SANDIA REPORT
SAND2008-81438143
Unclassified Unlimited Release
Printed December 2008

Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures

Calvin D. Jaeger, Nathaniel S. Roehrig and Teresa Torres

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia 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.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2008-8143
Unclassified Unlimited Release
Printed December 2008

Development of an Automated Security Risk Assessment Methodology Tool for Critical Infrastructures

Calvin D. Jaeger, Nathaniel S. Roehrig, and Teresa Torres
Security Risk Assessment Department
Security Systems and Technology Center
Sandia National Laboratories
Albuquerque, NM 87185-0759

Abstract

This document presents the security automated Risk Assessment Methodology (RAM) prototype tool developed by Sandia National Laboratories (SNL). This work leverages SNL's capabilities and skills in security risk analysis and the development of vulnerability assessment/risk assessment methodologies to develop an automated prototype security RAM tool for critical infrastructures (RAM-CI™). The prototype automated RAM tool provides a user-friendly, systematic, and comprehensive risk-based tool to assist CI sector and security professionals in assessing and managing security risk from malevolent threats. The current tool is structured on the basic RAM framework developed by SNL. It is envisioned that this prototype tool will be adapted to meet the requirements of different CI sectors and thereby provide additional capabilities.

Acknowledgments

This work was performed between May and September 2008 and was sponsored by the Laboratory Directed Research and Development program at Sandia National Laboratories.

CONTENTS

FIGURES

EXECUTIVE SUMMARY

This document presents the security automated Risk Assessment Methodology (RAM) prototype tool developed by Sandia National Laboratories (SNL). This work leverages SNL's capabilities and skills in security risk analysis and the development of vulnerability assessment (VA)/risk assessment methodologies to develop an automated prototype security RAM tool for critical infrastructures (RAM-CI™). The prototype automated RAM tool provides a user-friendly, systematic, and comprehensive risk-based tool to assist CI sector and security professionals in assessing and managing security risk from malevolent threats. The current tool is structured on the basic RAM framework developed by SNL. It is envisioned that this prototype tool will be adapted to meet the requirements of different CI sectors and thereby provide additional capabilities.

A very large number of security risk tools is currently being used by those responsible for security of CIs. Some of the tools are checklists to determine whether a facility is in compliance with delineated standards or requirements. Some of the tools require significant subjective input by the user. There are not very many security risk-based tools that rigorously address all three components of risk (threat, vulnerability, and consequences) in their analysis. The use of checklists and very subjective input may be appropriate for simple, low-consequence facilities, but checklists would generally not be desirable for more complex, higher-consequence facilities. Subjective input may be acceptable, but the effectiveness of such an approach is critically dependent on the qualifications of the people providing the input.

In contrast, the SNL RAMs provide a very comprehensive approach. The SNL automated prototype RAM tool:

- Provides a systems approach to security risk (i.e., how well do security features perform together to prevent undesired event).
- Provides an approach using fault trees to identify possible ways to cause an undesired event and identify what assets need to be protected.
- Provides the level of detail and leverages databases from physical security system testing to quantitatively assess the physical protection system effectiveness.
- Provides the ability to easily perform "what-if" analyses to evaluate possible designs for new facilities or upgrades to existing ones.
- Provides results that are repeatable and traceable.
- Meets the criteria for risk assessment methodologies as defined in the National Infrastructure Protection Plan (NIPP).

The automated RAM prototype tool is a functional tool that is both a risk assessment and a risk management tool. It follows the basic RAM process that includes the following steps:

1. The automated RAM prototype tool includes an optional high-level screening step in which the user can identify and prioritize numerous facilities based on a defined set of consequence criteria.

2. The planning step provides documented assessment goals and project scope, identification of the team members and required tools or equipment, defined facility missions, and the facility's security concerns and undesired events.
3. The facility characterization step includes the collection of facility information, development of a site-specific fault tree, and the identification of potential targets.
4. In the consequence assessment step, the user applies or adapts a default consequence table or develops a new consequence table, lists the undesired events and the targets that if attacked may cause the undesired event, provides input for each of the consequence criteria to estimate the severity level for the undesired events.
5. The threat assessment step provides the user with the ability to identify both outsider and insider threats and define their motives, objectives, and capabilities. If sufficient information is available, the user can also develop an estimate for the threat potential, which considers the likelihood of attack.
6. The protective objectives step includes the identification of the site's objectives for the protection system. The effectiveness of the protection system is evaluated on how well these objectives can be met.
7. The system effectiveness step for the automated RAM prototype tool is a very comprehensive approach that is unique among the many risk-based tools available. The user first estimates the adversary's most likely strategy to cause the undesired event and affect the associated targets. An adversary path diagram is developed that includes a graphical representation of the facility including layers or areas and path elements between these layers or areas. Using an SNL physical security database derived from many years of testing and subject matter expert (SME) review, the safeguard attributes for each of the path elements are defined. A path analysis is then performed to estimate the effectiveness level of the protection system to meet its specified protection objectives. Finally, a list of possible security weaknesses or vulnerabilities is identified for the physical protection system (PPS) functions of detection, delay and response when system effectiveness is assessed to be low.
8. The probability that an adversary would cause an undesired event and associated consequence are used to estimate security risk value.
9. The risk assessment is now complete and decision makers must determine if the risk is acceptable.
10. If the risk is too high, then the user can identify possible risk reduction measures and evaluate their impact. Upgrade packages are developed and the changes in risk, possible costs and impacts to operations, schedule and other areas can be provided to the decision makers.
11. The final step in the process is the reporting of the assessment results and metrics to help support risk managers make decisions.

