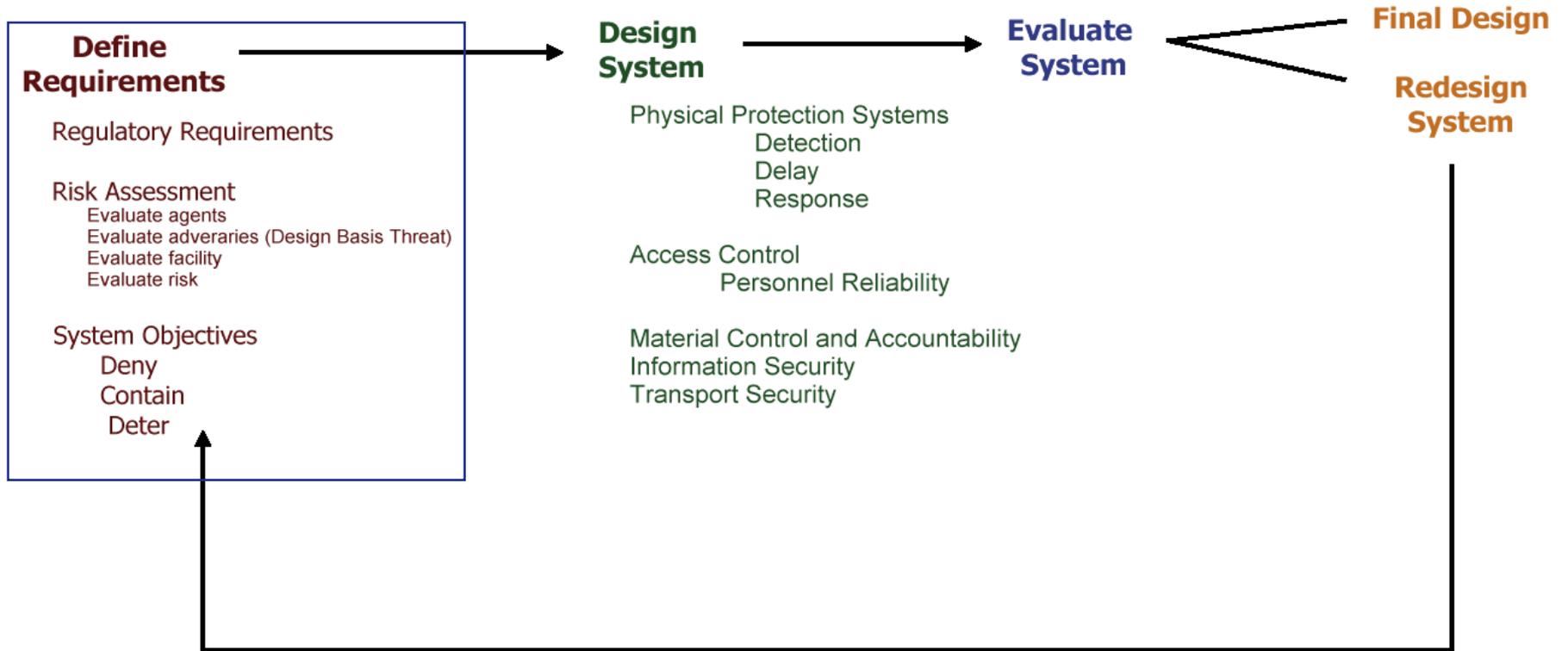




How Physical Security Supports Laboratory Biosafety

- **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







Define Requirements

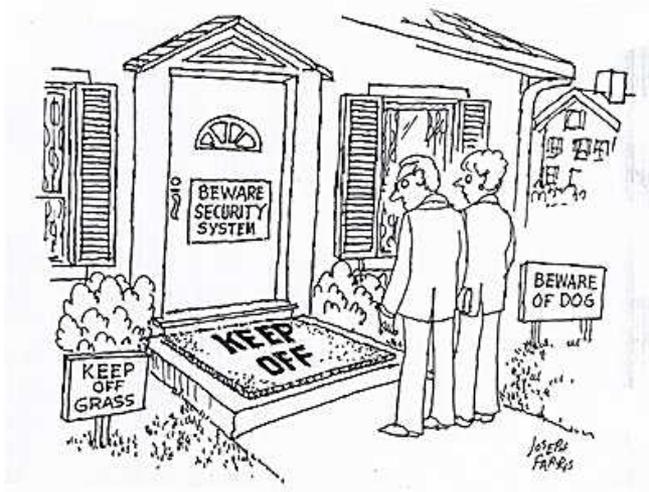
- **Management responsible for meeting all international, national, and local regulatory requirements**
 - **Biological Weapons Convention**
 - **UN Security Council Resolution 1540**
 - **National regulations**

- **Risk assessment**
 - Gives management a framework to decide which scenarios to are acceptable and which are unacceptable
 - Set performance requirements for the security system



