Overview

Sandia National Laboratories

Security Risk Assessment Methodology (RAM)*

Sandia National Laboratories
Albuquerque, New Mexico
February 2008

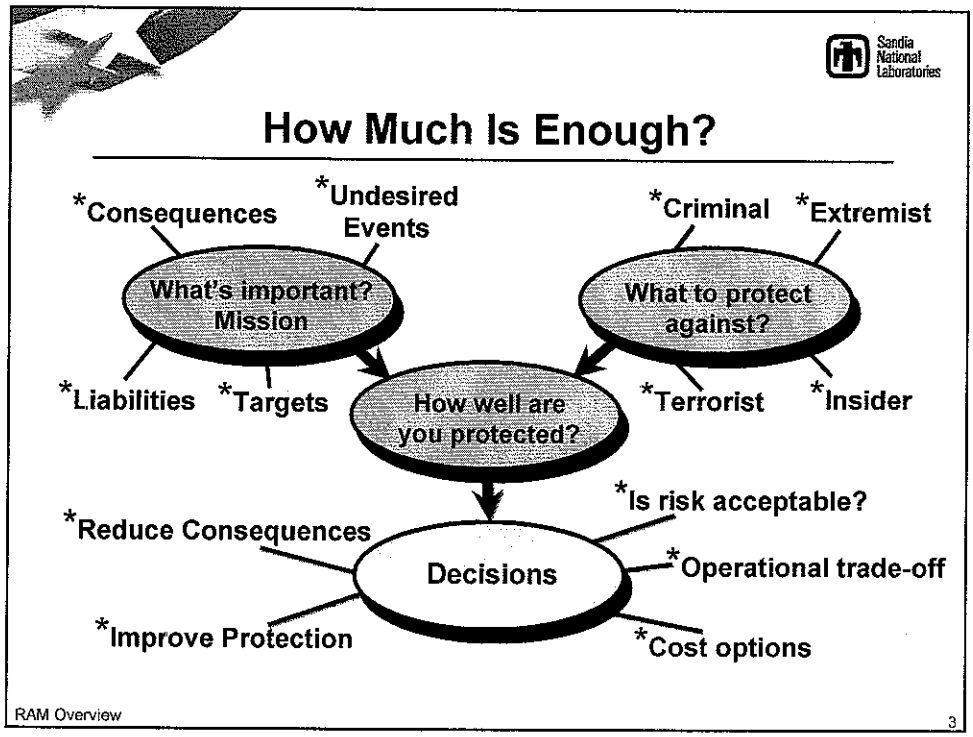
*Presented by Dr Rudy Matalucci with Permission from Sandia

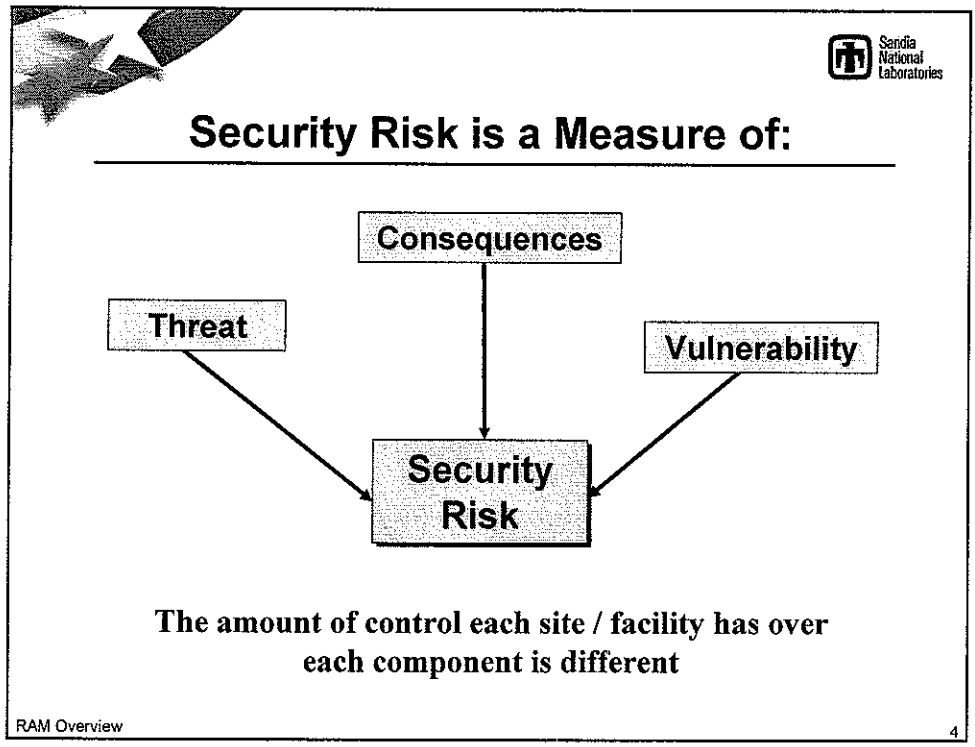
Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Presentation Outline

