

Security Risk Assessment Methodology (RAM) Overview and the Automated RAM Tool

Sandia National Laboratories
February 2008

Presentation Outline

■ Part I

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

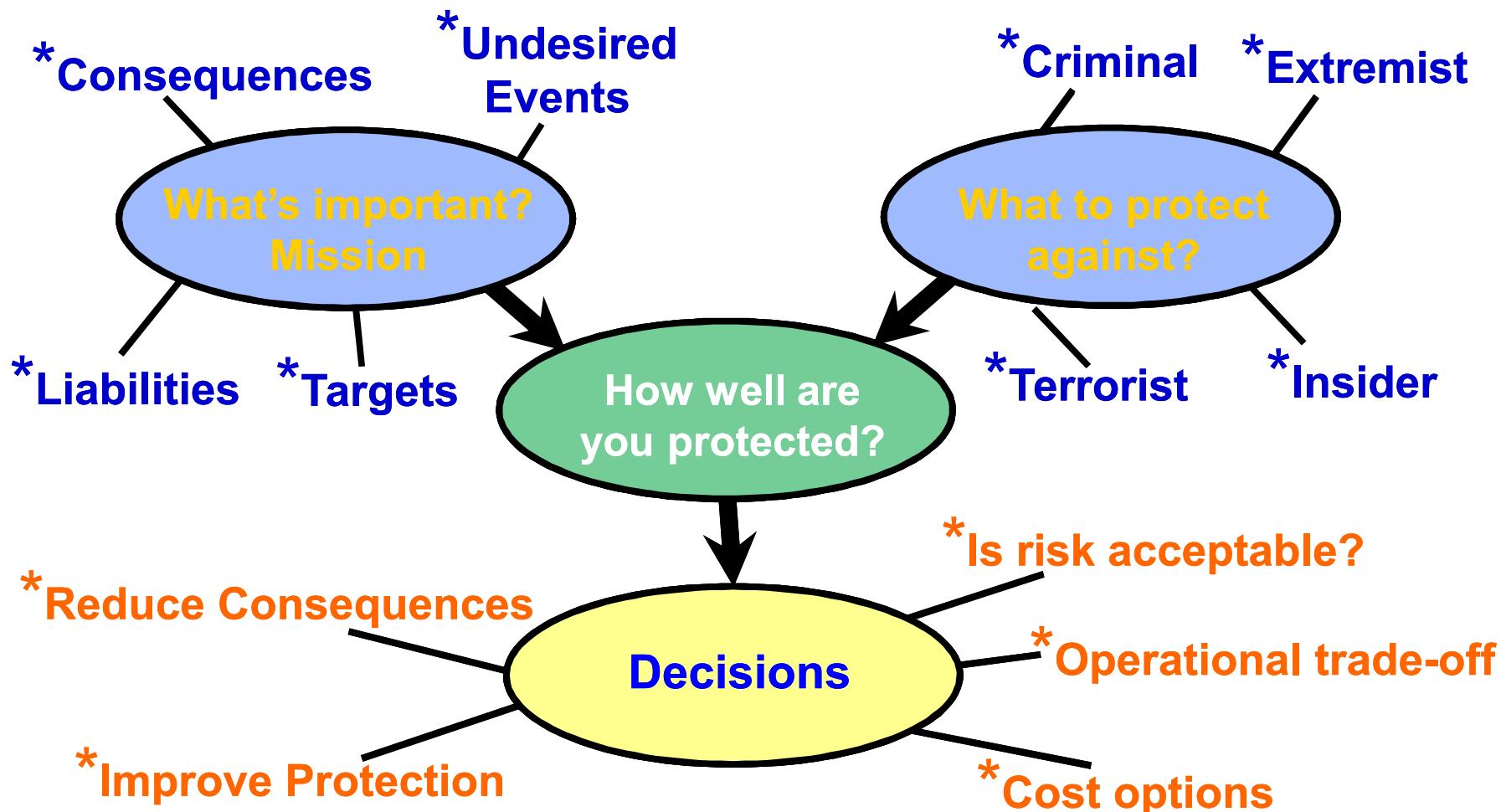
■ Part II

- Automated RAM Tool

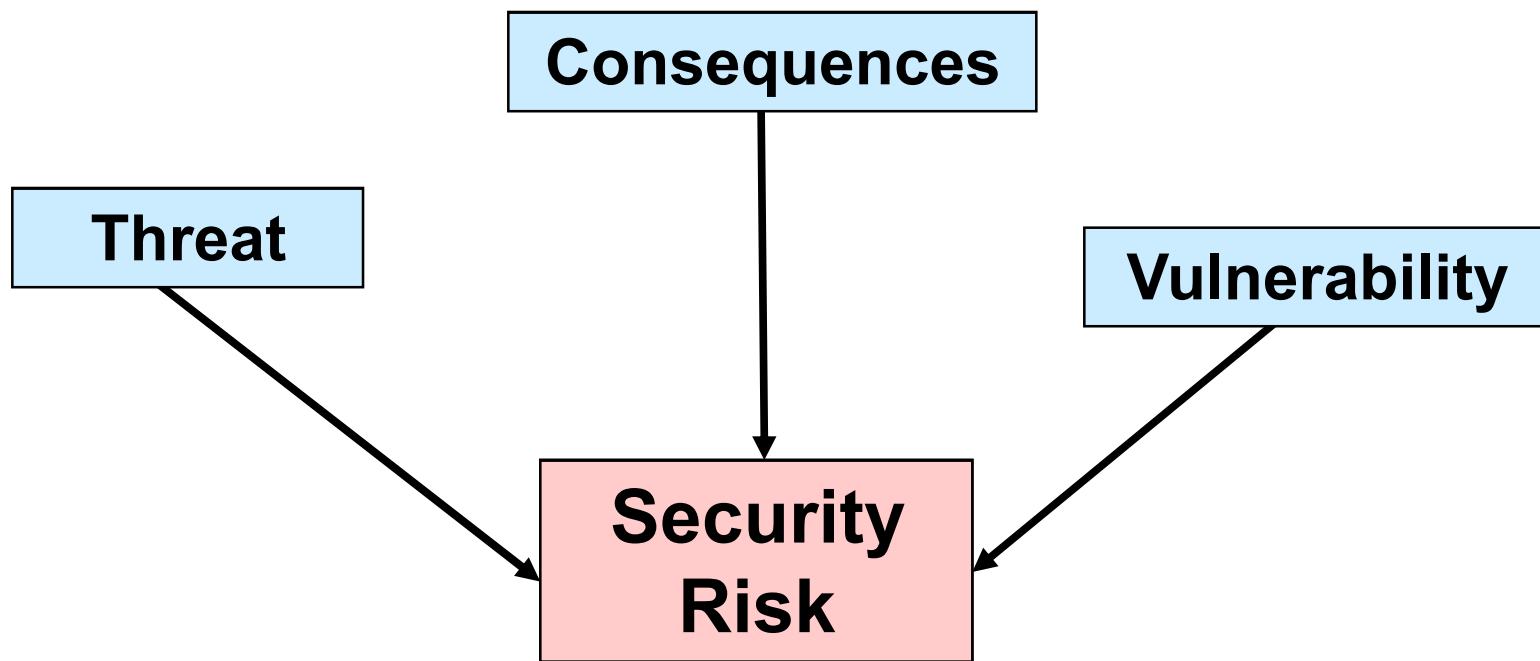


Part I: Security Risk Assessment Methodology (RAM) Overview

How Much Is Enough?



Security Risk is a Measure of:

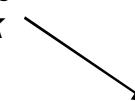


The amount of control each site / facility has over each component is different

Security Risk Equation

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

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

Probability of Attack  Probability of Adversary Success 

 System Risk  Consequences 

Security System Effectiveness 

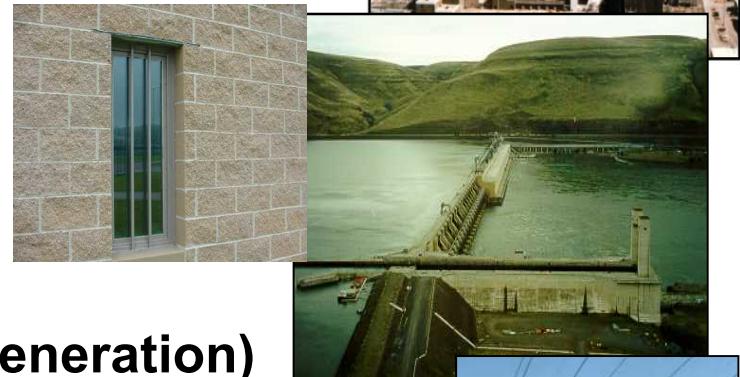
- Integrates many components into a single, consistent, approach for determining risk and making decisions