Define System Objectives

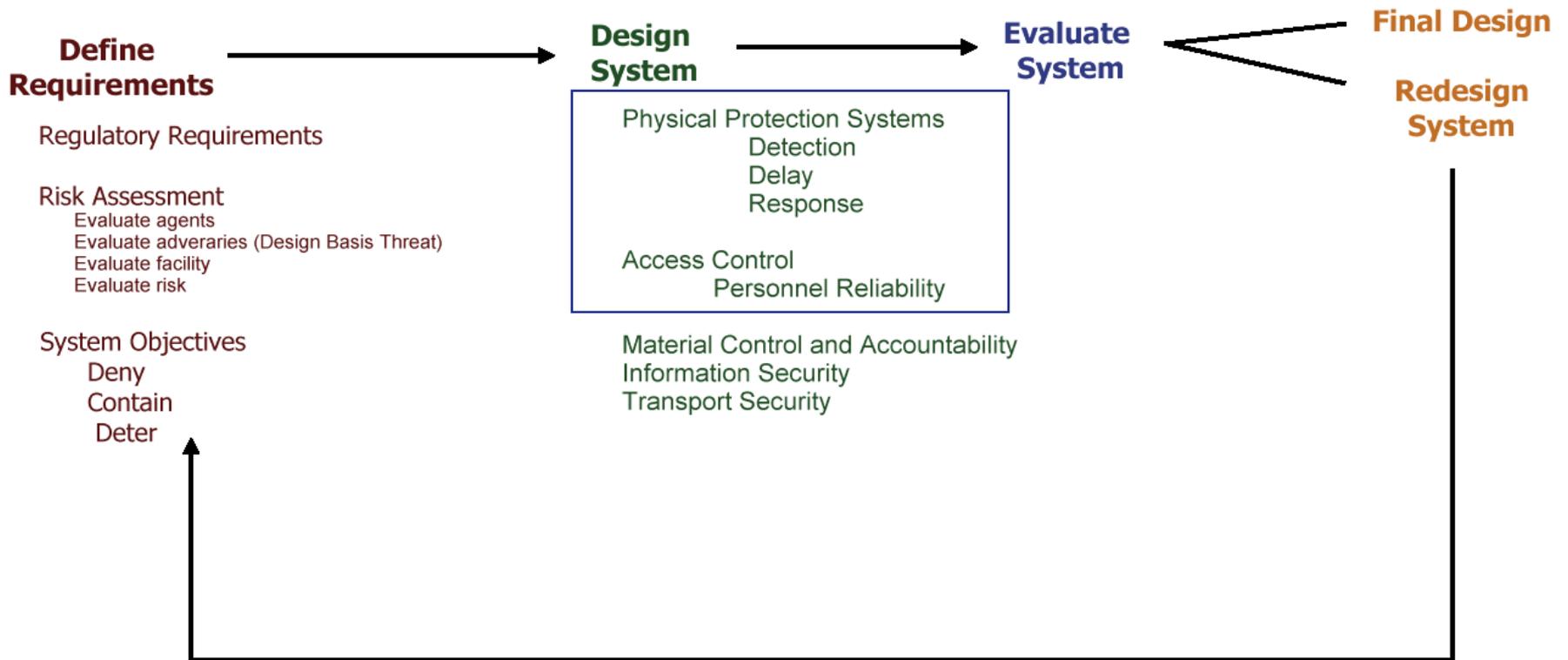
- **Management determines security system strategy:**
 - Deny: prevent adversary from gaining access to particular pathogen or toxin
 - Contain: prevent adversary from leaving facility while in possession of stolen pathogen or toxin
 - Deter: discourage adversary from stealing a particular pathogen or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





System Objectives: Discussion

- What would the *System Objective* be for a human clinical diagnostic laboratory: to deny, to contain, or to deter, and why?
- What would the *System Objective* be for a typical university research laboratory working with a regulated pathogen and why?
- What would the *System Objective* be for a facility containing the smallpox virus and why?





Physical Protection System Principles

- **Detection**

- Intrusion Detection is the process to determine that an unauthorized action has occurred or is occurring
- Detection includes sensing the action, communicating the alarm, and assessing the alarm

- **Delay**

- Slowing down an adversary's progress

- **Response**

- The act of alerting, transporting, and staging a security force to interrupt and neutralize the adversary
- Mitigation and recovery interface with the response function

- **Access Control**

- The mechanism to 'by-pass' the physical security system for authorized individuals



Graded Protection for Bioscience Laboratories

- **Property Protection Areas**

- Low risk assets

- **Limited Areas**

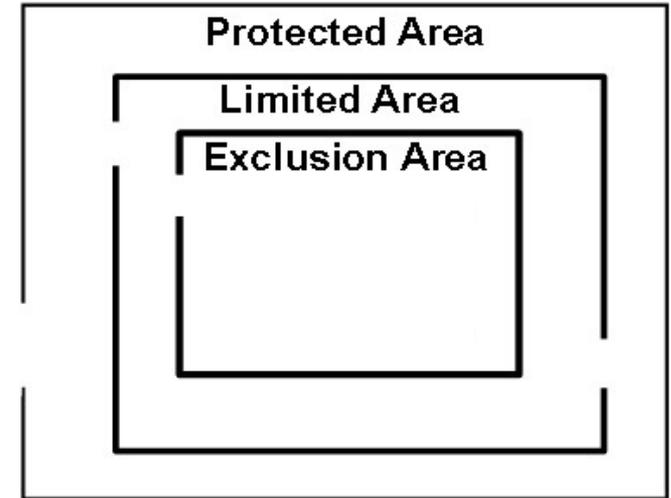
- Moderate risk assets

- **Exclusion Areas**

- High risk assets

- **In what security layer (property protection, limited or exclusion area), would you place the following:**

- Administration offices
- Clean animals
- Non-infectious bacteria (E-coli K12)
- Multi-drug resistant strain of *M. tuberculosis*
- Frozen vial containing Spanish Flu
- Network hubs





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



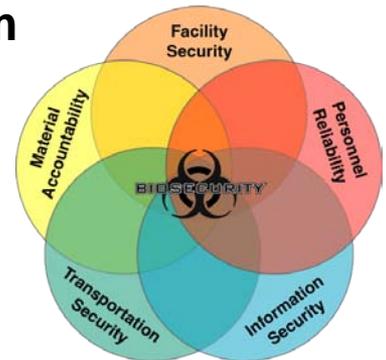
Physical Security: Performance Testing and Maintenance

