SAND2008-0796P

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

Sandia National Laboratories

February 2008

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.

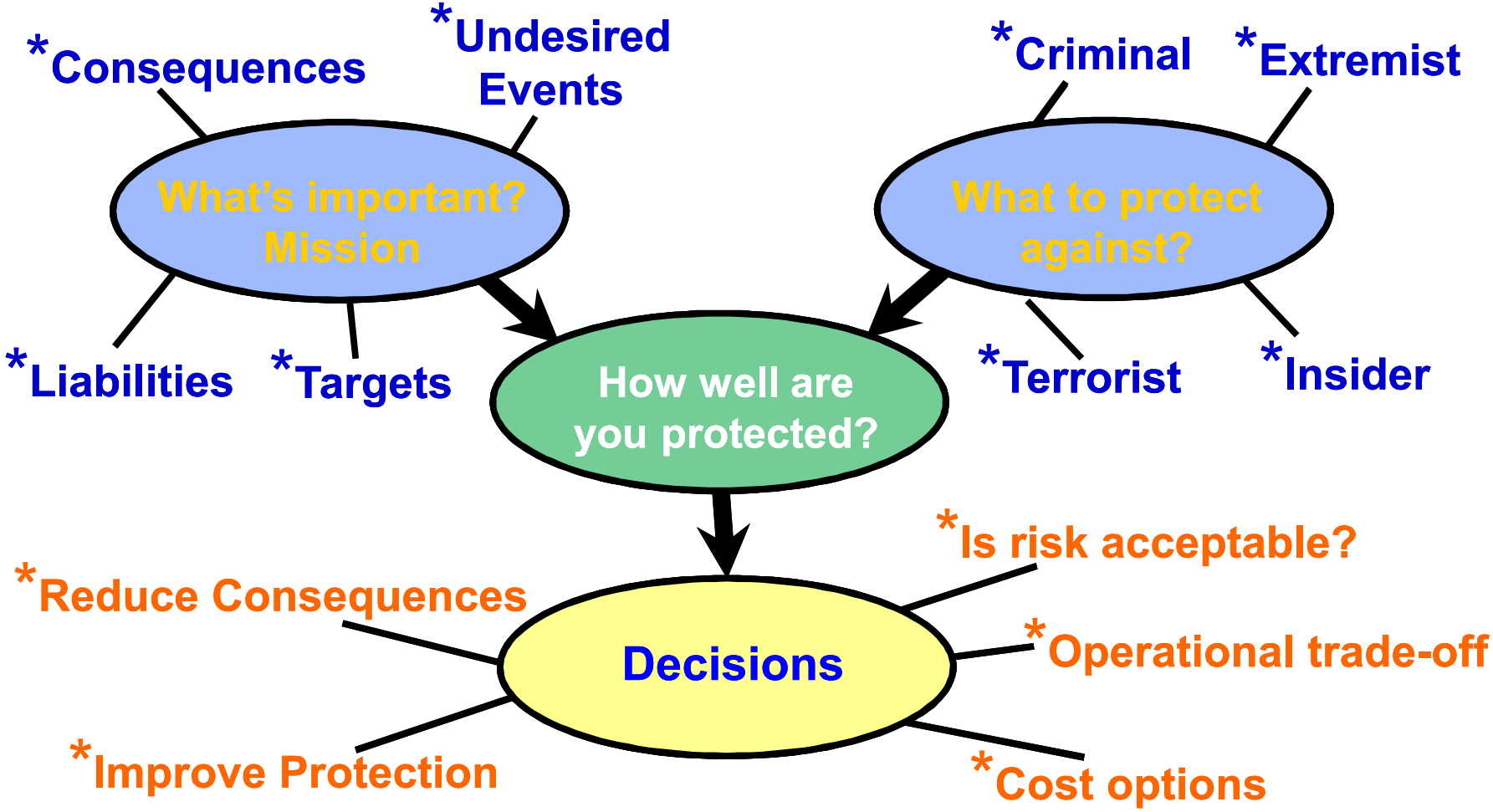
Presentation Outline

- 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

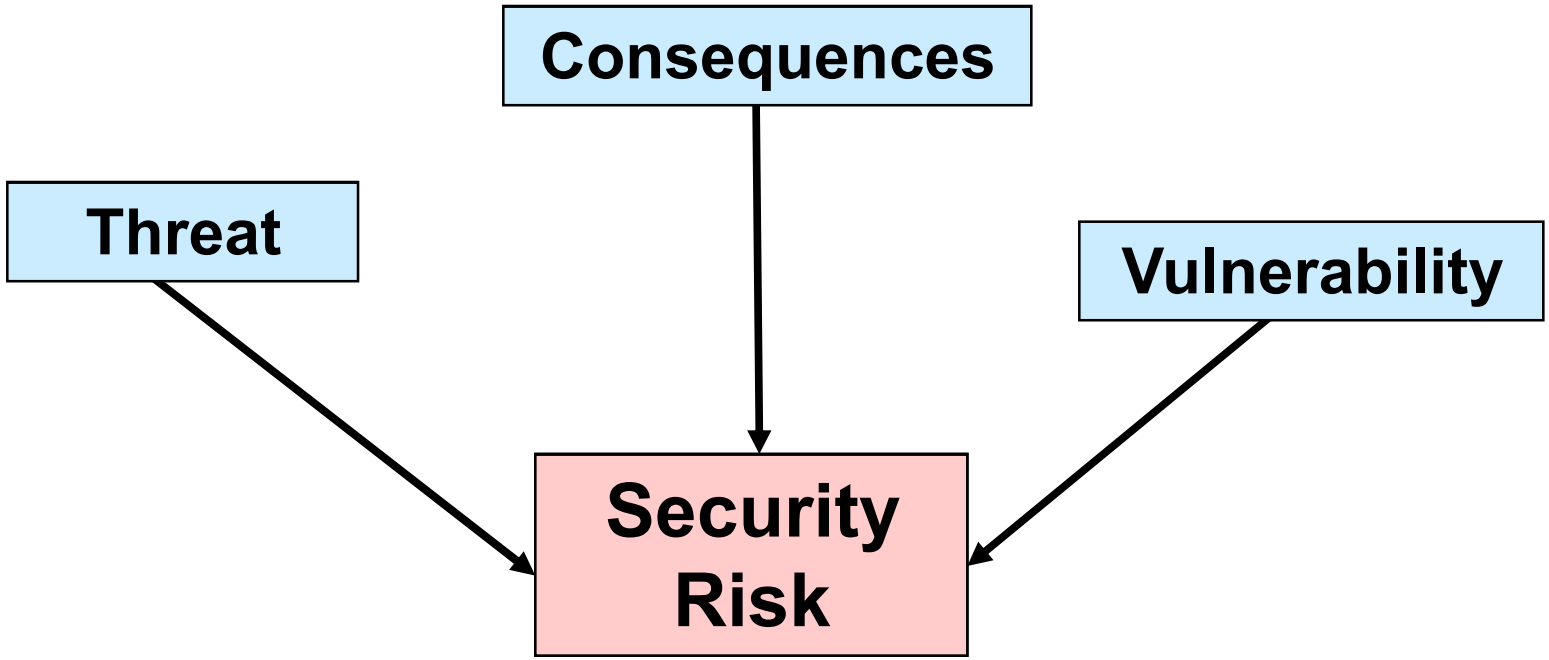
Sandia National Laboratories

Part I: Security Risk Assessment Methodology (RAM) Overview

How Much Is Enough?



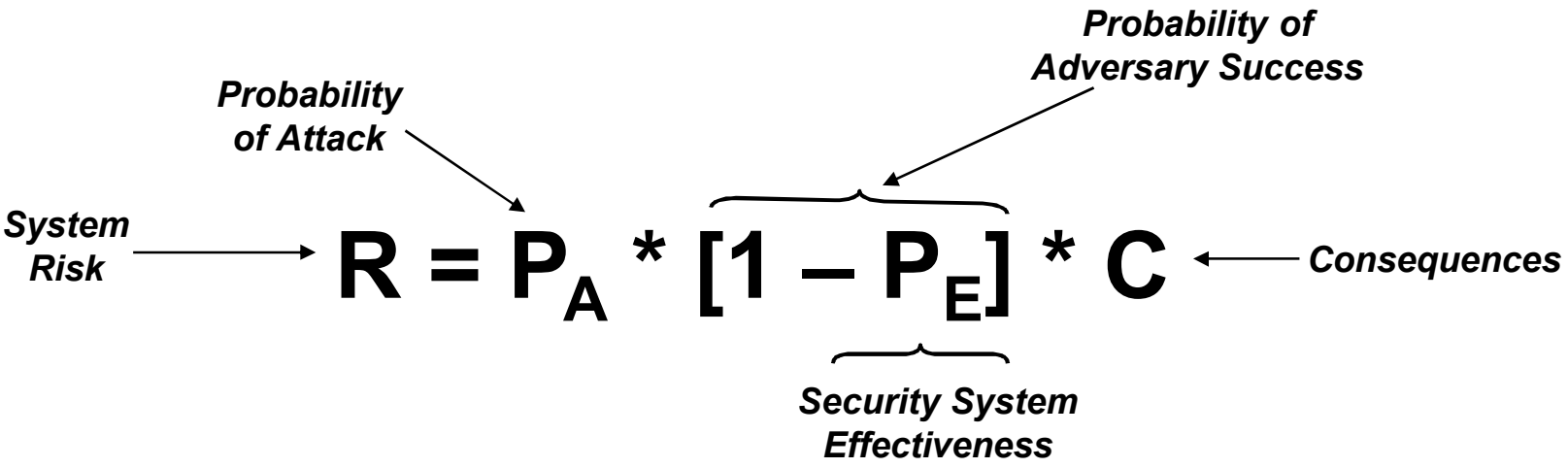
Security Risk is a Measure of:



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:



- 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

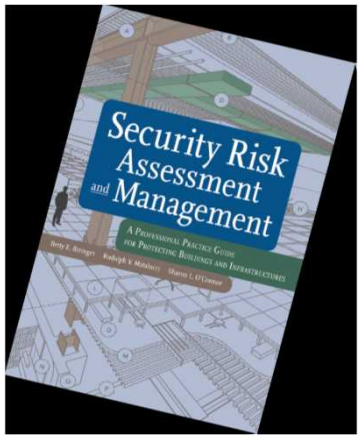
- RAM-D (Dams)
- RAM-T (Electrical Utility Transmission Systems)
- RAM-W (Municipal Water Systems)
- RAM-C (Communities)
- RAM-CF (Chemical Facilities)
- RAM-P (Prisons)
- RAM-E (Pipelines, Electric Power Generation)
- RAM-FAA (Airspace management facilities)
- RC RAM-W (RAMCAP/NIPP compliant version)

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

Threat Assessment

Consequence Assessment

Vulnerability Assessment

Risk Estimation

Risk Acceptable?

Y

N

Report (Periodic Review)

Propose Upgrades and Recommendations

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

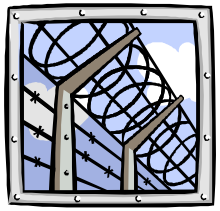
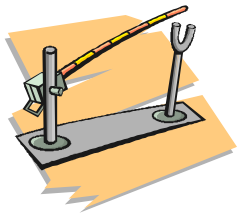
- **Analyze threat**
  - **Develop site-specific threat spectrum**
    - **Range of threats (VL - VH)**
    - **Insiders and outsiders**
      - **Motivations**
      - **Attributes**
      - **Capabilities**
  - **Estimate threat potential (P_A)**

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

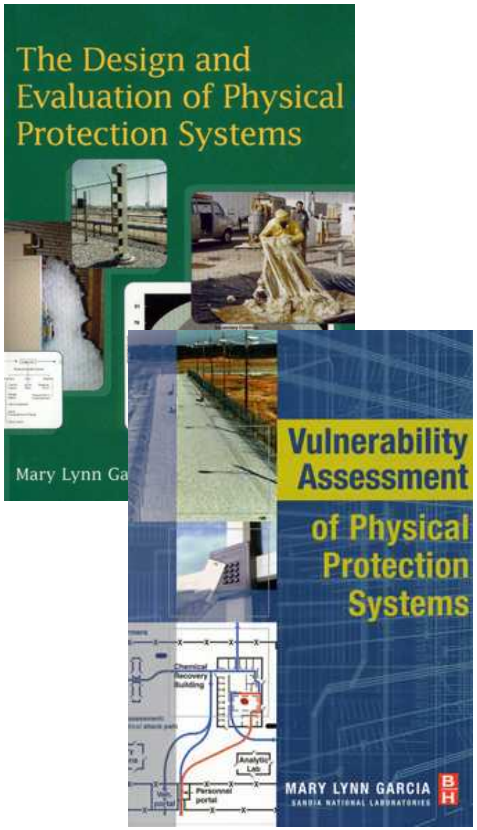
- Understand the current physical protection system (baseline analysis)
  - Detection, delay, response
  - Understand the integration of the PPS components
- Organize data and performance test
  - People, equipment / hardware (technologies), and procedures