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

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)**



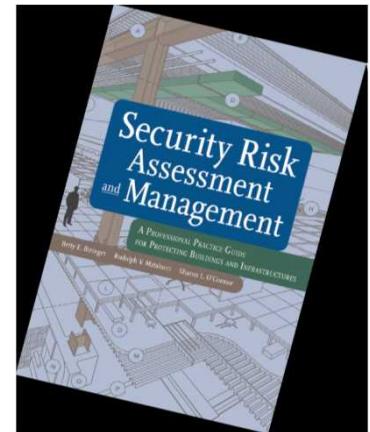
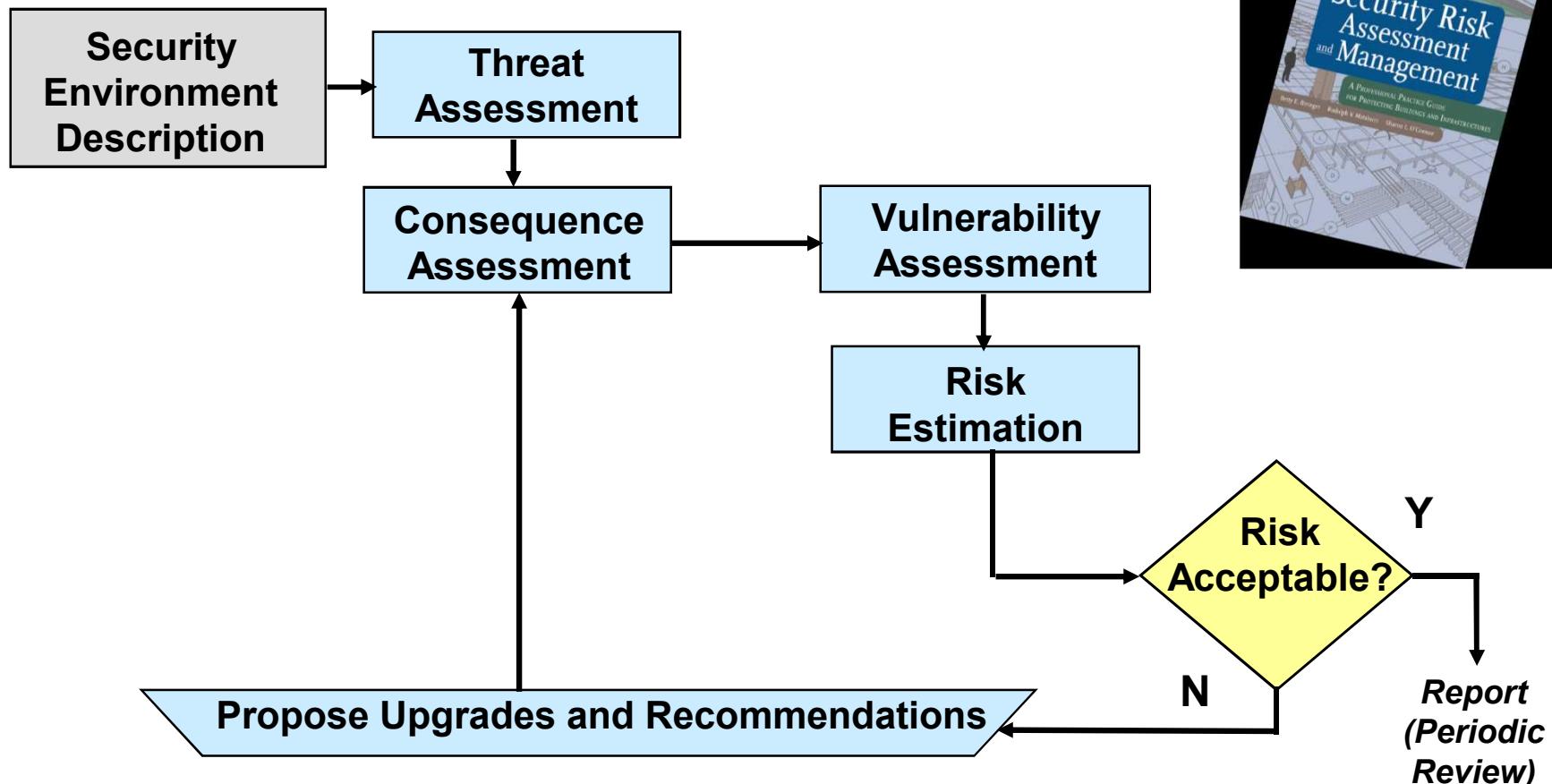
For more information see www.sandia.gov/ram

Security 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

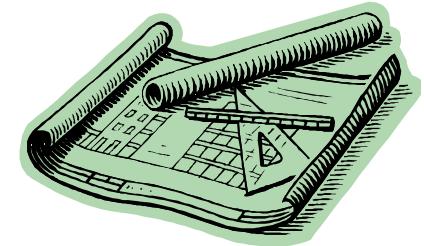
Security Risk Assessment

Methodology for Critical Infrastructures



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



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)**



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)**



Vulnerability Assessment

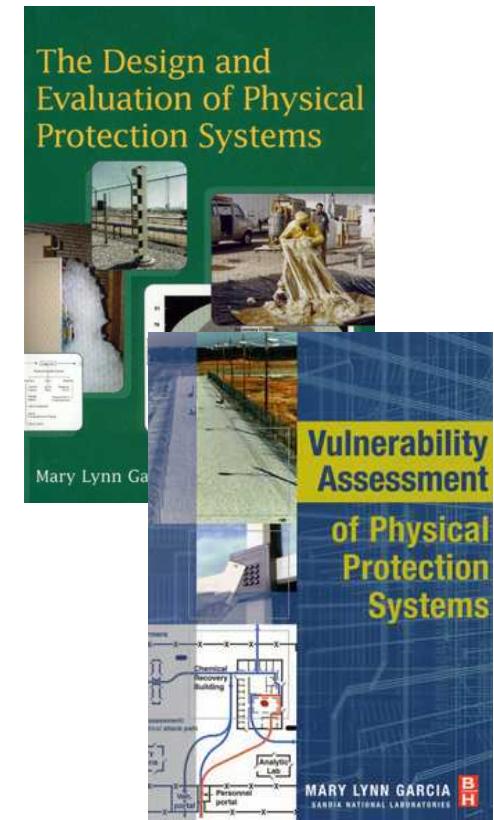
- Understand the current physical protection system (baseline analysis)
 - Detection, delay, response
 - Understand the integration of the PPS components
- Organize data and performance test
 - People, equipment / hardware (technologies), and procedures



Physical Protection System

PPS Definition:

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



www.bhusa.com/security/us

Vulnerability (System Effectiveness) Analysis

- 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

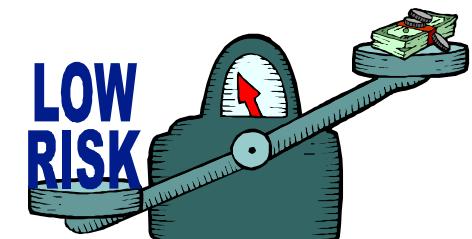


Risk Estimation

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

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



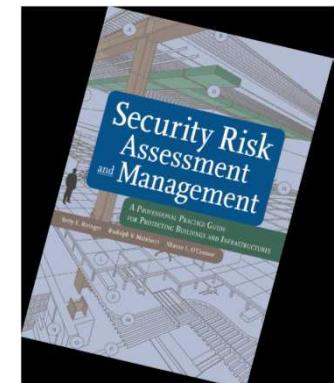
Upgrade Impact Evaluation

- Consider additional impacts other than risk reduction
 - Cost
 - Operation(s)
 - Schedule
 - Public opinion



