

Security Risk Assessment Methodology (RAM)

Automated Tool Overview*

*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-AC04-04AL85000.

Security Risk Equation

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

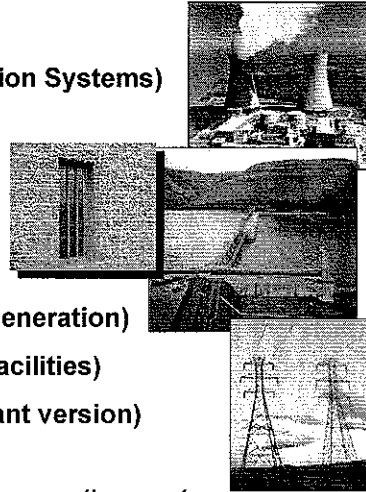
$$\text{System Risk} \rightarrow R = P_A * \underbrace{[1 - P_E]}_{\text{Security System Effectiveness}} * C \leftarrow \text{Consequences}$$

Likelihood of Adversary Success (Vulnerability)

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

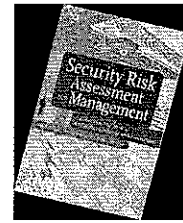
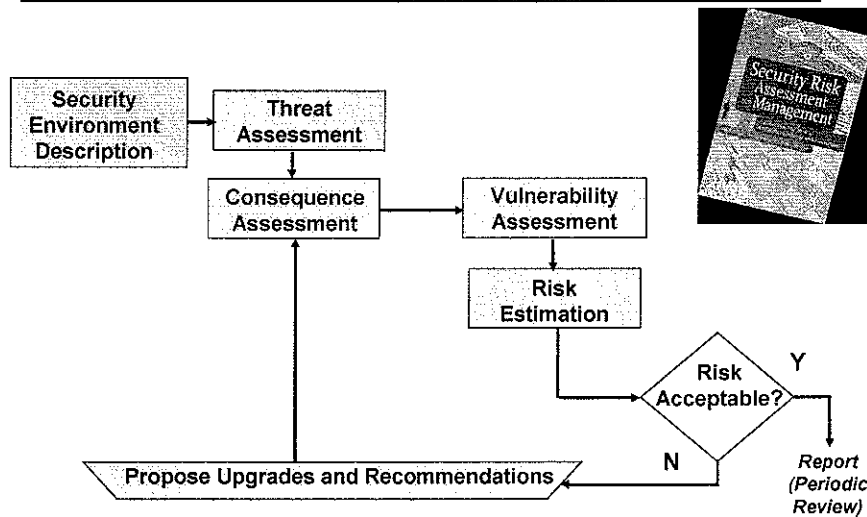
SNL Security RAMs

- 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)

