SAND2010-6256P

Detection of Insider Acts in a Nuclear Facility

Mark Snell
Sandia National Laboratories
mksnell@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

NNSA National Nuclear Security Administration

Sandia National Laboratories

Outline

- This presentation will start by providing background
  - Defining an Insider
  - Describing categories of Insiders and their attributes
  - Defining a multi-layered system for protecting against the insider threat
- We will then discuss several detection aspects of that system
- Finally, we will review testing considerations for administrative measures, procedures, and technology

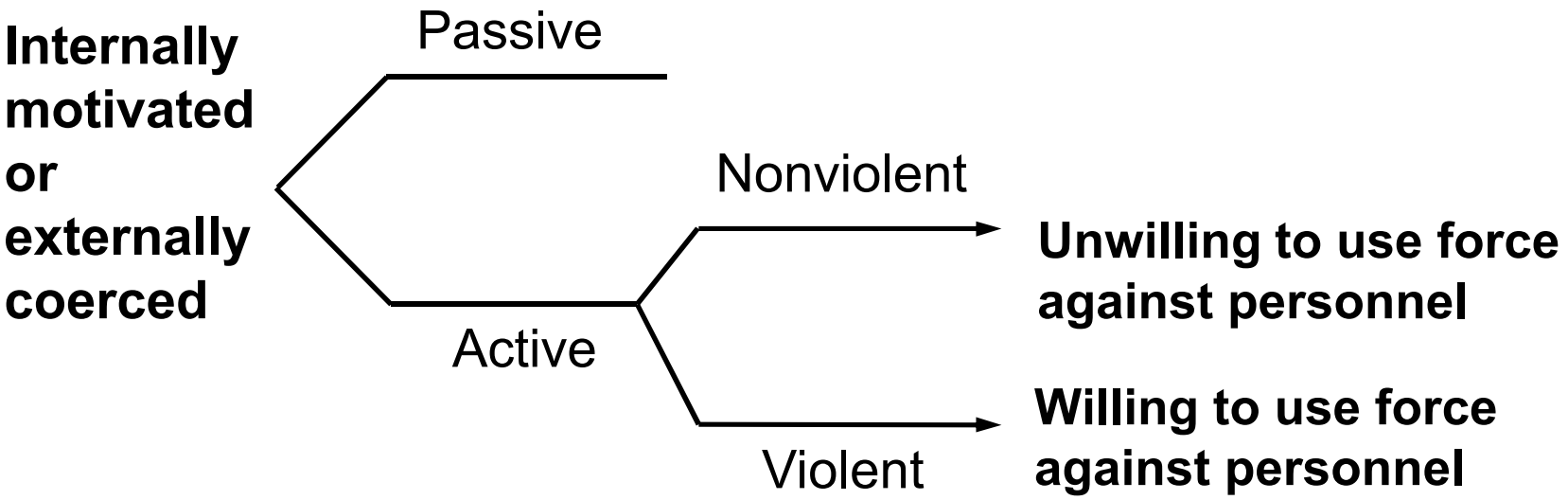
Insider Definition

Insider:

Any individual with authorized access to *nuclear facilities* or *transport* who might attempt unauthorized removal or sabotage, or who could aid *outsiders* to do so. (from IAEA Regional Training Course)