Benefits of a Systematic Approach

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

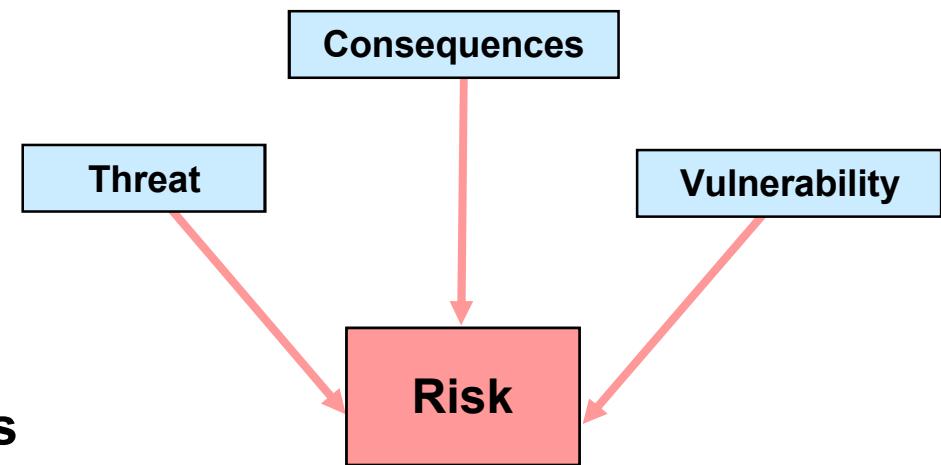


RAM Overview Summary

- 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

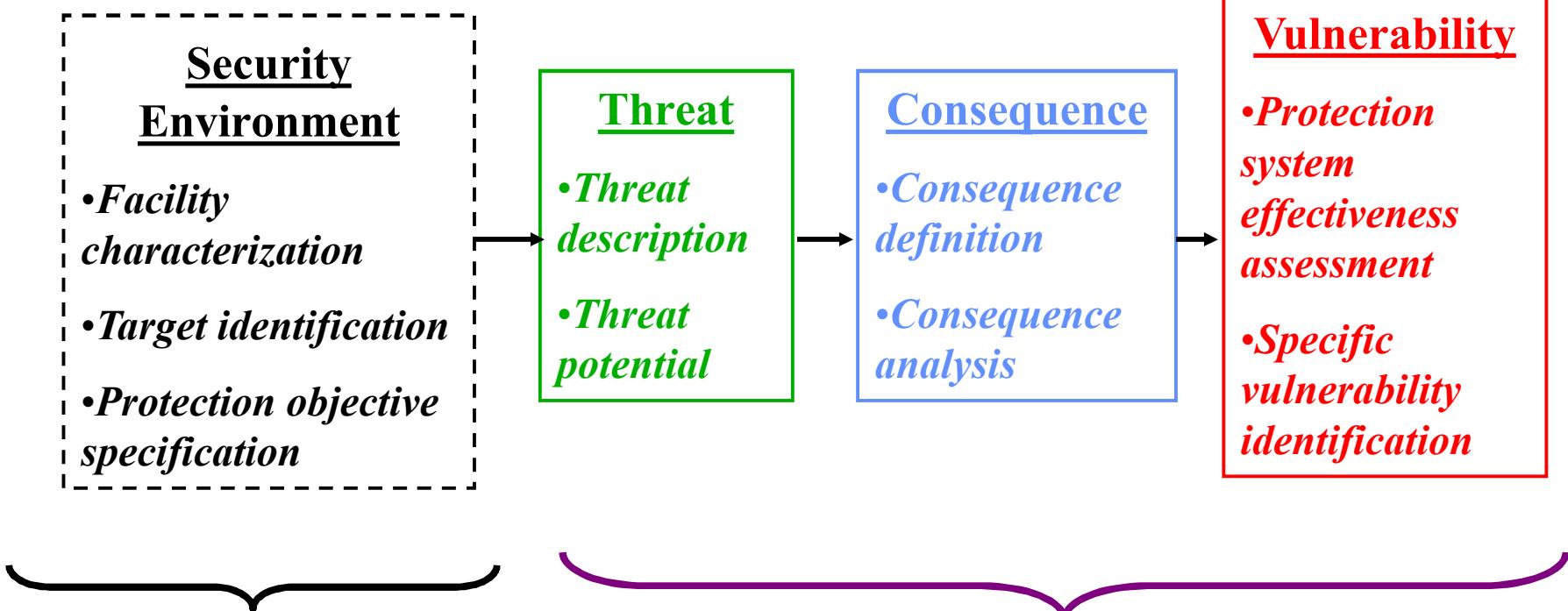
RAM Overview Summary (cont'd)

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



Part II: Automated RAM Tool Overview

Security Risk Assessment



Unique to each Site

Common to all Critical
Infrastructures

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

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?)**

Let's look at the Tool

Next Slide: The Start Window

Major Modules for the RAM



Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Introduction Files Project Take me to ...

Welcome to RAM-T

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\PreliminaryTestName.ram(Modified 2/22/2007) - RAM-T
C:\RamProjects\2ndPreliminaryTestName.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 its functions as the checklist as modules and sub-modules are completed

Back Skip Next

The diagram shows the 'Untitled - Risk Assessment Methodology' window. A blue arrow points from the title bar to the 'Start' button in the top menu bar. A red circle highlights the 'Start' button, and a red curved arrow points from the 'Start' button to the 'Start a RAM Project' button. A blue box surrounds the 'Start' button and the 'Screening' button. A red box surrounds the 'Start a RAM Project' button and the 'Continue with a Saved RAM-T Project' list. A red arrow points from the 'Start a RAM Project' button to the 'Continue with a Saved RAM-T Project' list. A red box surrounds the 'Outline of RAM and its functions as the checklist as modules and sub-modules are completed' text. A blue arrow points from the 'Outline of RAM and its functions as the checklist as modules and sub-modules are completed' text to the 'Start' button.

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**



Screening: Consequence Categories and Descriptions

User Defined or
can use Default
Categories and
Descriptions

Untitled - Risk Assessment Methodology

File Edit Tools Help

Screening Planning Site Survey Analysis Reduce Risk Final

Consequence Categories Evaluate Consequences Analysis Priority Worksheets

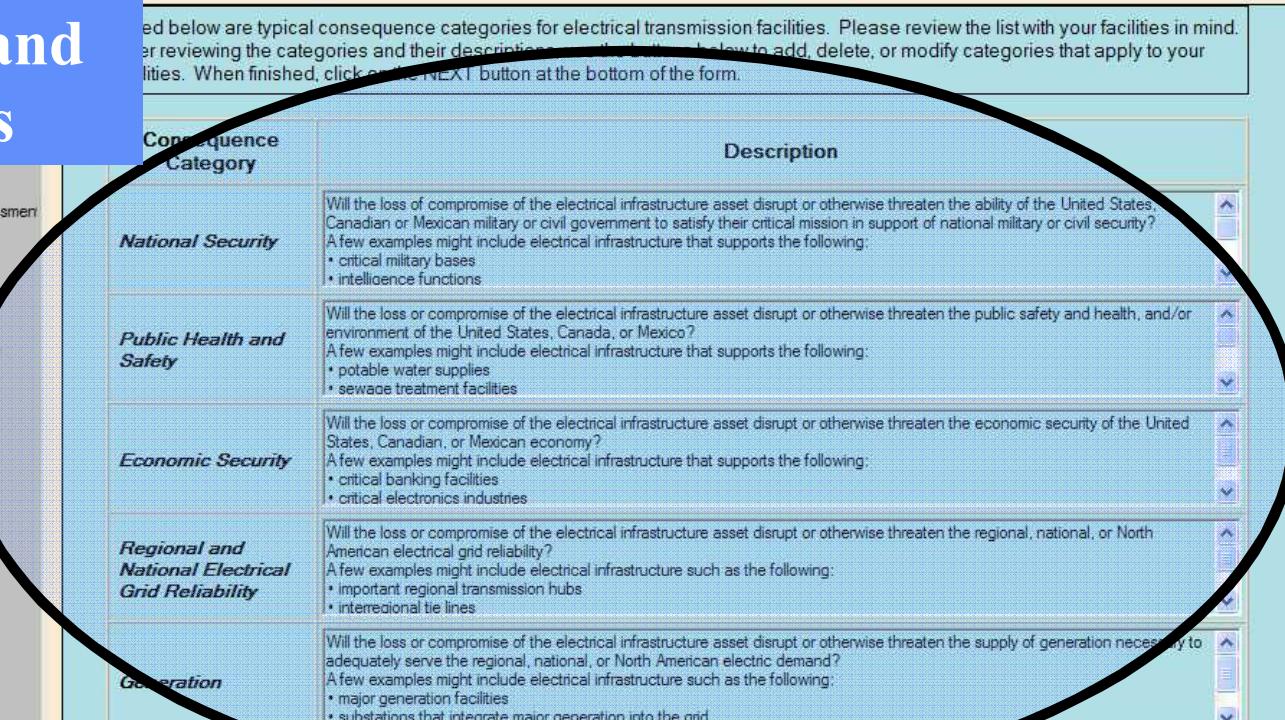
Consequence Categories

ed below are typical consequence categories for electrical transmission facilities. Please review the list with your facilities in mind. After reviewing the categories and their descriptions, click the buttons below to add, delete, or modify categories that apply to your facilities. When finished, click on the NEXT button at the bottom of the form.

Consequence Category	Description
National Security	Will the loss of compromise of the electrical infrastructure asset disrupt or otherwise threaten the ability of the United States, Canadian or Mexican military or civil government to satisfy their critical mission in support of national military or civil security? A few examples might include electrical infrastructure that supports the following: <ul style="list-style-type: none"> critical military bases intelligence functions
Public Health and Safety	Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the public safety and health, and/or environment of the United States, Canada, or Mexico? A few examples might include electrical infrastructure that supports the following: <ul style="list-style-type: none"> potable water supplies sewage treatment facilities
Economic Security	Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the economic security of the United States, Canadian, or Mexican economy? A few examples might include electrical infrastructure that supports the following: <ul style="list-style-type: none"> critical banking facilities critical electronics industries
Regional and National Electrical Grid Reliability	Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the regional, national, or North American electrical grid reliability? A few examples might include electrical infrastructure such as the following: <ul style="list-style-type: none"> important regional transmission hubs interregional tie lines
Generation	Will the loss or compromise of the electrical infrastructure asset disrupt or otherwise threaten the supply of generation necessary to adequately serve the regional, national, or North American electric demand? A few examples might include electrical infrastructure such as the following: <ul style="list-style-type: none"> major generation facilities substations that integrate major generation into the grid

Add Category Modify Category Delete Category

Back Skip Next



Choice of Number of Consequence Severity Levels

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Consequence Categories Evaluate Consequences Analysis Priority Worksheets

Evaluate Consequences

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
H (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 Severities
 Use Four Consequence Severities
 Use Five Consequence Severities
 Define Custom Consequence Severity Levels

Back Skip Next

Evaluate Consequences

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Consequence Categories Evaluate Consequences Analysis Priority Worksheets

Analysis Priority

Instructions for form use go here

Enter a name for the facility to be screened:

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

Output: Prioritization of Facilities

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Consequence Categories Evaluate Consequences Analysis Priority Worksheets

Screening Worksheets

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

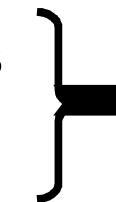
Add Worksheet Edit Worksheet Delete Item

Back Skip Next

Start Introduction Files Project Screening Consequence Categories Evaluate Consequences Analysis Priority Worksheets Planning Fault Tree Threat Assessment Consequence Assessment Site Survey Preparation Checklists Worksheets Analysis Adversary Strategies ASD Scenarios Estimate PE Vulnerabilities Summarize Risk Reduction Upgrade Package Risk for Upgrade Comparison DBT Final Impacts Final Report

Generic Fault Tree

- Generic fault tree provided for some critical infrastructures
 - User can delete events
 - User can add events
- 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



Site Specific Fault Tree

Creating a Site-Specific Fault Tree

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening **Planning** Site Survey Analysis Reduce Risk Final

Fault Tree Threat Assessment Consequence Assessment

Take me to ...

Fault Tree

Shapes RAM

Event with AND gate Drag and drop onto the drawing page.

Event with OR gate Drag and drop onto the drawing page.

Event with Undeveloped Event Drag and drop onto the drawing page.

Event with Connector Drag and drop onto the drawing page.

Dynamic connector Drag onto the page, then drag the ends to blue x's on shapes (red ind...)