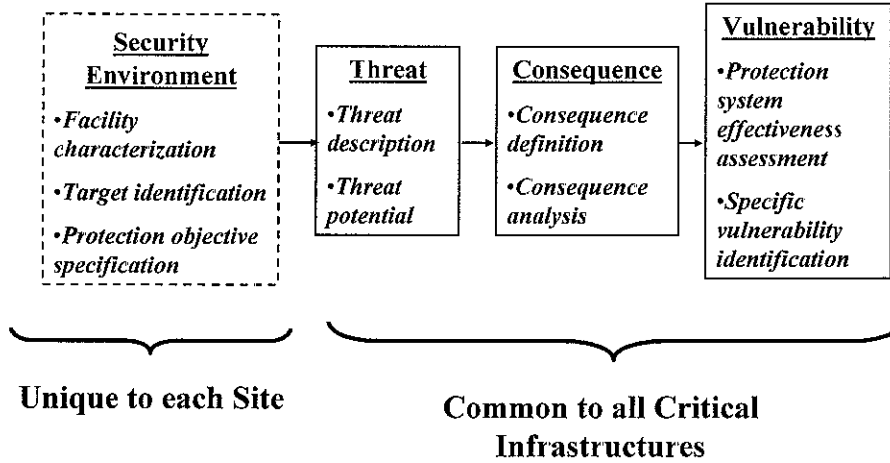


For more information see www.sandia.gov/ram

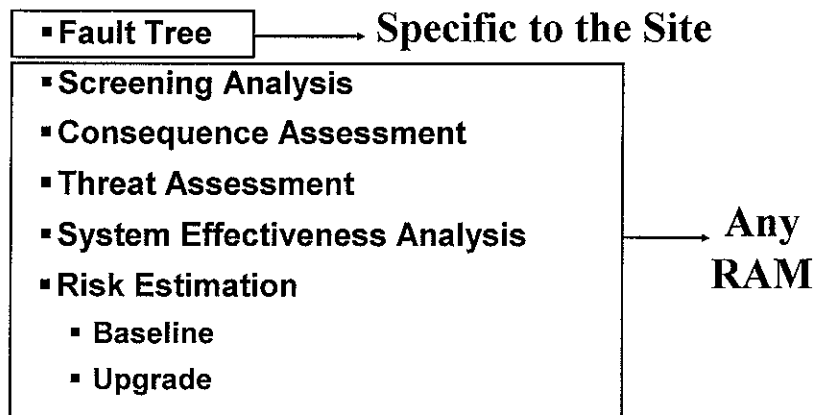
Security Risk Assessment Methodology for Critical Infrastructures





Security Risk Assessment



What will be Automated







What parts of the RAM are not Automated?

- 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?)

Automated RAM Tool 7



Let's look at the Tool

Next Slide: The Start Window

Major Modules for the RAM

Sandia National Laboratories

Start a new RA, or continue with existing file

Outline of RAM and its functions as the checklist as modules and sub-modules are completed

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

Browse Continue Selected RAM-T Project

Back Skip Next


Sandia National Laboratories

Screening Analysis

- **Consequence Table – Inputs:**
 - Sites / facilities
 - User defined criteria
 - User defined number of levels of criteria
 - User provide definitions for levels of criteria
- **Output: Screening Worksheet**
 - Prioritization of facilities

Automated RAM Tool 10

Screening: Consequence Categories and Descriptions




User-Defined or can use Default Categories and Descriptions

Below are typical consequence categories for electrical transmission facilities. Please review the list with your facilities in mind, reviewing the categories and their descriptions. You may add, delete, or modify categories that apply to your site. When finished, click the **Next** button at the bottom of the form.

| Consequence Category | Description |
|--|---|
| National Security | All facilities of consequence to the national security of the United States, including but not limited to those that support the national security of the United States. This category includes national infrastructure that supports the following: <ul style="list-style-type: none"> Energy Production Transportation Information Technology Water Supply Defense |
| Public Health and Safety | All facilities of consequence to the public health and safety of the United States, including but not limited to those that support the public health and safety of the United States. This category includes the following: <ul style="list-style-type: none"> Water Supply Transportation Information Technology Defense |
| Economic Security | All facilities of consequence to the economic security of the United States, including but not limited to those that support the economic security of the United States. This category includes the following: <ul style="list-style-type: none"> Water Supply Transportation Information Technology Defense |
| Regional and National Electrical Grid Reliability | All facilities of consequence to the regional and national electrical grid reliability of the United States, including but not limited to those that support the regional and national electrical grid reliability of the United States. This category includes the following: <ul style="list-style-type: none"> Water Supply Transportation Information Technology Defense |
| Other | All facilities of consequence to the site, including but not limited to those that support the site's operations. This category includes the following: <ul style="list-style-type: none"> Water Supply Transportation Information Technology Defense |

Automated RAM Tool
11

Choice of Number of Consequence Severity Levels



RAM-T

By default, RAM-T analysis uses three Consequence Severity levels as shown below. If desired, you may choose to use four or five levels, or you may choose your own level scheme. Please select a number of levels from the choices below and then click the **Next** button at the bottom of the form.

| Consequence Severity | Description | Consequence Severity | Description | Consequence Severity | Description |
|-----------------------|-----------------|-----------------------|---------------------------|-----------------------|---------------------------|
| HH (Very High) | Critical Impact | VH (Very High) | Extremely Critical Impact | VH (Very High) | Extremely Critical Impact |
| M (Medium) | Moderate Impact | H (High) | Critical Impact | H (High) | Critical Impact |
| L (Low) | Minimal Impact | M (Medium) | Moderate Impact | M (Medium) | Moderate Impact |
| | | L (Low) | Minimal Impact | L (Low) | Minimal Impact |
| | | | | VL (Very Low) | Negligible Impact |