The automated RAM tool provides a comprehensive, risk-based systems view of the ability of a facility to protect against a malevolent threat. The automated RAM tool also supports the goal of the NIPP to "build a safer, more secure, and resilient America by enhancing protection of the Nation's critical CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts

by terrorist to destroy, incapacitate, or exploit them …" (NIPP, 2006). In particular, it provides processes for combining consequence, vulnerability, and threat information for a comprehensive and systematic risk assessment and management capability that can be applied to all CI/KR (critical infrastructure/key resource) sectors. It meets the requirements for risk assessment methodologies outlined in the NIPP and supports national objectives identified by the United States Department of Homeland Security (DHS) and other federal agencies. It will provide an enhanced capability to address the determination of security risk in the different CI/KR sectors.

The automated RAM tool provides a proven risk-based systems approach to help decision makers to make optimal cost-effective security decisions based on a rigorous systematic process. It is an integrated systems engineering approach. It provides the level of detail necessary to identify system vulnerabilities and possible risk reduction measures. Finally, the data used and the results produced by RAM process and data used are repeatable, traceable, and defensible.

Acronyms

ASD	Adversary Sequence Diagram
C	consequence (of loss)
CDP	critical detection point
CI	critical infrastructure
CI/KR	critical infrastructure/key resource
DBT	design basis threat
DHS	United States Department of Homeland Security
GIS	Geographic Information System
H	high
L	low
LDRD	Laboratory Directed Research and Development
M	medium
NIPP	National Infrastructure Protection Plan
P_I	probability of interruption
P_N	probability of neutralization
PC	personal computer
PPS	physical protection system
R	risk
RAM	Risk Assessment Methodology
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RAM-CI™	Risk Assessment Methodology for Critical Infrastructure™
RFT	response force time
SCADA	Supervisory Control and Data Acquisition
SME	subject-matter expert
SNL	Sandia National Laboratories
T	Threat
V	Vulnerability
VA	vulnerability assessment
VH	very high
VL	very low
WMD	weapon of mass destruction

1. INTRODUCTION

This report presents the automated security Risk Assessment Methodology (RAM) prototype tool developed by Sandia National Laboratories (SNL). This work, performed between May and September of 2008, was sponsored by the Laboratory Directed Research and Development (LDRD) program at SNL. The work leverages SNL's long-standing capabilities and skills in security analysis and vulnerability assessment (VA) with its new security risk assessment methodologies to develop an automated prototype security RAM tool for critical infrastructures called RAM-CI™.

This automated RAM prototype tool provides a user-friendly, systematic, and comprehensive risk-based tool to assist critical infrastructure (CI) sector and security professionals in assessing, and managing security risk from malevolent threats. The current tool is structured on the basic RAM framework developed by SNL. It is envisioned that the capabilities of this tool will be adapted and enhanced to meet the specific requirements for different CI sectors.

1.1 Background

Since 1949 SNL has developed science-based technologies that support our national security. SNL and the Security Systems and Technology Center are uniquely qualified to develop critical infrastructure security risk assessment tools due to their experience and success with developing and implementing security RAMs and VA approaches for various government agencies, commercial nuclear power facilities, military installations, local communities, and other critical infrastructures. SNL has developed a number of security RAMs for various infrastructures including federal dams, water systems, electrical transmission, chemical facilities, and communities (see http://www.sandia.gov/ram). All these RAMs consider potential malevolent attacks from different threats, possible undesired events and consequences, and the effectiveness of the protection system to determine potential adversary success. The RAMs assess these infrastructures to help identify security weaknesses and develop measures to mitigate the consequences from possible adversary attacks.

The basic process for all RAMs is very similar. Security risk is a function of T (threat), V (vulnerability), and C (consequences). The RAM process and its steps will be discussed in the this report. The RAMs are primarily manual systems that consist of a field or user's manual and perhaps a separate document with appendices that provide examples, discussions, illustrations, or explanations. The RAMs use a series of worksheets that guide the user through the steps in the RAM process. Because the RAM process is a comprehensive approach, the level of effort required to perform the analysis may be significant depending on the complexity of the facility and the number of factors to be considered. The automated RAM tool has not only made the process much more user-friendly and efficient, but it has also incorporated many of the lessons learned from previous RAM development activities and subsequent applications.

1.2 Problems and Challenges

A very large number of security risk tools are currently in use. Some of the tools are checklists that determine whether a facility is in compliance with specified standards or requirements. Some of the tools require significant subjective input by the user. There are not very many security risk-based tools that rigorously address all three components of risk (threat, vulnerability, and consequence) in their analyses. The use of checklists and very subjective input may be appropriate for simple, low-consequence facilities, but would not be well-suited for more complex, higher-consequence facilities. Subjective input may be acceptable in some cases, but its accuracy is heavily dependent on the qualifications of the people providing the input. The SNL automated RAM prototype tool:

- Provides a systems approach to security risk risk (i.e., how well do security features perform together to prevent undesired event).
- Provides an approach using fault trees to identify possible ways to cause an undesired event and identify what assets need to be protected.
- Provides the level of detail and leverages databases from physical security system testing to quantitatively assess the physical protection system effectiveness.
- Provides the ability to easily perform "what-if" analyses to evaluate possible designs for new facilities or upgrades to existing ones.
- Provides results that are repeatable and traceable.
- Meets the criteria for risk assessment methodologies as defined in the National Infrastructure Protection Plan (NIPP).

1.3 Purpose

This development project leverages existing RAM tools, the knowledge gained from automation of SNL VA tools, and input from RAM developers and users to create a prototype automated security RAM tool. It provides a sound scientific and technical framework to security risk assessment. This work provides the basic RAM framework in an automated tool that can then be adapted for application to different CI sectors and other areas.

1.4 Scope

This report provides a brief description of the RAM process and discusses the different steps of the automated tool. Only malevolent threats – both outsider and insider threats - are considered in the automated tool, although some SNL RAMs do consider non-malevolent and natural external threats as well. The discussions of the automated tool focus on physical security effectiveness improvements and consequence mitigation measures. The manual RAM approach has been used to evaluate threats to cyber and process control systems, but these are not currently part of the prototype tool. The RAM prototype tool provides the basic RAM framework; it does

not include a specific CI area. Once the prototype tool is complete, specific CI modules can then be developed for the tool.