- **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



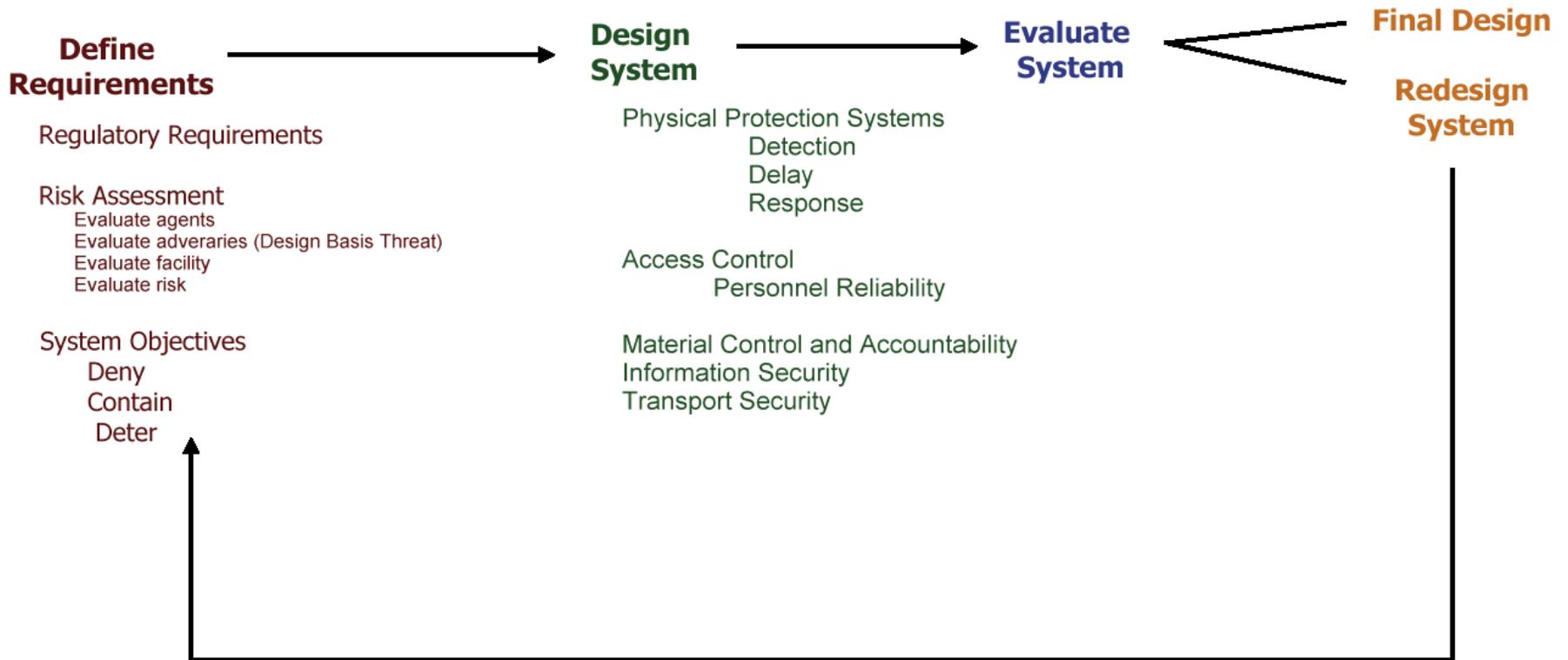
Considerations in Designing a Physical Security System

- **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!**





Access Controls





Purpose of Access Controls

- **Allow entry of**
 - Authorized persons
- **Prevent entry of**
 - Unauthorized persons
- **Allow exit of**
 - Authorized persons





Basis of Access Controls

- **Something you have**
 - Key
 - Card
- **Something you know**
 - Personal Identification Number (PIN)
 - Password
- **Something you are**
 - Biometric feature (i.e., fingerprints)
- **Combining factors greatly increases security**
 - Combinations typically used for Exclusion or Special Exclusion Areas