Use Three Consequence Severity Levels
 Use Four Consequence Severity Levels
 Use Five Consequence Severity Levels
 Define Custom Consequence Severity Levels

Automated RAM Tool
12

Evaluate Consequences



RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Panel

Consequence Categories Evaluate Consequences Worksheets

Instructions for form use go here

Enter a name for the facility to be screened:

Facility : Test Facility AA

| Consequences of Undesired Events >> | Consequence Category | Consequence Severity* |
|-------------------------------------|---|---|
| | National Security | <input type="radio"/> H <input type="radio"/> M <input type="radio"/> L |
| | Public Health and Safety | <input type="radio"/> H <input type="radio"/> M <input type="radio"/> L |
| | Economic Security | <input type="radio"/> H <input type="radio"/> M <input type="radio"/> L |
| | Regional and National Electrical Grid Reliability | <input type="radio"/> H <input type="radio"/> M <input type="radio"/> L |
| | Generation | <input type="radio"/> H <input type="radio"/> M <input type="radio"/> L |

*H = critical impact
M = moderate impact
L = minimal impact

Highest Consequence Severity: H

Occurrences: 2

Next Facility >>

Back Skip Next

Automated RAM Tool

Output: Prioritization of Facilities



RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Panel

Consequence Categories Evaluate Consequences Analysis Priority

You have created the worksheets listed below. You may edit any of these worksheets to reflect any changes for this project. If appropriate, the items may also be deleted or printed.

| Facility Name | Number |
|-----------------|--------|
| Test Facility A | 1 |
| Test Facility B | 2 |
| Test Facility C | 3 |
| Test Facility D | 4 |

+ Add Worksheet ✓ Edit Worksheet ✗ Delete Item

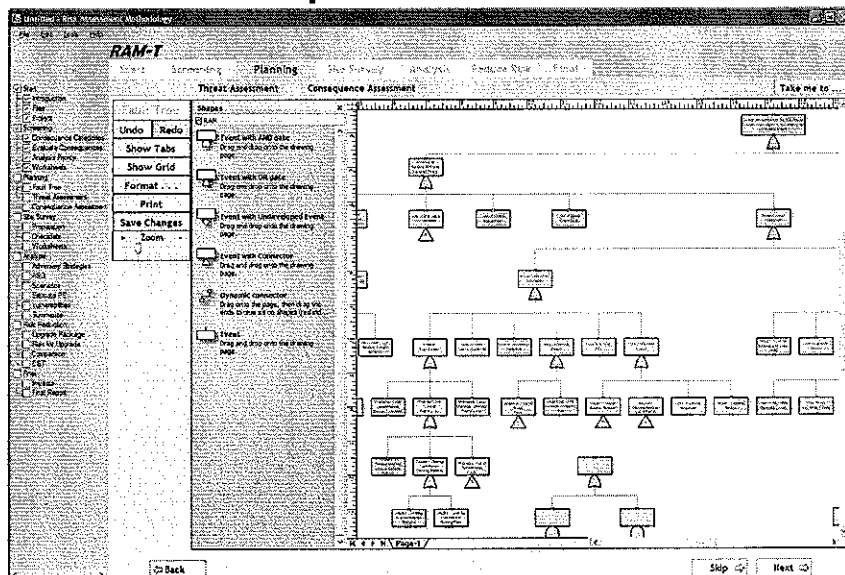
Back Skip Next

Automated RAM Tool

Generic Fault Tree

- Generic fault tree provided for some critical infrastructures
 - User can delete events
 - User can add events
- } → *Site Specific Fault Tree*
- Used to determine undesired events
 - Used to determine critical assets to be protected in order to prevent undesired events
 - Adversary strategies and scenarios can be developed from fault tree
 - Ensures completeness

Creating a Site-Specific Fault Tree



Threat Analysis

- **Input:**
 - **Site-specific threats**
 - Outsiders
 - Insiders
 - **Threat capabilities and attributes**
- **Output:**
 - **Threat Description Table**
 - Full range of threats (H to L)
 - **Threat level estimate**