1.5 Security Risk Assessment Methodology

The following sections provide an introduction to risk as it applies to security at CI facilities. The components of risk and how these components apply to malevolent threats are discussed.

1.5.1 The Components of Risk

SNL describes risk as a function of threat, consequence, and vulnerability. The components of risk are depicted in Figure 1.

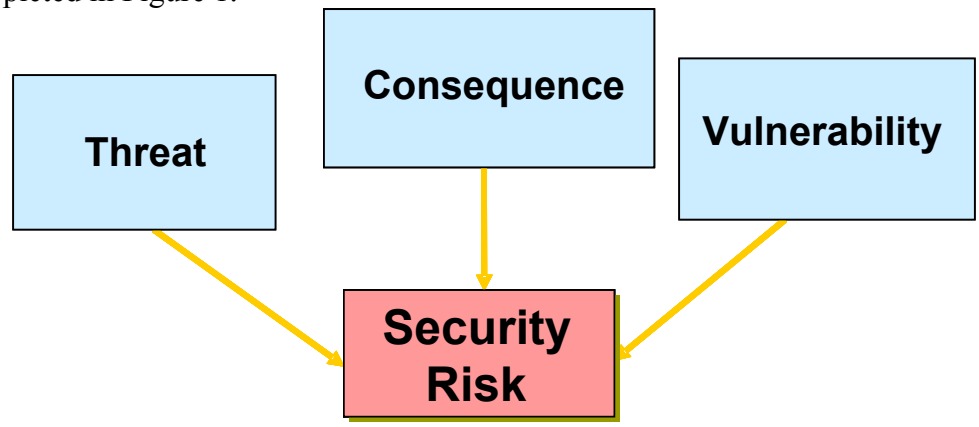

Figure 1. Components of Risk

1.5.2 Risk Equation for the Malevolent Threat

The general risk equation to calculate a relative risk from a malevolent threat for each identified critical asset is the following risk equation:

$$R = P_A * (1 - P_E) * C$$

where:

R = risk associated with the adversary attack;

P_A = likelihood of the attack (threat potential);

P_E = probability the security system is effective against the attack; protection system effectiveness in meeting its protection objectives;

$(1 - P_E)$ = probability that the adversary attack is successful causing undesired events (also, the probability that the security system is not effective against the attack); vulnerability; and

C = consequence of loss.

1.5.3 Decisions and Risk

The automated prototype RAM tool supports both risk assessment and risk management. It is a systematic, thorough security risk assessment tool designed to assist CI facilities in making a determination about the risks from malevolent threats to the operations of a CI facility. When applying the tool, many decisions must be made that will directly impact the final results. These decisions, which include the defined threat (a site-specific threat spectrum), the measures of consequence, and the facility's mission objectives, are difficult to make, but they are necessary to complete the assessment. There will always be adversaries sophisticated beyond the capabilities of any facility to defeat; thus it is important to make improvements that both bring the greatest returns and, if possible, are adaptable to changing threats and the environment.

The decision process begins with identifying the facility's overall mission and mission objectives. By understanding the mission and mission objectives, the facility can identify the mission critical operations, functions, and processes that affect the most important mission objectives. For example, if public safety is the most important mission objective, then lowering the potential consequences from catastrophic release of chemicals may be the area of greatest risk and the first candidate to investigate. Using a priority ranking process allows the CI facility to invest in risk reduction in a systematic manner that is in line with the mission objectives and provides clear documentation of the data that informs the decisions process.

The automated prototype RAM tool requires a clear statement of the protection objectives of the CI facility. The process determines the ability of the protection system to meet those protection objectives. Through a systematic analysis, the threat is defined, the undesired events are determined, and the associated critical assets are identified. (Compromise of critical assets can bring about serious consequences.) Worst-case paths for the adversary to cause undesired events are postulated and analyzed. The existing security system effectiveness is evaluated and vulnerabilities are identified. The vulnerabilities identified are then used as input to create recommendations and propose upgrades to reduce risk from malevolent attacks.

After vulnerability and consequence assessment steps are completed, the risk analysis is performed to determine whether the protection objectives have been met. If the protection objectives have not been met, the choice must be made to select more realistic requirements, mitigate consequences, or increase the effectiveness of the security system. The overarching decision that must be made by CI facility management is how much risk is acceptable and how much risk reduction is enough. Acceptable risk levels are defined and established by the senior decisions makers.