Physical Protection System

PPS Definition:

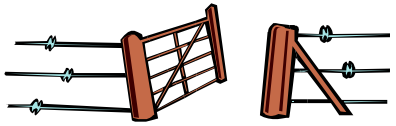
Integration of people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks



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

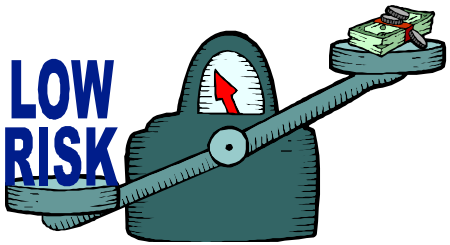


Risk Estimation

- 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

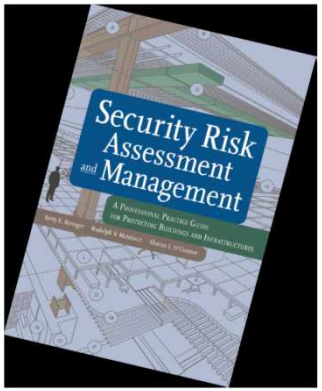


Upgrade Impact Evaluation

- 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

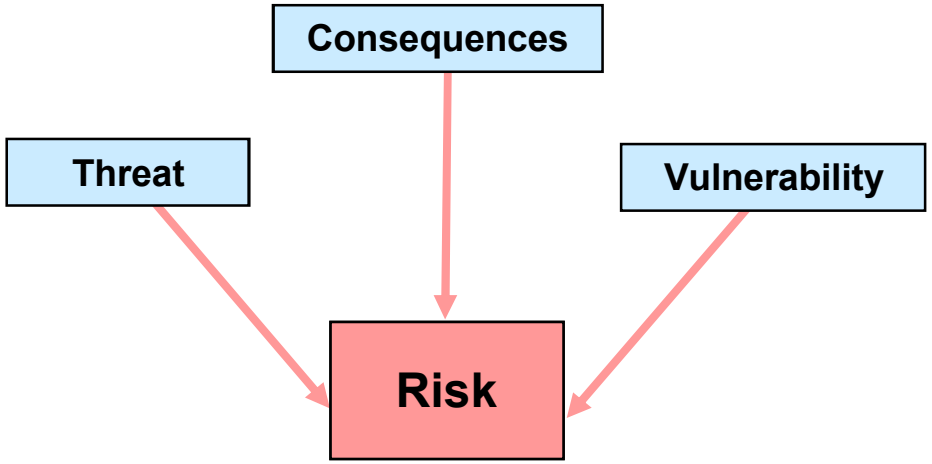


RAM Overview Summary

- 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)*

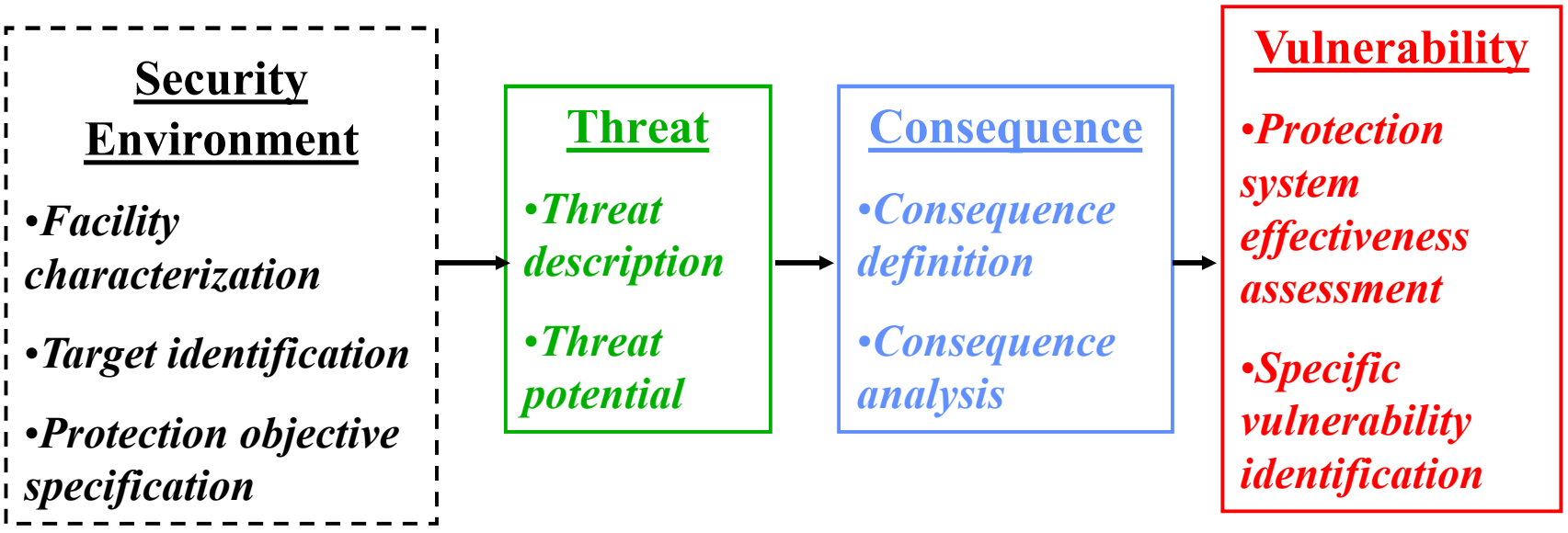
- **Security Risk is a function of**
  - **Threat**
    - **Likelihood of attack**
  - **Vulnerability**
    - **System effectiveness**
  - **Consequences of adversary success**
- **Critical infrastructure owners and / or senior management are responsible for final decisions**



Sandia National Laboratories

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?

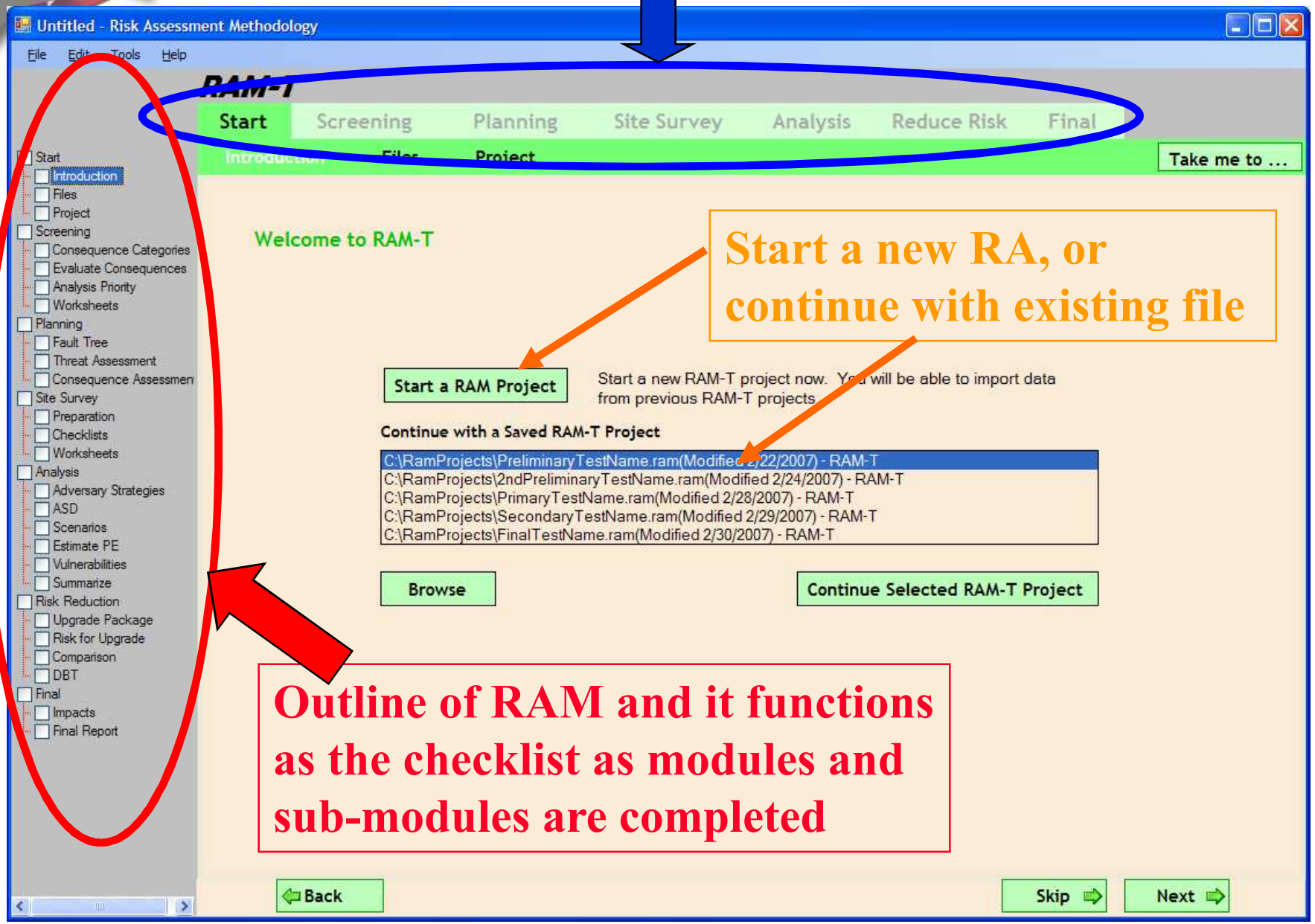
- Protection objectives
- Project definition
  - Scope of project, team, schedule
- Site survey data collection
  - Drawings, reports, policies, procedures, etc.
  - Site interviews
- Performance testing data
- Cyber security (TBD later?)

