International
BIOLOGICAL THREAT REDUCTION

SAND2007-5500C

BIOSECURITY ENGAGEMENT PROGRAM

Elements of Physical Security Systems I: Access Controls

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

Physical Security for Bioscience Laboratories
ABSA pre-conference course

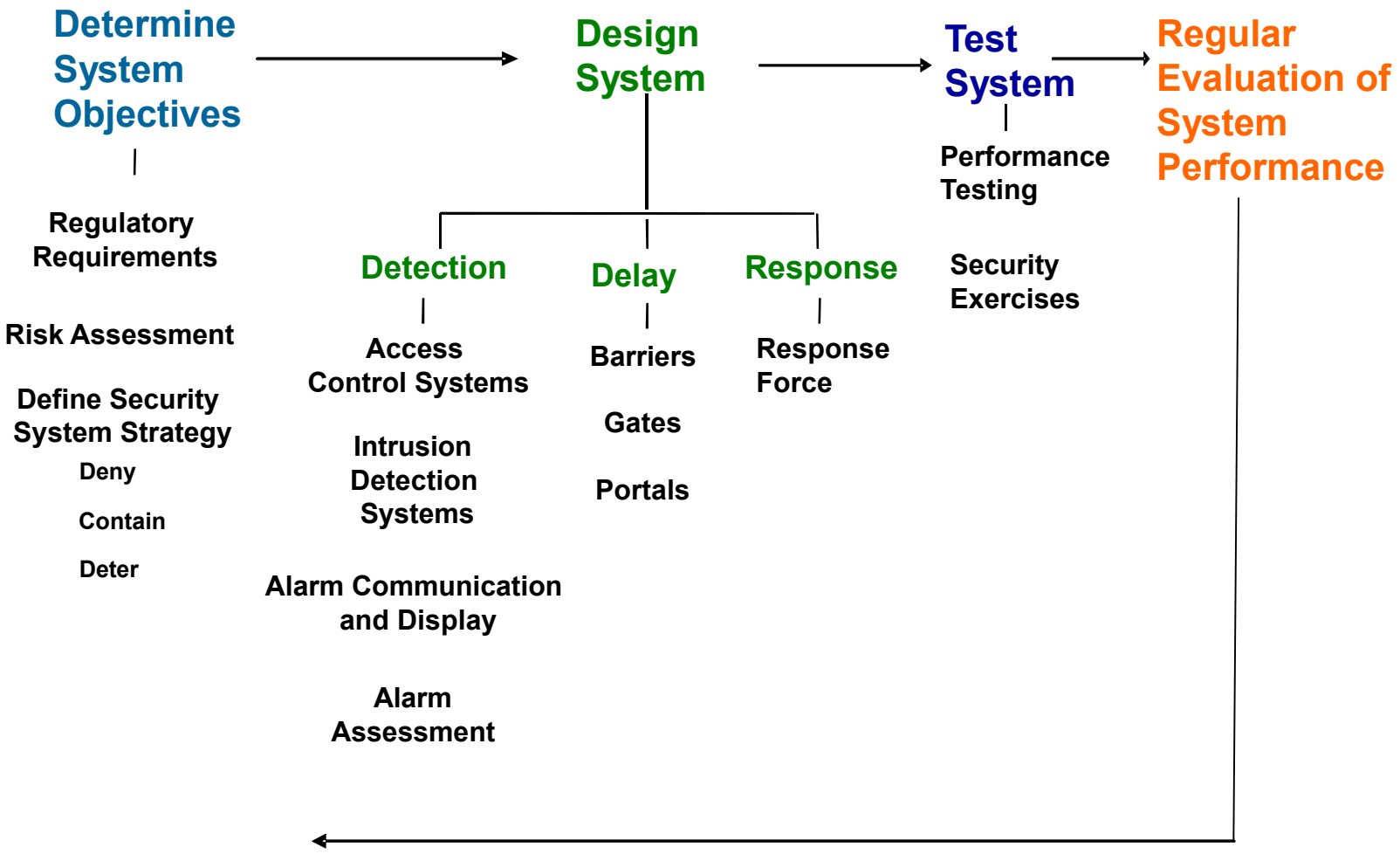
www.biosecurity.sandia.gov

SAND No. 2006-4329C
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.