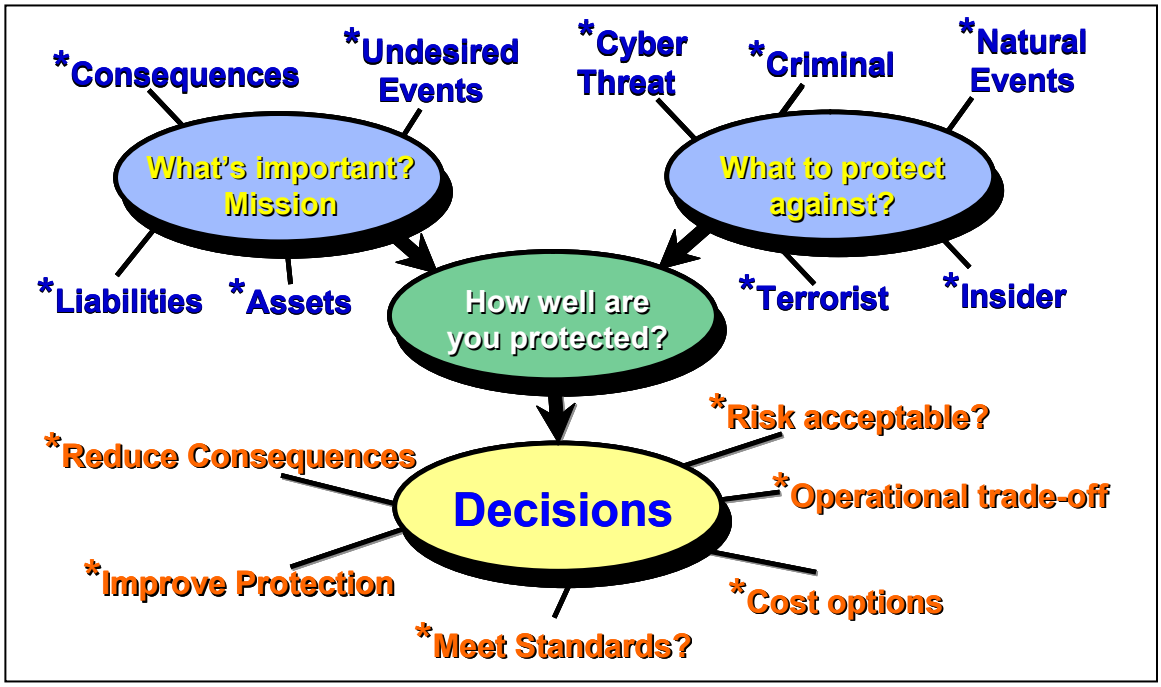

Figure 2. Decisions and Risk: How Much Is Enough?

1.5.4 Risk Assessment Methodology Process

The RAM process includes both risk assessment and risk management steps. The process begins with identifying the facility's overall mission and mission objectives. By understanding the mission and mission objectives, the facility can identify the mission critical operations, functions, and processes that affect the most important mission objectives. The RAM process requires a clear statement of the protection objectives for the facility. The RAM process determines the ability of the protection system to meet those protection objectives. Through a systematic analysis, the threat is defined, the undesired events are determined, and the associated critical assets are identified. Worst-case paths for the adversary to cause undesired events are postulated and analyzed. The existing security system effectiveness is evaluated on how well the PPS meets the defined protection objectives and system vulnerabilities are identified. The vulnerabilities identified are then used as input to create recommendations and propose upgrades to reduce risk from malevolent attacks. After vulnerability and consequence assessment steps are completed, if the relative estimated security risk is not acceptable the choice must be made to select more realistic requirements, mitigate consequences, and/or increase the effectiveness of the security system. The overarching decision that must be made by facility management is how much risk is acceptable and how much risk reduction is enough. Acceptable risk levels are defined and established by the senior decisions makers.

Figure 3 shows the process flow diagram used in the automated RAM prototype. The subsequent chapters will follow this process.

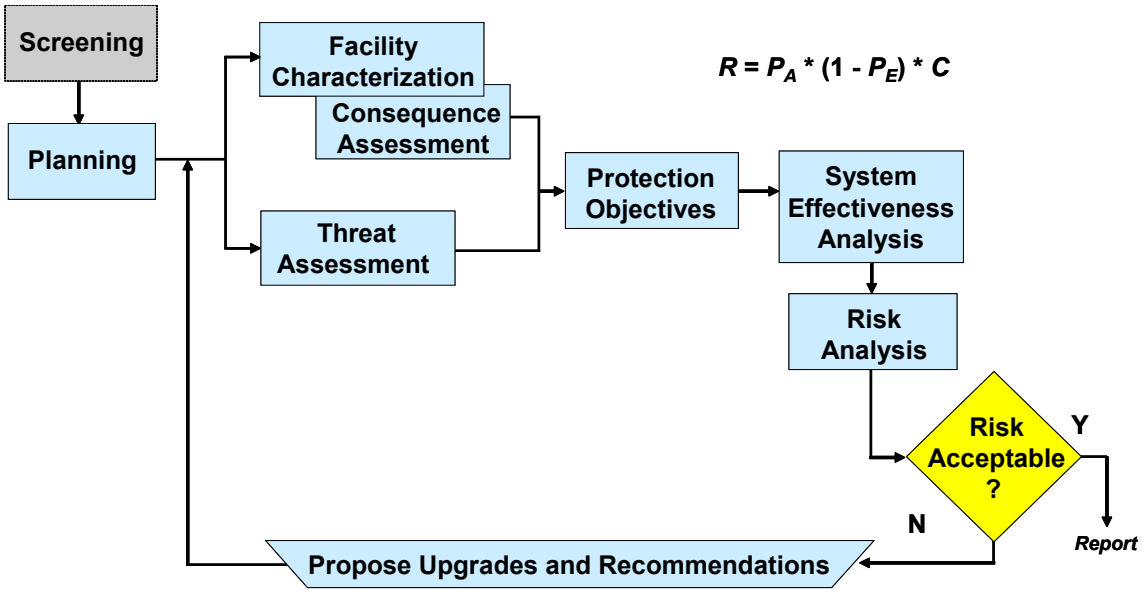

Figure 3. Risk Assessment Methodology Process Flow Diagram

The following is a brief description of the RAM process steps.

1. The automated RAM prototype tool includes an optional high-level screening step in which the user can identify and prioritize numerous facilities based on a defined set of consequence criteria.
2. The planning step provides documented assessment goals and project scope, identification of the team members and required tools or equipment, defined facility missions, and the facility's security concerns and undesired events.
3. The facility characterization step includes the collection of facility information, development of a site-specific fault tree, and the identification of potential targets.
4. In the consequence assessment step, the user applies or adapts a default consequence table or develops a new consequence table, lists the undesired events and the targets that if attacked may cause the undesired event, provides input for each of the consequence criteria to estimate the severity level for the undesired events.
5. The threat assessment step provides the user with the ability to identify both outsider and insider threats and define their motives, objectives, and capabilities. If sufficient information is available, the user can also develop an estimate for the threat potential, which considers the likelihood of attack.