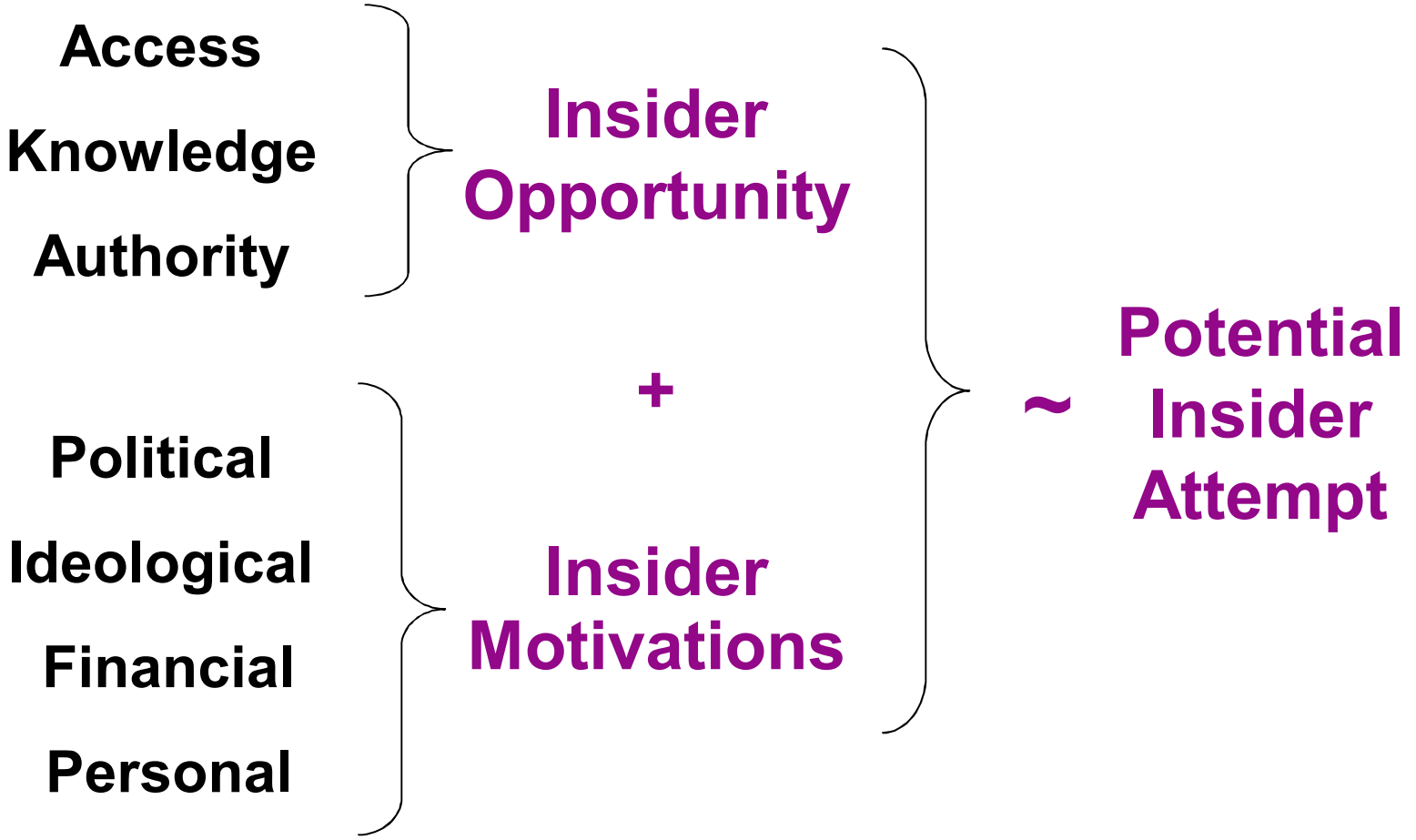
- **Insiders might include, but are not limited to:**
  - **Management**
  - **Regular employees**
  - **Security personnel**
  - **Service providers**
  - **Visitors**
  - **Inspectors**

Insider Categories



- **All insiders can use stealth and deceit**
- **Violent insiders may be rational or irrational**

Factors Affecting Insider Attempt



Insider Attributes

Access

- Limited areas
- Protected areas
- Vital areas
- Nuclear materials
- Emergency Access
- Central alarm station
- Alarms
- Keys
- Badging
- Information management of access system
- Nuclear material records
- Nuclear material forms
- Site vehicles
- Tools
- Controlled information