Sandia National Laboratories

Let's look at the Tool

Next Slide: The Start Window

Major Modules for the RAM



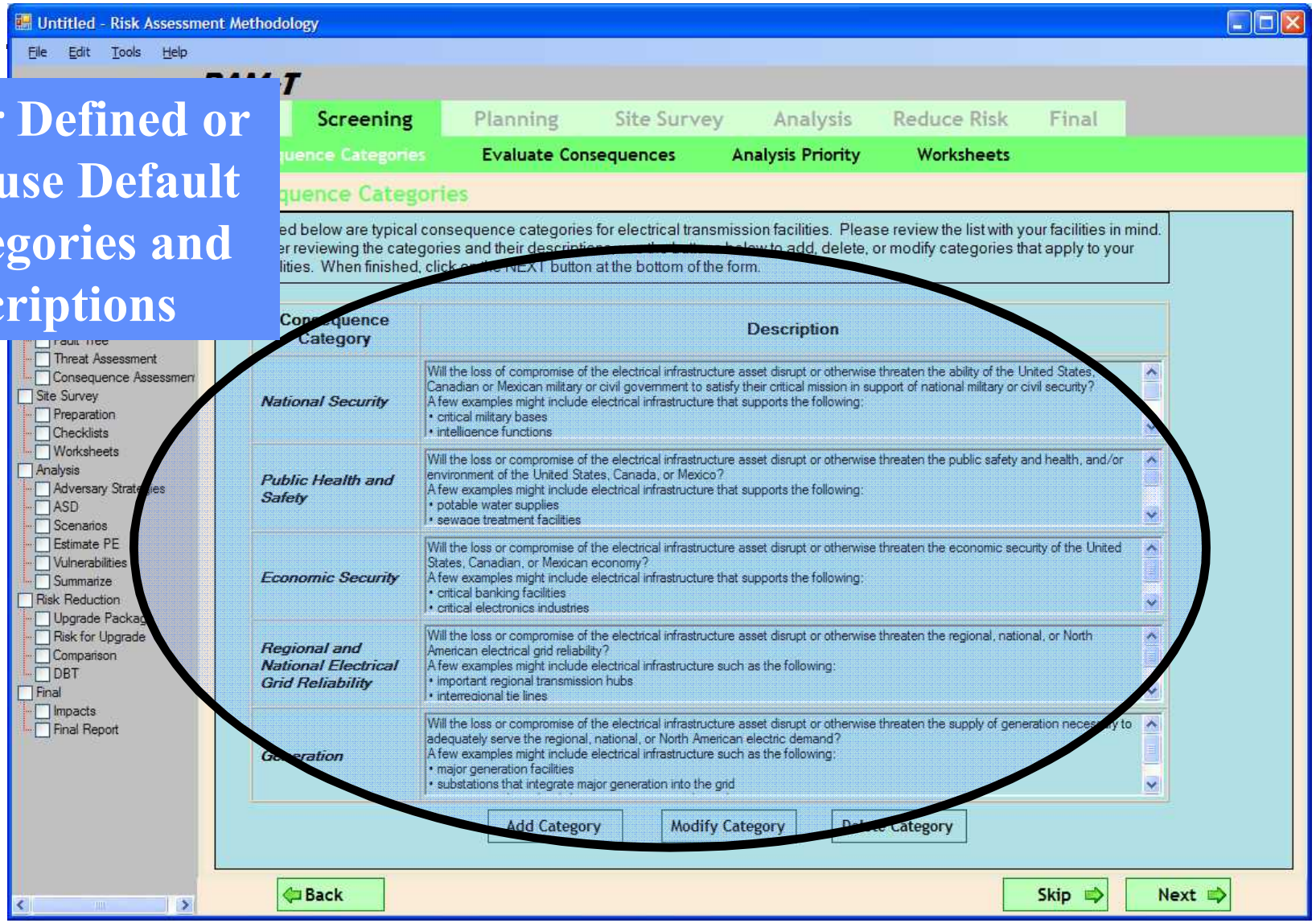
Screening Analysis

- **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**

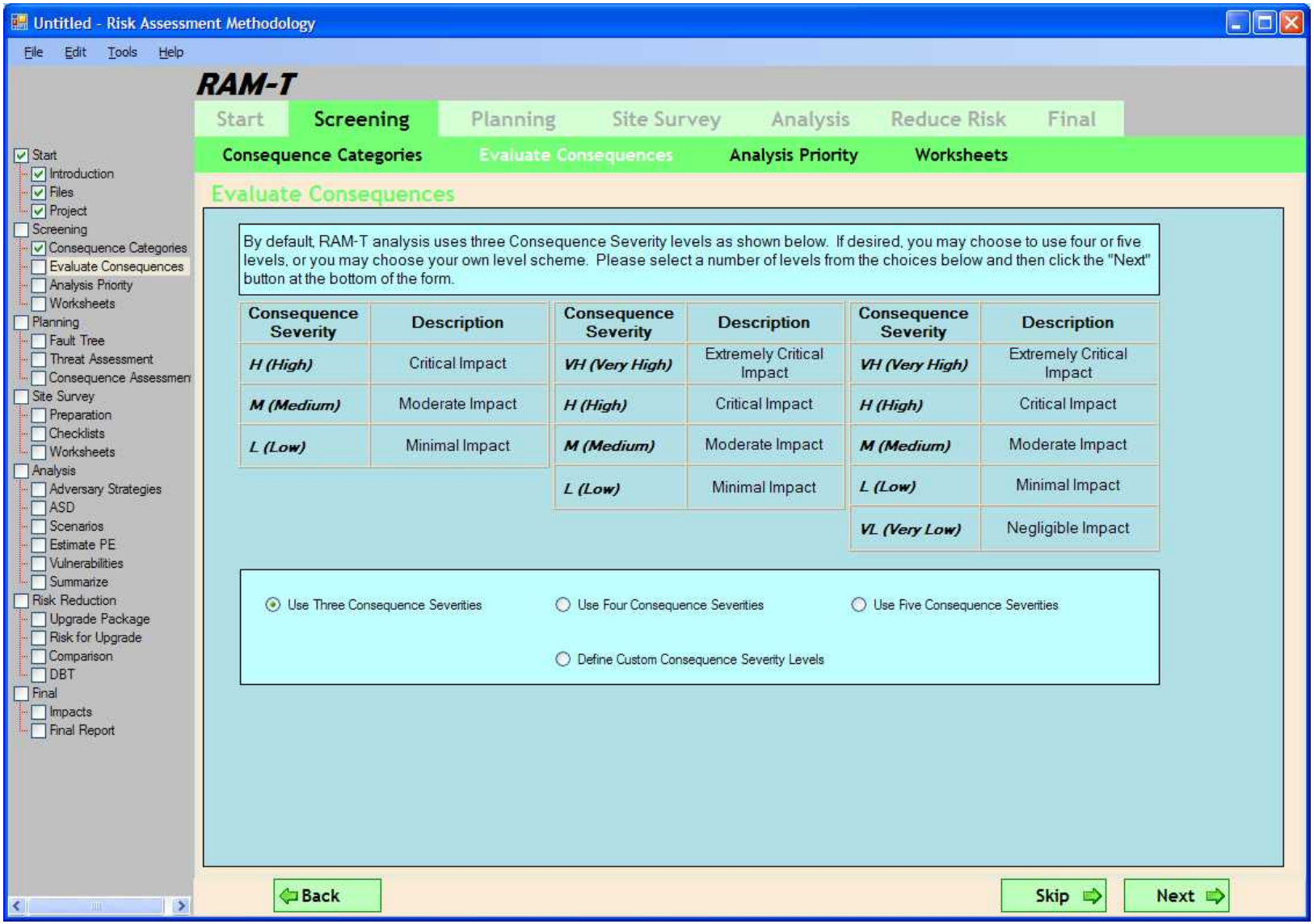
Screening: Consequence Categories and Descriptions

Sandia National Laboratories

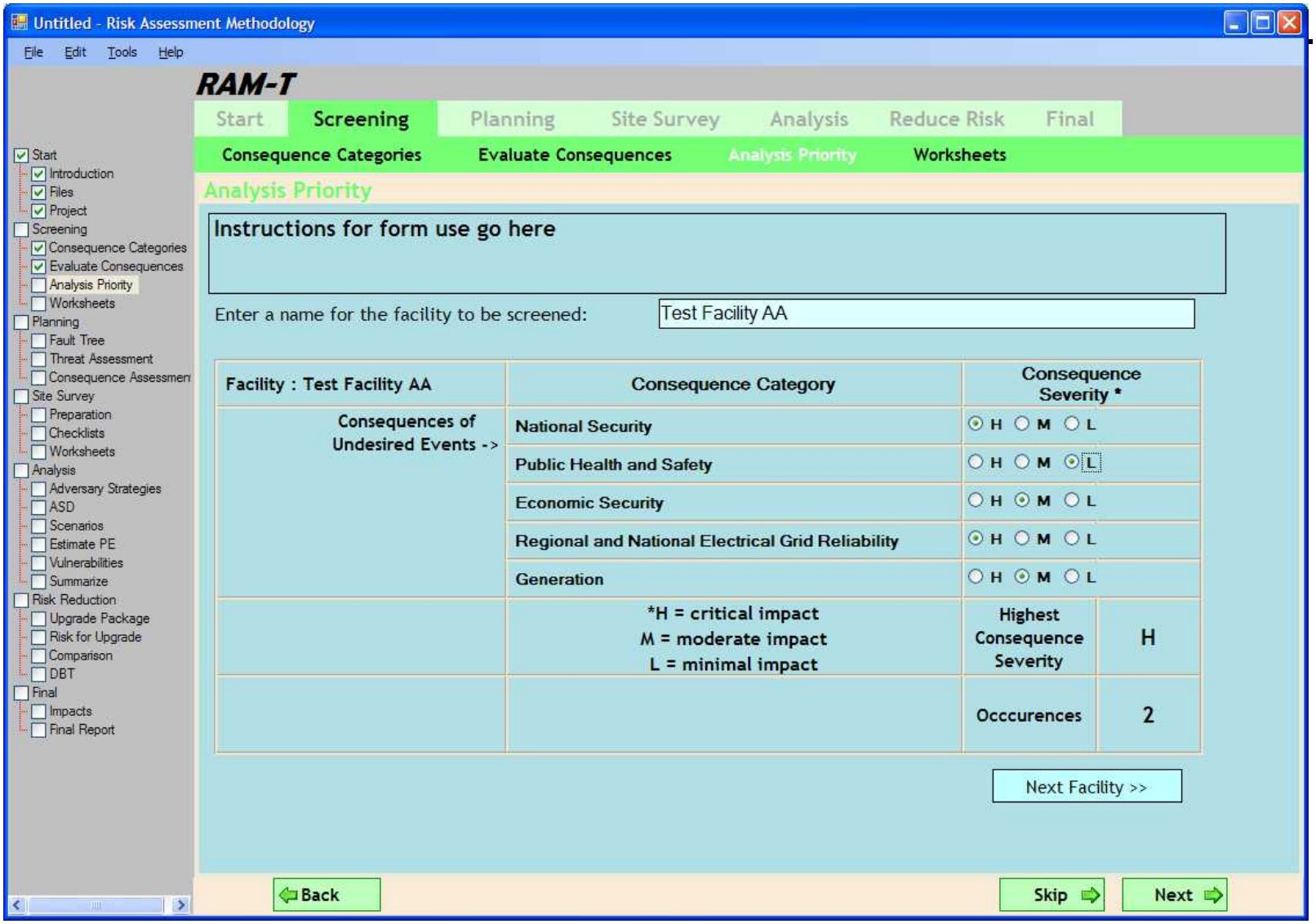
User Defined or can use Default Categories and Descriptions



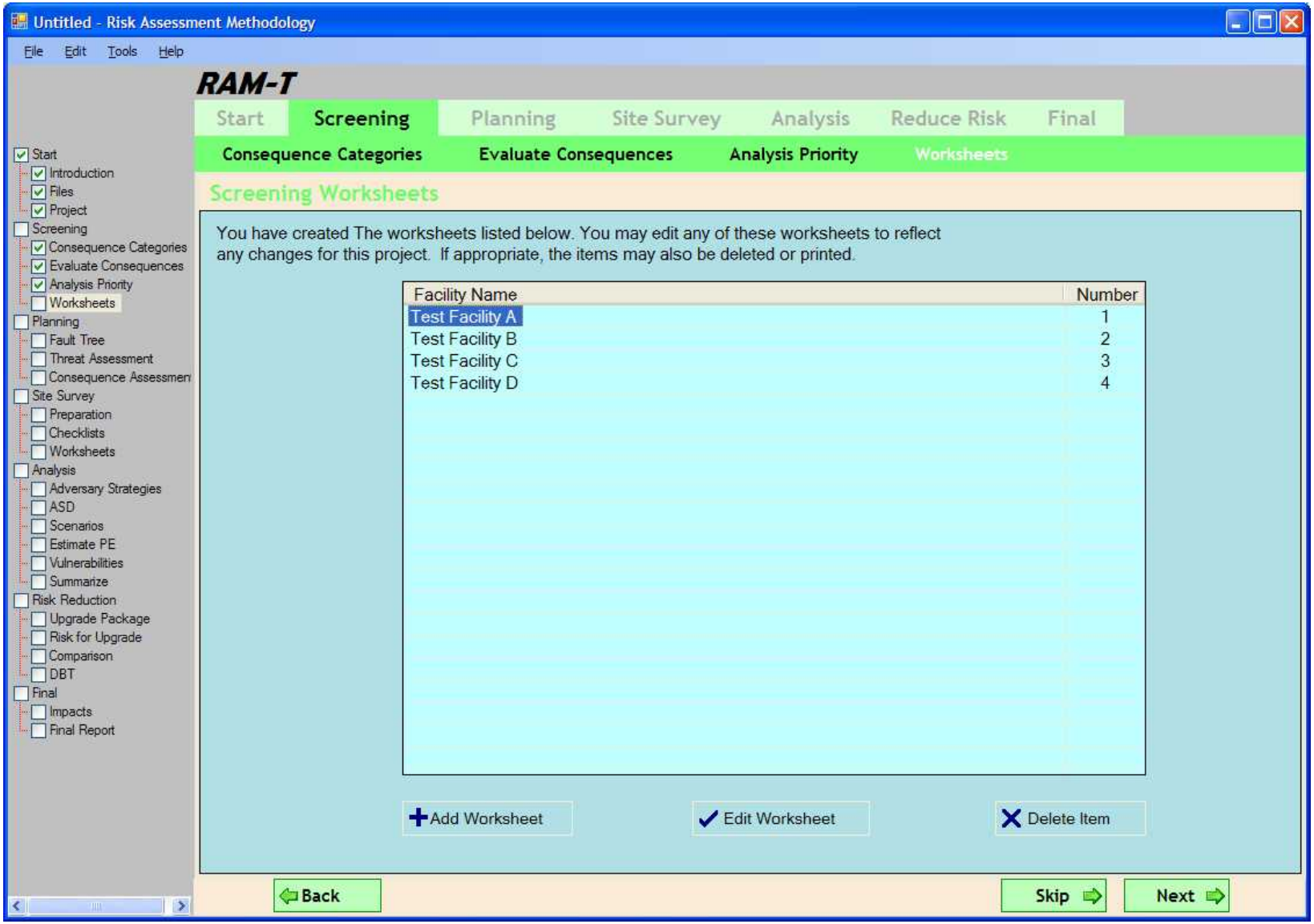
Choice of Number of Consequence Severity Levels