- Decisions required for a security risk assessment
- Security risk equation
- Security definitions
- Overview of the Risk Assessment Methodology for Critical Infrastructures
- Potential Automation Process

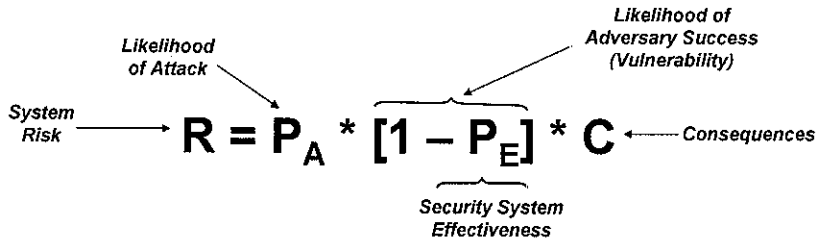

Sandia National Laboratories
How Much Is Enough?
*Consequences
*Undesired Events
*Criminal
*Extremist
What's important? Mission
What to protect against?
*Liabilities
*Targets
How well are you protected?
*Terrorist
*Insider
*Is risk acceptable?
*Reduce Consequences
Decisions
*Operational trade-off
*Improve Protection
*Cost options
RAM Overview
3


Sandia National Laboratories
Security Risk is a Measure of:
Consequences
Threat
Vulnerability
Security Risk
The amount of control each site / facility has over each component is different
RAM Overview
4

Sandia National Laboratories

Security Risk Equation

- Process for risk and resource management using a suite of tools and information
- Based on the security risk equation:



- Integrates many components into a single, consistent, approach for determining risk and making decisions

Sandia National Laboratories

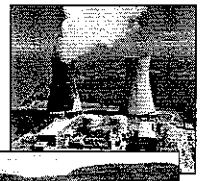
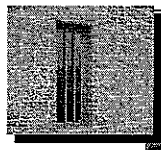
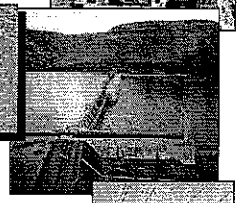
Benefits of Using Security Risk

- Combines three relevant factors into a single parameter
- Allows comparisons of threat, security system, and consequence variations
- Helps in prioritizing / justifying requirements and budgeting
  - Efficient allocation of resources

Sandia National Laboratories

SNL Security RAMs

- RAM-D (Dams)
- RAM-T (Electrical Utility Transmission Systems)
- RAM-W (Municipal Water Systems)
- RAM-C (Communities)
- RAM-CF (Chemical Facilities)
- RAM-P (Prisons)
- RAM-E (Pipelines, Electric Power Generation)
- RAM-FAA (Airspace management facilities)
- RC RAM-W (RAMCAP/NIPP compliant version)


For more information see www.sandia.gov/ram

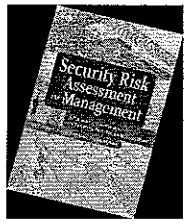
Sandia National Laboratories

Security Definitions

- Security Risk – *Measure* of the potential damage to, or loss of, an asset based on the likelihood of an undesired event
- Security Risk Assessment – *Process* of analyzing threats to, and vulnerability of, a facility; determining the potential for losses; and identifying cost-effective corrective measures
- Vulnerability Assessment – *Process* in which qualitative / quantitative techniques are applied to identify vulnerabilities and to assess the effectiveness level for a security system

Security Risk Assessment Methodology for Critical Infrastructures

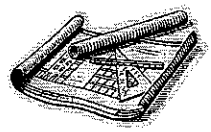
Sandia National Laboratories



Sandia National Laboratories

Security Environment Description

- Site / facility characterization
  - Drawings, reports, policies / procedures, photos
  - Cyber and physical security data
- Site-specific fault tree
  - Customize a generic fault tree for specific CI
  - Identify undesired events and targets (assets)
- Protection objectives