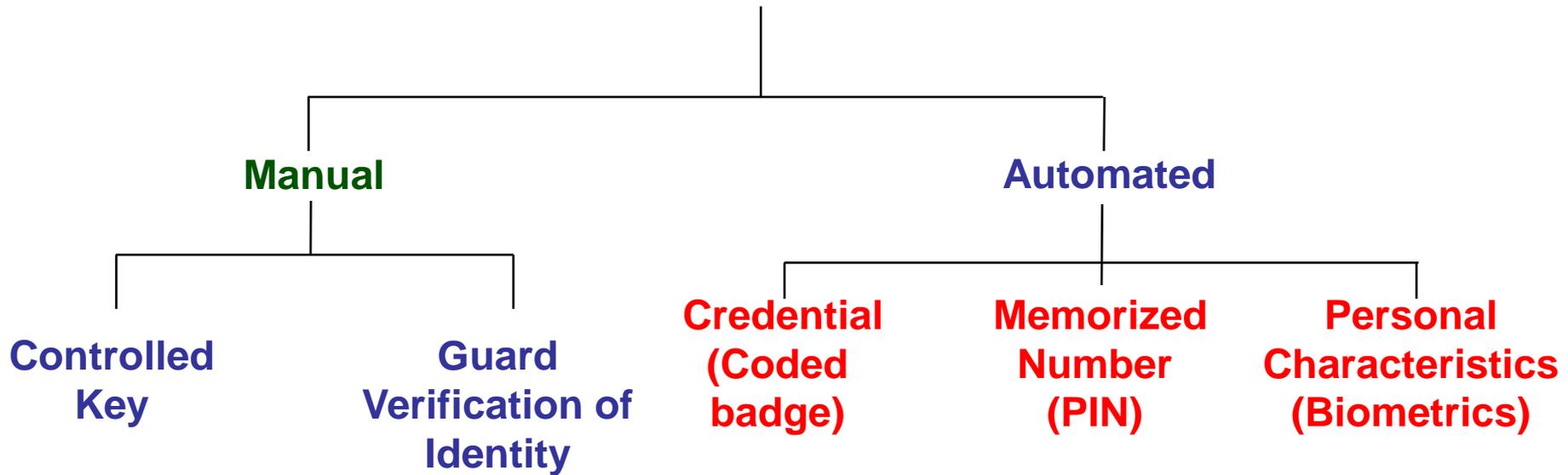
Badge swipe
and PIN

Hand-geometry
Biometrics



Access Control Techniques

Personnel Entry Control

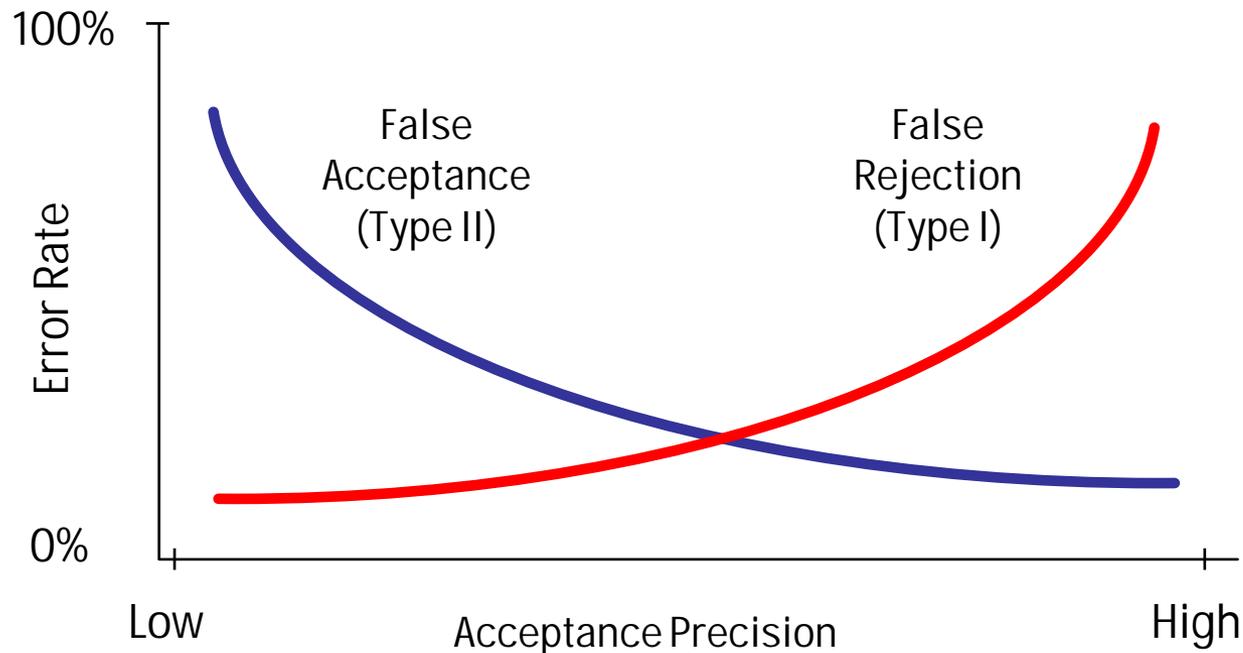






Errors for Access Control

- **False rejection - Type I**
 - Authorized persons are not allowed to enter
 - Easy to quantify
- **False acceptance - Type II**
 - Unauthorized persons are allowed to enter
 - Difficult to quantify





Manual Access Controls

- **Mechanical Keys**

- Controlled keys
- Pros
 - **Familiar to user**
 - **Inexpensive**
- Cons
 - **Can be copied**
 - **May be lost or stolen**
 - **Relatively easy to defeat**
 - **Must be recovered when authorization is terminated**



- **Guard verification of identity**

- May use photo badges or id cards
- Pros
 - **Easy to implement**
 - **Recognize personnel**
- Cons
 - **Labor intensive**
 - **Easy to tamper with badge**





Coded Badges

Positive Features

- Control access by area and time
- Record each access
- Have low false rejection rate
- Perform consistently
- Easy to Change Authorization

Negative Features

- | Identify badge, not person
- | Require maintenance
- | May be defeated by counterfeit badge



Proximity Badges

- **Induction powered**
 - Coded RF transmitter
- **Pros**
 - Hands-free operation
 - Can be worn under Personal Protective Equipment
 - Difficult to counterfeit
- **Cons**
 - Requires maintenance
 - Identifies the badge, not the person





Characteristics of Magnetic Stripe Badges

- **Two magnetic “strengths” (coercivity)**
 - Low coercivity, 300 Oerstead (e.g., bank card stripes)
 - High coercivity, 2500 to 4000 Oerstead, typically used for badges
- **Pros**
 - Widespread use of magnetic stripes
 - Users are familiar with the technology
 - Easy to use
 - Difficult to counterfeit high coercivity card
- **Cons**
 - Requires maintenance (replacement cards)
 - Easy to counterfeit low coercivity card
 - Identifies the badge, not the person





Characteristics of Wiegand Cards

- **Card consists of a series of embedded wires with special magnetic properties**
- **Position of wires and their magnetic polarities determine the encoding**
- **Pros**
 - Widespread use
 - Easy to use; card is read via a “swipe” action similar to magnetic stripes
 - Output format is an industry standard
 - Average ease to counterfeit
- **Cons**
 - Average ease to counterfeit
 - Requires maintenance (replacement cards)
 - Identifies the badge, not the person





Characteristics of Smart Cards

- **Credit-card-sized device with CPU, memory, I/O, and operating system**
- **Onboard EEPROM allows storage of ID information, including**
 - PIN / password
 - biometric template
- **Pros**
 - Easy to use
 - Difficult to counterfeit
 - Capable of doing encryption
- **Cons**
 - Relatively high cost
 - Requires maintenance (replacement cards)





Biometric Access Controls

- **Identification is based on a unique feature, such as:**
 - Fingerprint
 - Face
 - Hand geometry
 - Retinal pattern
 - Iris pattern
- **Most biometric systems verify identity**
 - You claim to be someone by presenting a card or PIN
 - System compares recorded template for the claimed identity with the live biometric (one-to-one)
- **Some biometric systems recognize you**
 - No claim of identity is required
 - System searches through database to find a match (one-to-many)



Fingerprint Scanner

- **Reads Fingerprint**

- Different types:
 - **Direct contact with chip**
 - **Ultrasound**
 - **Can combine with pin number or badge swipe**
- Verification time: fast (approx 5 seconds)
- Cost per terminal: approx \$1200 per unit + software and installation costs

- **Pros**

- Easy to use
- Low False Acceptance error rate (0.001%)

- **Cons**

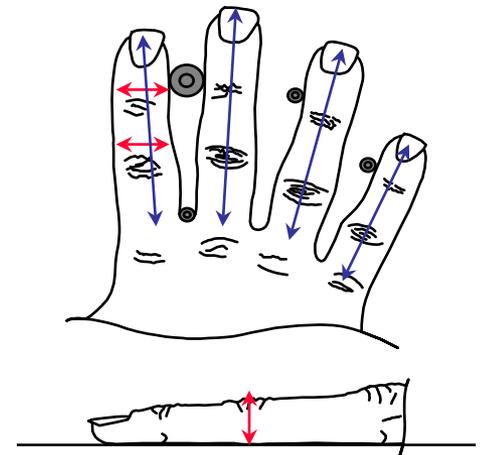
- Cannot be wearing gloves
- Tests have shown higher False Reject rates for laborers with dirty hands or worn fingerprints
 - **1% is normal, dirty hands can increase up to 40%**
- Requires maintenance – keep it clean
- 1-3% of the population is incompatible with any biometric device