Identify Site-Specific Threats

The screenshot shows the RAM-T software interface. The main window is titled 'Threat Identification Worksheet' for 'Facility: Test Facility AD'. It asks the user 'Which adversaries are threats to this facility?'. Below this, there are several categories of adversaries with checkboxes:

- Terrorists
 - International
 - Domestic: Ecological
 - Domestic: Militia / Paramilitary
- Extremist Group
- Criminal
- Gang
- Vandal
- Insider(s)
- Other

 A callout box with a bracket points to the 'Terrorists' section, containing the text 'User Selects Site-Specific Threats'. The interface also includes a navigation menu on the left, a 'Take me to...' button, and 'Previous', 'Next', and 'Back' buttons at the bottom.

User Defines Threat Attributes and Capabilities



Facility Identifier: Test Facility AD

Type of Adversary: Criminal

Information Category

| | |
|--|--|
| 1. Incidents (Historically, currently, future potential) | Nearly annual theft incidents. |
| 2. Has the adversary shown interest in this facility or the same type of facility? | Yes |
| 3. Number of adversaries | 2-3 |
| 4. Equipment | Hand tools |
| 5. Vehicles | Car, pickup |
| 6. Weapons | Handguns, automatics, knives |
| 7. Motivation | Financial gain, Steal property |
| 8. Tactics | Property theft. |
| 9. Intelligence gathering means | Local media, Limited observation. |
| 10. Targets of Interest | Equipment room. |
| 11. Potential for collusion with insider | Defeat sensors or other protective measures. |

Automated RAM Tool

Site-specific Threat Spectrum



Threat Spectrum includes both Outsiders and Insiders

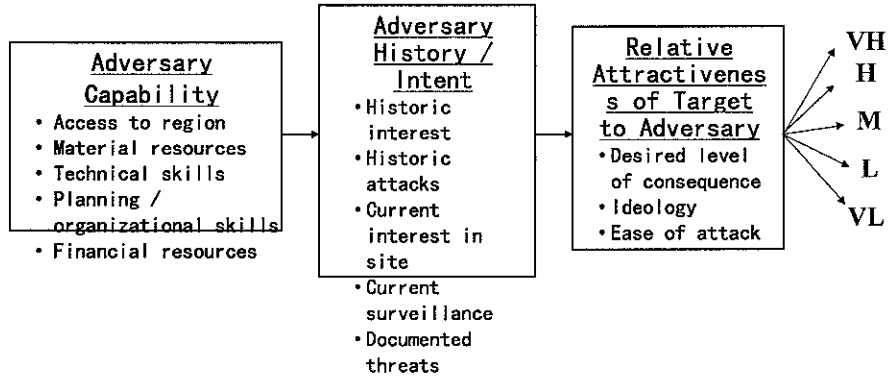
Facility Specific Threat Worksheet

| Type of Adversary | Number of Adversaries | Equipment | Vehicles | Weapons | Motivation | Tactics | Targets of Interest |
|----------------------|-----------------------|------------------|----------|--------------------|----------------|-------------|---------------------|
| Criminal | 2-3 | Hand tools | SUV | Automatic, handgun | Financial gain | Theft | Equipment storage |
| Insider - Engineer | 1 | Pocket protector | Prius | Side rule | Revenge | Destruction | Galentia |
| Insider - Accountant | 1 | Eye shade | Yaris | Sharpened pencil | Revenge | Violence | Cash drawer |
| Insider - Laborer | 1 | Shovel | Pickup | Explosives | Disgruntled | Theft | Equipment storage |

Automated RAM Tool

Threat Potential

- Relative score – not a probability
- Scored per undesired event and per adversary type



Estimating Threat Level for each Threat

User is asked a series of questions for each threat. Numerical scores are assigned and a qualitative value is determined.

| Adversary History / Intent | Score |
|--|-------|
| <input checked="" type="checkbox"/> Documented evidence that this adversary group has shown interest <input type="checkbox"/> Speculation, but no evidence that this adversary has shown interest <input type="checkbox"/> No evidence this adversary has shown interest | 5 |
| Total Score for Adversary Group (sum all scores) | |
| | 65 |