Sandia National Laboratories

Threat Assessment

- Analyze threat
  - Develop site-specific threat spectrum
    - Range of threats (VL - VH)
    - Insiders and outsiders
      - Motivations
      - Attributes
      - Capabilities
  - Estimate threat potential (P_A)



Sandia National Laboratories

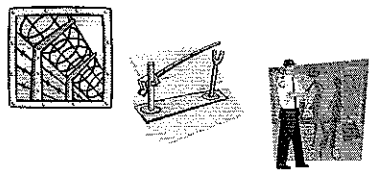
Consequence Assessment

- Define consequences (C)
  - Costs, lives, impacts, etc.
  - Estimate C for each undesired event
    - Usually a qualitative value: VH, H, M, or L
- Prioritize undesired events
  - Prioritize targets (assets)

Sandia National Laboratories

Vulnerability Assessment

- Understand the current physical protection system (baseline analysis)
  - Detection, delay, response
  - Understand the integration of the PPS components
- Organize data and performance test
  - People, equipment / hardware (technologies), and procedures

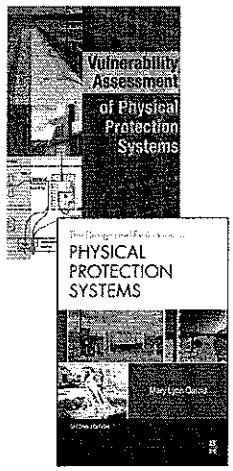


Sandia National Laboratories

Physical Protection System

PPS Definition:

Integration of <u>people, procedures, and equipment</u> for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks



www.bhusa.com/security/us

Vulnerability (System Effectiveness) Analysis

Sandia National Laboratories

- Identify adversary objectives
  - What does the adversary want to achieve?
- Identify worst-case paths and scenarios
- Analyze adversary patterns
- Evaluate physical security and mitigation features
  - Identify system weaknesses
- Determine system effectiveness

Risk Estimation

Sandia National Laboratories

- Risk is a function of
  - Threat
  - Consequences
  - Vulnerability (system effectiveness)
- Calculate baseline risks
- Consider constraints
  - Legal, operational, budget, resources, culture, etc.

Sandia National Laboratories

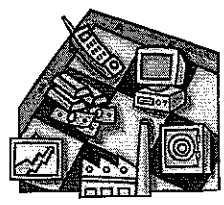
Risk Management and Reduction

- Determine what is acceptable risk
  - Senior management / facility owner decision
- Reduce the risks - identify and propose security upgrades
  - Increase security system effectiveness
    - Detection, delay, response
  - Reduce consequences
    - Upgrade consequence mitigation features
- Evaluate impact of upgrades
  - Re-calculate risk
  - Compare to baseline risk

Sandia National Laboratories

Upgrade Impact Evaluation

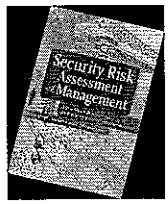
- Consider additional impacts other than risk reduction
  - Cost
  - Operations
  - Schedule
  - Public opinion



