SAND2016-12089C

Exceptional service in the national interest

Sandia National Laboratories



Vulnerability Assessment Approach for Radiological Materials

David Ek, John Pelletier

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

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.

Why do we need to conduct Security Vulnerability Assessments?

Sandia National Laboratories

A gang of 6-10 criminals previously 'operating' as a landscape company in a nearby building, dug a tunnel measuring 78 m (256 ft) long, at 4 m (13 ft) below street-level directly below the bank vault. The criminals stole an estimated at $69.8 million.

Approaches to Regulate Effective Security

Sandia National Laboratories

- There are generally two methods employed to regulate effective security
  - Prescriptive-based approach
    - Regulations describe specific security measures that must be in place, e.g.:
      - Intrusion sensors must be installed on all approaches to target
      - Two different barriers must be provided
  - Performance-based approach
    - Regulations describe overall system performance that must be achieved, e.g.:
      - Adversaries must be detected prior to breaching barriers
      - Barriers must be sufficient to delay adversary long enough for response to arrive

Why do we need to conduct Security Vulnerability Assessments?

Sandia National Laboratories

- To actually assess security system performance is adequate
  - For *prescriptive approach,* a vulnerability assessment provides a check that the application of specific prescriptive measures at a facility indeed succeed in minimizing likelihood of adversary success
  - For *performance approach*, a vulnerability assessment provides the validation that the installed measures meet the regulatory requirements

Objective of Presentation

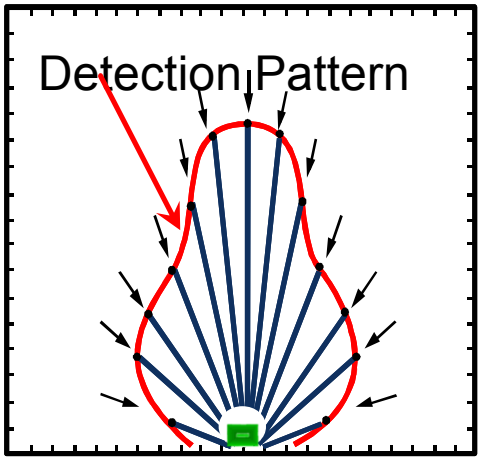
- This presentation will outline a systematic holistic vulnerability assessment approach:
  - to verify that a system follows accepted international security design principles
  - to investigate gaps in the security system, both spatial and time-dependent
  - to assess the integration of detection, delay and response

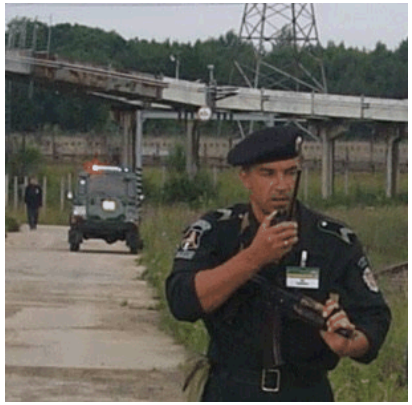
- Use of this VA approach is intended:
  - to supplement prescriptive assessments of security system compliance with regulations
  - to provide confidence to operators, regulators and the public that security system appropriately protect nuclear and radioactive materials

This approach is not intended to supplant the current quantified, scenario-based VA approach, but to supplement it for targets of lesser consequence

Current Vulnerability Assessment Approach

- **Gather quantified performance data**

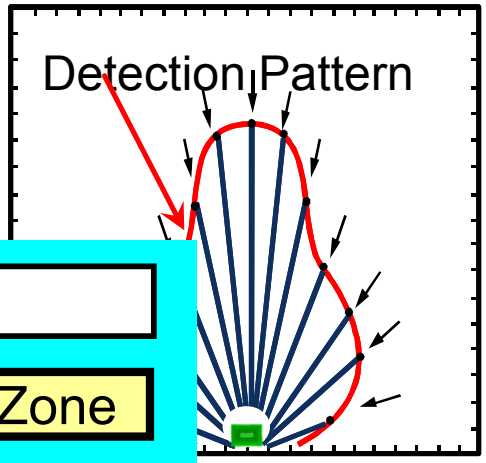


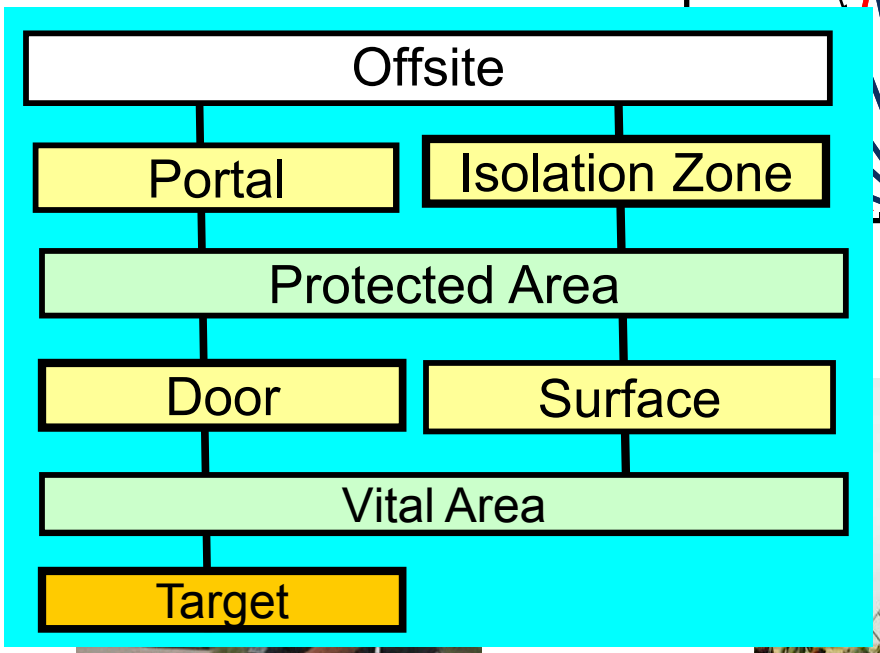


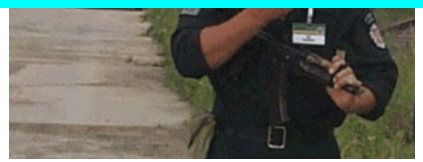
Current Vulnerability Assessment Approach