P A **VH**

Undesired Event vs. Threat Level

For each threat in the Threat Spectrum, a threat level value (qualitative) is determined for each Undesired Event

Automated RAM Tool

Consequence Analysis

- **Consequence Table – Input:**
 - **User defined criteria**
 - Measures – qualitative and quantitative
 - **User defined number of levels of criteria**
 - **User provide definitions for levels of criteria**
 - Consequence severity levels (L to VH)
- **Output: Consequence analysis worksheet(s)**

Consequence Criteria and Values

Automated RAM Tool

Consequence Assessment Table

A consequence severity level will be determined for each undesired event

| Undesired Event | Relevant Event? Yes or No | Measure of Consequence | | Consequence Severity | |
|---|---------------------------|---|--------------------------------|----------------------|--|
| | | Type | Value | By Type | By Event |
| Loss of Flood Control | Yes | Population at Risk | > 1,000 - 10,000 | M | Highest Consequence VH |
| | | Deaths | > 1,000 | VH | |
| | | Economic Loss | > \$100 million - \$1 billion | H | |
| Loss of Hydroelectric Generation | Yes | Economic Loss | > \$1 million - \$10 million | L | Highest Consequence VH |
| | | Duration | Years | VH | |
| | | Geographic Impact | State | M | |
| Loss of Commercial Navigation on River | Yes | Economic Loss | > \$1 million - \$10 million | L | Highest Consequence M |
| | | Duration | Weeks | M | |
| | | Geographic Impact | State | H | |
| Loss of Water Supply (Irrigation, Domestic, Industrial) | Yes | Economic Loss | > \$1 million - \$10 million | L | Highest Consequence H |
| | | Duration | Months | H | |
| | | Geographic Impact | Neighborhood | VL | |
| Environmental/Ecological Loss | Yes | Economic Loss | > \$10 million - \$100 million | M | Highest Consequence VH |
| | | Duration | Hours | VL | |
| | | Geographic Impact | National | VH | |
| | | Highest priority for an undesired event | | VH | Highest Consequence Number of occurrences of highest priority category 3 |

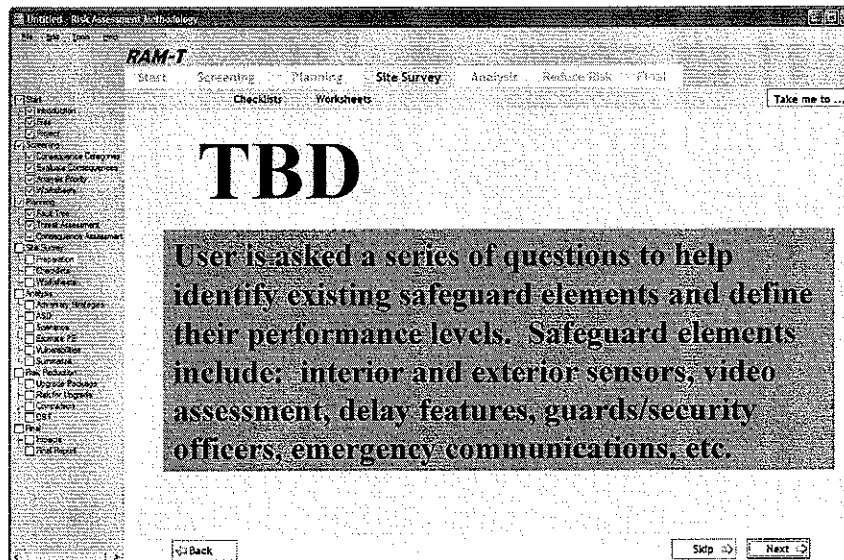
Automated RAM Tool

Site Survey

- Evaluate detection, delay, response elements along potential adversary paths
 - Evaluation based on threat attributes and capabilities from the threat assessment module
- Determine performance data to be used in analysis
 - Qualitative and quantitative data



Site Survey



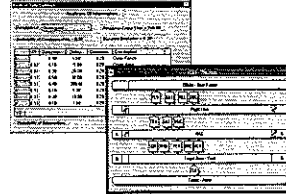
TBD

User is asked a series of questions to help identify existing safeguard elements and define their performance levels. Safeguard elements include: interior and exterior sensors, video assessment, delay features, guards/security officers, emergency communications, etc.