Event Drag and drop onto the drawing page.

Undo Redo

Show Tabs

Show Grid

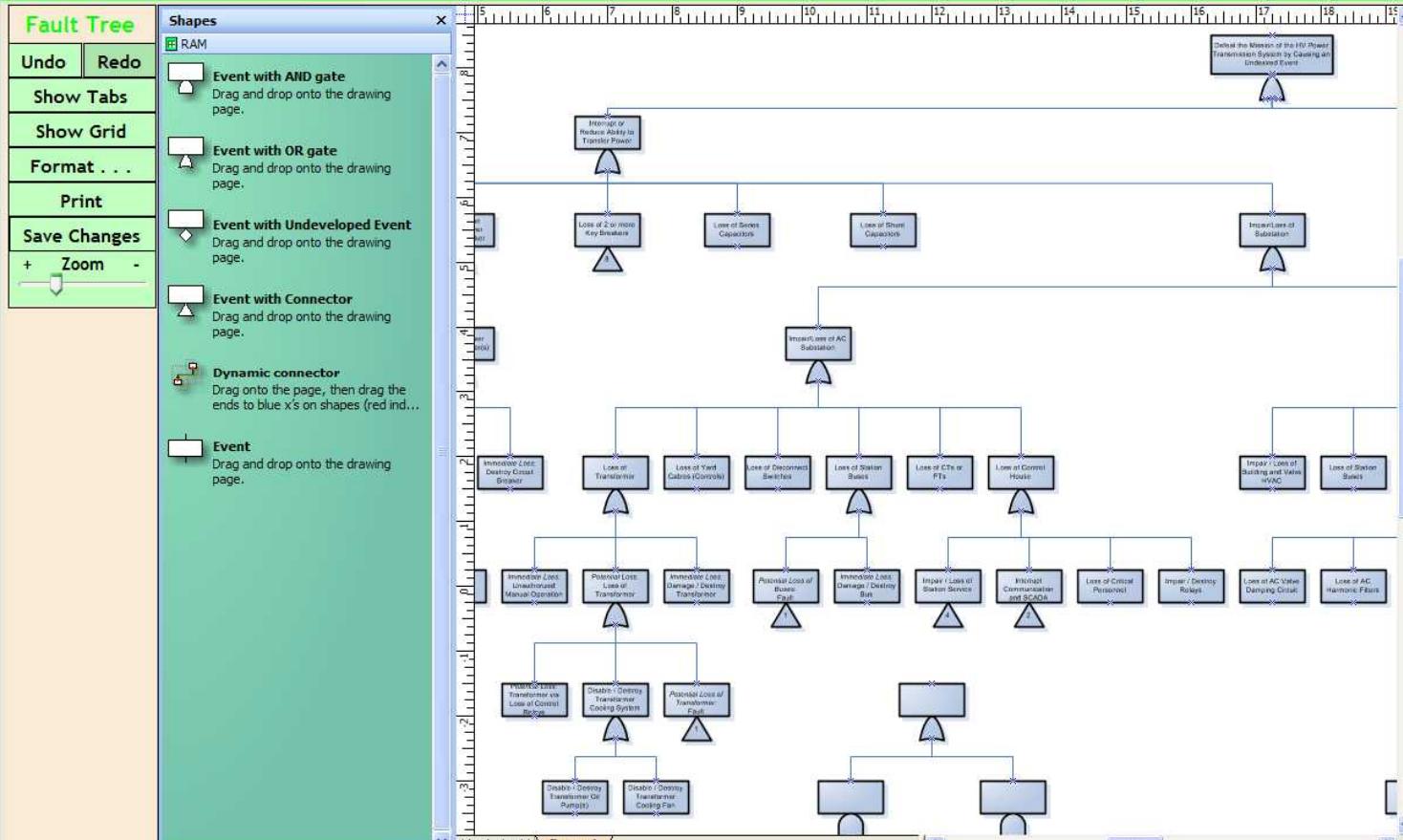
Format ...

Print

Save Changes

+ Zoom -

Diagram (Page 1)



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

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening **Planning** Site Survey Analysis Reduce Risk Final

Fault Tree Threat Assessment Consequence Assessment

[Take me to ...](#)

Threat Assessment

Threat Identification Worksheet

Facility: Test Facility AD

Which adversaries are threats to this facility?

Instructions:
If the listed adversary is a threat, check the box; otherwise leave it unchecked.
When finished, click the "Next >>" button below.

Adversary - Outsider(s)

Terrorists

- International
- Domestic: Ecological
- Domestic: Militia / Paramilitary

Extremist Group

Criminal

Gang

Vandal

Insider(s)

Other

<< Previous Next >>

Back Skip **Next >**

User Selects Site-Specific Threats

User Defines Threat Attributes and Capabilities

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Fault Tree Threat Assessment Consequence Assessment

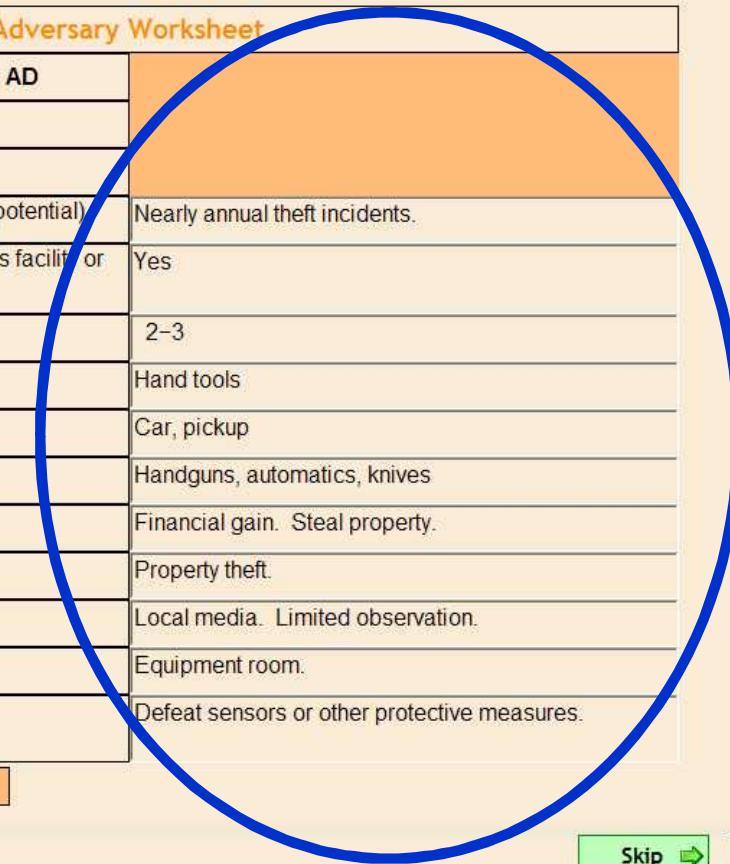
Threat Assessment

Adversary Worksheet

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.

<< Previous Next >>

Back Skip Next



Start
Introduction
Files
Project
Screening
Consequence Categories
Evaluate Consequences
Analysis Priority
Worksheets
Planning
Fault Tree
Threat Assessment
Consequence Assessment
Site Survey
Preparation
Checklists
Worksheets
Analysis
Adversary Strategies
ASD
Scenarios
Estimate PE
Vulnerabilities
Summarize
Risk Reduction
Upgrade Package
Risk for Upgrade
Comparison
DBT
Final
Impacts
Final Report

Site-specific Threat Spectrum

Threat Spectrum includes both Outsiders and Insiders

Methodology

4-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Fault Tree Threat Assessment Consequence Assessment

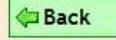
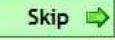
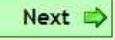
Threat Assessment

Facility Specific Threat Worksheet

Facility Identifier: Test Facility AD

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	Slide rule	Revenge	Destruction	Cafeteria
Insider - Accountant	1	Eye shade	Yaris	Sharpened pencil	Revenge	Violence	Cash drawer
Insider - Laborer	1	Shovel	Pickup	Explosives	Disgruntled	Theft	Equipment storage

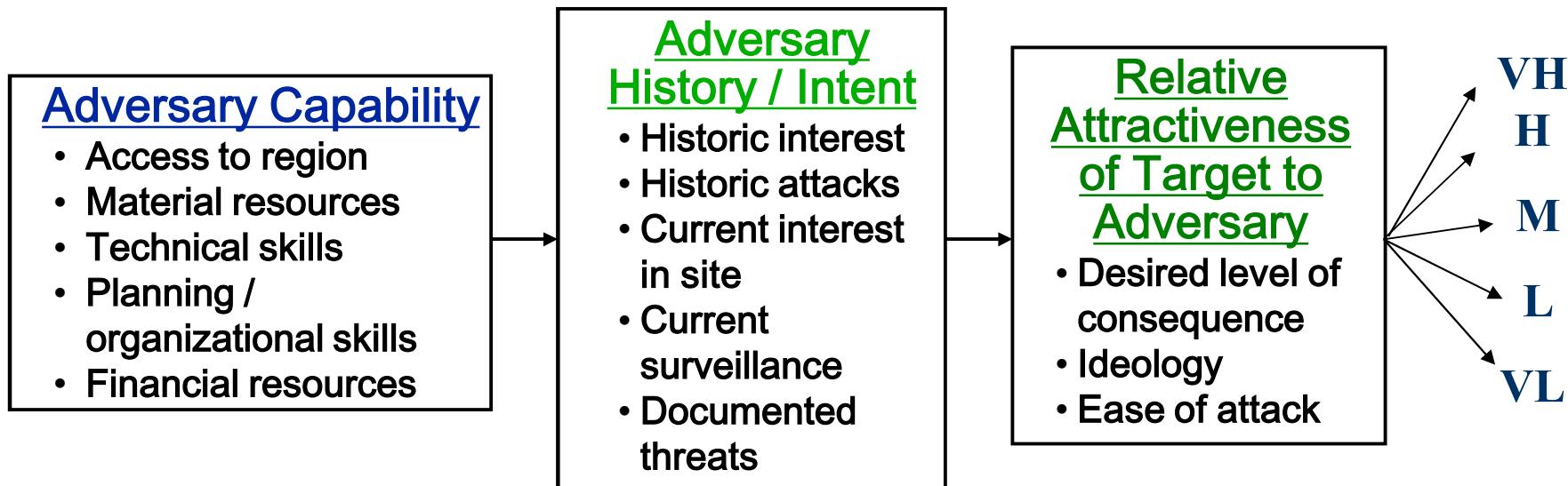
<< Previous Next >>

 Back  Skip  Next

Fault Tree
Threat Assessment
Consequence Assessment
Site Survey
Preparation
Checklists
Worksheets
Analysis
Adversary Strategies
ASD
Scenarios
Estimate PE
Vulnerabilities
Summarize
Risk Reduction
Upgrade Package
Risk for Upgrade
Comparison
DBT
Final
Impacts
Final Report

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.