Sandia National Laboratories

- Gather quantified performance data
- **Develop model of adversary paths**

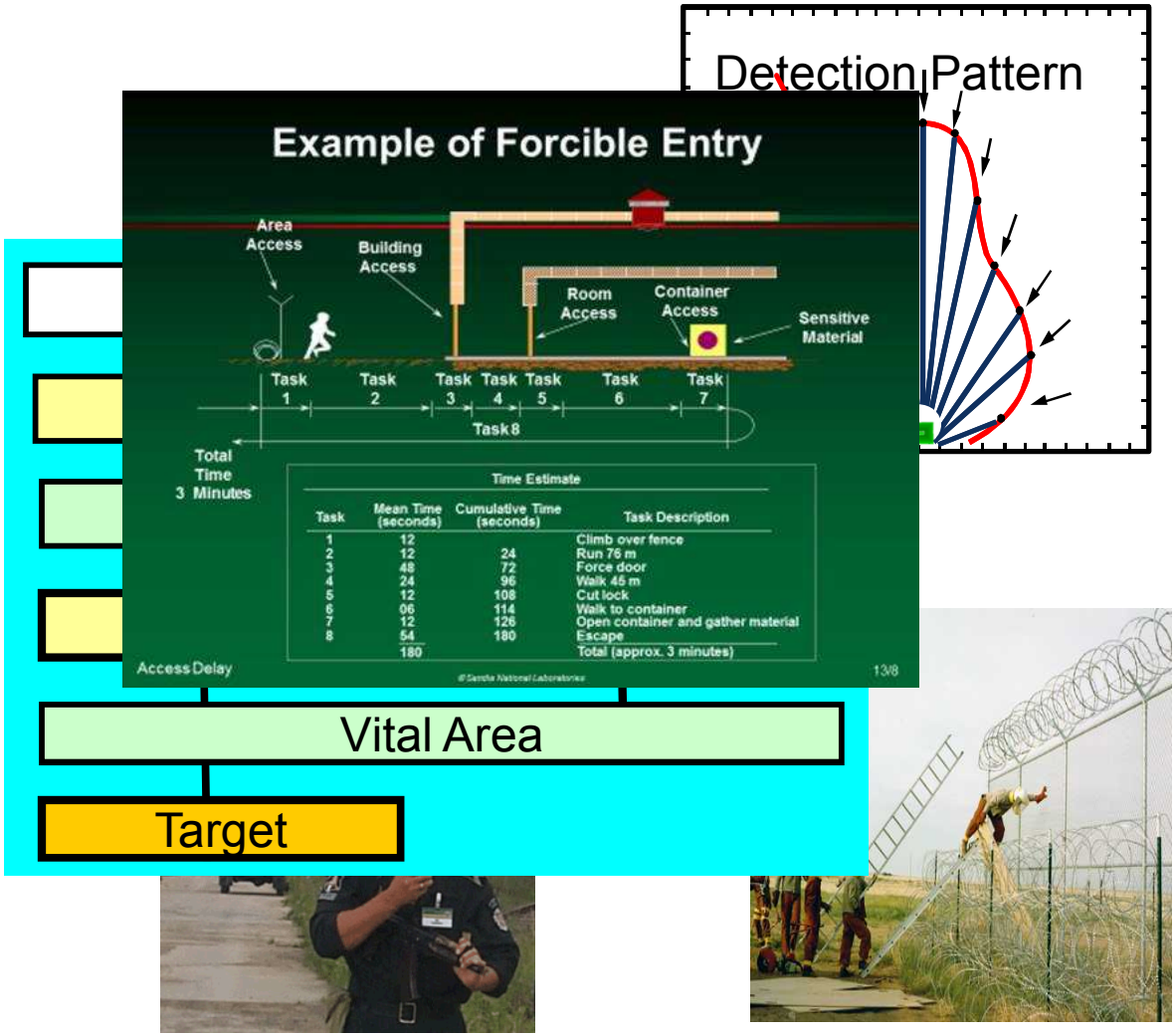






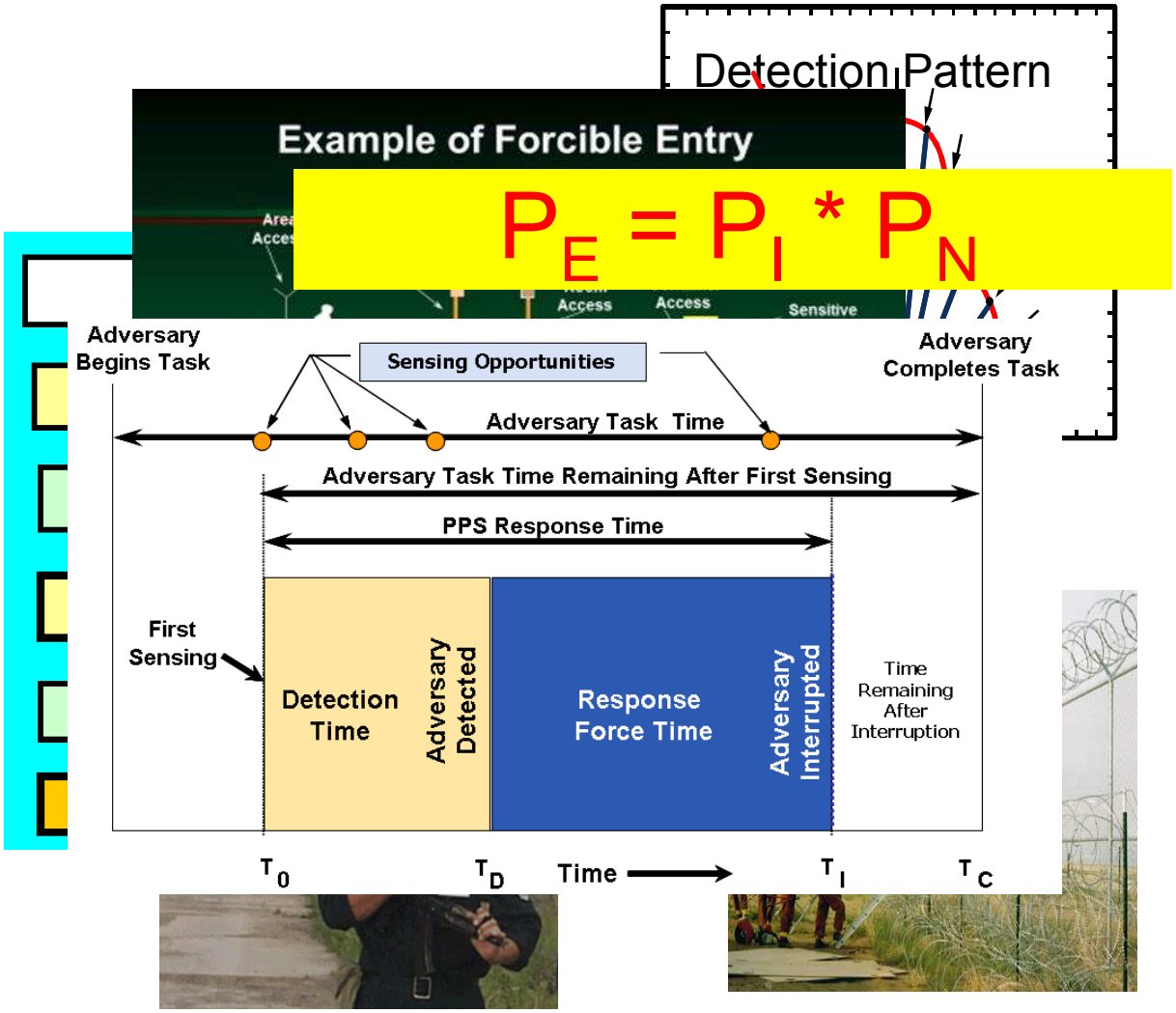
Current Vulnerability Assessment Approach

- Gather quantified performance data
- Develop model of adversary paths
- **Develop worst-case adversary scenarios**



Current Vulnerability Assessment Approach

- Gather Quantified performance data
- Develop model of adversary paths
- Develop worst-case adversary scenarios
- **Determine timely detection and system effectiveness for each scenario**