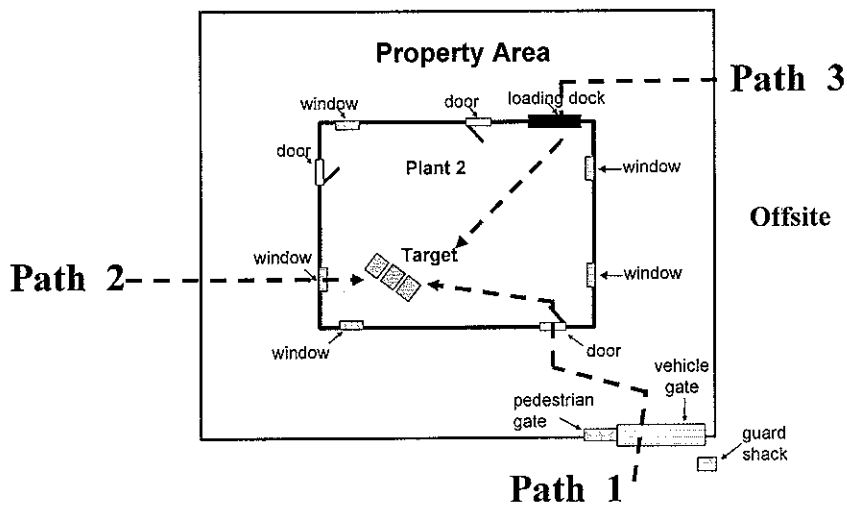


System Effectiveness Analysis

- Adversary Sequence Diagrams
 - User defined protection layers
 - User defined path elements
 - User defined connectedness
- TBD: Plans to incorporate a structured user-friendly system effectiveness tool
 - Analyzes at a systems level
 - Employs SNL security database for protection elements
- Identifies vulnerabilities



Physical Paths (Protection Layers and Path Elements)



Adversary Sequence Diagram

User is asked a series of questions to help develop the protection layers and path elements

Output: ASD

Automated RAM Tool

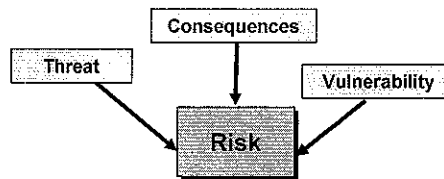
Estimating System Effectiveness

P_E Tool to be Included

Automated RAM Tool

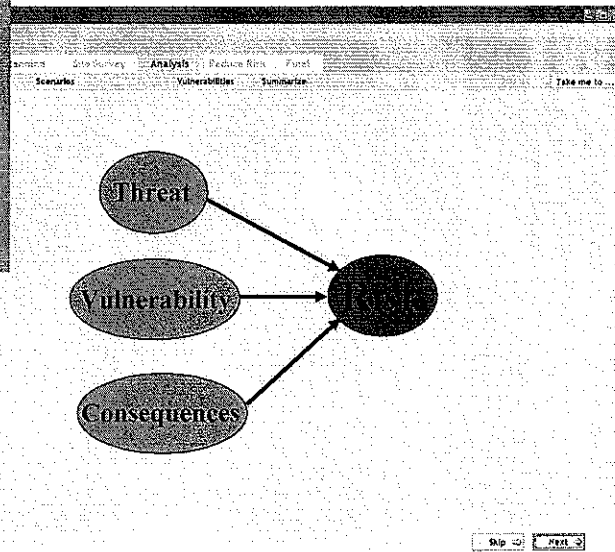
Risk Level Estimation

- Logically combine estimates for Threat, System Effectiveness (Vulnerability), and Consequence to estimate security risk
 - Risk is reported as a qualitative value - based on quantitative and qualitative inputs



Estimating Risk

The tool combines the qualitative output from each of the major modules and calculates Risk (VL to VH)