Hand Geometry Scanner

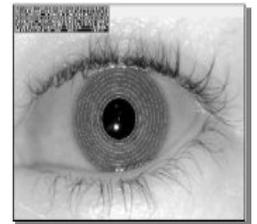
- **90 readings of length, width, thickness, and surface area of the fingers**
 - Can combine with pin number or badge swipe
 - Verification time: fast (approx 5 seconds)
 - Cost per terminal: \$1500 per unit + software and installation costs
- **Pros**
 - Most popular Biometric device
 - Easy to use
 - Low False Accept and False Reject error rate (0.1% for both errors)
 - Relatively inexpensive and reliable
 - Can use with some types of gloves
- **Cons**
 - Requires maintenance





Retinal or Iris Scanner

- **Iris scanner uses camera to look at patterns of the iris**
 - Verification time: Approx. 5-10 seconds
 - Cost per terminal: Approx. \$3,000 - \$5000 + software / installation
 - Pros:
 - **False Accept error of 0.0%**
 - **Operates in “Recognize Mode” - no need for pin number or card**
 - **Can use with Glasses, Contacts, or PPE**
 - **No physical contact between face and scanner (10 inch / 25cm away)**
 - Cons:
 - **False Reject error is 1% (some people have an iris that is so dark that the TV camera and software cannot enroll them)**
 - **Eyeglasses / PPE will interfere if have a reflection**
 - **Does not operate in “Verification Mode”**





Key Considerations in Selecting Access Controls

- **Access control systems**
 - Can be low or high tech
 - Give varying levels of assurance of person's identity
 - **Risk assessment!**
 - Have error rates and enrollment issues
 - **1-3% of the population is incompatible with any biometric device**
 - **Must have secondary method for those who cannot pass automated inspection**
 - Needs to accommodate peak loads
 - Should be designed for both entry and exit



Intrusion Detection, Alarm Communication and Assessment, Delay, and Response

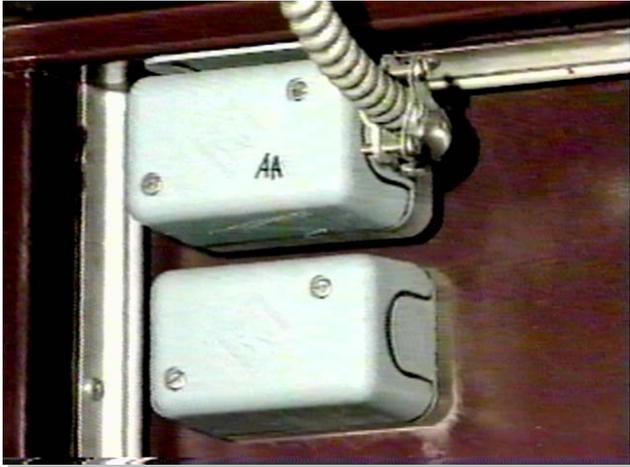


Intrusion Detection

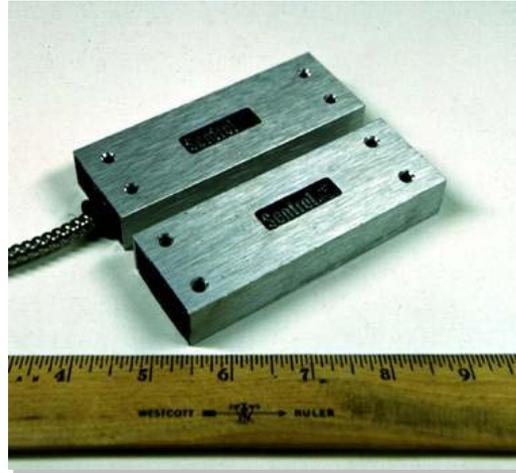
- **Objective: Detect unauthorized access**
- **Many types of intrusion detection**
 - Personnel notice unauthorized access attempt
 - **Training**
 - Boundary sensors most applicable for bioscience facilities
 - **Magnetic switches on doors**
 - **Glass break sensors on windows**
 - Volumetric sensors may be appropriate for low-use areas of high risk (e.g. culture collection storage rooms)
 - **Microwave**
 - **Passive infrared**