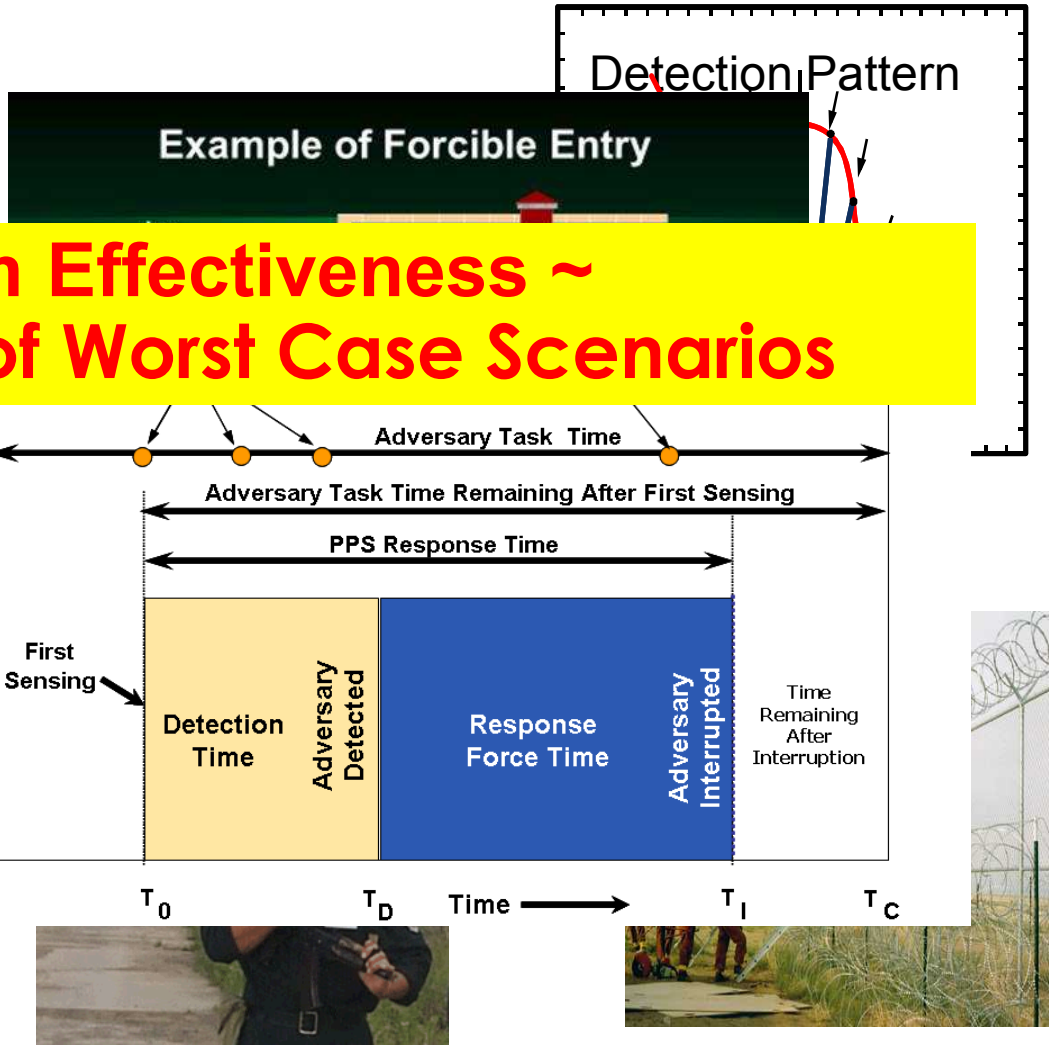


Current Vulnerability Assessment Approach

Sandia National Laboratories

- Gather Quantified performance data
- Develop Worst Case Adversary Scenarios
- Determine timely detection and system effectiveness for each scenario
- **Determine overall system probability of effectiveness**

Overall System Effectiveness ~ Effectiveness of Worst Case Scenarios



Current Vulnerability Assessment Approach

Sandia National Laboratories

- Provides confidence in assessment of security system performance
  - Is a scenario-based assessment
  - Employs quantified data to measure effectiveness
  - Value of result depends on skill and expertise of analyst
- May be difficult to implement for facilities and regulatory bodies with limited security expertise
  - Who often employ a prescriptive regulatory approach
  - Yet still need VA approach to validate that implemented security system minimizes adversary success