Sandia National Laboratories

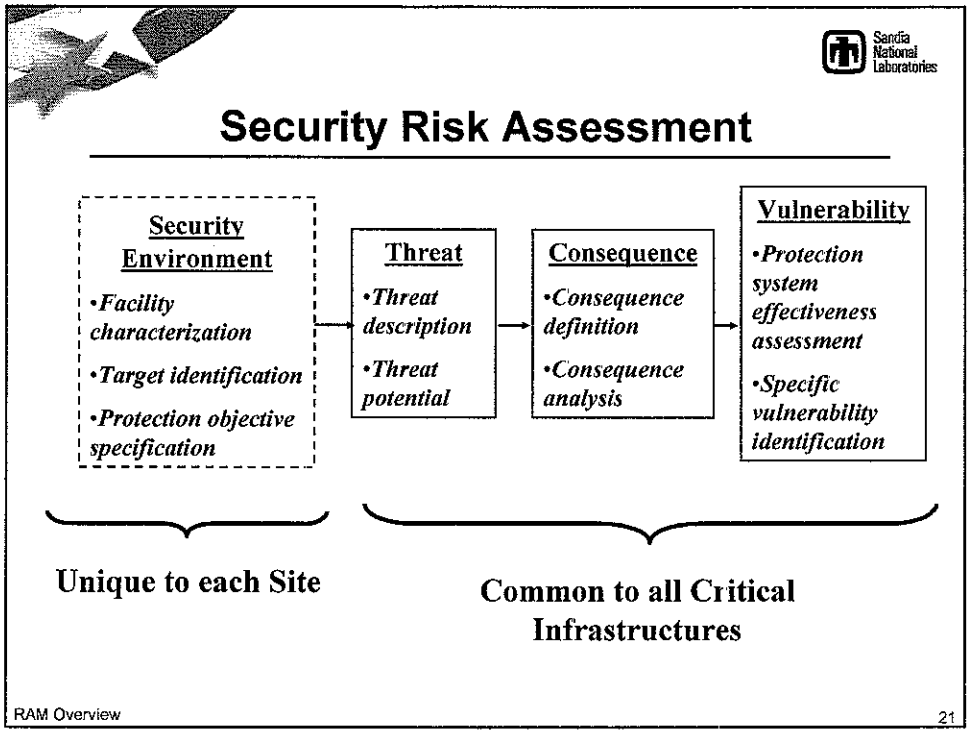
Benefits of a Systematic Approach

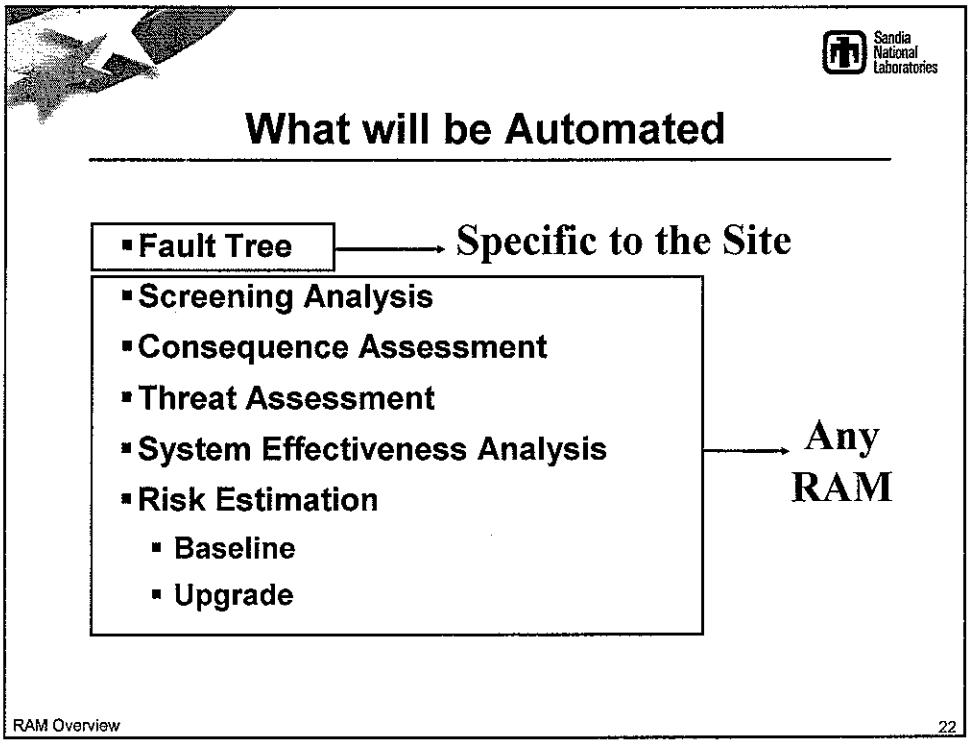
- Repeatability
- Quantified
- Standardized
- Accountability
- Traceability
- Consistent terminology
- Defensibility
- Ease of automation



Sandia National Laboratories

Automation of RAM


Sandia National Laboratories
Security Risk Assessment
Security Environment
•Facility characterization
•Target identification
•Protection objective specification
Threat
•Threat description
•Threat potential
Consequence
•Consequence definition
•Consequence analysis
Vulnerability
•Protection system effectiveness assessment
•Specific vulnerability identification
Unique to each Site
Common to all Critical Infrastructures
RAM Overview
21


Sandia National Laboratories
What will be Automated
▪ Fault Tree
Specific to the Site
▪ Screening Analysis
▪ Consequence Assessment
▪ Threat Assessment
▪ System Effectiveness Analysis
▪ Risk Estimation
▪ Baseline
▪ Upgrade
Any RAM
RAM Overview
22