6. The protective objectives step includes the identification of the site's objectives for the protection system. The effectiveness of the protection system is evaluated on how well these objectives can be met.
7. The system effectiveness step for the automated RAM prototype tool is a very comprehensive approach that is unique among the many risk-based tools available. The user first estimates the adversary's most likely strategy to cause the undesired event and affect the associated targets. An adversary path diagram is developed that includes a graphical representation of the facility including layers or areas and path elements between these layers or areas. Using an SNL physical security database derived from many years of testing and subject matter expert (SME) review, the safeguard attributes for each of the path elements are defined. A path analysis is then performed to estimate the effectiveness level of the protection system to meet its specified protection objectives. Finally, a list of possible security weaknesses or vulnerabilities is identified for the physical protection system (PPS) functions of detection, delay and response when system effectiveness is assessed to be low.
8. The probability that an adversary would cause an undesired event and associated consequence are used to estimate security risk value.
9. The risk assessment is now complete and decision makers must determine if the risk is acceptable.
10. If the risk is too high, then the user can identify possible risk reduction measures and evaluate their impact. Upgrade packages are developed and the changes in risk, possible costs and impacts to operations, schedule and other areas can be provided to the decision makers.
11. The final step in the process is the reporting of the assessment results and metrics to help support risk managers make decisions.

1.6 Requirements

Because the development of the automated prototype RAM tool was performed under SNL's LDRD program, there were no specific customers available to identify requirements. However, the basic criteria established as part of SNL's RAM process and also those identified in the revised NIPP (2006), Appendix 3A, were followed. Some of those criteria are listed below:

- *Documentation*: Must document information used and how it is applied to determine the risk components.
- *Objective*: Must support comparisons even performed by different users; must minimize impact of subjective judgments.
- *Defensible*: Must be technically sound with no errors or omissions.
- *Complete*: Must assess the three components of risk (threat, consequences, and vulnerability),
- *Threat Assessment*: Must identify and assess specific scenarios and incorporate threat likelihood estimates. (If likelihoods are unknown, use conditional risk values.)

- *Consequence Assessment*: Must identify specific scenarios, including worst credible cases, consider human and economic consequences, and consider protective or consequence mitigation measures.
- *Vulnerability Assessment*: Must account for protective measures and how they reduce the vulnerability, identify vulnerabilities, estimate mathematical probability of adversary success for each attack scenario, and consider how the PPS can detect, assess, delay, and respond to an adversary attack.

1.7 Tools

The automated prototype RAM tool methodology makes use of fault trees, consequence tables, threat spectrums, path analysis tools, and databases for physical protection elements. All tools employed are discussed in either the body of this report or in the attachments.

It is highly recommended that the user of the automated RAM prototype tool be trained in the fundamentals of SNL's RAMs. A security professional, trained and experienced in performance-based security system design and risk assessment, may be a desirable member of the assessment team. As a team is trained and becomes proficient at applying the process, they will be able to complete updates and analyze proposed system changes in the conceptual stage without such significant guidance.

2. AUTOMATED SECURITY RISK ASSESSMENT METHODOLOGY PROTOTYPE

2.1 Automated Risk Assessment Methodology Description

The process flow diagram for the automated RAM prototype tool was shown in Figure 3. RAM is both a risk assessment and a risk management tool. Figure 4 shows activities that must be performed for the different steps or modules and how the assessment and management functions link.

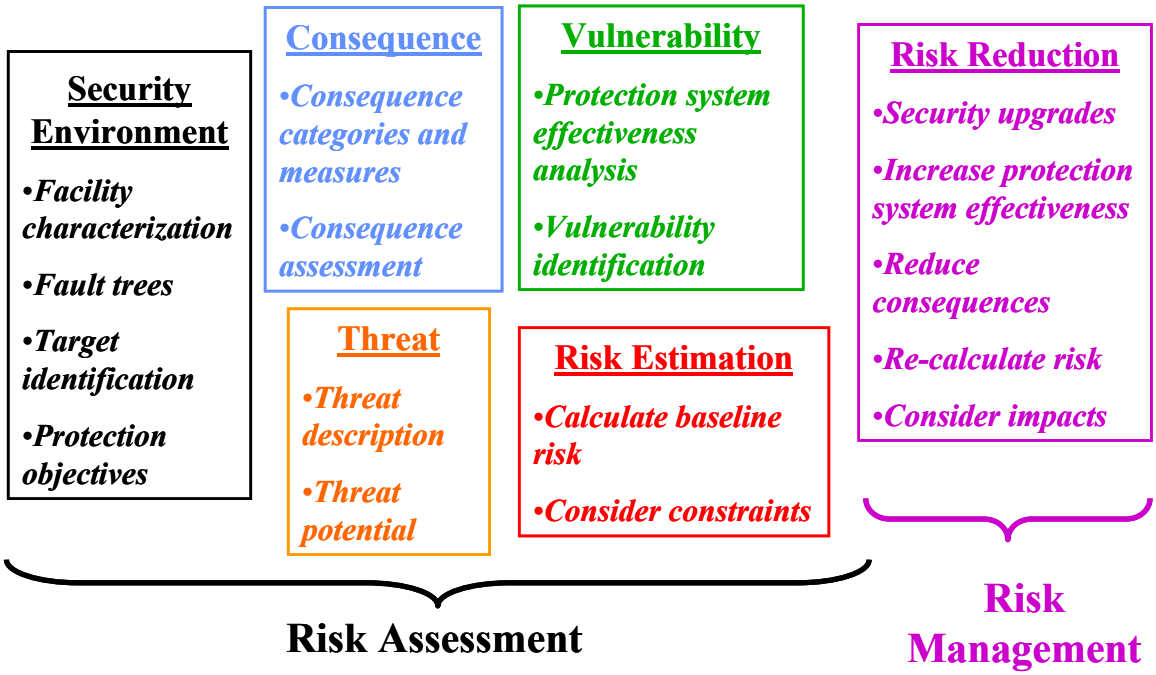

Figure 4. Major Modules Common to All Risk Assessment Methodologies

Specific CI sector requirements (e.g., adapted fault trees and consequence reference tables) or other capabilities (e.g., blast effects, chemical dispersion, economic calculator, and natural/non-malevolent threats) may be added to later versions of the automated RAM tool.