Features of Effective Security System

Sandia National Laboratories

Layered Security

- All security measures are organized along layers
- Layers surround target

Defense in Depth

- Multiple security layers

Balanced Security

- No weakness along layer
- Detection, delay, and access control

Detection Before Delay

- Detection of adversary must precede delay measures

PROPOSED VA APPROACH WILL VERIFY THESE

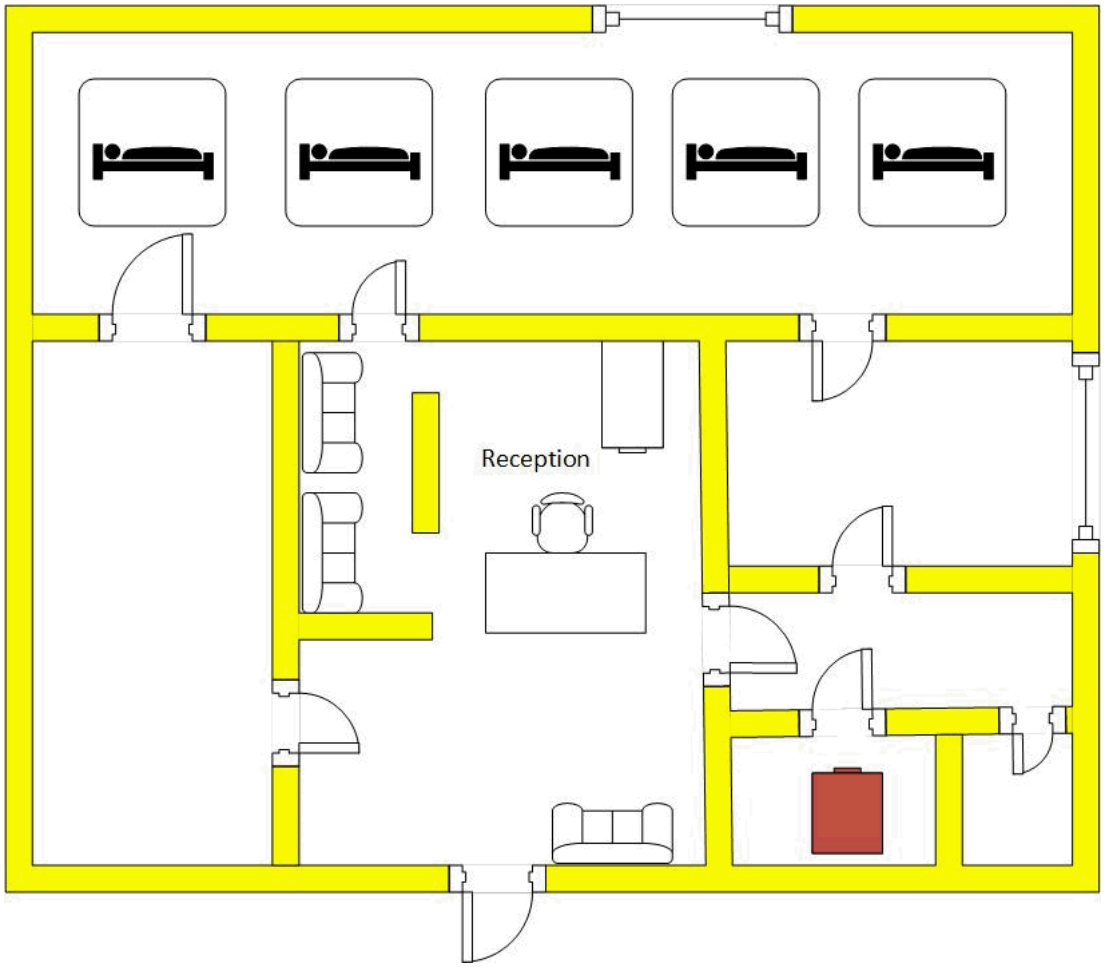
Steps for Proposed VA Approach

- Identify layers/depth
- Identify balance/gaps on each layer
  - Confirm detection before delay
  - Assess barrier significance (H, M, L)
  - Assess/Test sensor condition/arming
  - Assess access control/key control
  - Assess alarm monitoring
- Assess insider protection