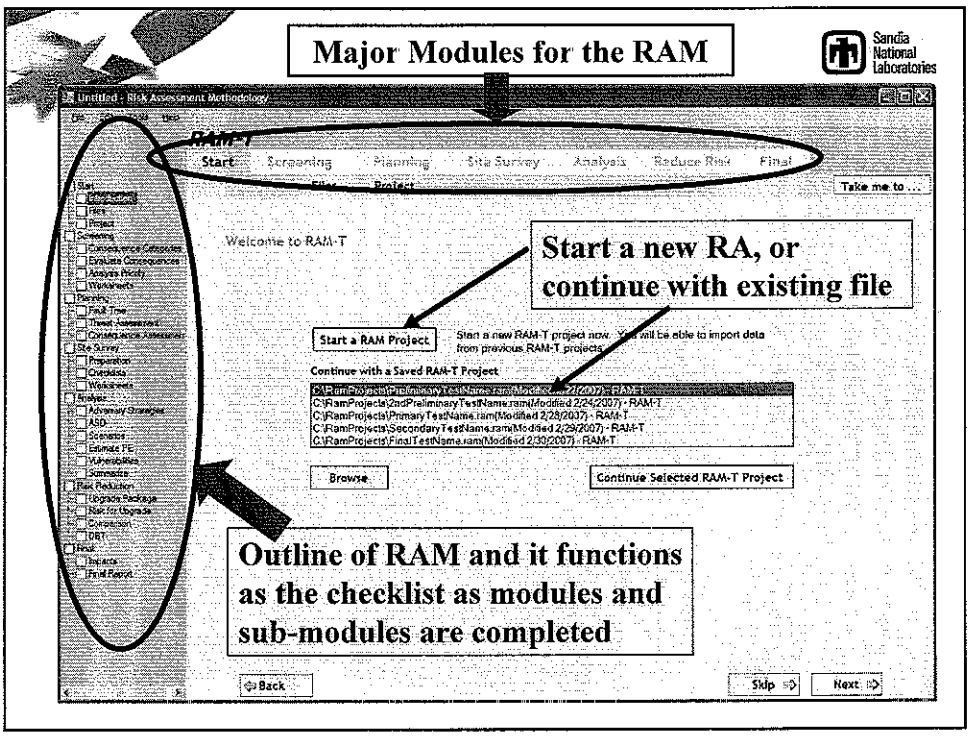
What parts of the RAM are not Automated?

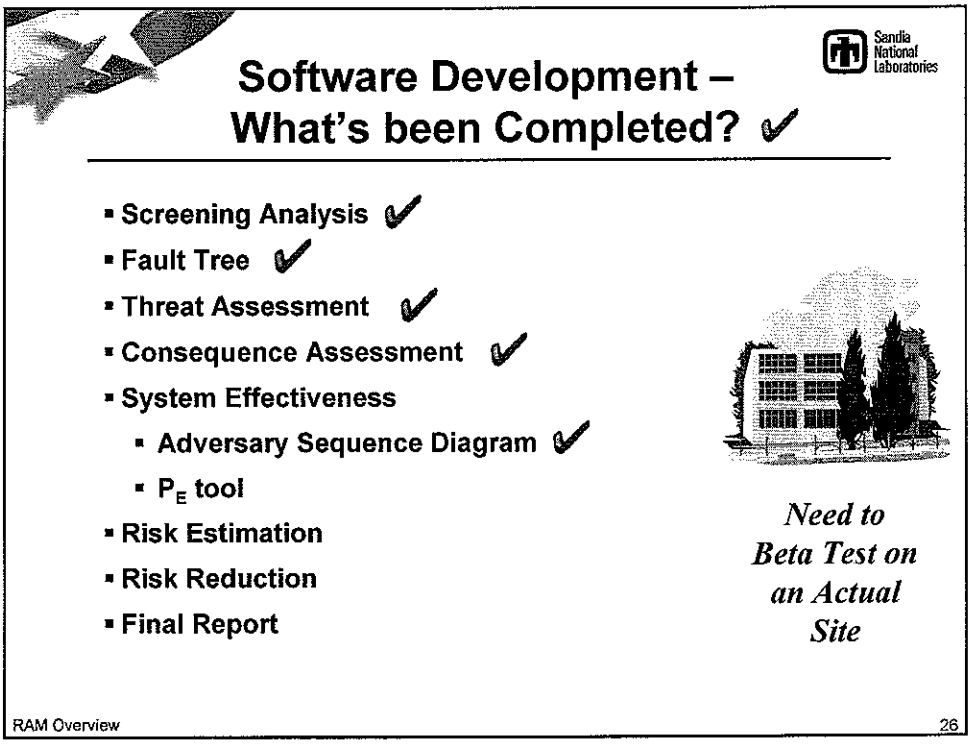
Sandia National Laboratories

- Protection objectives
- Project definition
  - Scope of project, team, schedule
- Site survey data collection
  - Drawings, reports, policies, procedures, etc.
  - Site interviews
- Performance testing data
- Cyber security (TBD later?)