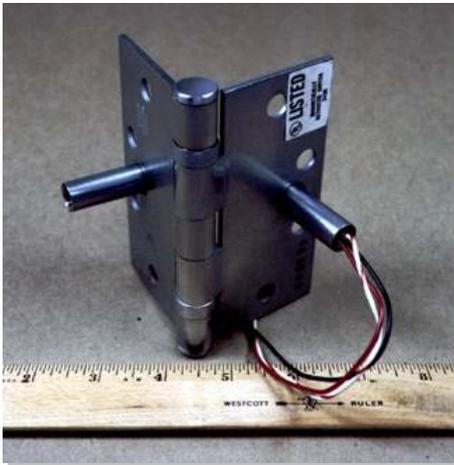
Magnetic Switches



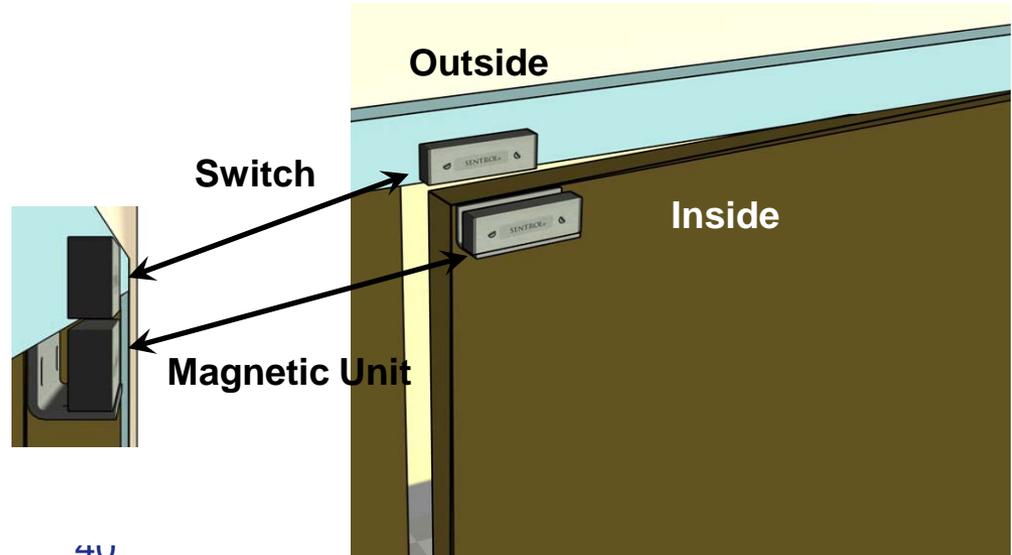
Balanced magnetic switch



Complex balanced magnetic switch



Covert magnetic switch



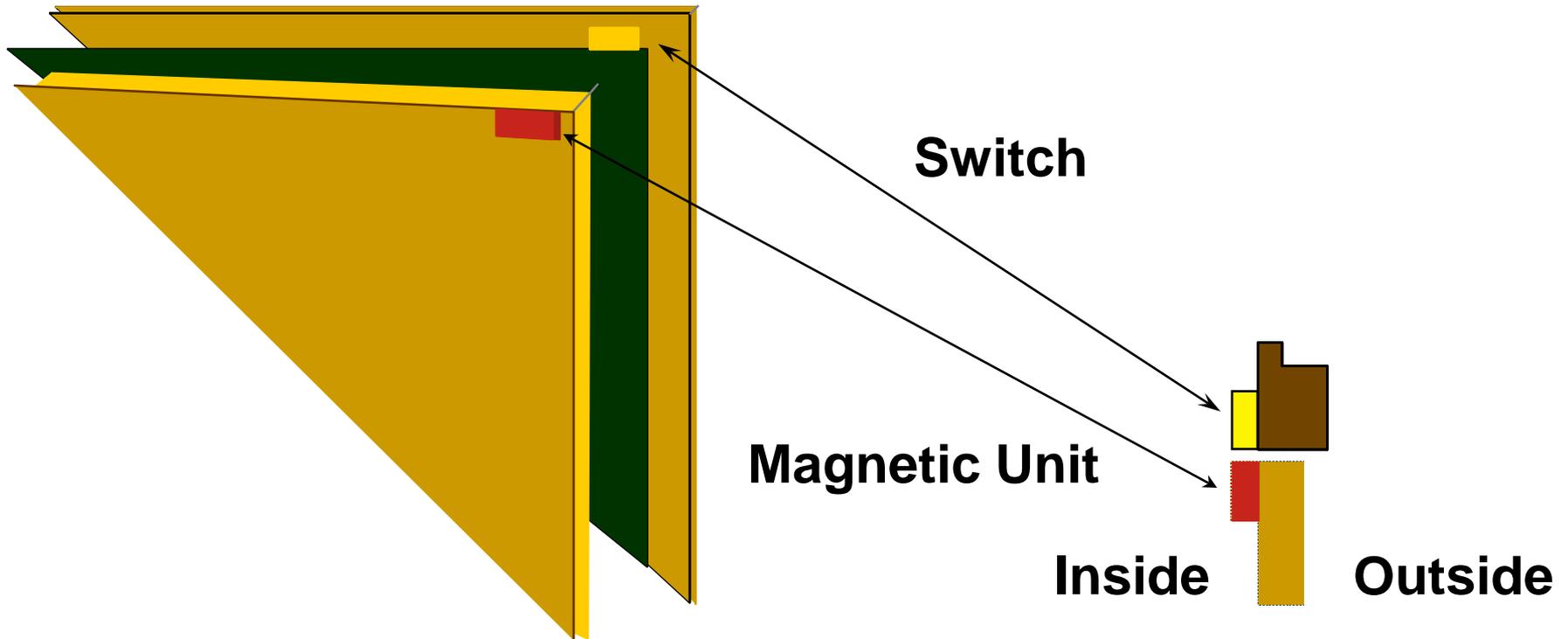


Balanced Magnetic Switches

- **An internal magnet and reed switches are usually mounted on the door/window frame and a balancing (or external) magnet is mounted on the moveable door/window.**
- **An alarm condition occurs when a change in the magnetic field between the parts is detected.**
- **Major Causes for Nuisance Alarms:**
 - Poorly fit doors or windows
 - Improper installation
 - Extreme weather conditions which cause excessive movement of the door or window



Magnetic Switch

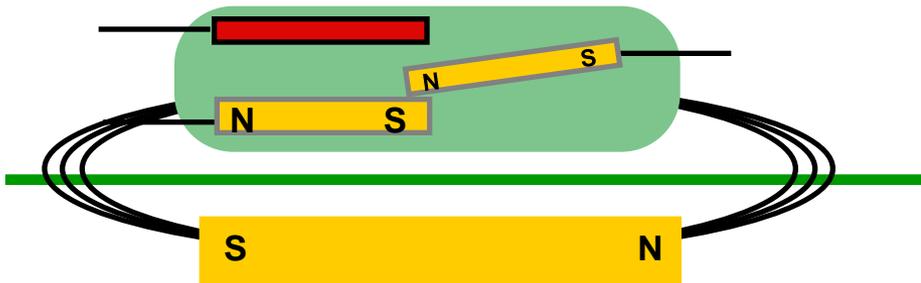




Magnetic Reed Switch

Non-Mag = 

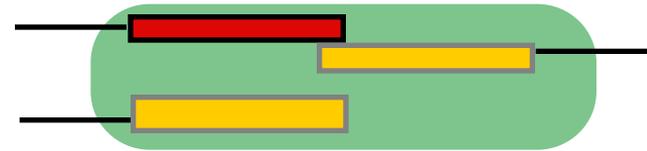
Switch Unit



Magnet Unit

(Door Closed)