Methodology

M-T

Start Screening **Planning** Site Survey Analysis Reduce Risk Final

Attack Tree Threat Assessment Consequence Assessment

Threat Assessment

Estimating Likelihood of Attack (PA) Worksheet

Facility Identifier: Test Facility AD

Adversary: Criminals

Question: Is the adversary group capable of conducting a successful attack on this facility?

Question: Is the adversary group ...

Located near or is able to gain access to the region? Yes No

Expected to have the material resources to attack this facility? Yes No

Expected to have the technical skills to attack this facility? Yes No

Interest / Intent

	Score	
Historic interest	<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

PA **VH**

<< Previous Next >>

Back Skip Next

Upgrade Package
 Risk for Upgrade
 Comparison
 DBT
 Final
 Impacts
 Final Report

Undesired Event vs. Threat Level

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

Untitled - Risk Assessment Methodology

File Edit Tools Help

Planning

Threat Assessment

Consequence Assessment

Assessment

Undesired Event vs. Likelihood of Attack (PA) Worksheet

Adversary: Test Facility AD

Adversary ->

Likelihood of Attack (PA) by Adversary (VL/L/M/H/VH)

Terrorist		Extremist		Criminal		Gang		Vandal		Insider		Other					
Internal	Military	Ecological	Extremist	Criminal	Gang	Vandal	Insider	Other	Internal	Military	Ecological	Extremist	Criminal	Gang	Vandal	Insider	Other
VL	VL	VL	M	VH	VH	M	VH	VH	VL	VL	VL	M	M	VL	VL	M	VL
VH	VH	VH	VL	VL	VL	VL	VL	VL	M	M	M	M	M	M	M	M	M
M	M	M	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL
VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL	VL
M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L

Undesired Event

1. Loss of Flood Control

2. Loss of Hydroelectric Generation

3. Loss of Water Supply

4. Loss of Commercial Navigation on River

5. Environmental / Ecological Loss

<< Previous

Next >>

Back

Skip

Next

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

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Fault Tree Threat Assessment Consequence Assessment

Consequence Assessment

Is Loss of Flood Control a relevant event? Yes No

For each of the consequence measures listed below, select (highlight) the appropriate value.

Population at Risk

<100
>100 - 1,000
>1,000 - 10,000
>10,000 - 100,000
>100,000

Deaths

0
1 - 10
>10 - 100
>100 - 1,000
>1,000

Economic Loss

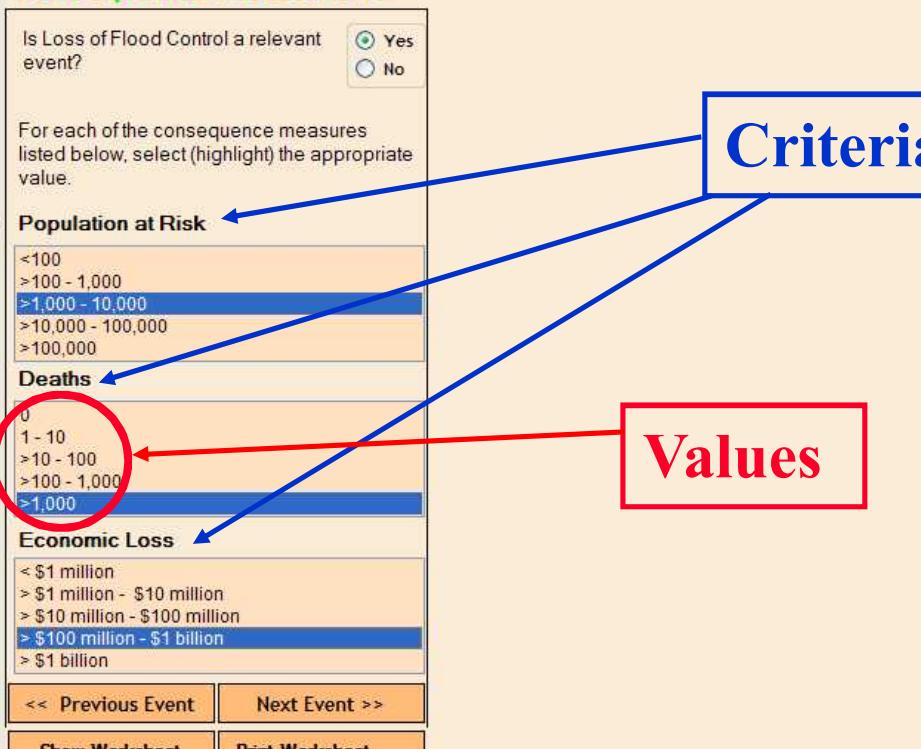
< \$1 million
> \$1 million - \$10 million
> \$10 million - \$100 million
> \$100 million - \$1 billion
> \$1 billion

<< Previous Event Next Event >> Show Worksheet Print Worksheet ...

Criteria

Values

Back Skip Next



Consequence Assessment Table

A consequence severity level will be determined for each undesired event

- Fault Tree
- Threat Assessment
- Consequence Assessment
- Site Survey
- Preparation
- Checklists
- Worksheets
- Analysis
- Adversary Strategies
- ASD
- Scenarios
- Estimate PE
- Vulnerabilities
- Summarize
- Risk Reduction
- Upgrade Package
- Risk for Upgrade
- Comparison
- DBT
- Final
- Impacts
- Final Report

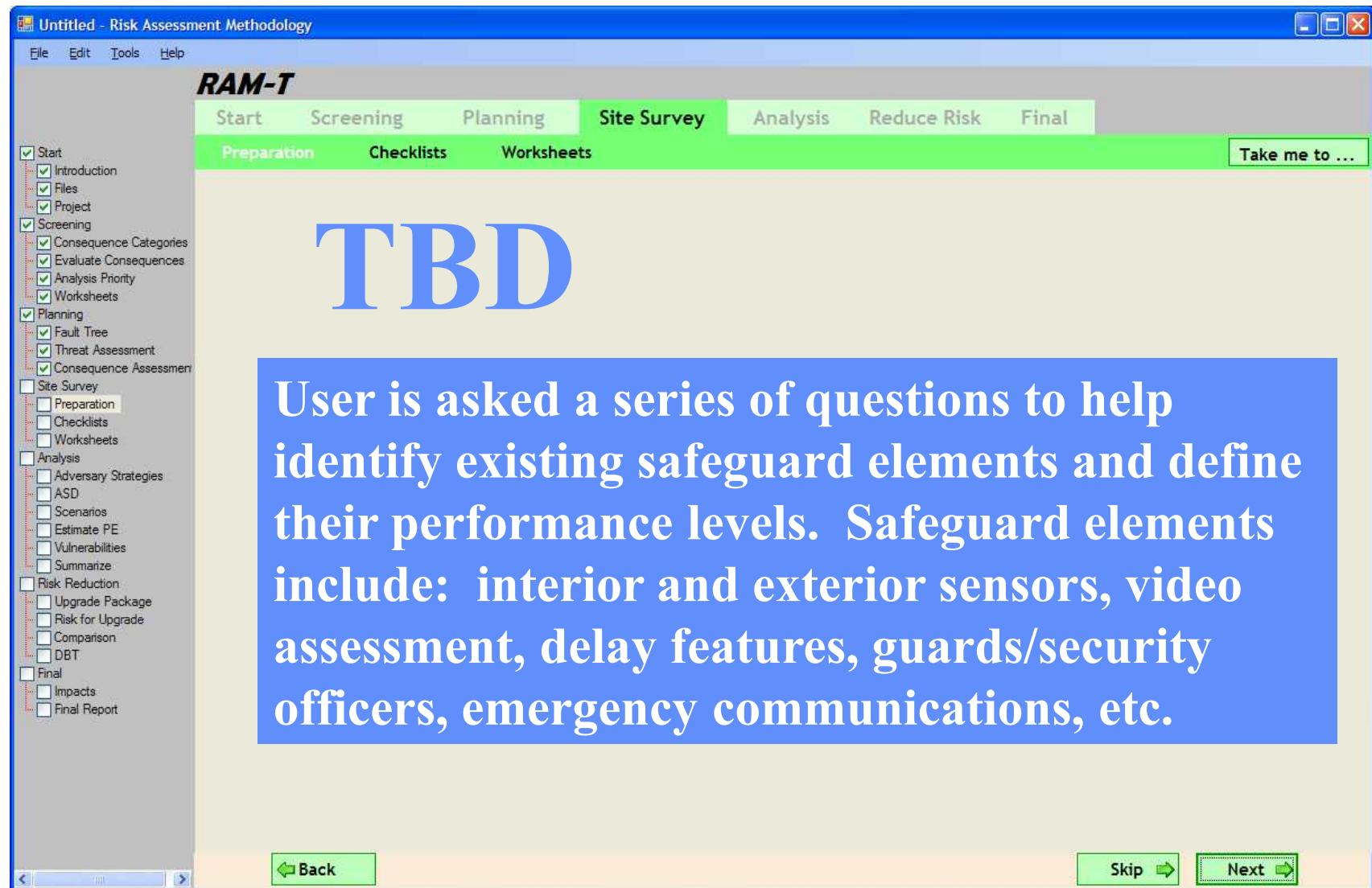
Planning						
Threat Assessment		Consequence Assessment				
Undesired Event	Relevant Event? Yes or No	Measure of Consequence		Consequence Severity		
		Type	Value	By Type	By Event	
Loss of Flood Control	Yes	Population at Risk	>1,000 - 10,000	M	Highest Consequence	VH
		Deaths	>1,000	VH		
		Economic Loss	> \$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		
		Extent of Social Impact	Neighborhood	VL		
Loss of Water Supply (Irrigation, Domestic, Industrial)	Yes	Economic Loss	> \$1 million - \$10 million	L	Highest Consequence	H
		Duration	Months	H		
		Extent of Social 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 all undesired events		VH	Number of occurrences of highest priority category		3	
Back	Next	Skip	Next			