Sandia National Laboratories

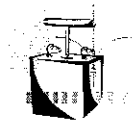
Let's look at the RAM Automation Tool Start Window


Major Modules for the RAM
Sandia National Laboratories
Untitled - Risk Assessment Methodology
RAM-T
Start
Screening
Planning
Site Survey
Analysis
Reduce Risk
Final
Take me to ...
Welcome to RAM-T
Start a new RA, or continue with existing file
Start a RAM Project
Start a new RAM-T project now. You will be able to import data from previous RAM-T projects.
Continue with a Saved RAM-T Project
C:\RamProjects\PrelimaryTestName.ram(Modified 2/24/2007) - RAM-T
C:\RamProjects\2ndPrelimaryTestName.ram(Modified 2/24/2007) - RAM-T
C:\RamProjects\PrimaryTestName.ram(Modified 2/28/2007) - RAM-T
C:\RamProjects\SecondaryTestName.ram(Modified 2/29/2007) - RAM-T
C:\RamProjects\FinalTestName.ram(Modified 2/30/2007) - RAM-T
Browse
Continue Selected RAM-T Project
Outline of RAM and it functions as the checklist as modules and sub-modules are completed
Back
Skip
Next


Sandia National Laboratories
Software Development – What's been Completed?
Screening Analysis
Fault Tree
Threat Assessment
Consequence Assessment
System Effectiveness
Adversary Sequence Diagram
P_E tool
Risk Estimation
Risk Reduction
Final Report
Need to Beta Test on an Actual Site
RAM Overview
26

Future Add-ons to Automated Tool

- First-order blast calculations
  - Determines effects – human and structural
  - Provides stand-off distances
- Natural hazards screening
  - Sites can identify what natural hazards might affect them
- Compatibility with RAMCAP
  - Risk Analysis and Management for Critical Asset Protection



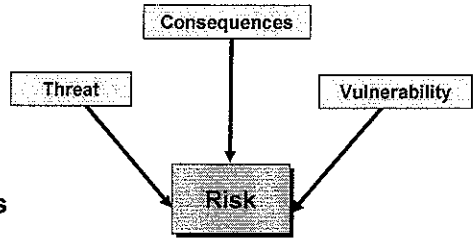
RAM Overview Summary

- A RAM approach can help critical infrastructures make security decisions based on a rigorous systematic process
  - Integrated system engineering approach
- Critical infrastructure security goals usually include:
  - Protection of life (employees and public)
  - Continuity of mission and critical operations
  - Protection of facilities, property, and equipment

Sandia National Laboratories

RAM Overview Summary *(cont'd)*

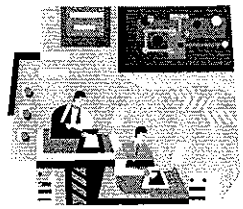
- Security Risk is a function of
  - Threat
    - *Likelihood of attack*
  - Consequences of adversary success
  - Vulnerability
    - *System In- effectiveness*
- Critical infrastructure owners and / or senior management are responsible for final decisions
- RAM Automation Underway



Sandia National Laboratories

A Word about Cyber Security

- Cyber security is not included in the automated tool
  - Focus is on physical security
  - However, extremely important to evaluate
- May be incorporated into the tool at a much later date
- Every site should evaluate and analyze cyber security
  - Identify critical cyber assets
  - Ensure assets are protected
  - Understand the interdependency between cyber and physical security



Presentation Summary

- Decisions required for a security risk assessment
- Security risk equation
- Security definitions
- Overview of the Risk Assessment Methodology for Critical Infrastructures
- Automated RAM Tool Underway

Sandia National Laboratories Point of Contact

- For more information concerning RAMs for critical infrastructures or the automated RAM tool, contact:

Betty E. Biringer, Manager
Security Risk Assessment Department
Sandia National Laboratories
Albuquerque, New Mexico USA
bebirin@sandia.gov
505-844-3985
www.sandia.gov/ram