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

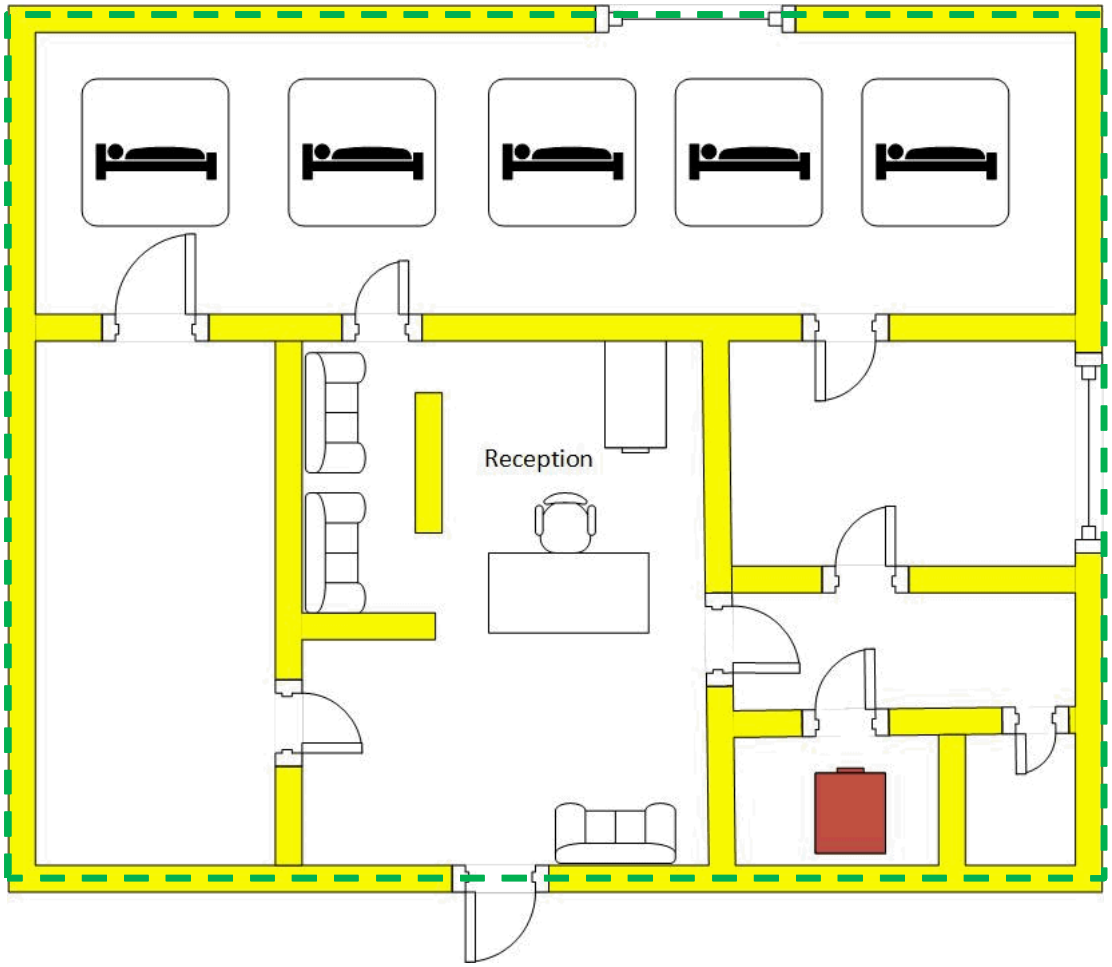
- **Identify Layers/Depth**



Proposed Vulnerability Assessment Approach

Sandia National Laboratories

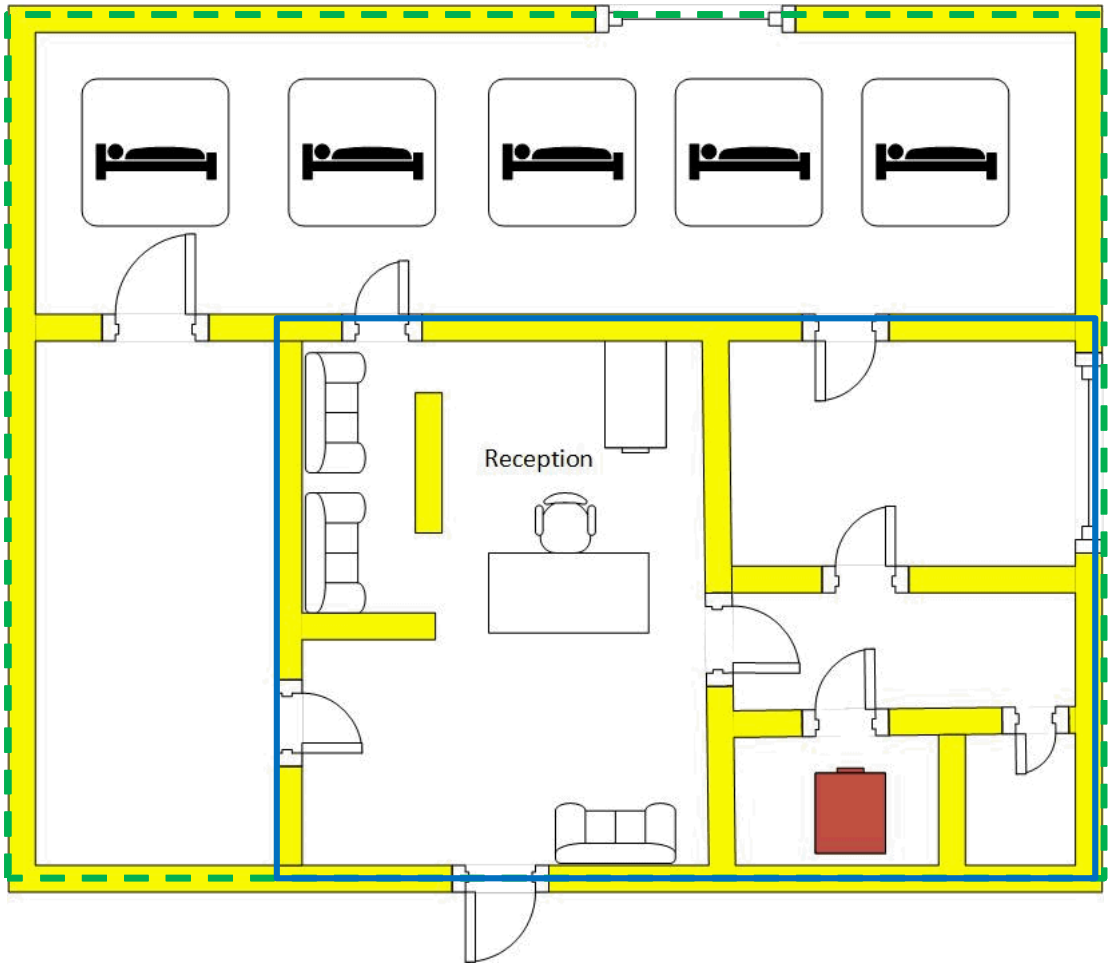
- **Identify Layers/Depth**



Proposed Vulnerability Assessment Approach

Sandia National Laboratories

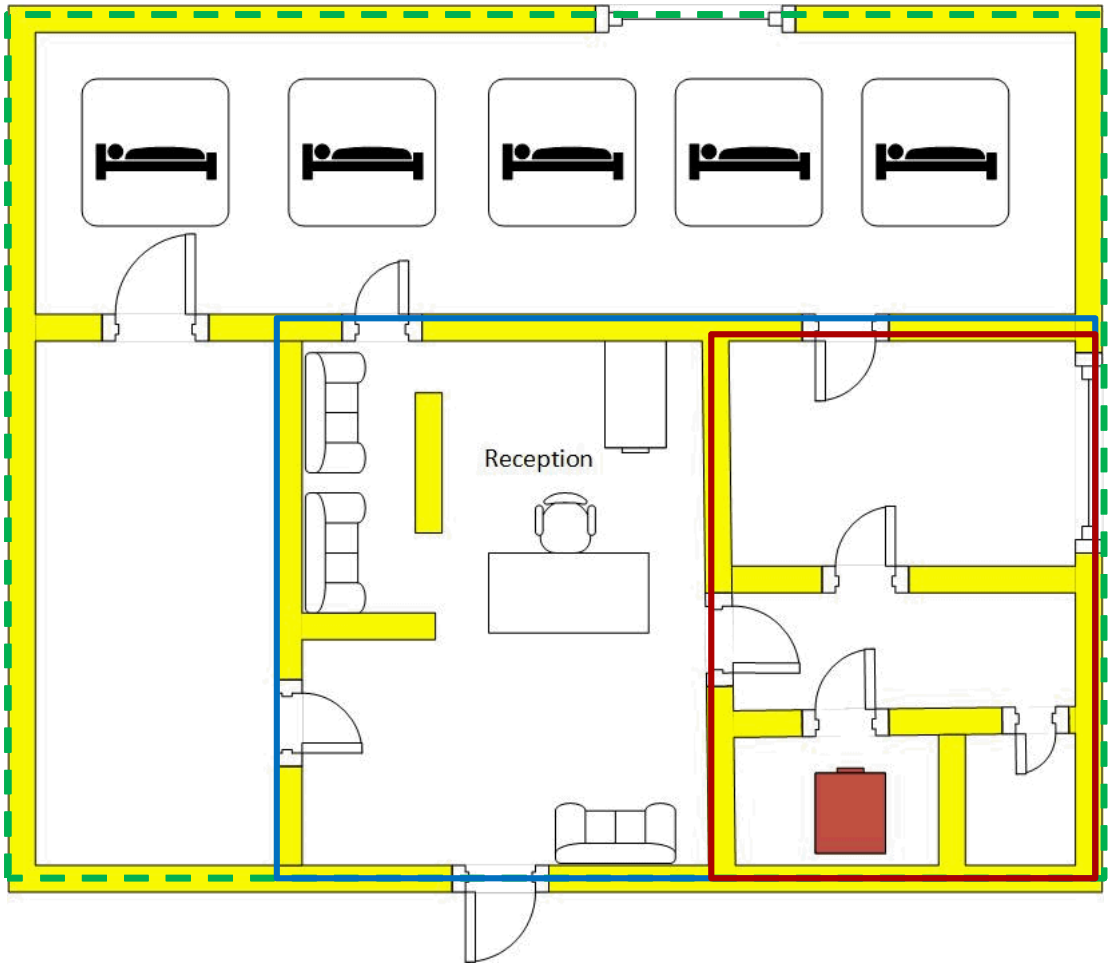
- **Identify Layers/Depth**



Proposed Vulnerability Assessment Approach

Sandia National Laboratories

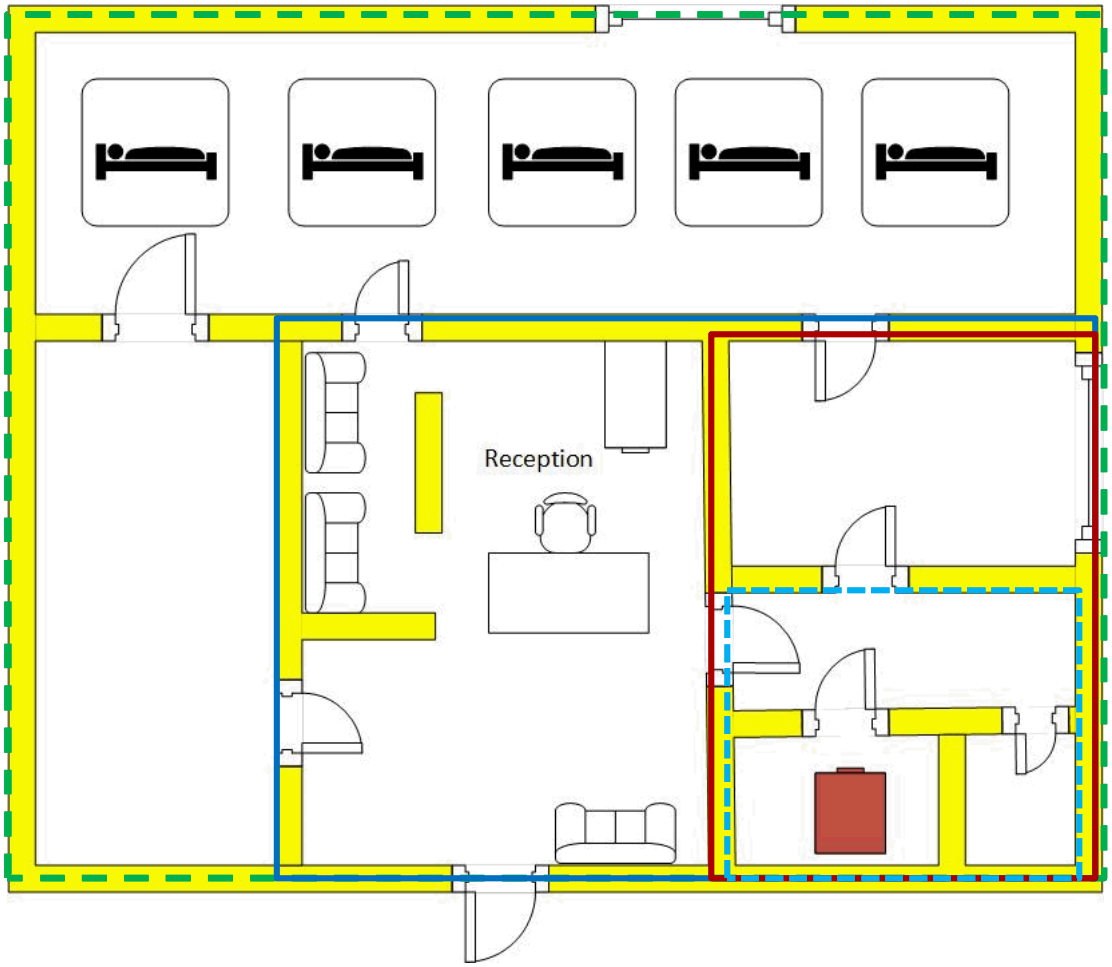
- **Identify Layers/Depth**



Proposed Vulnerability Assessment Approach