2.2 Computer/Software Description

The computer requirements and operating system for the automated prototype RAM tool software are a personal computer (PC)-based system using Microsoft Windows OS XP or higher. The automated prototype RAM tool has been designed as a stand-alone, single-user system, although it may be possible to interface the tool with other web-based sources (e.g., top-level

screening tools, Geographic Information System [GIS] data). The hardware requirements are a 1.0 GHz CPU and at least 1 GB of RAM. The software does not use any data encryption or data authentication algorithms, although if selected information were to be transferred to another system, the data may require some form of protection. No auxiliary or third-party software is required except Microsoft .NET Framework 2.0, Microsoft Visio (future versions may eliminate the need for this software), and Infragistics NetAdvantage 2006 CLR 2.0.

Figure 5 shows a very high-level representation of the structure of the automated prototype RAM tool software.

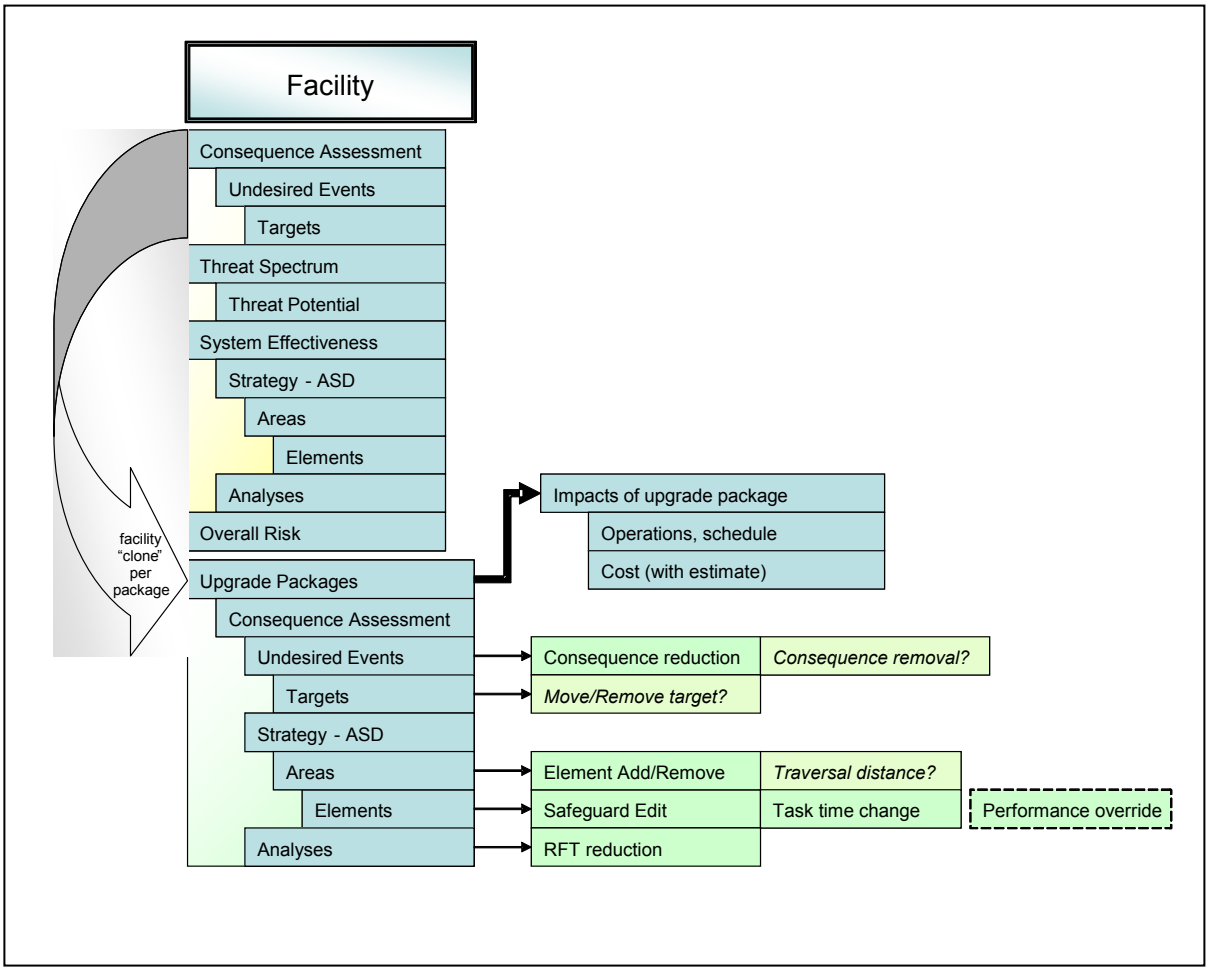

Figure 5. Structure for the Automated Prototype Risk Assessment Methodology Tool

Currently the only graphics software in the automated prototype RAM tool is Microsoft Visio, which is used for the review, development, or modification of the fault tree. The generic fault tree information would generally be applicable to a specific CI sector and should be considered and protected as sensitive information. Other SNL security risk or VA software tools have provided the ability to import GIS or other drawing files. Such a capability could be added in later versions.

The information in the automated prototype RAM tool is maintained in a data base. As part of the adversary path analysis performed in the vulnerability assessment module, performance data for specific physical protection elements are used. The data used in this tool are based on many years of testing to define the detection and delay values for the specific physical protection elements against specific adversary capabilities. The user can use these default values or override the specific safeguard data for the path elements if credible and realistic performance data so indicate.