Switch Unit



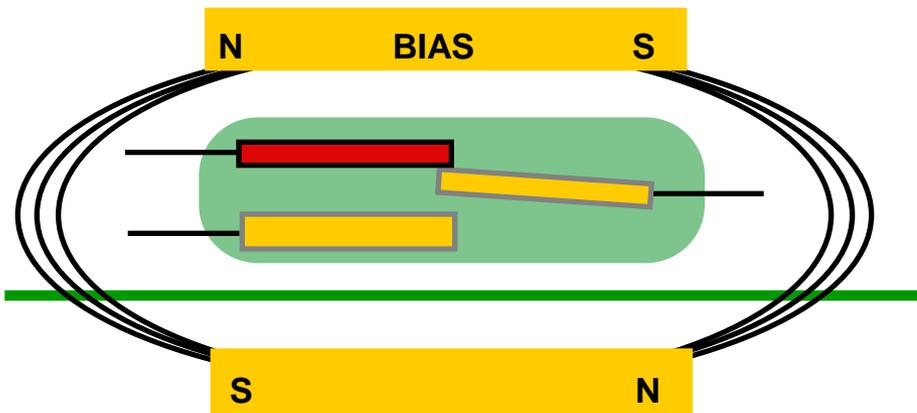
(Door Opened)



Balanced Magnetic Switch (BMS)

Non-Mag = 

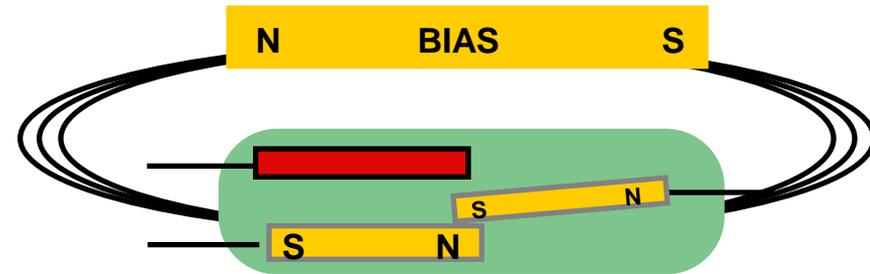
Switch Unit



Magnet Unit
(On Door)

(Door Closed)

Switch Unit

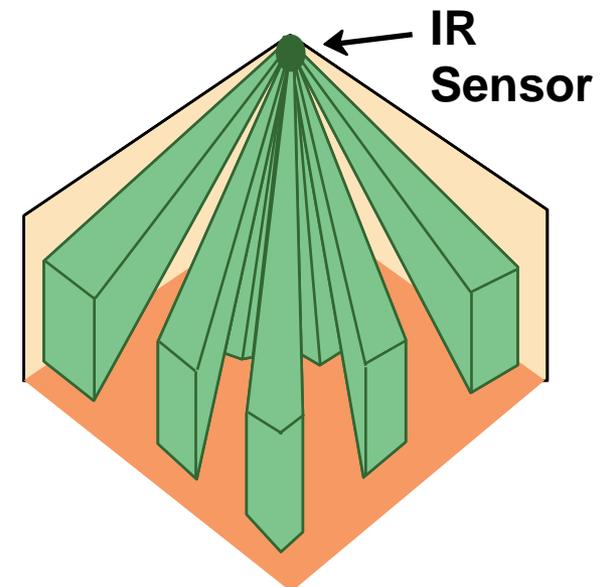


(Door Opened)



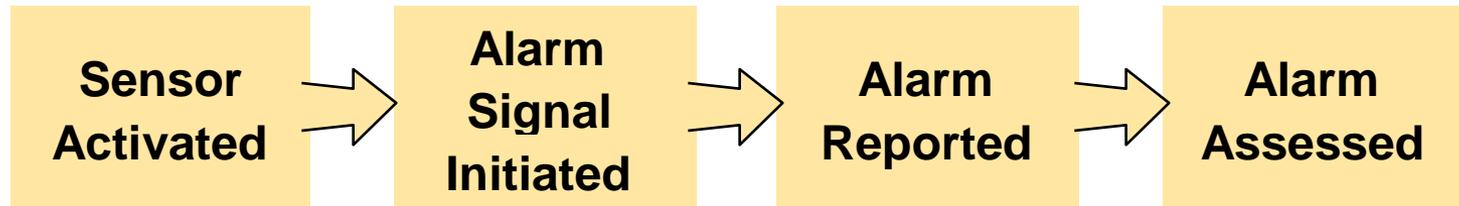
Volumetric Sensors

- **Microwave**
 - Most sensitive to movement toward or away from sensor
 - Nuisance alarms include: movement of metallic objects, fluorescent lighting, insects, movement outside of room
- **Passive infrared**
 - Most sensitive across field of view
 - Nuisance alarms include: heaters, thermal gradients, animals, sunlight, vibrations
- **Limited applications in bioscience facilities:**
 - Most appropriate for low use, high risk areas
 - E.g. Storage area for culture collection with very high risk pathogens





Alarm Communication and Assessment



- **Designer must decide:**
 - What information should be presented to the operator?
 - How should the information be presented?
 - How does the operator interact with the system?
 - How should the equipment be arranged at the operator's workstation?
- **Alarms must be communicated and displayed**
- **Alarms must be assessed before response is dispatched**
 - Can be direct (guards) or remote (video)
 - Determine cause of each sensor alarm
 - **Valid or nuisance alarm**
 - Requires adequate lighting
 - **Deters opportunistic adversaries**



BONG! BONG! BONG!
WHAAAAAAA

?



Alarm Assessment

Direct observation by guards

- Can be campus police or other on-site security
- Takes time and can put guard in danger
- Can provide immediate response
- Can only tolerate low rate of nuisance alarms
- Labor intensive

Remote assessment by video

- Video is immediate and focused
- Video is displayed to an alarm station operator for assessment
- Assessment of an alarm can occur almost immediately
 - Pre-event and post-event recording possible
- Later audit and review
- Efficient use of people
- Requires video infrastructure
- Can have high initial expense
- Maintenance can be expensive