Evaluate Consequences



Output: Prioritization of Facilities

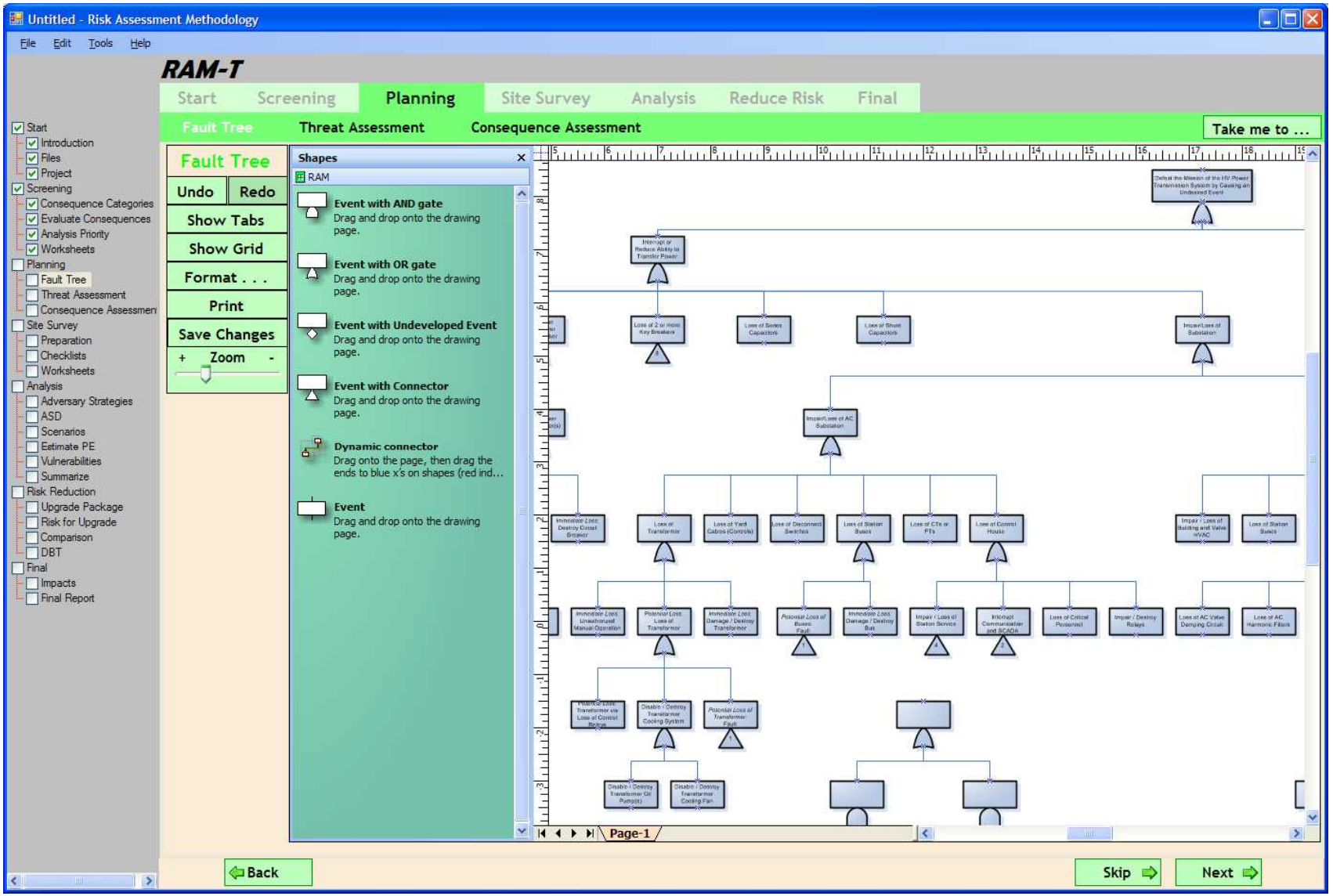


Generic Fault Tree

- 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

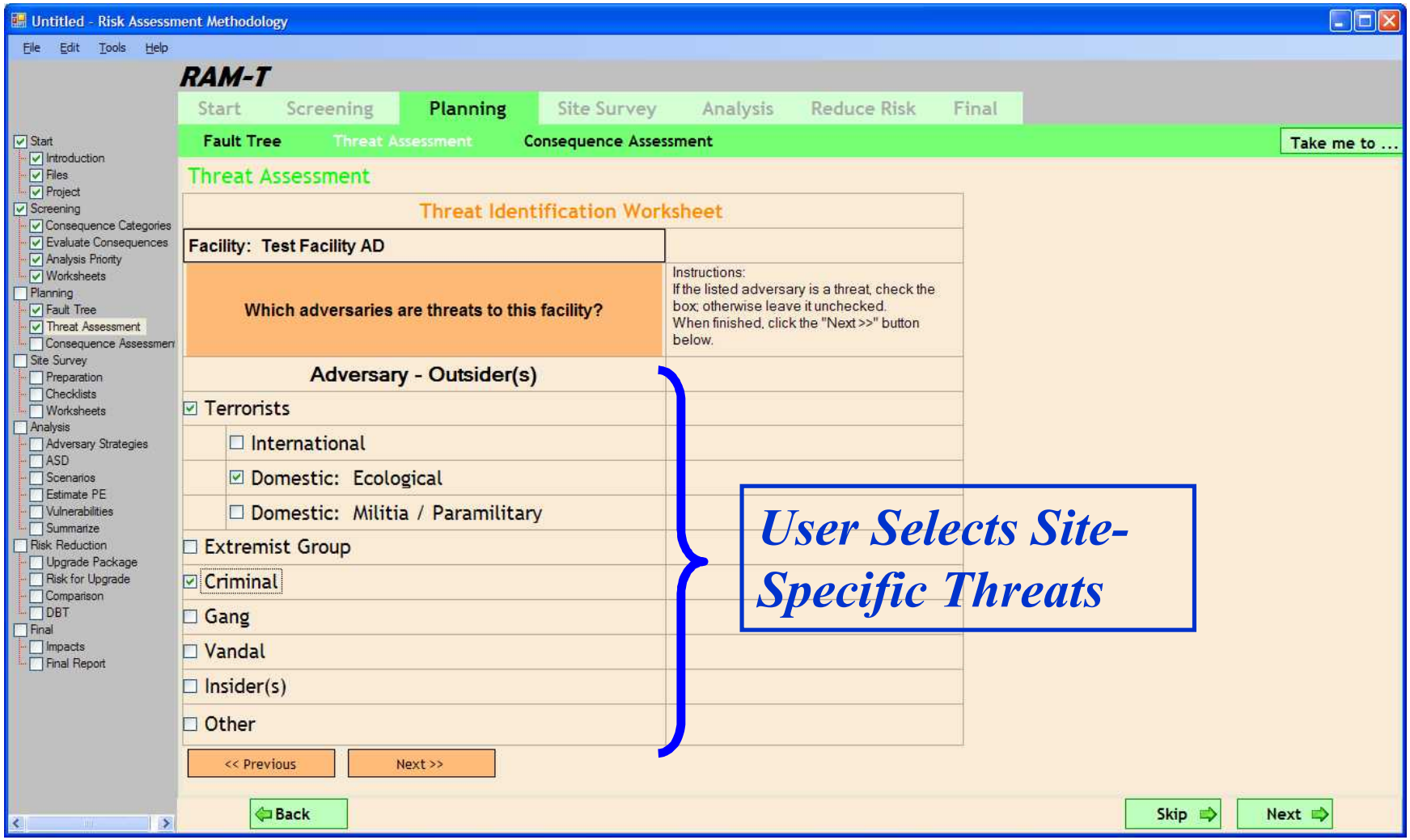
Creating a Site-Specific Fault Tree



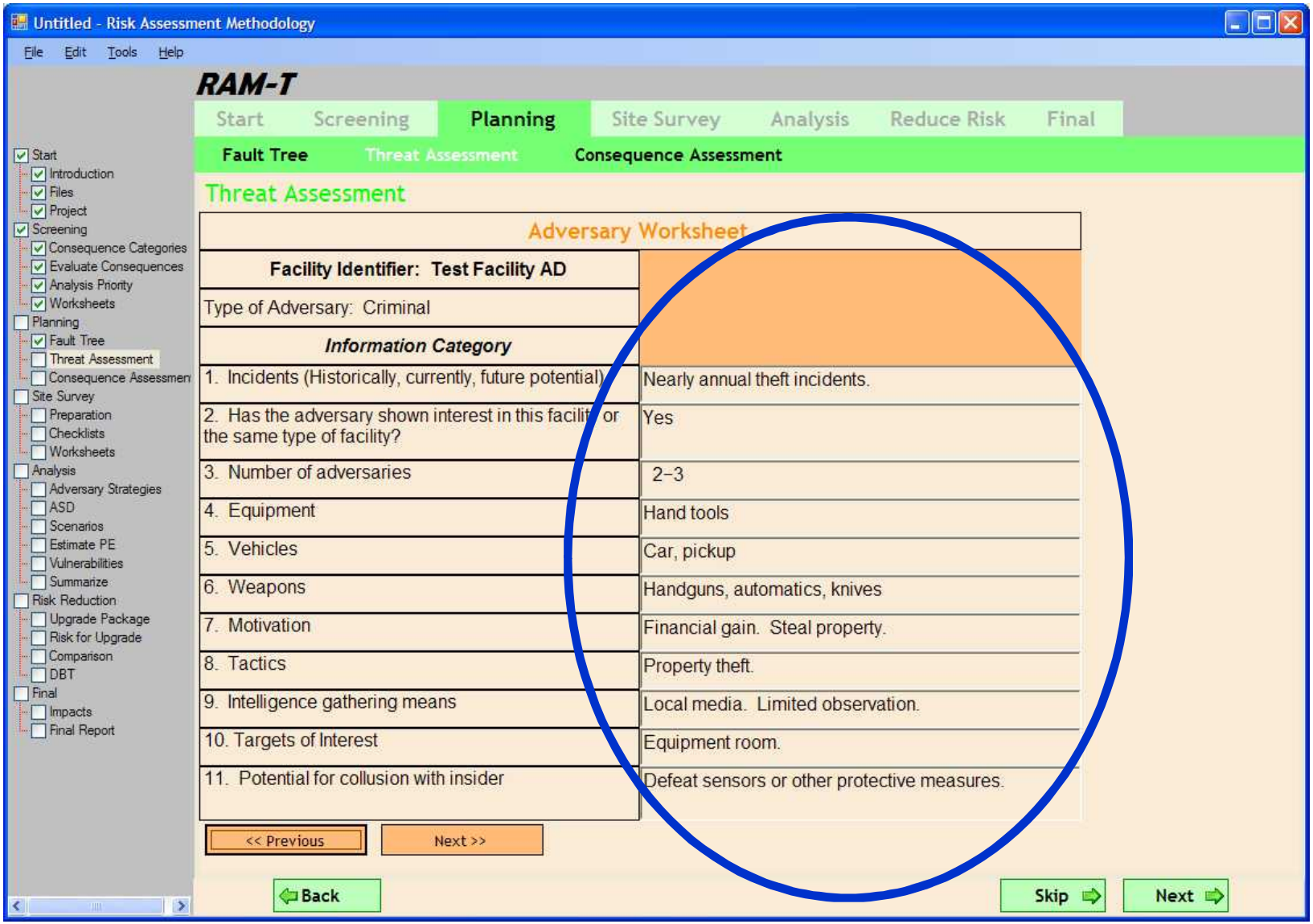
Threat Analysis

- **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

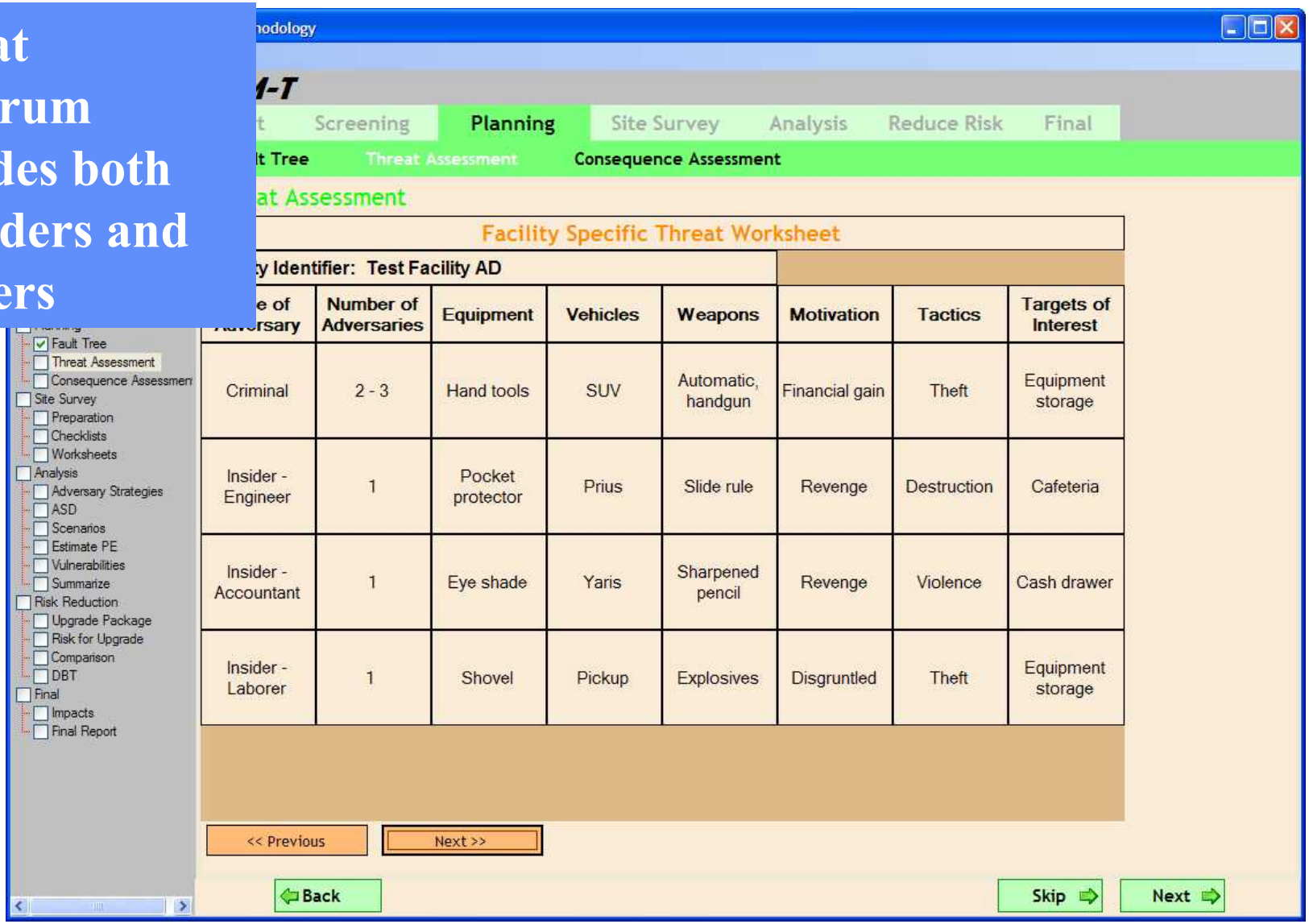


User Defines Threat Attributes and Capabilities



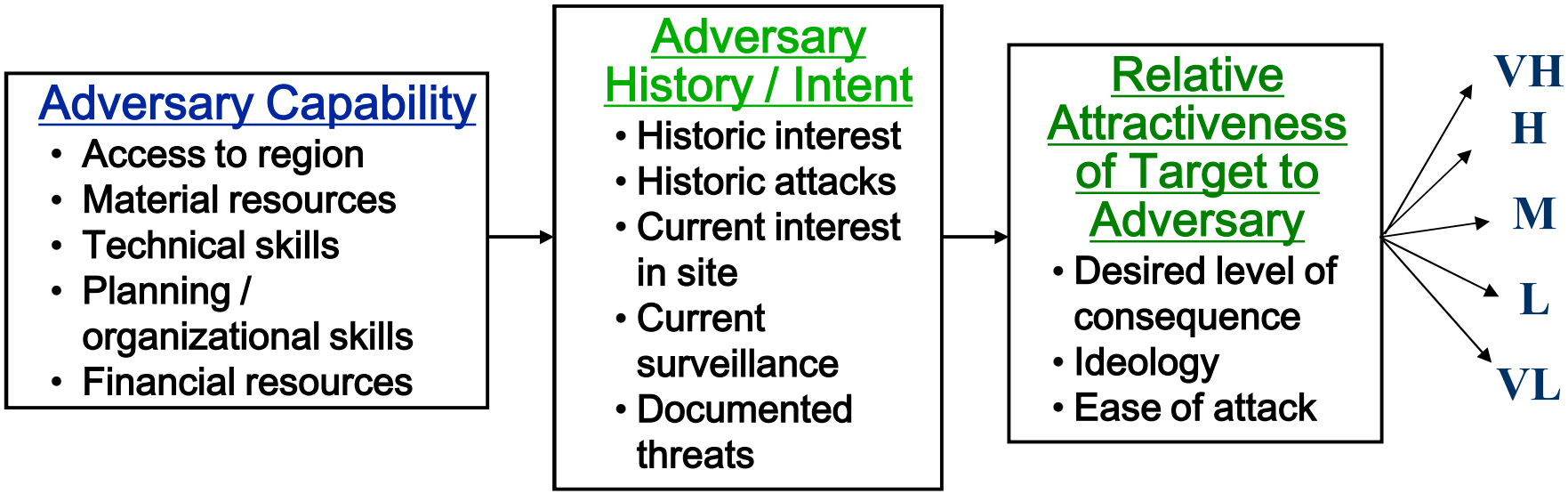
Site-specific Threat Spectrum

Threat Spectrum includes both Outsiders and Insiders



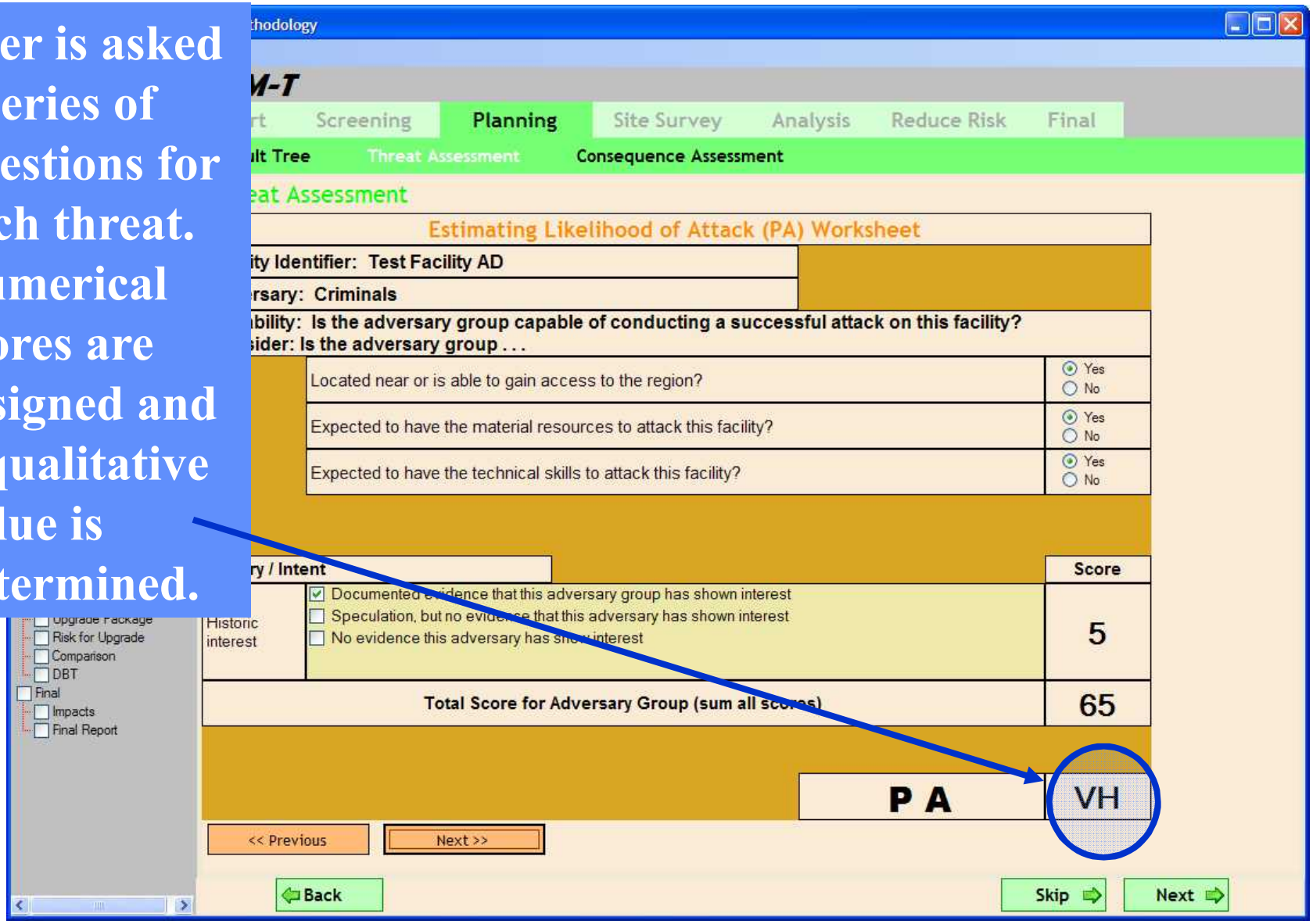
Threat Potential

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