2.3 Navigation Within the Automated Prototype Risk Assessment Methodology Tool

In the following sections, screen captures are shown for the various steps and activities in the automated prototype RAM tool. The user will proceed through the RAM process. All screens have the same basic structure with a *Utility Tree* on the left-hand side that shows the different screens and inputs that have been created. Items that would be listed in the *Utility Tree* include the facilities listed in the screening step, the undesired events, the targets for the undesired events, the threats, the scenarios and Adversary Sequence Diagram (ASD) layers and path elements, the analysis runs, and upgrade packages. The user can click on any area to go to the applicable screen. To the right of the *Utility Tree* and at the bottom left are two buttons (<< and >>) that allow the user to move back or forward to the previous or next screen. At the bottom right are two buttons (*Previous Node* and *Next Node*) that allow the user to move to the node before or after the current screen. Figure 6 is an example screen that shows these three ways to move within the tool. More information will be provided in the user's manual to be developed for later versions.

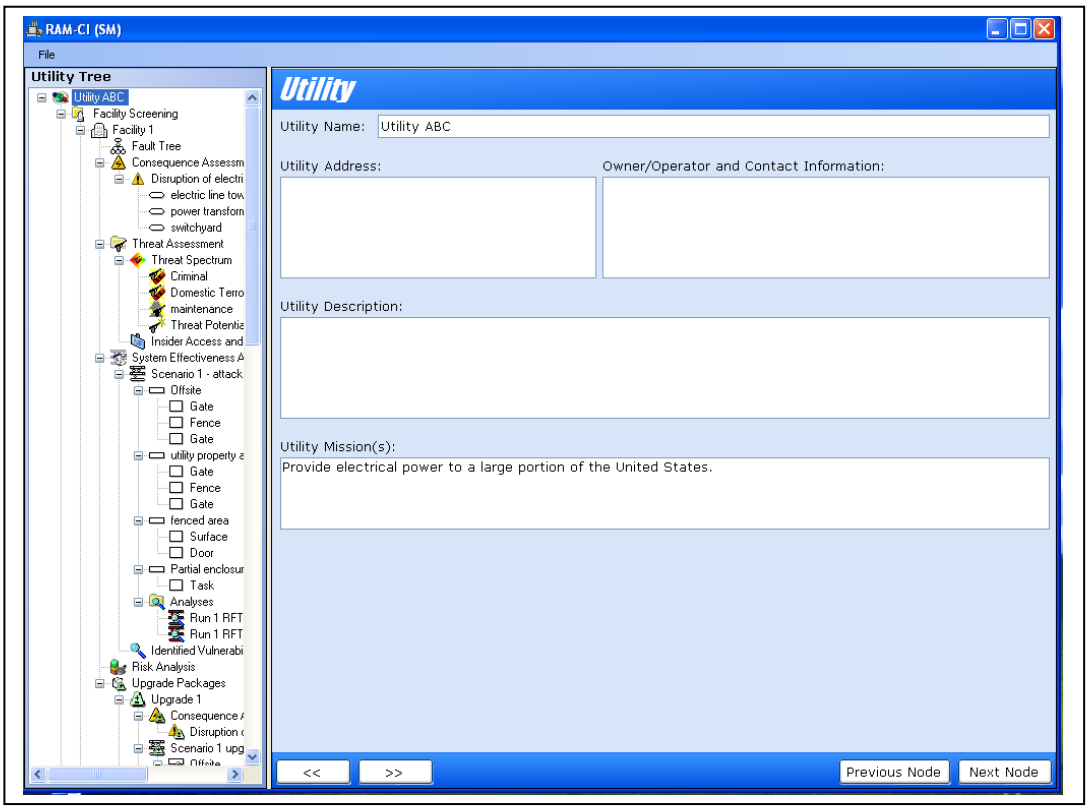

Figure 6. Example Screen Showing Navigation Options

More features and functions will be added to later versions of the automated RAM tool, including a short list of the key inputs at the beginning of each step, activities to be performed within the step, and the key outputs. Other functionalities will be added based on input from potential users. A user's manual and training course will be developed.

3. SCREENING

The top-level screening is used to identify those facilities with operations that if compromised would incur national or regional high-level damage to the infrastructure, public health, or the economy, as defined by the U.S. Department of Homeland Security (DHS). It could also be used by an owner or government agency with many different facilities in different locations. This screening process was designed to help the senior decision makers determine which facilities and assets were most important and should be evaluated first or in more detail. In the case of assets not considered critical by DHS definition but of high importance to the owner/operator, the owner/operator can choose to proceed to validate the security program, identify vulnerabilities, and support the internal decision-making process.

The first screen in the automated prototype RAM tool is the "*Utility*" screen, which enables the user to provide relevant information about the higher level organization (e.g., Utility ABC) that owns the facility. Figure 7 shows this screen.