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



RAM-T

Untitled - Risk Assessment Methodology

File Edit Tools Help

Start Screening Planning Site Survey Analysis Reduce Risk Final

Preparation Checklists Worksheets Take me to ...

Start

Introduction

Files

Project

Screening

Consequence Categories

Evaluate Consequences

Analysis Priority

Worksheets

Planning

Fault Tree

Threat Assessment

Consequence Assessment

Site Survey

Preparation

Checklists

Worksheets

Analysis

Adversary Strategies

ASD

Scenarios

Estimate PE

Vulnerabilities

Summarize

Risk Reduction

Upgrade Package

Risk for Upgrade

Comparison

DBT

Final

Impacts

Final Report

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.

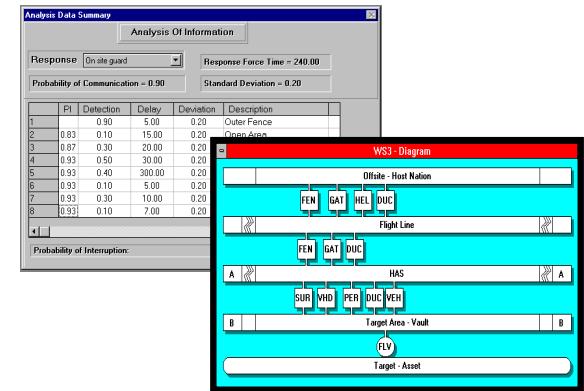
Back Skip Next

System Effectiveness Analysis

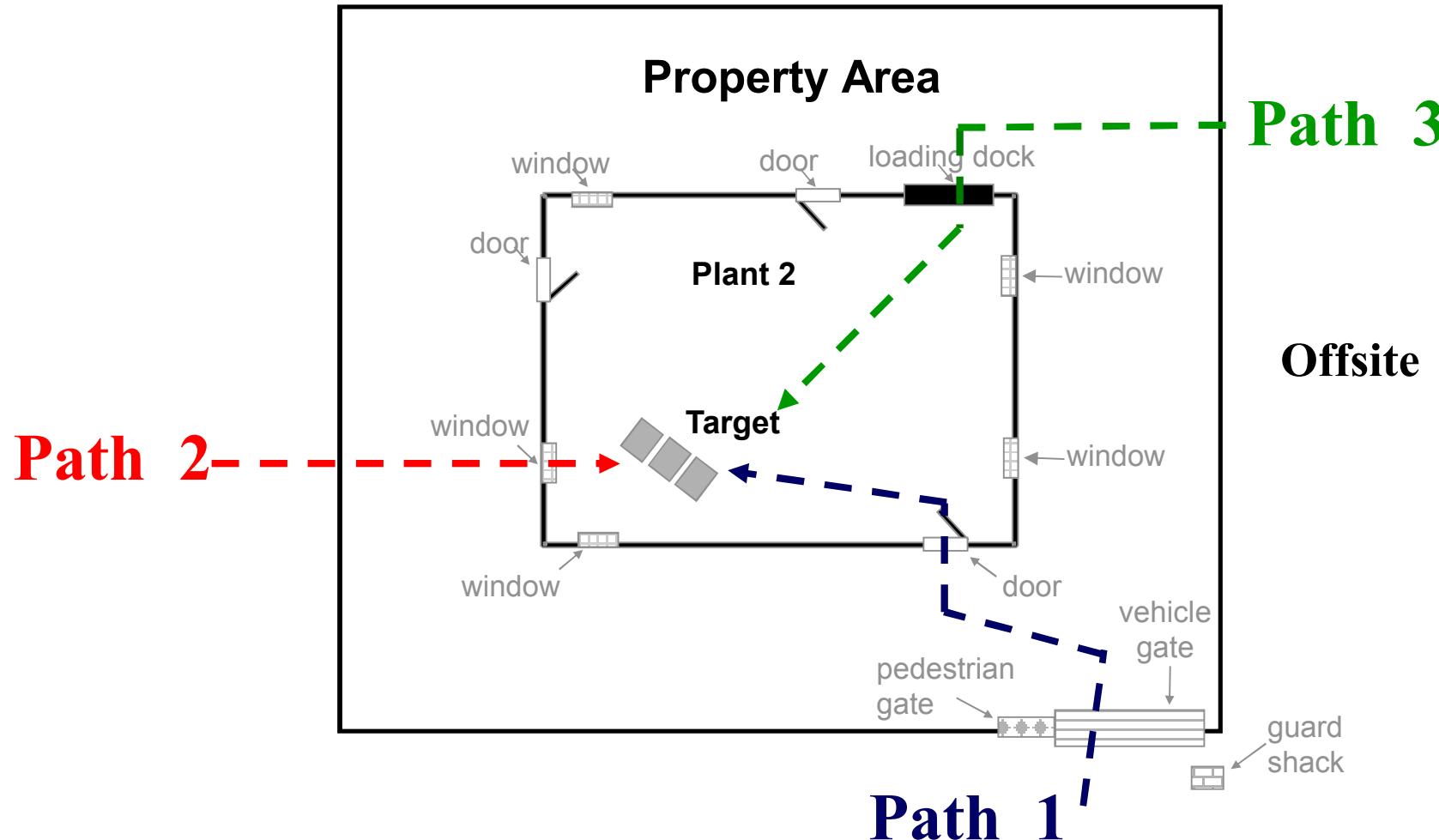
- **Adversary Sequence Diagrams**

- **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**

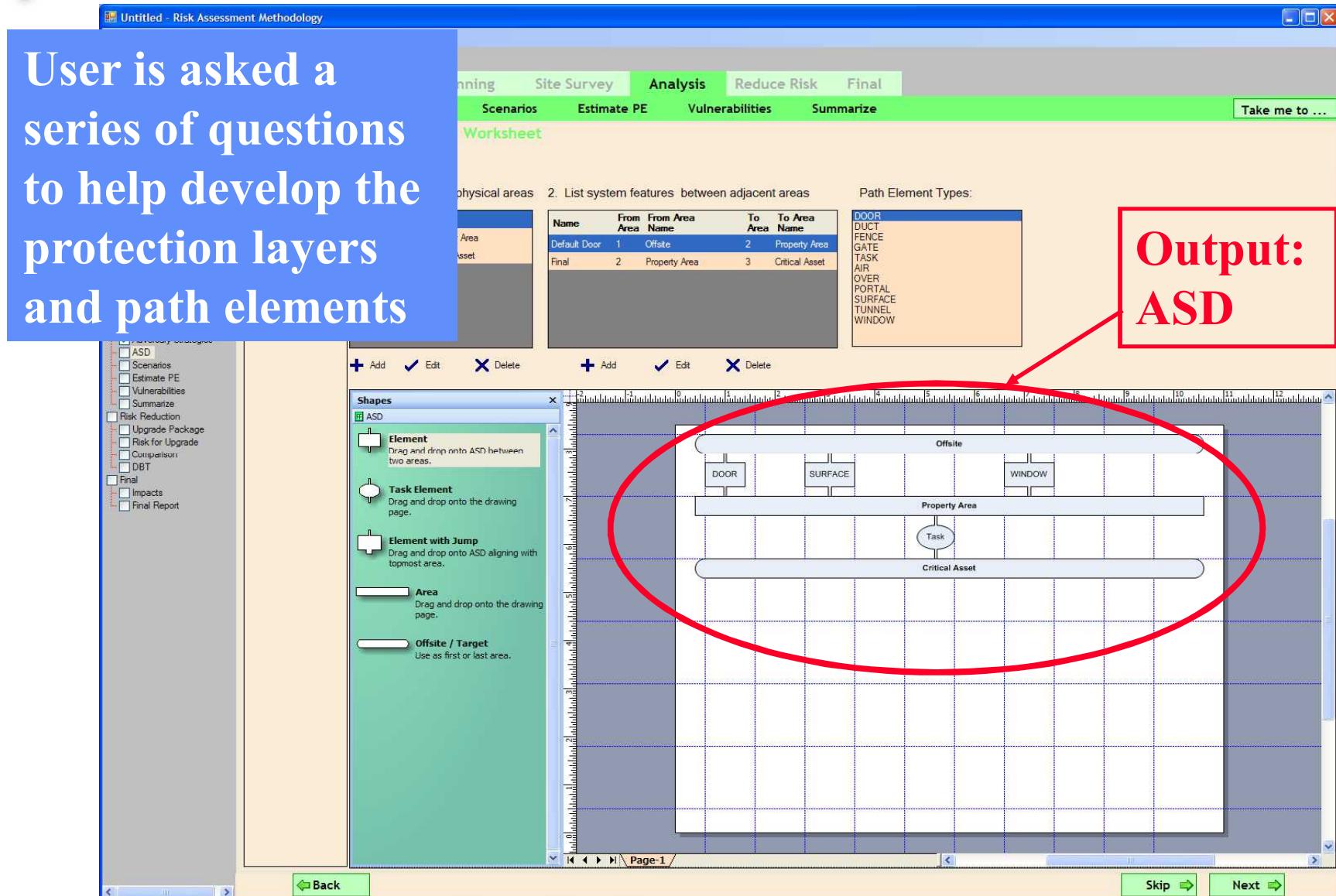


Physical Paths (Protection Layers and Path Elements)