Sandia National Laboratories

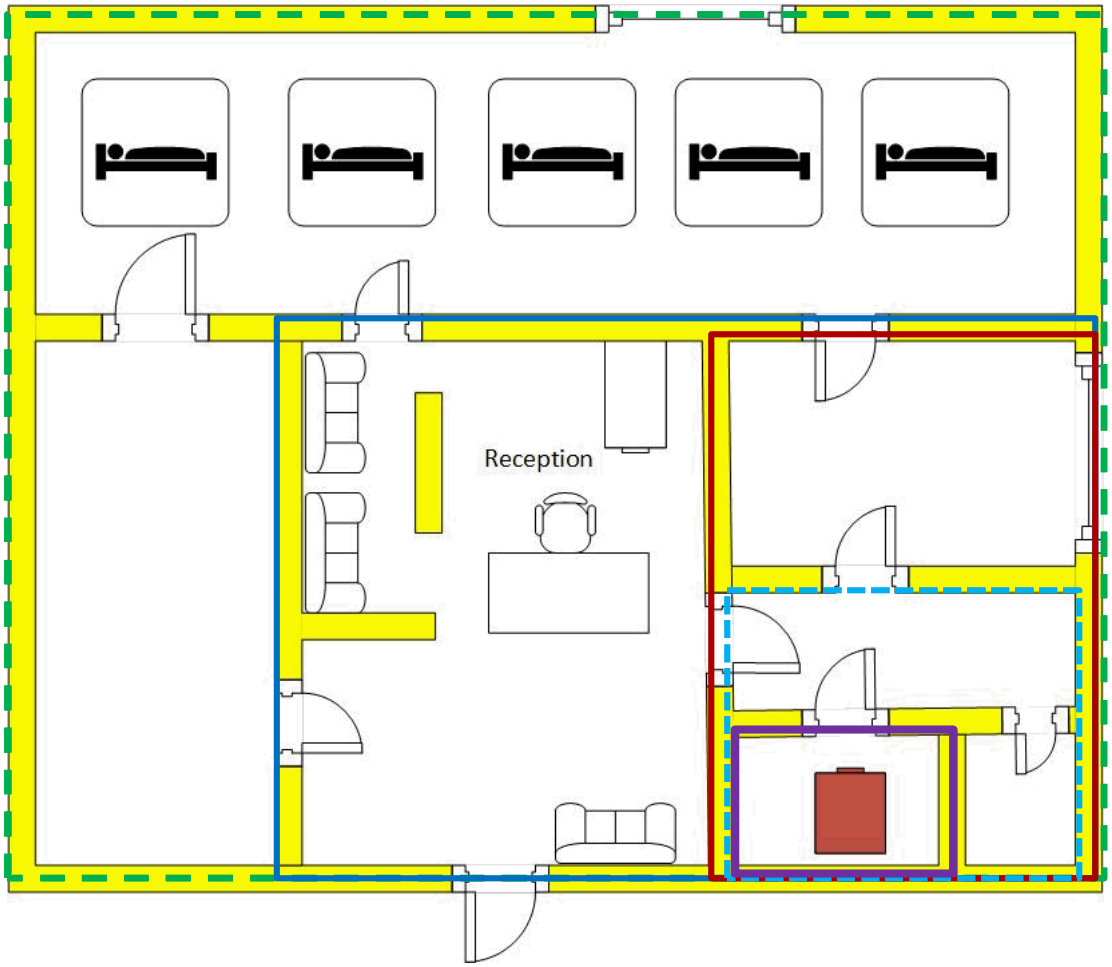
- **Identify Layers/Depth**



Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- **Identify Layers/Depth**

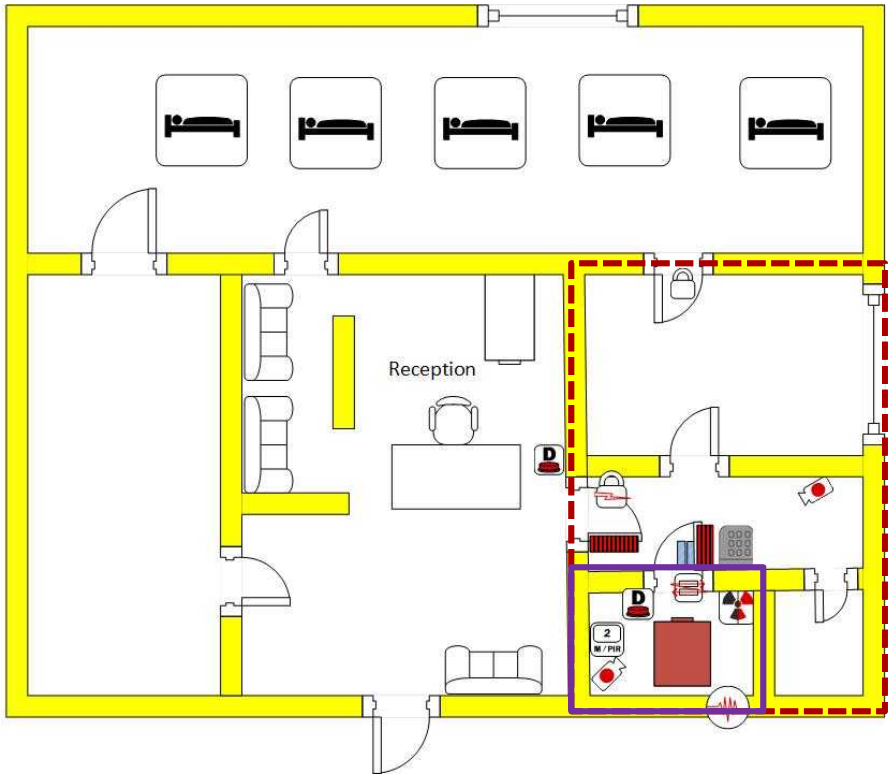


Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**

Legend		
Enhancements		
Symbol	Count	Description
	1	Radiation Detector
	1	Balanced Magnetic Switch
	1	Motion sensor (dual tech)
	1	Magnetic lock
	2	Fixed Camera w/IR (day/ night)
	1	Card reader w/ PIN
	2	Duress button/ switch
	1	Electric lock/ strike
	1	Vibration sensor
	2	Harden or replace door
	1	Lock