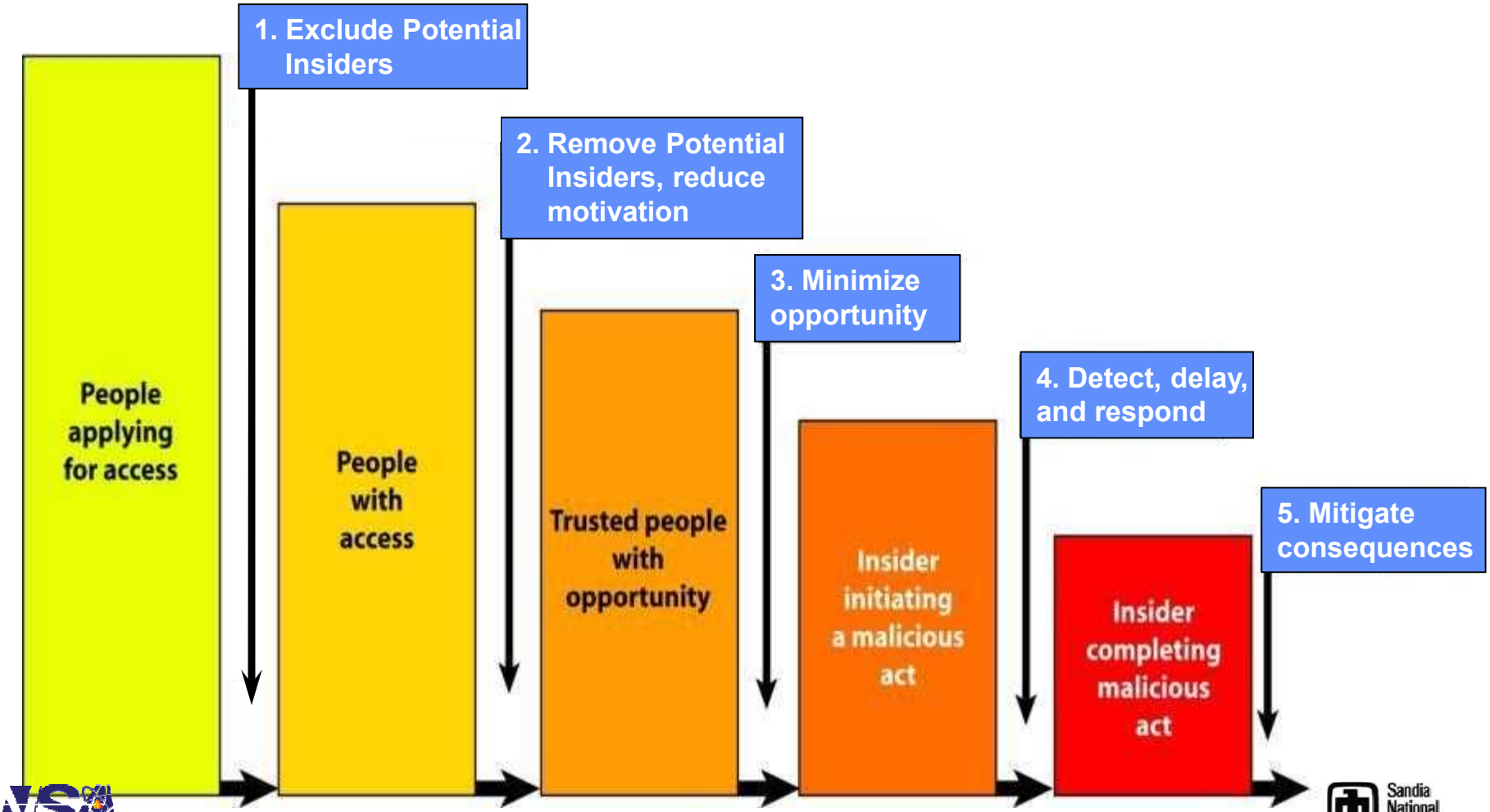
Authority

- Supervisory
- Supervisory over guards
- Personal vehicle
- Exempt searches
- Exempt metal detector
- Exempt nuclear material detector
- Authorize nuclear material transfers
- Prepare nuclear material transfers
- Verify nuclear material transfers
- Verify inventory
- Assess alarms
- Issue badges
- Issue codes
- Prepare access lists
- Equipment maintenance

Knowledge

- Procedures
- Processes
- Locations
- Site details
- Physical protection system
- Frequency of events
- Potential vulnerabilities
- Tools, equipment
- Procedure violations

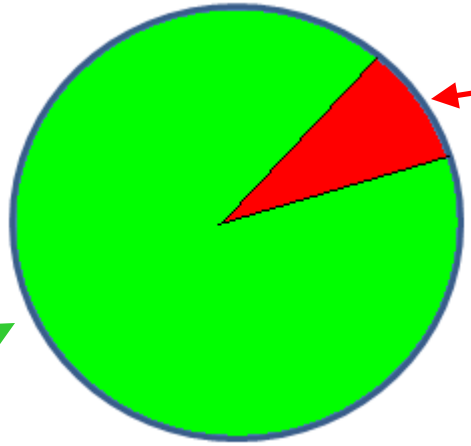
System Approach to Prevent and Protect Against Insiders