Adversary Sequence Diagram

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



Output:
ASD

ASD

Scenarios

Estimate PE

Vulnerabilities

Summarize

Risk Reduction

Upgrade Package

Risk for Upgrade

Comparison

DBT

Final

Impacts

Final Report

Planning Site Survey Analysis Reduce Risk Final

Scenarios Estimate PE Vulnerabilities Summarize

Worksheet

Physical areas

2. List system features between adjacent areas

Name	From Area	From Area Name	To Area	To Area Name
Default Door	1	Offsite	2	Property Area
Final	2	Property Area	3	Critical Asset

Path Element Types:

- DOOR
- DUCT
- FENCE
- GATE
- TASK
- AIR
- OVER
- PORTAL
- SURFACE
- TUNNEL
- WINDOW

Shapes

- Element
- Task Element
- Element with Jump
- Area
- Offsite / Target

Element

Drag and drop onto ASD between two areas.

Task Element

Drag and drop onto the drawing page.

Element with Jump

Drag and drop onto ASD aligning with topmost area.

Area

Drag and drop onto the drawing page.

Offsite / Target

Use as first or last area.

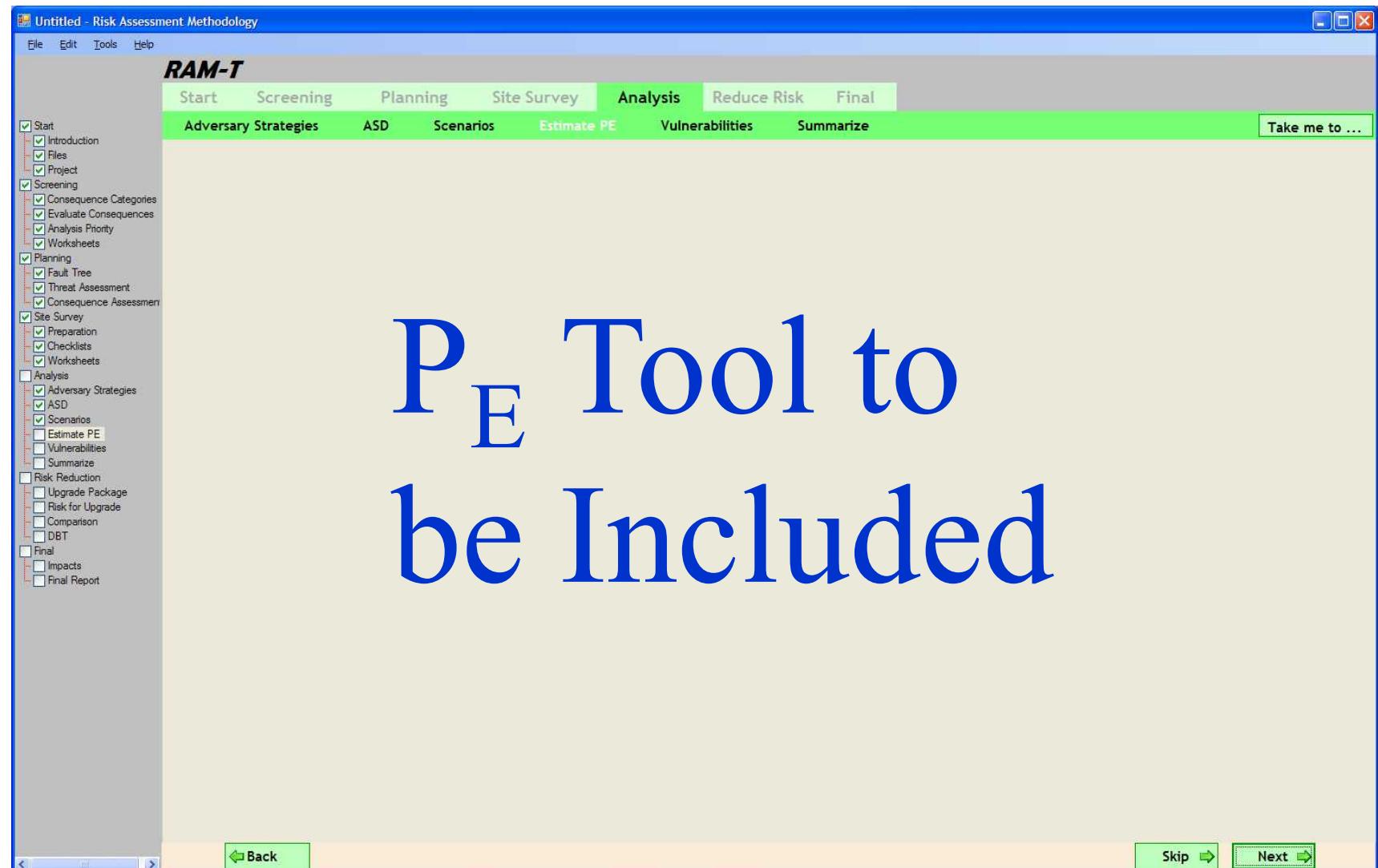
Page-1

Back

Skip

Next

Estimating System Effectiveness



PE Tool to be Included

Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey **Analysis** Reduce Risk Final

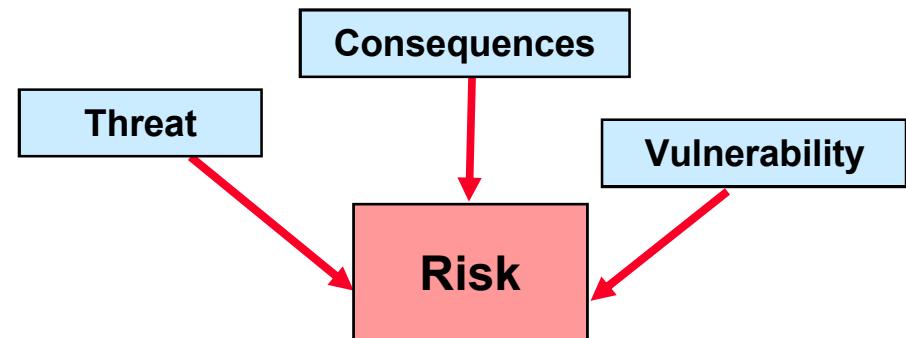
Adversary Strategies ASD Scenarios Estimate PE Vulnerabilities Summarize Take me to ...

Start
Introduction
Files
Project
Screening
Consequence Categories
Evaluate Consequences
Analysis Priority
Worksheets
Planning
Fault Tree
Threat Assessment
Consequence Assessment
Site Survey
Preparation
Checklists
Worksheets
Analysis
Adversary Strategies
ASD
Scenarios
Estimate PE
Vulnerabilities
Summarize
Risk Reduction
Upgrade Package
Risk for Upgrade
Comparison
DBT
Final
Impacts
Final Report