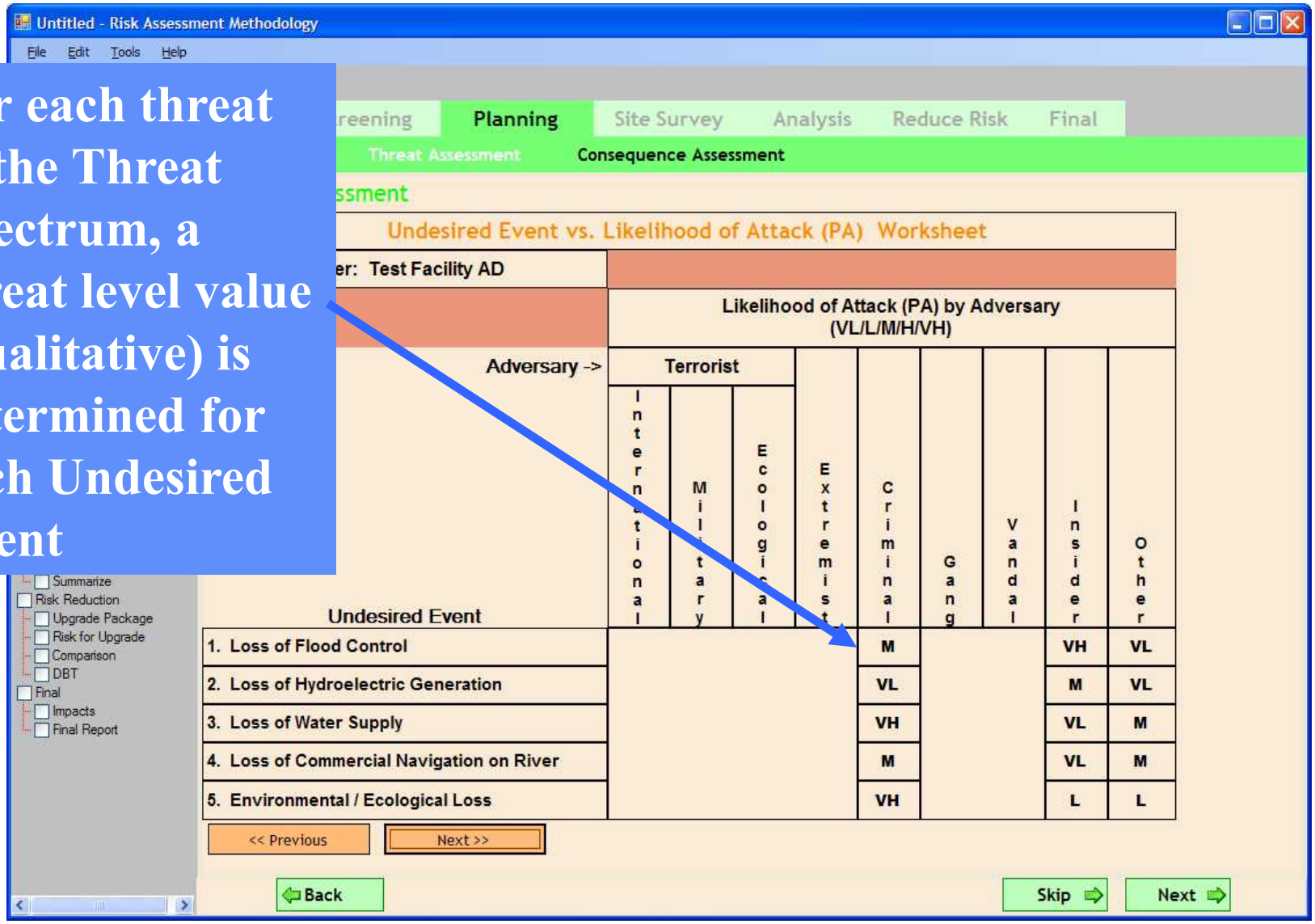
Estimating Threat Level for each Threat

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



Undesired Event vs. Threat Level

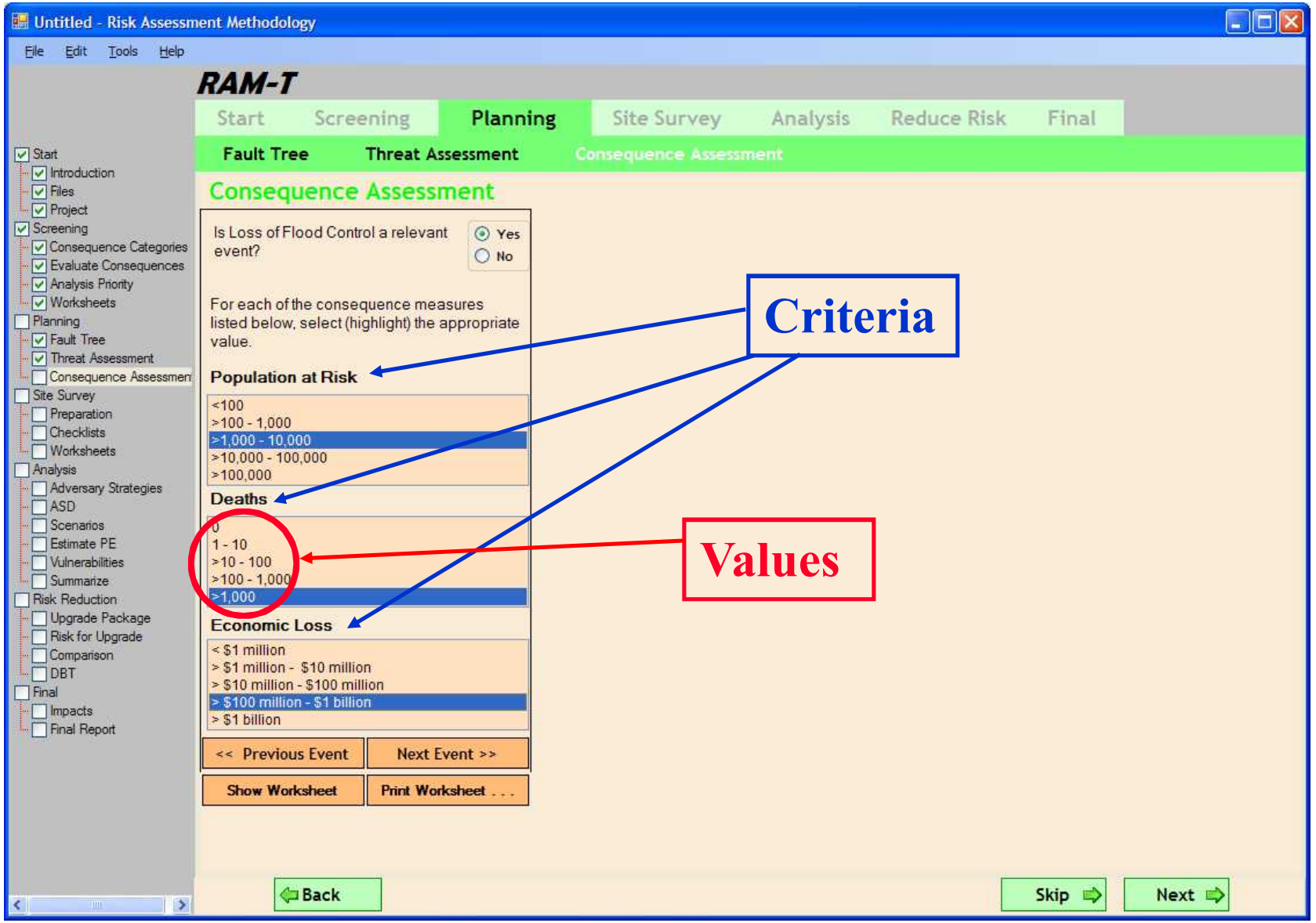
For each threat in the Threat Spectrum, a threat level value (qualitative) is determined for each Undesired Event



Consequence Analysis

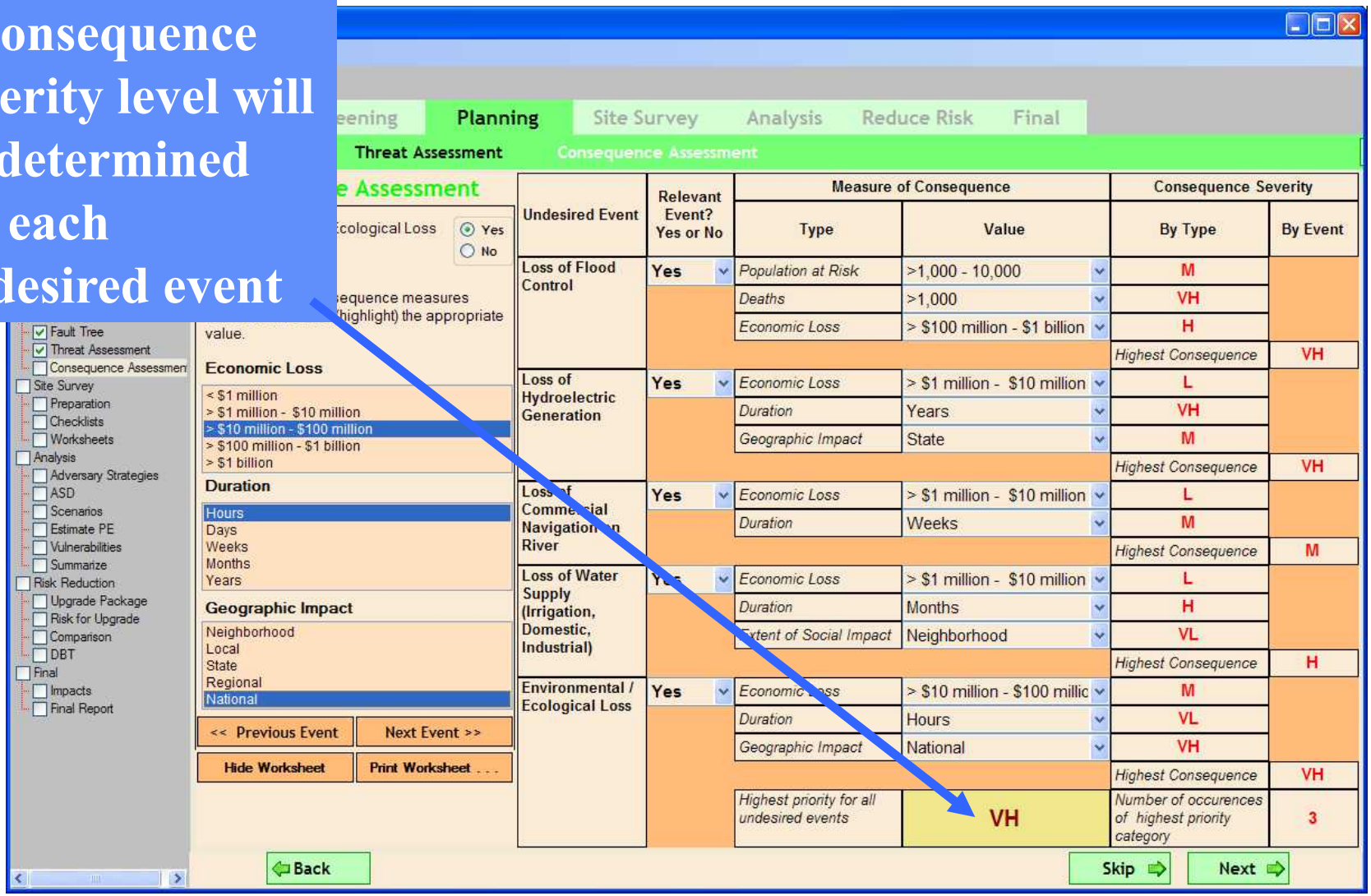
- **Consequence Table – Input:**
  - **User defined criteria**
    - **Measures – qualitative and quantitative**
  - **User defined number of levels of criteria**
  - **User provide definitions for levels of criteria**
    - **Consequence severity levels (L to VH)**
- **Output: Consequence analysis worksheet(s)**