1. Exclude Potential Insiders

- Filter by:
  - Pre-employment checks:
    - Background checks
      - Criminal
      - Ideological
    - Financial obligations, credit history
    - Work history
    - Substance (Drug/Alcohol) testing
  - Security Clearances
- Detection achieved by the above measures

2. Remove Potential Insider, Reduce Motivation



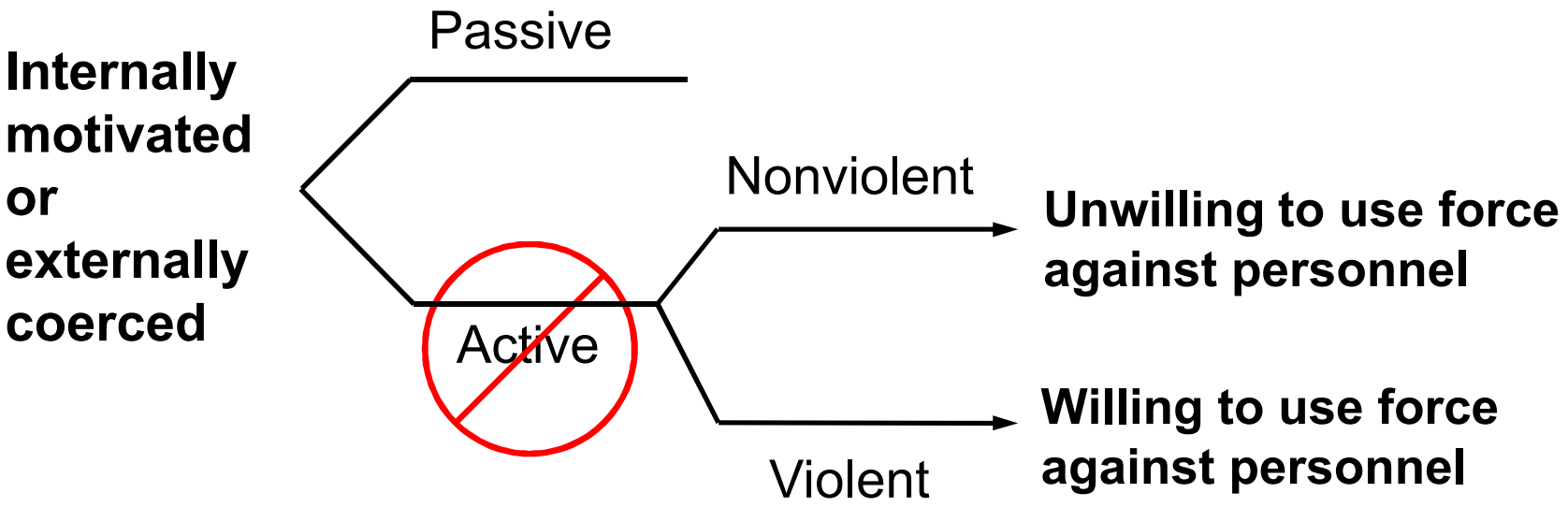
- For persons with critical Access/authority/knowledge
  - Human reliability programs
    - More frequent checks (like pre-employment phase)
    - Review by immediate managers
    - Observation by co-workers
    - Psychiatric examinations

- For all persons who are authorized to conduct activities at the site:
  - Security awareness
  - Periodic reinvestigations or background checks
  - Fitness for duty programs
  - Employee Assistance Programs
  - Employee satisfaction programs
  - Quality control programs

Spectrum of Response

- Bar from critical activities/areas
- Retrain
- Discipline
- Terminate from employment
- Prosecute

Assumptions Regarding Insider Categories for Critical Employees in Human Reliability Program



- Assume if HRP is effective, all employees in HRP are not active
- Thus, Only non-HRP employees can be active
- Note: May require active insider analysis for all insider categories or just those outside of HRP