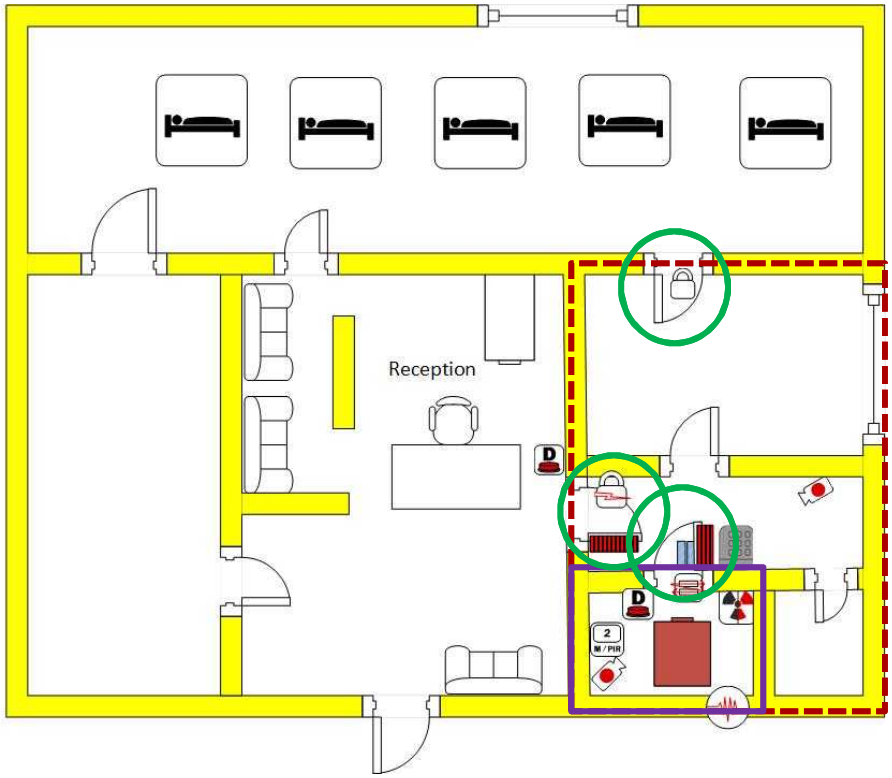


Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**
  - **Detect before delay**

Legend		
Enhancements		
Symbol	Count	Description
	1	Radiation Detector
	1	Balanced Magnetic Switch
	1	Motion sensor (dual tech)
	1	Magnetic lock
	2	Fixed Camera w/IR (day/ night)
	1	Card reader w/ PIN
	2	Duress button/ switch
	1	Electric lock/ strike
	1	Vibration sensor
	2	Harden or replace door
	1	Lock

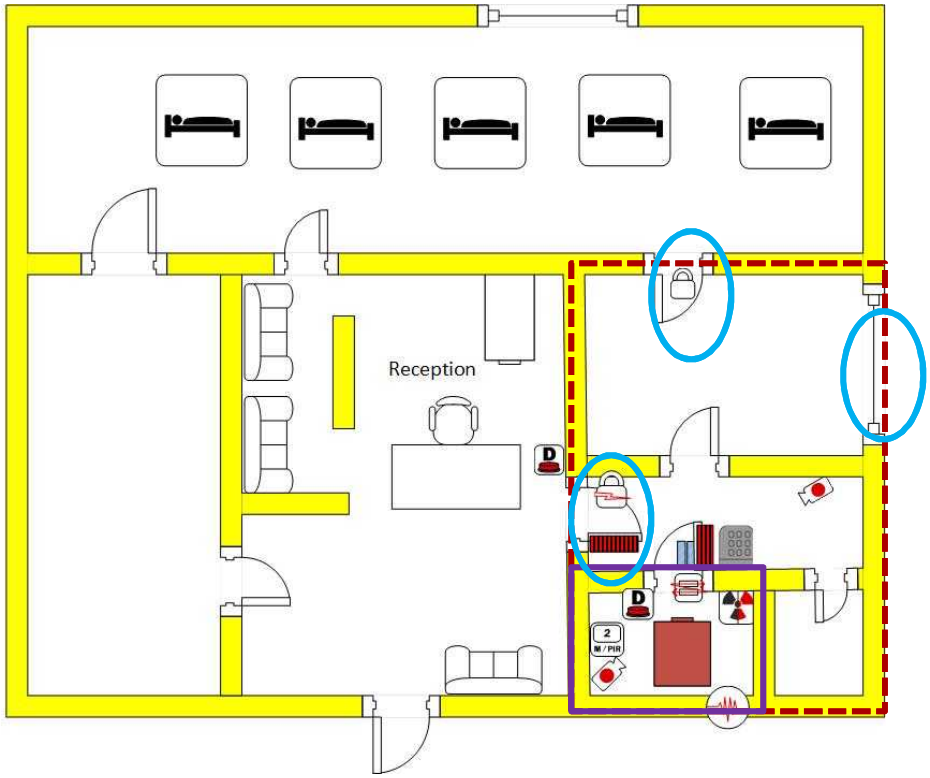


Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**
  - **Delay imbalance**

Legend		
Enhancements		
Symbol	Count	Description
	1	Radiation Detector
	1	Balanced Magnetic Switch
	1	Motion sensor (dual tech)
	1	Magnetic lock
	2	Fixed Camera w/IR (day/ night)
	1	Card reader w/ PIN
	2	Duress button/ switch
	1	Electric lock/ strike
	1	Vibration sensor
	2	Harden or replace door
	1	Lock



Include:

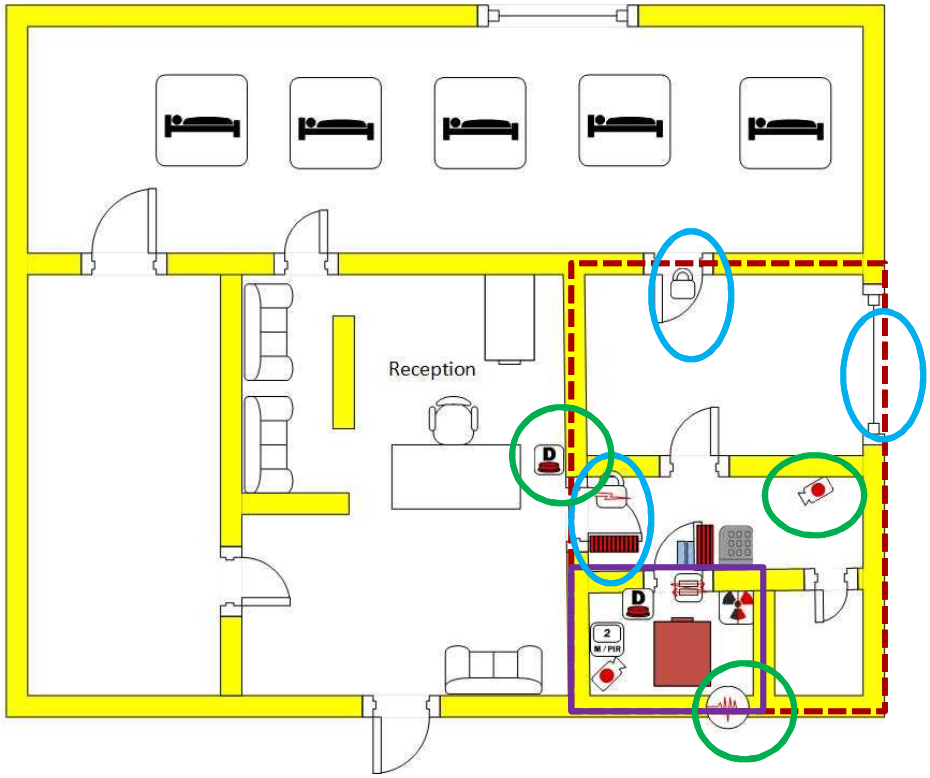
- delay: walls, floors/ceiling, access doors, locks, vents, windows, guards on post