Consequence Criteria and Values



Consequence Assessment Table

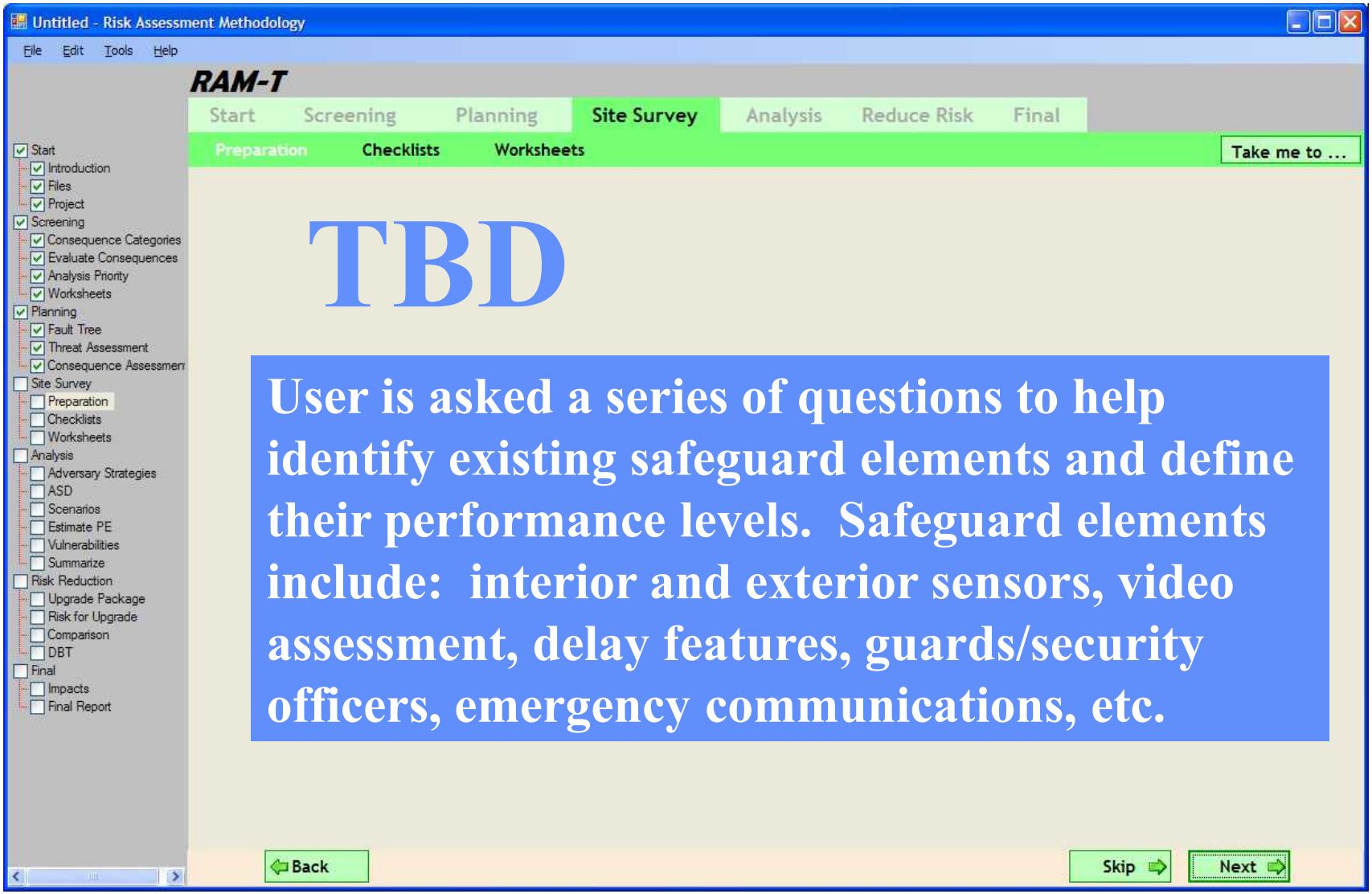
A consequence severity level will be determined for each undesired event



Site Survey

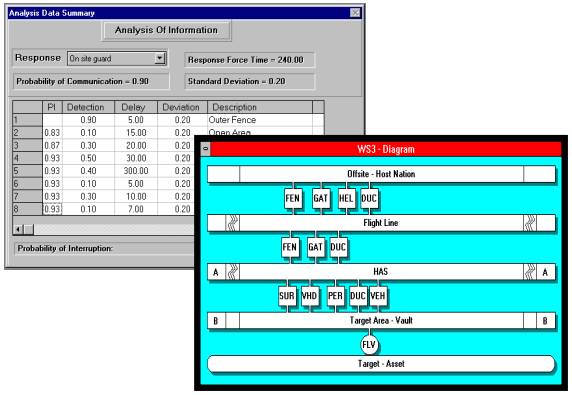
- Evaluate detection, delay, response elements along potential adversary paths
  - Evaluation based on threat attributes and capabilities from the threat assessment module
- Determine performance data to be used in analysis
  - Qualitative and quantitative data

Site Survey


Untitled - Risk Assessment Methodology
File Edit Tools Help
RAM-T
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 Assessmen
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