NNSA National Nuclear Security Administration

Sandia National Laboratories

Physical Security System



Purpose of Access Controls

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

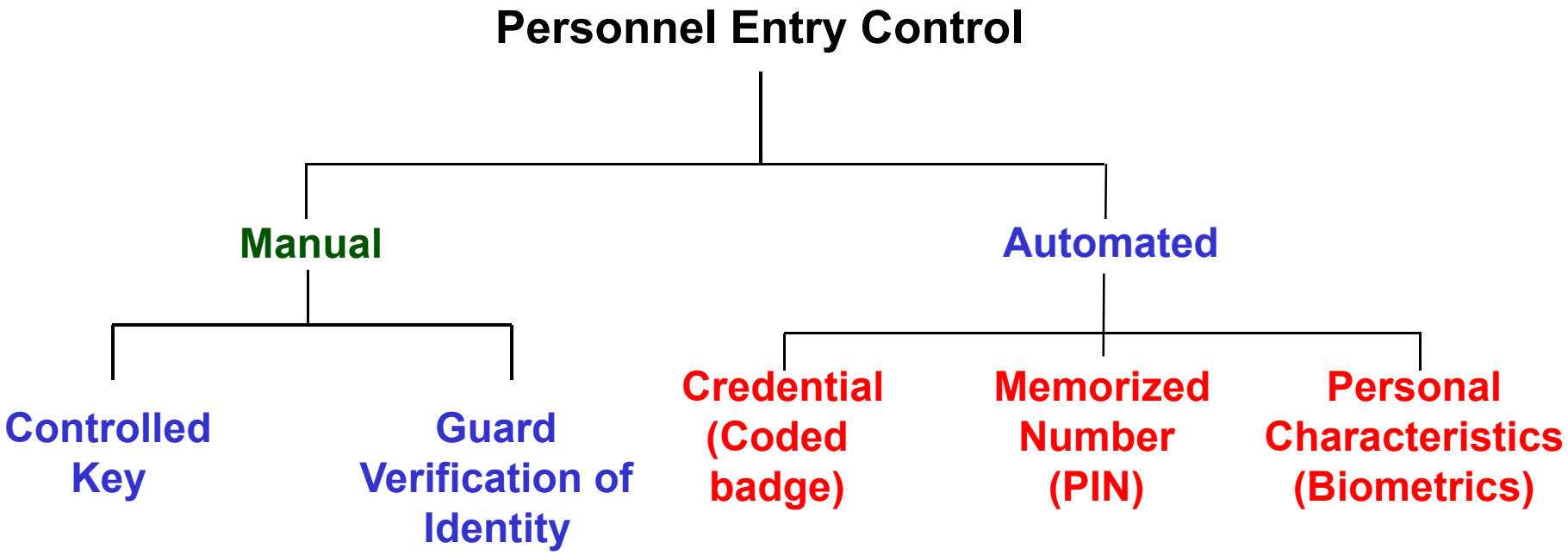
Basis of Access Controls

- **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

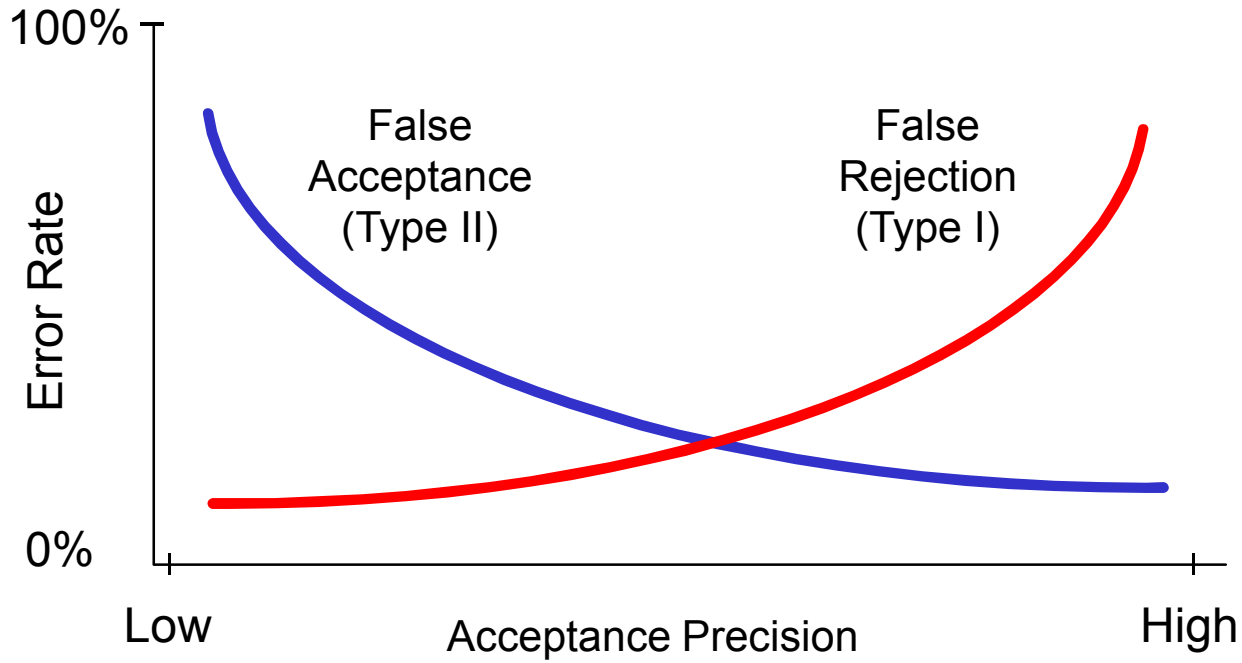
Hand-geometry Biometrics

Access Control Techniques



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

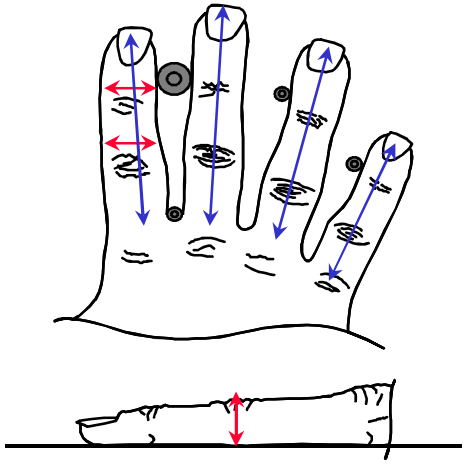
- **Reads Fingerprint**
  - **Different types:**
    - **Direct contact with chip**
    - **Ultrasound**
    - **Can combine with pin number or badge swipe**
  - **Verification time: fast (approx 5 seconds)**
  - **Cost per terminal: approx $1200 per unit + software and installation costs**

- **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

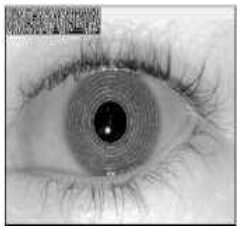
- Pros
  - Most popular Biometric device
  - Easy to use
  - Low False Accept and False Reject error rate (0.1% for both errors)
  - Relatively inexpensive and reliable
  - Can use with some types of gloves



- 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”



Conclusions

- 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