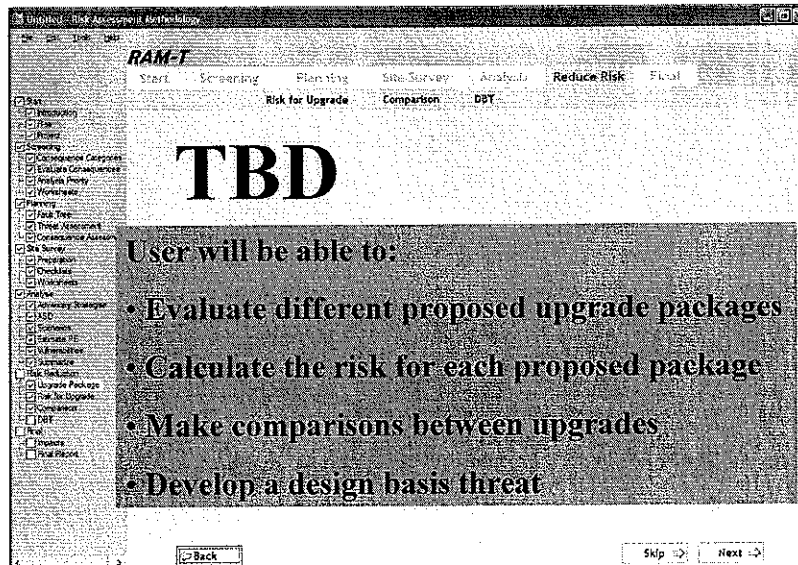


Reducing Security Risk

- Reduce threat level
 - Deterrence
 - Difficult to measure
- Reduce vulnerability
 - Increase detection, delay, response
- Reduce consequence level
 - Mitigation features
 - Redundancy
 - Transfer
 - System robustness
- Improve emergency response




Reduce Risk



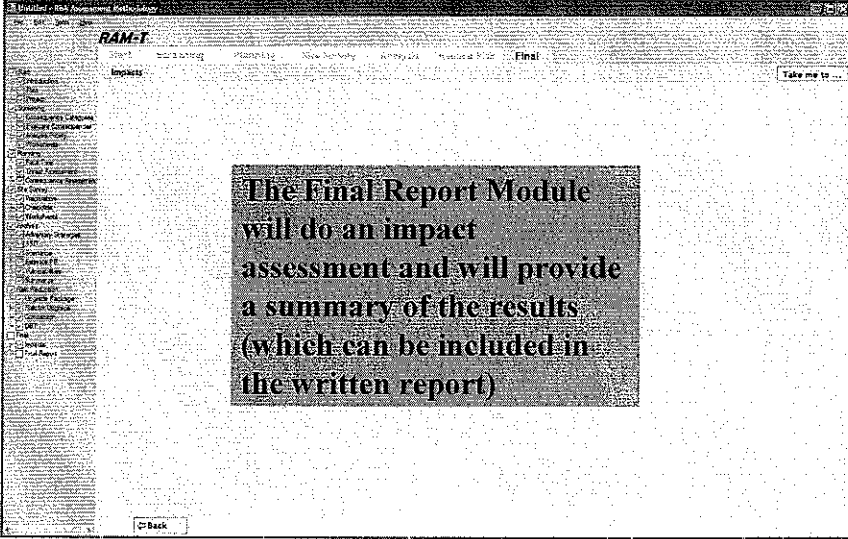
TBD

User will be able to:


- Evaluate different proposed upgrade packages
- Calculate the risk for each proposed package
- Make comparisons between upgrades
- Develop a design basis threat



Final Report

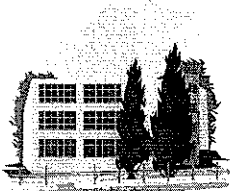


Automated RAM Tool 37



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

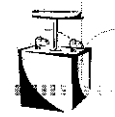


*Need to
Beta Test on
a Real Site*

Automated RAM Tool 38

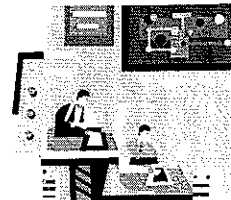
Future Add-ons to Automated Tool

- **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



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

- **Automated RAM Tool**
 - Input Site-Specific Parameters
 - Generate Site-Specific Fault Tree
 - Risk Equation Parameters Incorporated in the Tool
 - Automation Calculates Risk
 - Mitigation Measures Show Risk Reduction
- **Development Continuing**
- **Beta Testing to be Scheduled**

QUESTIONS??

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**