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**

Legend		
Enhancements		
Symbol	Count	Description
	1	Radiation Detector
	1	Balanced Magnetic Switch
	1	Motion sensor (dual tech)
	1	Magnetic lock
	2	Fixed Camera w/IR (day/ night)
	1	Card reader w/ PIN
	2	Duress button/ switch
	1	Electric lock/ strike
	1	Vibration sensor
	2	Harden or replace door
	1	Lock



Include:

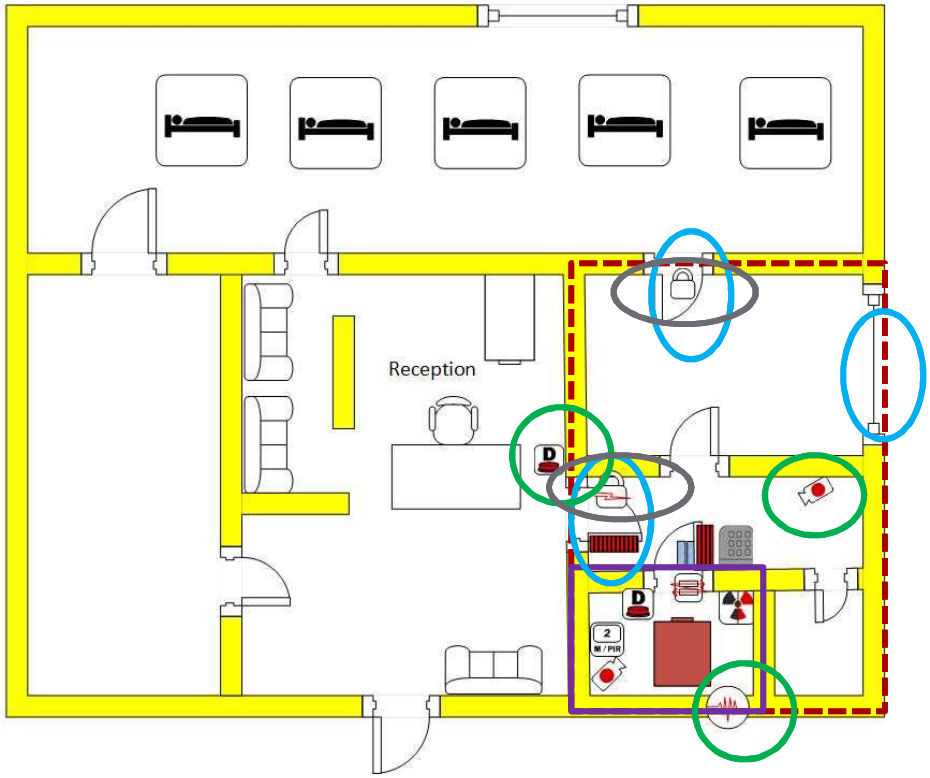
- delay: walls, floors/ceiling, access doors, locks, vents, windows, guards on post,
- detection: sensors, surveillance, and general observation of staff if trained

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**

Legend		
Enhancements		
Symbol	Count	Description
	1	Radiation Detector
	1	Balanced Magnetic Switch
	1	Motion sensor (dual tech)
	1	Magnetic lock
	2	Fixed Camera w/IR (day/ night)
	1	Card reader w/ PIN
	2	Duress button/ switch
	1	Electric lock/ strike
	1	Vibration sensor
	2	Harden or replace door
	1	Lock



Include:

- delay: walls, floors/ceiling, access doors, locks, vents, windows, guards on post,
- detection: sensors, surveillance, and general observation of staff if trained, &
- Access Control: badges, procedures, keys

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**

Investigate measure installation/condition

- Installed improperly
  - Sensors/cameras installed on non-secure side
  - Sensors/cameras not oriented correctly
- In disrepair
  - Walls water damaged
  - Cabling exposed
  - Detection/camera view covered by equipment
  - Camera lens covered by dust

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**

Check for vulnerable times and situations (e.g., during working vs non-working hours, during maintenance or reloading):

- Alarms disabled
- Doors unlocked
- How is detection, delay, and access control compensated for during these times

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- Identify Balance/Gaps
- **Assess Insider**

Verify *Trustworthiness Program* exists

- *Verify that procedures exist to prevent access until trustworthiness completed successfully*
- Verify that areas and information are *compartmentalized* according to sensitivity
- Verify that *Surveillance Program* exists to prevent alone to be unsupervised with materials

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/ Depth
- Assess Detect-Delay
- Identify Balance/Gaps
- Assess Insider
- **Assess Response Coordination**

- Verify Response Contingency Plan exists
- Verify MOU exists with law enforcement
- Verify that Target Folder exists

- For Category 1 materials, conduct periodic security response tabletop exercise to confirm timely effective response

Benefits of VA Approach

- Provides a less rigorous and complex approach to:
  - Validate that prescriptive based security requirements achieve the overall security objective of preventing theft and sabotage
  - Identify specific security gaps and imbalances in order to resolve the vulnerabilities
  - Ensure that the regulatory system is adequately protecting the public from the adverse consequences of radioactive materials.

Summary

- VA approach is described to enable operators and regulators of facilities using or storing radioactive materials to conduct a security vulnerability assessment.
- The approach does not use quantified data, nor formal path analysis, and is therefore not as rigorous an assessment as that undertaken for nuclear facilities
- The approach helps gain insight into performance issues, gaps, and overall effectiveness of the system

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth
- **Identify Balance/Gaps**

Image of strong (locks and doors), medium (walls), weak (padlocks) barriers

Following a look up table

- Categorize barrier delay along layer
  - High (concrete walls, floors, high security doors, reinforced high security locks—multiple deadbolts)
  - Medium (masonry walls, solid wooden/hollow metal non-security doors, deadbolt cylinders in metal frame)
  - Low (plasterboard walls, windows, large vents, simple door locks, hollow wooden doors, simple padlocks, weak lock hasps)

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth

  Images of access control

- **Identify Balance/Gaps**

  Following a look up table for properly installed/correctly followed written procedures
  - Categorize sensor detection along layer
    - High (Panic alarms, BMS on doors, radiation alarms, passive infrared, video motion indoors)
    - Medium (guard on post with no other responsibility, two person control, glass break sensor)
    - Low (surveillance by camera for long period, observation by staff)

Proposed Vulnerability Assessment Approach

Sandia National Laboratories

- Identify Layers/Depth

Images of access control

- **Identify Balance/Gaps**

Following a look up table for properly installed/correctly followed written procedures

- Categorize access control along layer
  - High (two factor access control-includes biometric, with no undetected bypass)
  - Medium (two factor access control with no undetected bypass)
  - Low (one factor access control, bypass/piggybacking possible)