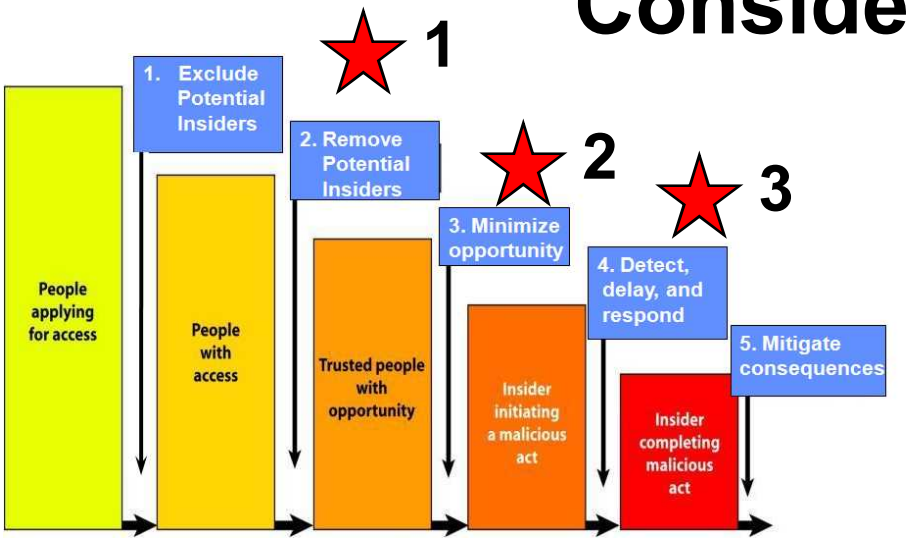
3. Minimize Opportunity

- Confidentiality and partitioning of information
- Operational security program
- Compartmentalize facility
- Automate hands-on activities
- Monitor and restrict vital equipment operations
- Inventory management
- Nuclear safety
- Nuclear facility design
- Strict adherence to operational plans and quality assurance programs

4. Detection Measures

- Operations
  - Observation by co-workers or supervisors
    - Administrative or technology controlled
    - Procedure compliance or non-compliance
  - Operational Process Alarms
  - Quality Assurance
- Security System
  - Entry/exit control
    - Searches
    - X-ray inspections
    - Special nuclear material detectors
    - Metal detectors
  - Signal line supervision
  - Nuclear material control and accountancy programs

Examples of Detection Aspects of Insider Detection and Testing Considerations



- **Examples:**
  - **Administrative Measures: Criminal Record Check, Drug Testing**
  - **Procedures: Two-person rule (e.g., locks)**
  - **Technology: Metal Detectors, Video Motion Detection**

Administrative Measure – Criminal Record Check

- **Weaknesses of measure**
  - Doesn't contain data from all parts of country/world
  - Doesn't contain minor crimes or those crimes for which person not caught
- **Potential defeat methods**
  - Alter records by bribery, stealth, or hacking
  - Intercept report and alter it
  - Influence recipient of record
  - Name change
- **Test: See if report can be altered without detection**

Administrative Measure – Drug Testing

- **Weaknesses of Measure**
  - May not cover all drugs that might be available on the black market
  - There may not be enough drug remaining in the bloodstream to cause a positive result
- **Potential Defeat Method**
  - Clean sample introduced surreptitiously
- **Test: See if a clean sample can be introduced by a willing person taking the test**

Procedure – Two Person (2P) Rule

- **Issue with an actual performance test of 2P rule against a malicious act: Can build up mistrust between co-workers if one of them actively violates rule**
- **Alternate "testing" approaches taken that mitigate this concern but have limitations**
  - First principles violation: 1 person leaves for a smoke break
  - Passive surveillance: Verify compliance to the 2P rule by observing the actions of the personnel involved and monitoring the associated records – did anyone record a mistake?
  - Historical record checks: Are accidents occurring that indicate mistakes are not being observed by second person?

Technology– Metal Detector

- **Direction of Travel: Exit**
- **Detection objectives assigned to the equipment**
  - Detect SNM shielding (need to be specific about type)
- **Define Defeat strategies**
  - Normal exit (risk detection)
  - Collusion with operator
  - Bypass:
    - Smuggle around portal
    - Hide in with other authorized equipment
  - Distract operator