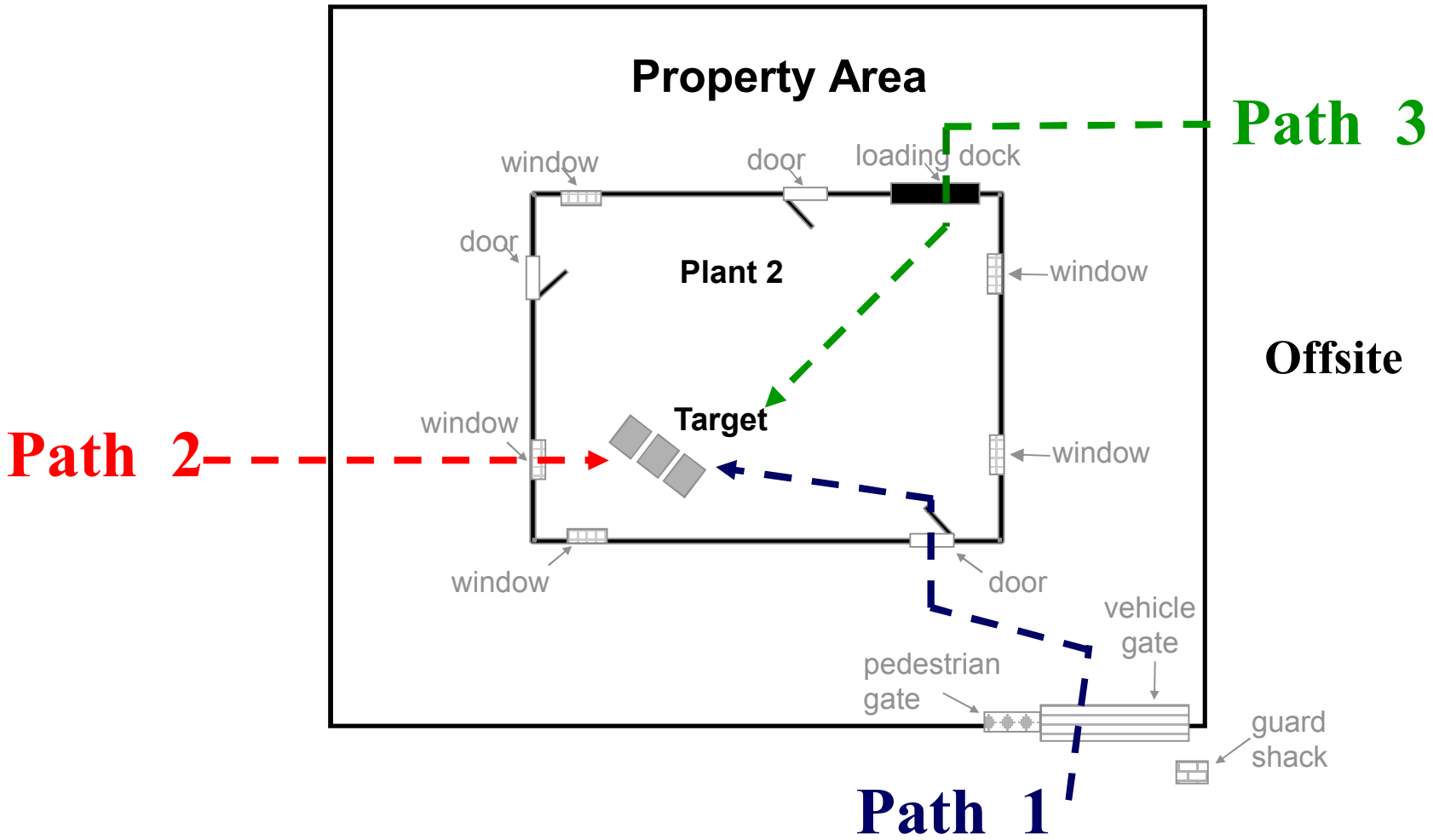
System Effectiveness Analysis

- Adversary Sequence Diagrams
  - User defined protection layers
  - User defined path elements
  - User defined connectedness



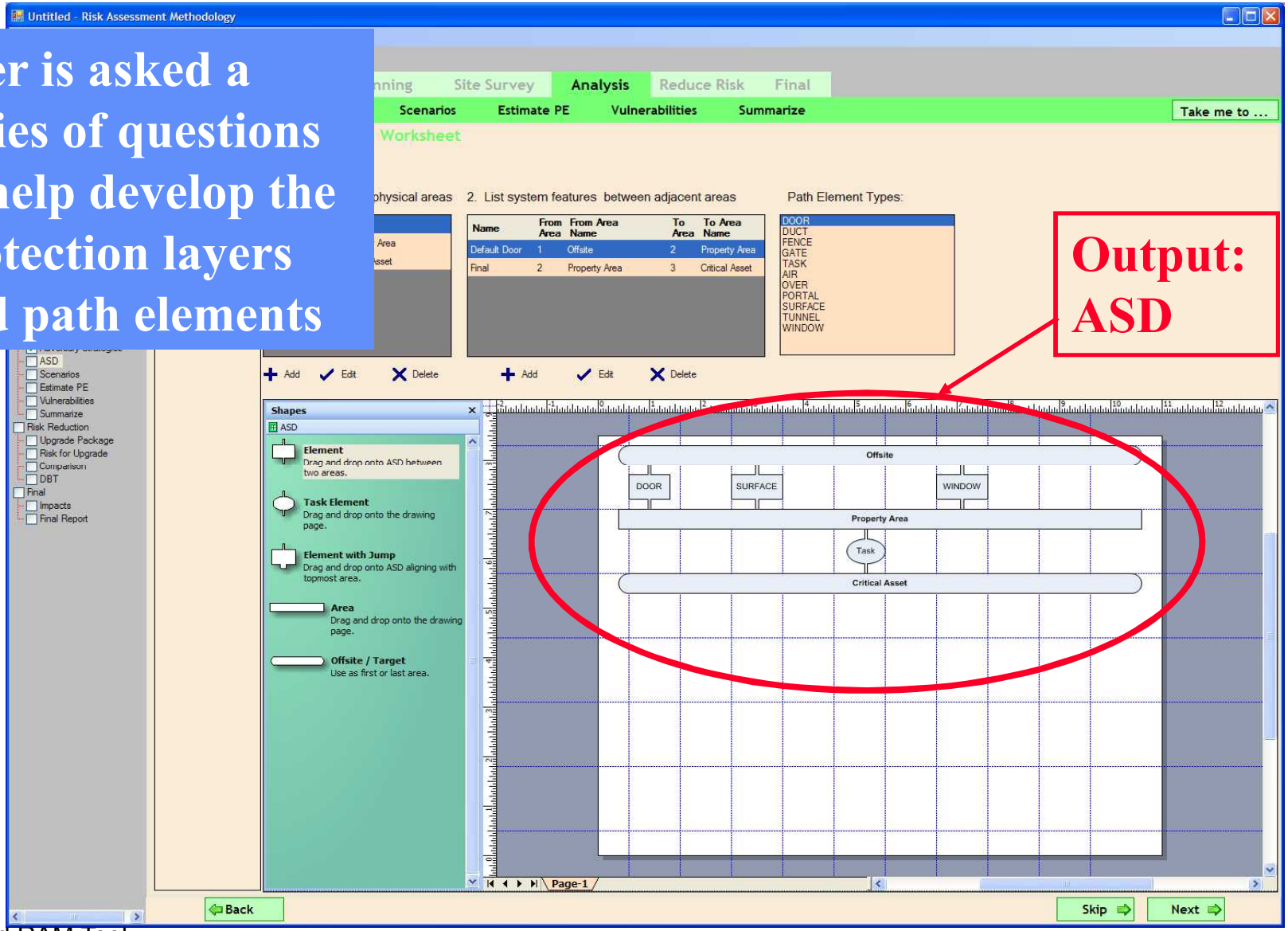
- TBD: Plans to incorporate a structured user-friendly system effectiveness tool
  - Analyzes at a systems level
  - Employs SNL security database for protection elements
- Identifies vulnerabilities

Physical Paths (Protection Layers and Path Elements)