Back Skip Next

Risk Level Estimation

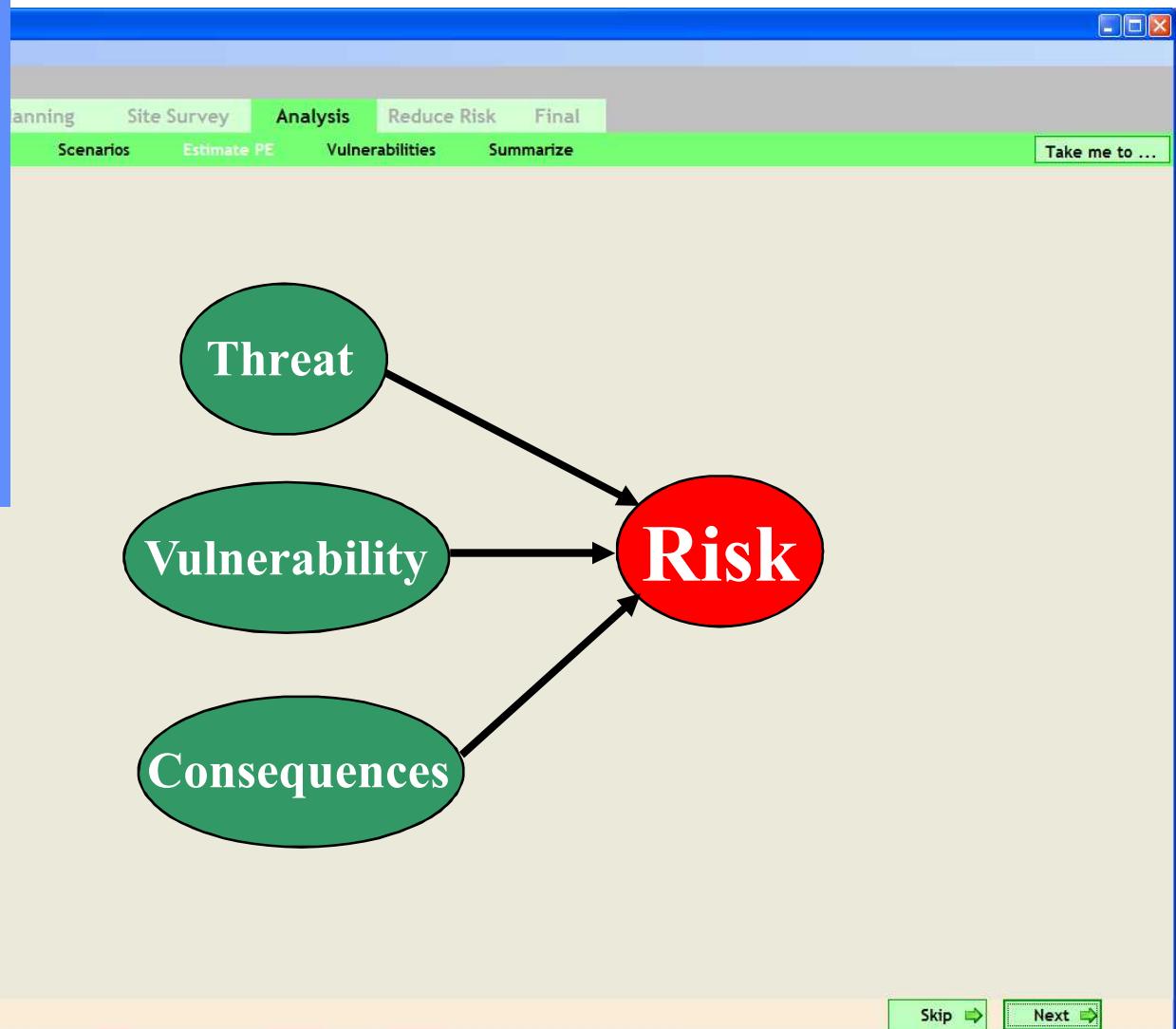
- Logically combine estimates for Threat, System Effectiveness (Vulnerability), and Consequence to estimate security risk
 - Risk is reported as a qualitative value - based on quantitative and qualitative inputs

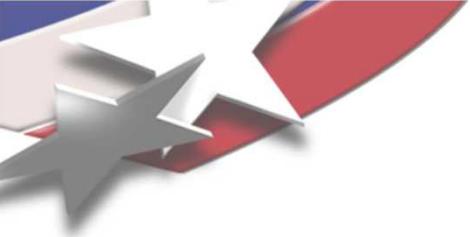


Estimating Risk

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

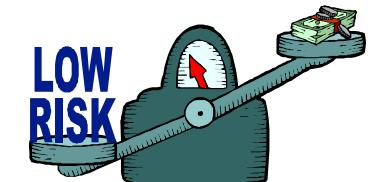
- Estimate PE
- Vulnerabilities
- Summarize
- Risk Reduction
- Upgrade Package
- Risk for Upgrade
- Comparison
- DBT
- Final
- Impacts
- Final Report





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



Untitled - Risk Assessment Methodology

File Edit Tools Help

RAM-T

Start Screening Planning Site Survey Analysis Reduce Risk Final

Upgrade Package Risk for Upgrade Comparison DBT

TBD

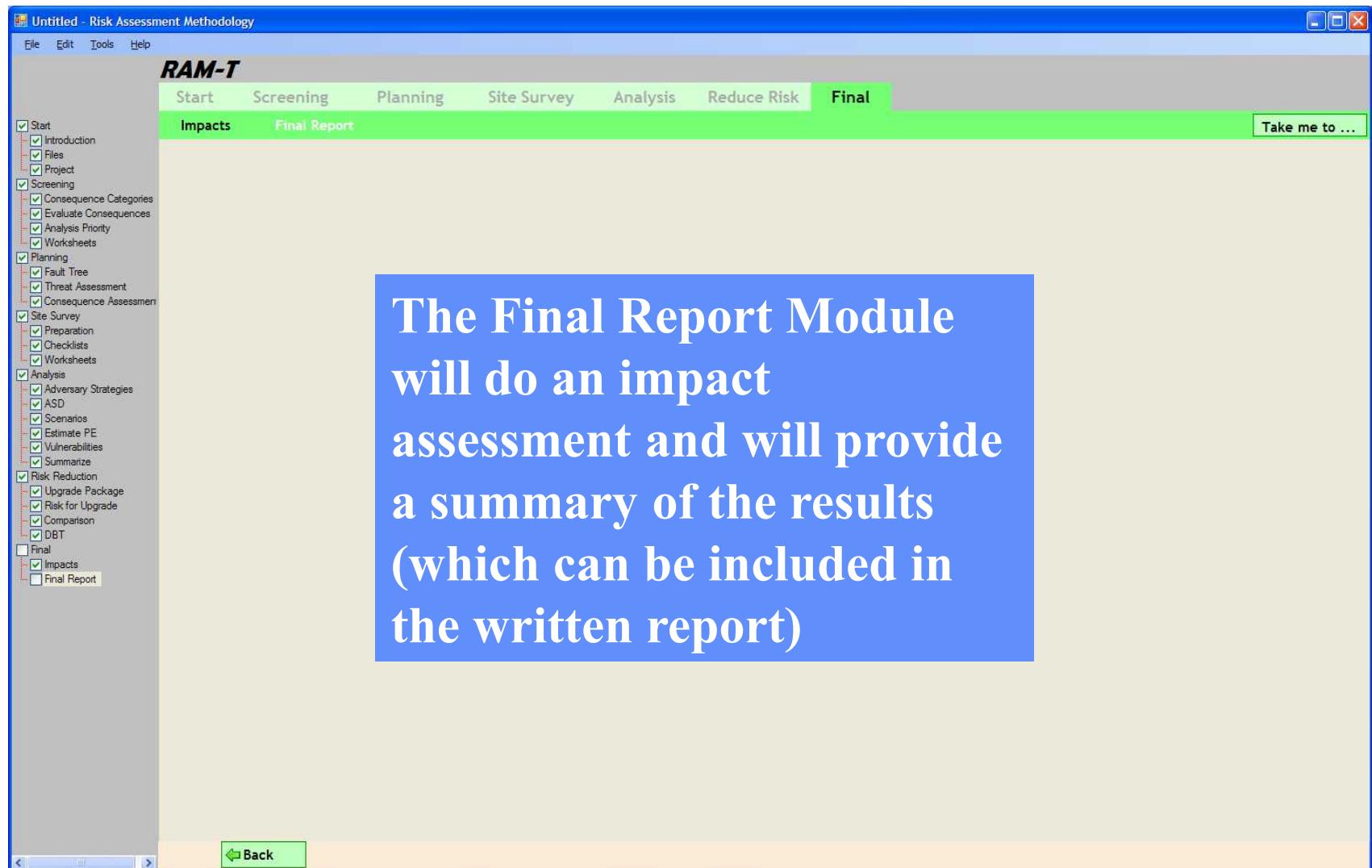
User will be able to:

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

Back Skip Next

Start Introduction Files Project Screening Consequence Categories Evaluate Consequences Analysis Priority Worksheets Planning Fault Tree Threat Assessment Consequence Assessment Site Survey Preparation Checklists Worksheets Analysis Adversary Strategies ASD Scenarios Estimate PE Vulnerabilities Summarize Risk Reduction Upgrade Package Risk for Upgrade Comparison DBT Final Impacts Final Report

Final Report



The screenshot shows the RAM-T software interface. The title bar reads "Untitled - Risk Assessment Methodology". The menu bar includes "File", "Edit", "Tools", and "Help". The main menu bar has tabs: "Start", "Screening", "Planning", "Site Survey", "Analysis", "Reduce Risk", and "Final". The "Final" tab is selected, and its sub-tabs are "Impacts" and "Final Report". A green box highlights the "Final Report" tab. On the left, a sidebar lists various risk assessment steps with checkboxes: Start (Introduction, Files, Project), Screening (Consequence Categories, Evaluate Consequences, Analysis Priority, Worksheets), Planning (Fault Tree, Threat Assessment, Consequence Assessment), Site Survey (Preparation, Checklists, Worksheets), Analysis (Adversary Strategies, ASD, Scenarios, Estimate PE, Vulnerabilities, Summarize), Risk Reduction (Upgrade Package, Risk for Upgrade, Comparison, DBT). The "Final Report" checkbox is checked. A "Take me to ..." button is in the top right. A large blue box in the center contains the text: "The Final Report Module will do an impact assessment and will provide a summary of the results (which can be included in the written report)". At the bottom, there is a "Back" button.

The Final Report Module will do an impact assessment and will provide a summary of the results (which can be included in the written report)

Software Development – What's been Completed?

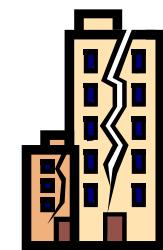
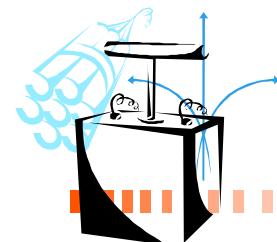
- Screening Analysis ✓
- Fault Tree ✓
- Threat Assessment ✓
- Consequence Assessment ✓
- System Effectiveness
 - Adversary Sequence Diagram ✓
 - P_E tool
- Risk Estimation
- Risk Reduction
- Final Report



*Need to
Beta Test on
a Real Site*

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

- **Part I**

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

- **Part II**

- **Automated RAM Tool**

Ques'ons??



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