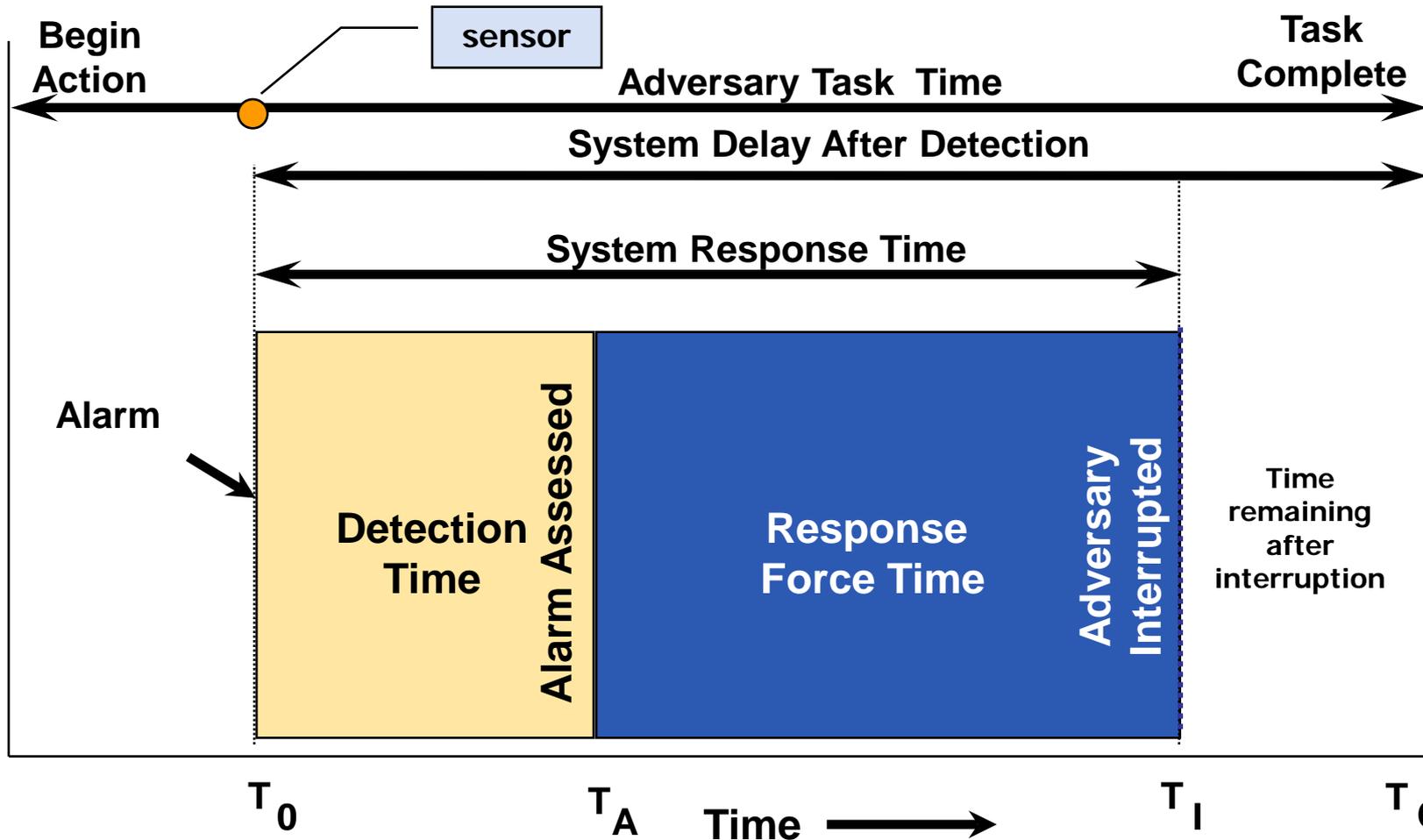
Video Assessment vs. Video Surveillance

- **Assessment**
 - Alarm information triggered by sensor activation and directed to a human to determine if unauthorized access has occurred in a sensed area
 - Cameras located at sensor locations – e.g. pointed at doors
- **Surveillance**
 - Continuous use of a human as an intrusion detector to monitor several restricted areas that are NOT sensed by intrusion technologies
 - Systems often have many cameras
 - Someone must watch all video screens all the time
 - **Personnel can only watch a few screens for a limited amount of time before fatigue**





Adversary Time vs. Response Time





Delay

- **Slow down an intruder**
- **Detection should come before delay**

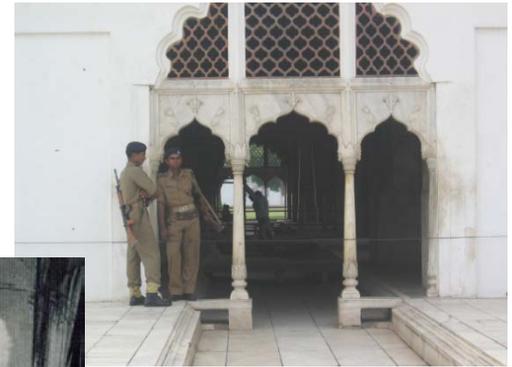
- **Many types of delay methods**
 - Guards
 - Perimeter Fencing
 - Solid doors with locks
 - Bars on windows
 - Magnetic switches on doors





Guards

- Guards delay and detect the intruders and in some cases also provide response





Response

- **The objective of response is tied to the overall system objective**

Deny: To prevent an adversary from reaching the target/objective

Contain: To 'catch' an adversary before they leave with the target or before they accomplish the objective

Deter: To initiate consequence mitigation measures



Response Force Options

- **On-site guard force**
 - Can serve intrusion detection and alarm assessment roles in mechanically-based physical security systems
 - 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 Post 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



Security Considerations

- **Administrators have full control**
 - The ultimate insider
- **Protect the system using procedures**
 - Two person control
 - Configuration management
 - Password control
- **Restrict operator privileges**
- **Provide physical protection for equipment**
- **Backup equipment and procedures must be provided to maintain security**
- **Emergency power and uninterruptible power supply required for computers**



Physical Protection System **Discussion**

- **What types of detection devices would be appropriate in a bioscience facility and why?**
 - Are there types of detection devices that can not be used and why?
- **What are appropriate delay mechanisms for a bioscience facility?**
- **How should a bioscience facility respond to an alarm?**
- **What types of access controls can be used?**
 - Where?
 - Are there types that can not be used in a bioscience facility and why?



Conclusions

- **Physical security systems will vary based on:**
 - Resources
 - Choice of technology
 - Security system strategy
 - **Physical security is more substantive for deny or contain than deter**
 - Risk Assessment!
- **Physical security systems should be performance based**
 - Low and higher technology options
- **Must consider unique aspects and requirements of bioscience laboratories**