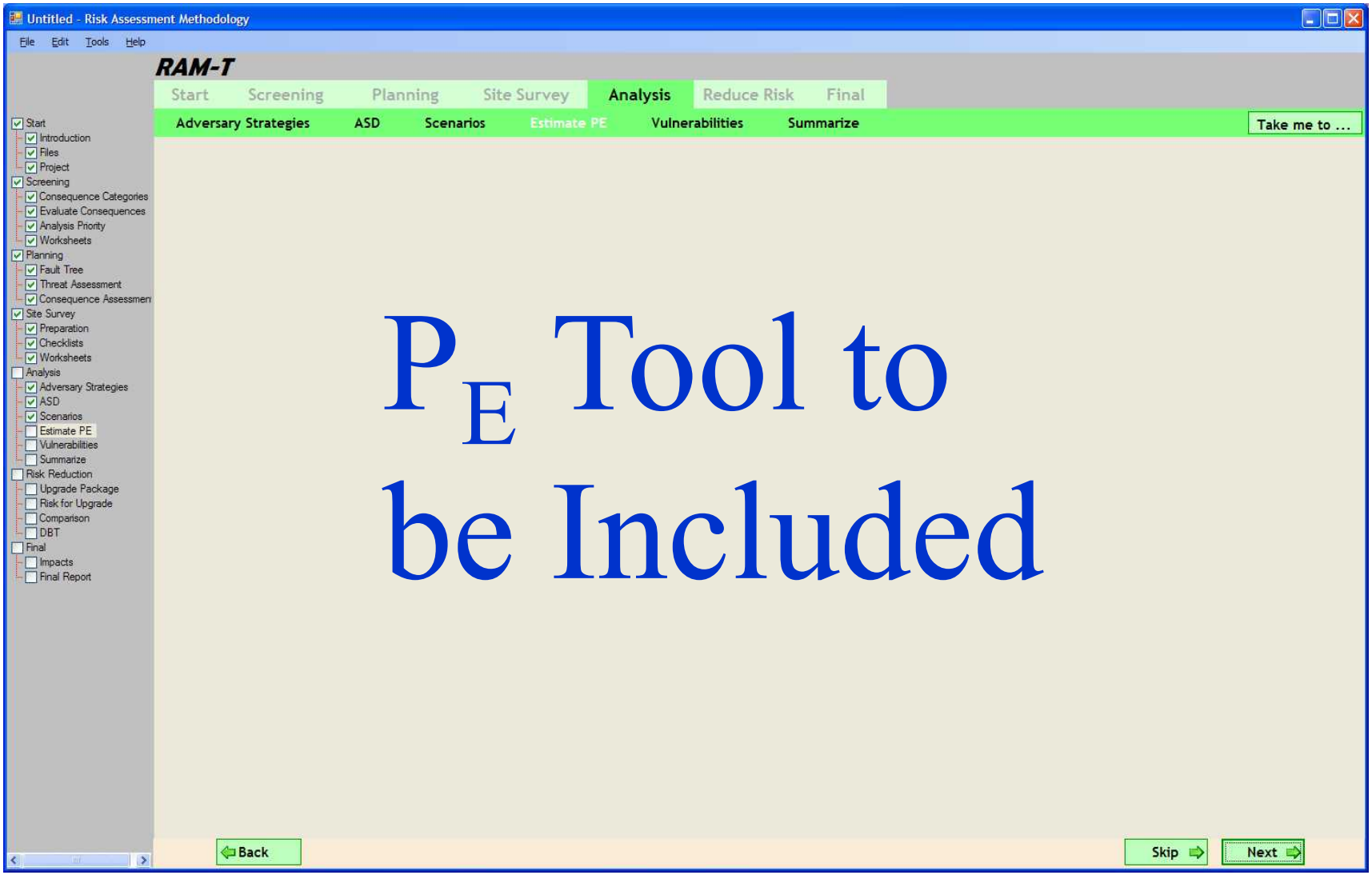


Adversary Sequence Diagram

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



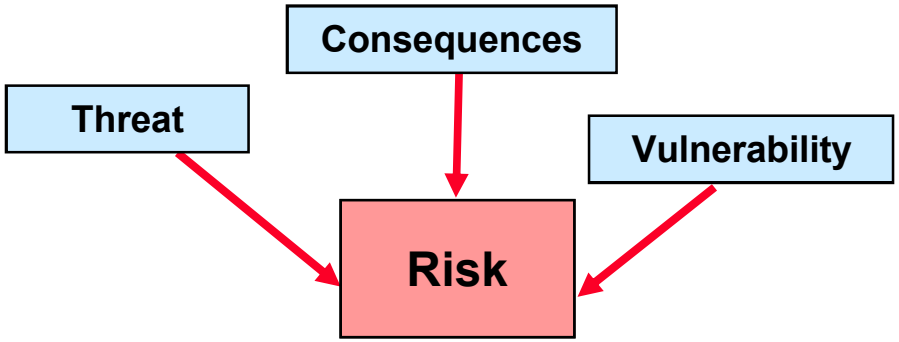
Estimating System Effectiveness



P_E Tool to be Included

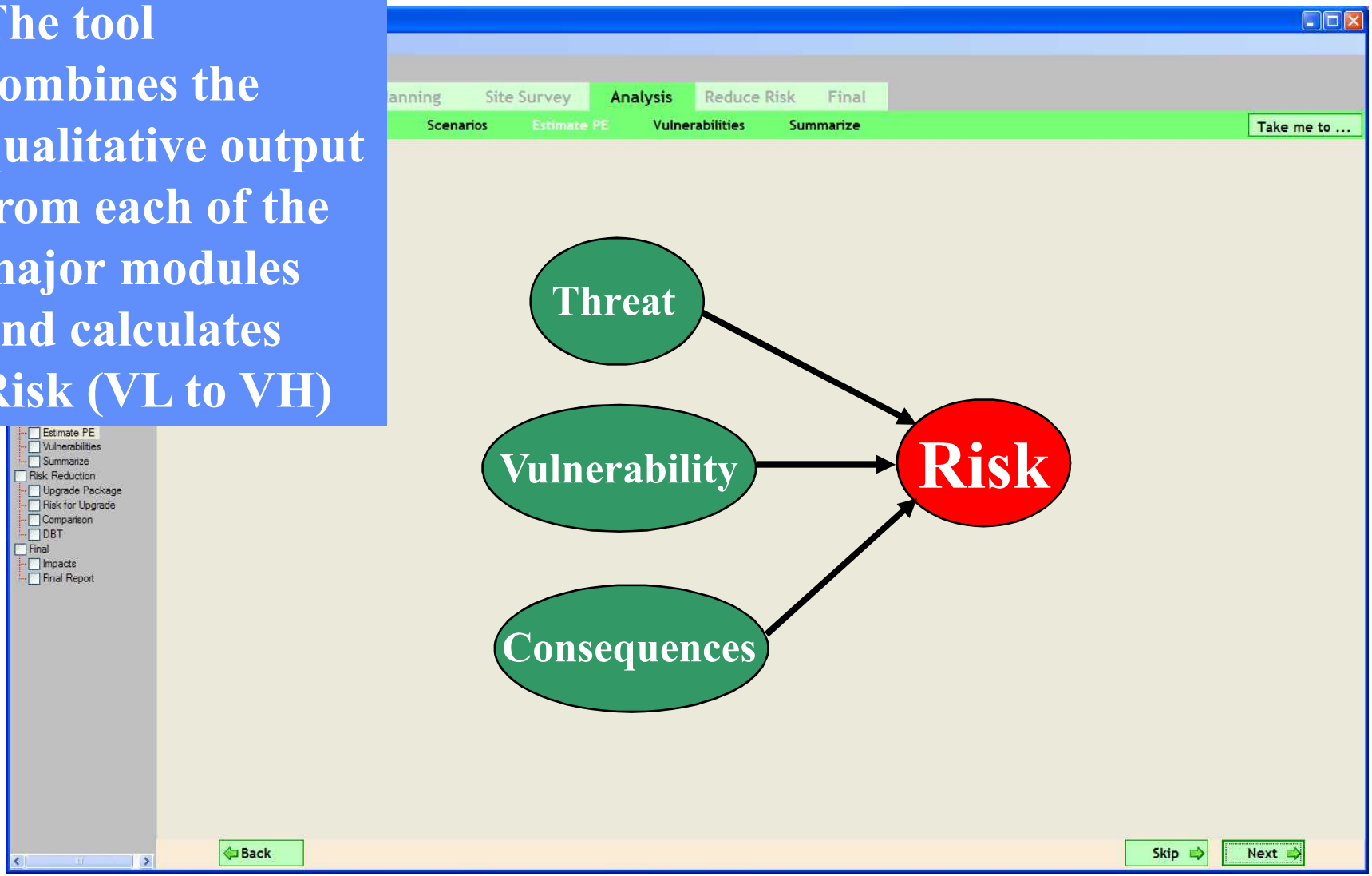
Risk Level Estimation

- 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



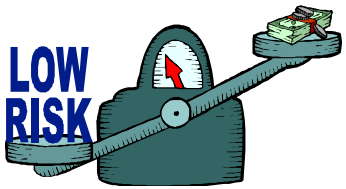
Estimating Risk

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

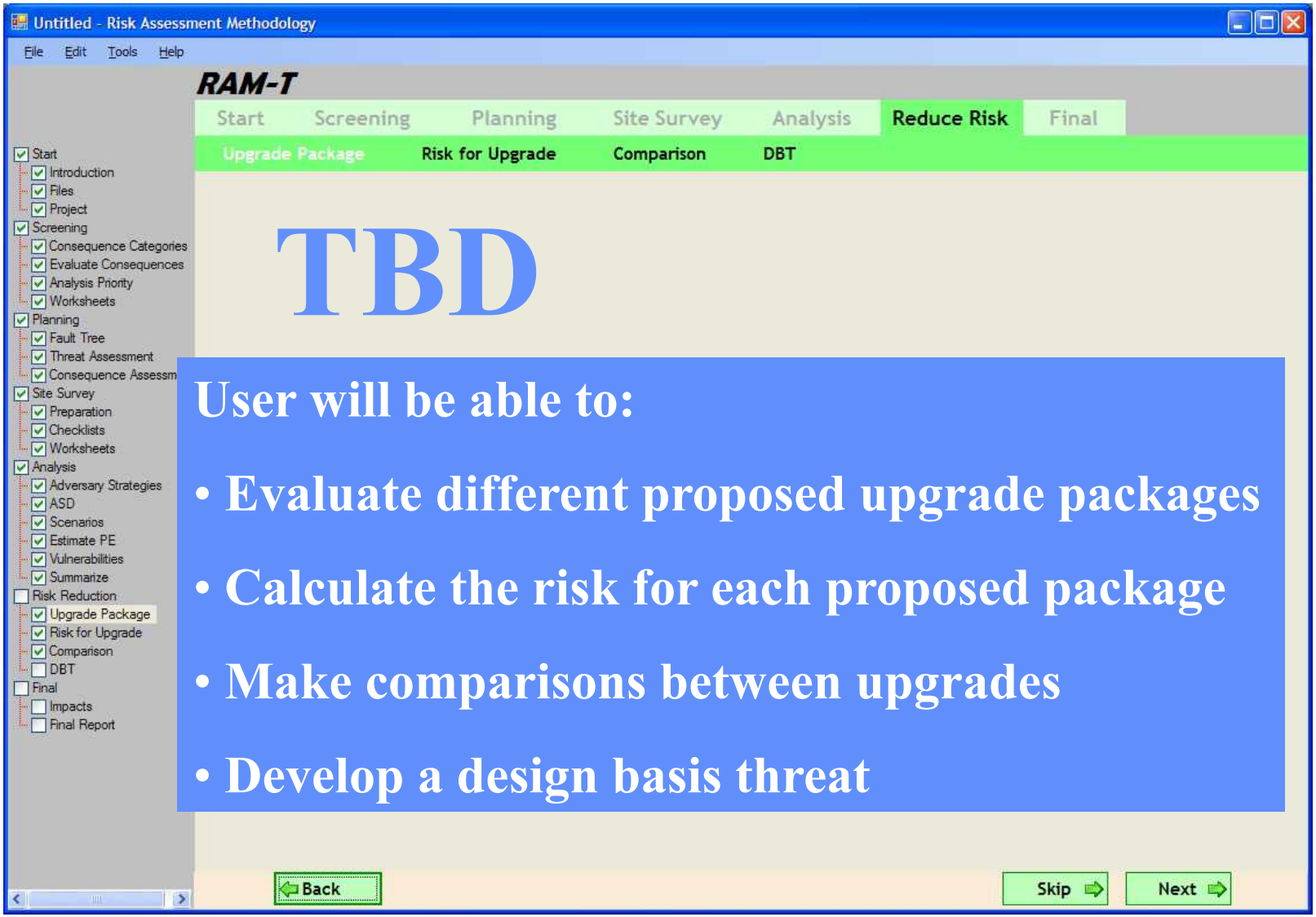


Reducing Security Risk

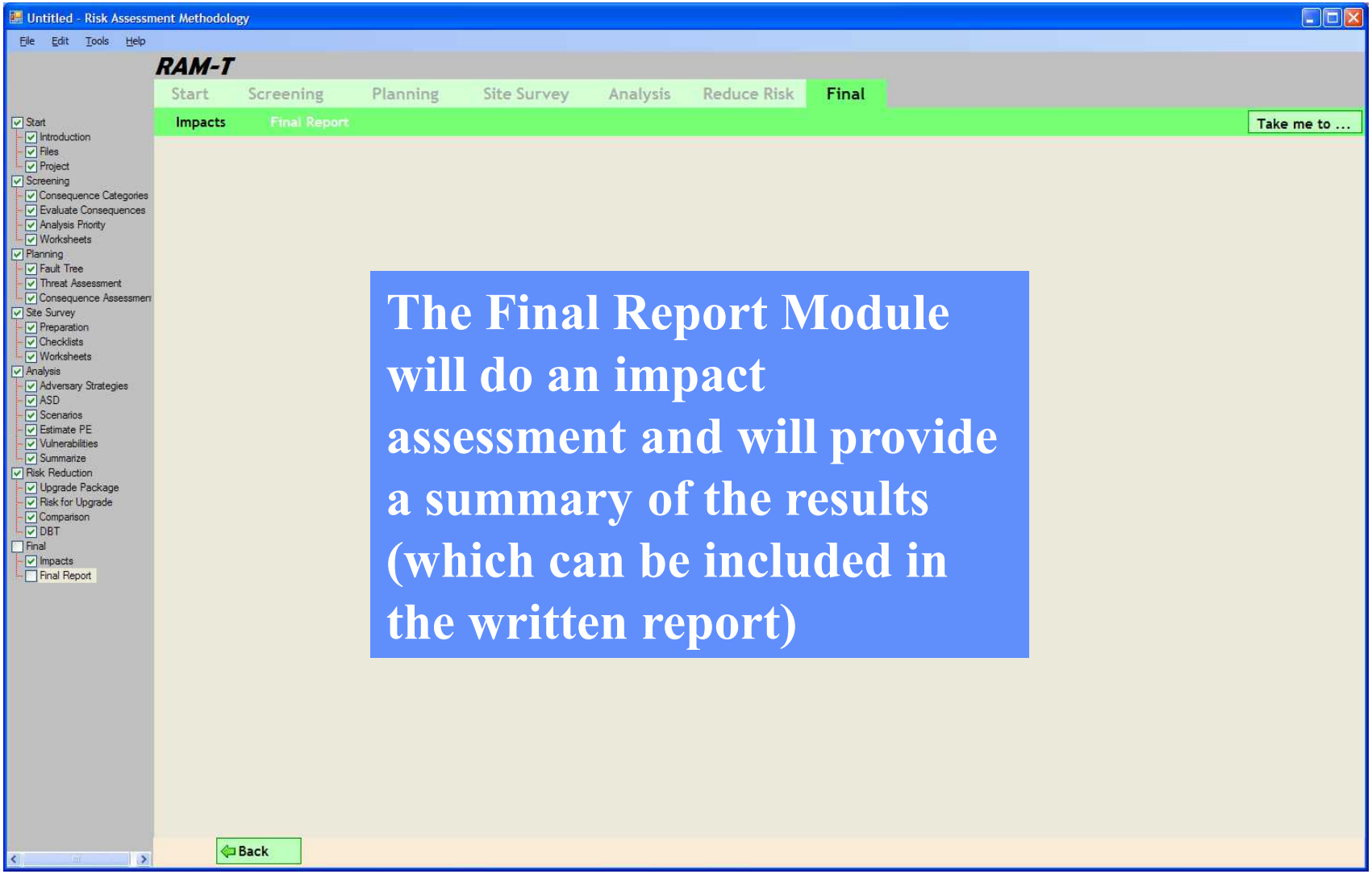
- Reduce threat level
  - Deterrence
  - Difficult to measure
- Reduce vulnerability
  - Increase detection, delay, response
- Reduce consequence level
  - Mitigation features
    - Redundancy
    - Transfer
    - System robustness
  - Improve emergency response



Reduce Risk


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
Start
Introduction
Files
Project
Screening
Consequence Categories
Evaluate Consequences
Analysis Priority
Worksheets
Planning
Fault Tree
Threat Assessment
Consequence Assessm
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 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

Final Report



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)

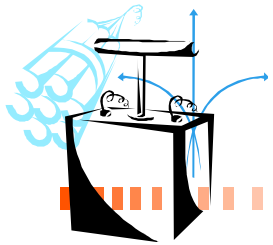
Software Development – What's been Completed?

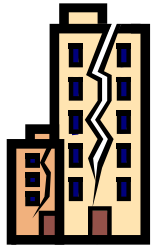
- Screening Analysis ✔
- Fault Tree ✔
- Threat Assessment ✔
- Consequence Assessment ✔
- System Effectiveness
  - Adversary Sequence Diagram ✔
  - P_E tool
- Risk Estimation
- Risk Reduction
- Final Report

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

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