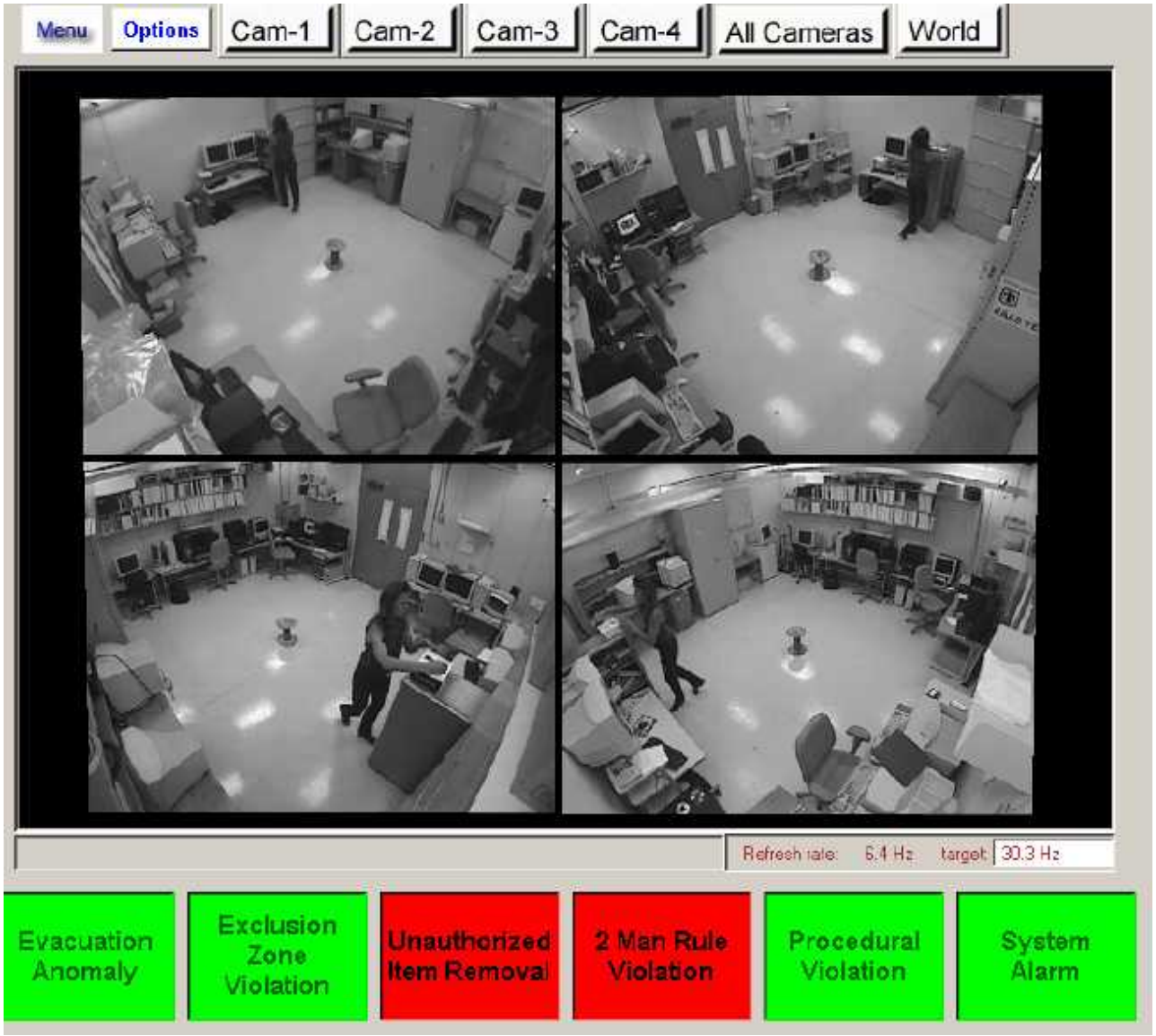
Technology– Video Motion Detection

- Sandia Video Motion Detection Activities
  - 2D Video Motion Detection test reports
  - Research on 3D Video Motion Detection (3D VMD)
  - Development of a video motion detection test suite
    - Intrusion scenarios
    - Examples of nuisance alarm sources

Tests of Commercial VMD's for Interior Applications

- **Intrusion test combinations combined**
  - Distance from camera to intruder
  - Adversary running, walking, slow walking, or crawling
  - Use of light or dark adversary clothes
  - Detection algorithm parameters
- **Each combination run once and taped; test scene then played through each VMD 6-9 times, each**
- **Nuisance alarms were counted for different detection algorithm parameters over about 240 hours.**
  - Nuisance Alarm Sources: animals/insects, loose paper, objects shadows, unknown
- **Office and high-bay applications considered**

3D VMD R&D Prototype Testing



Summary

- Defined a multi-layered system for protecting against the insider threat
- Described several different detection aspects of the system
- Reviewed testing considerations for administrative measures, procedures, and technology

backup

System Approach to Prevent and Protect Against Insiders