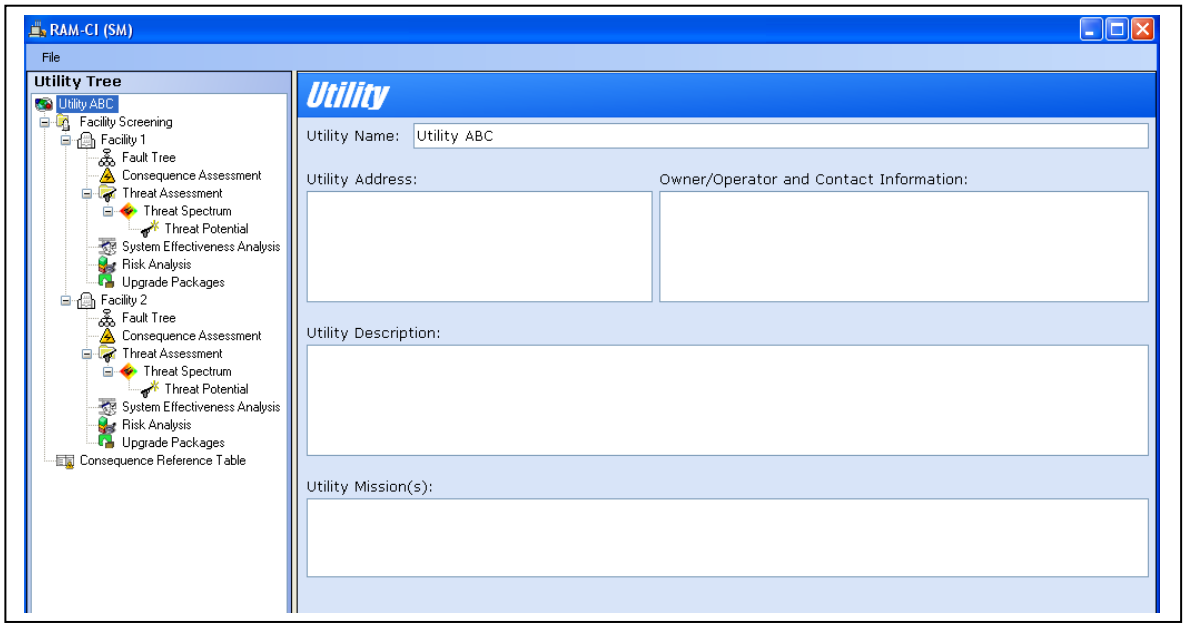

Figure 7. Screening Utility Description

After completing the input for the utility, the user can then identify the specific facilities for that utility and provide input on for the high-level screening criteria for the facilities. The criteria shown here are specific to an electric power utility. The consequence criteria may be different for other CI sectors. The criteria used for this screening step may or may not be the same criteria used later for the consequence assessment. Figure 8 shows the screen that lists the facilities. The *Utility Tree* on the left side of the screen would show each of the listed facilities. The initial screen for the *Facility Screening* would list one facility, named *New* facility, with the highest consequence level of very low and five occurrences. The user would click *Edit Facility* for the *New* facility and provide input on the facility, including the consequences of undesired events. The user would add each facility to be considered as part of the screening step and the required

information about each facility. Also in Figure 8 to the right of each facility would be the value of the highest consequence level and the number of occurrences. The automated RAM prototype tool does not prioritize the facilities, but later versions will perform prioritization. Figure 9 shows the input screen for Facility 2 and the input for the five screening consequence criteria.

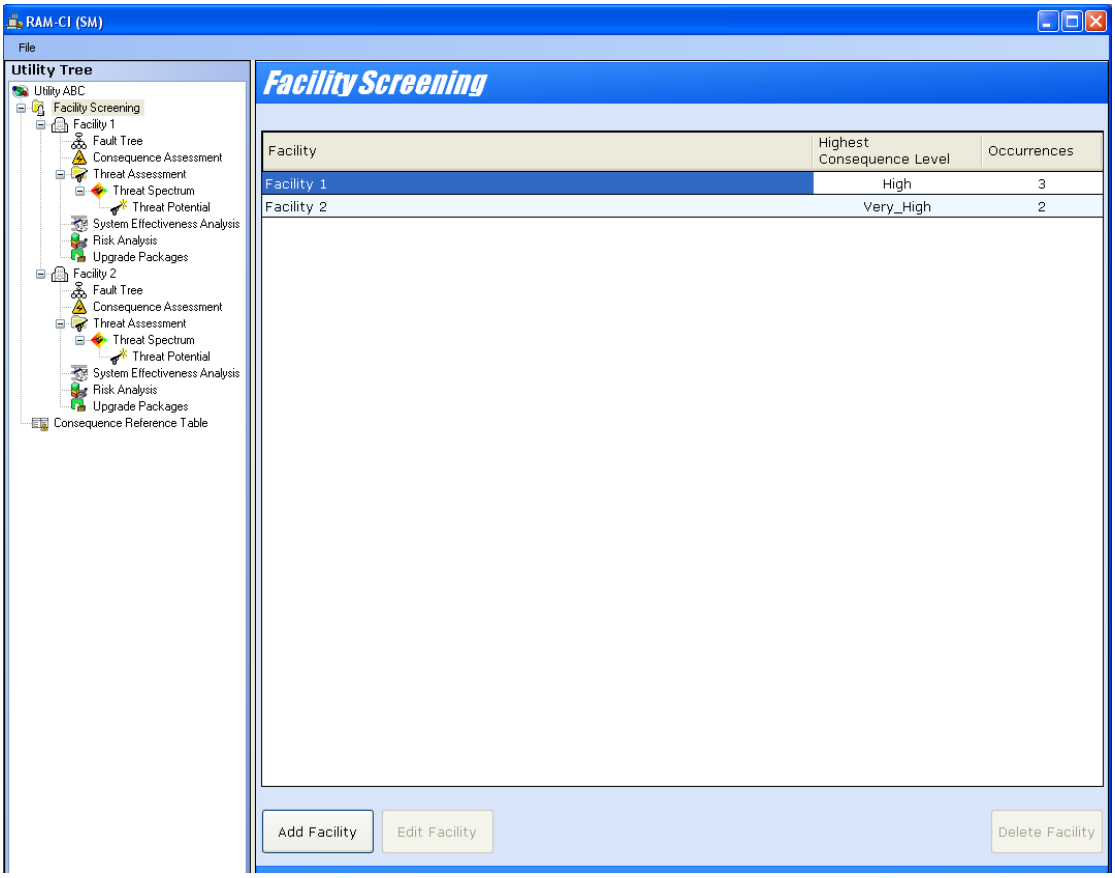

Figure 8. List of Facilities and Screening Results

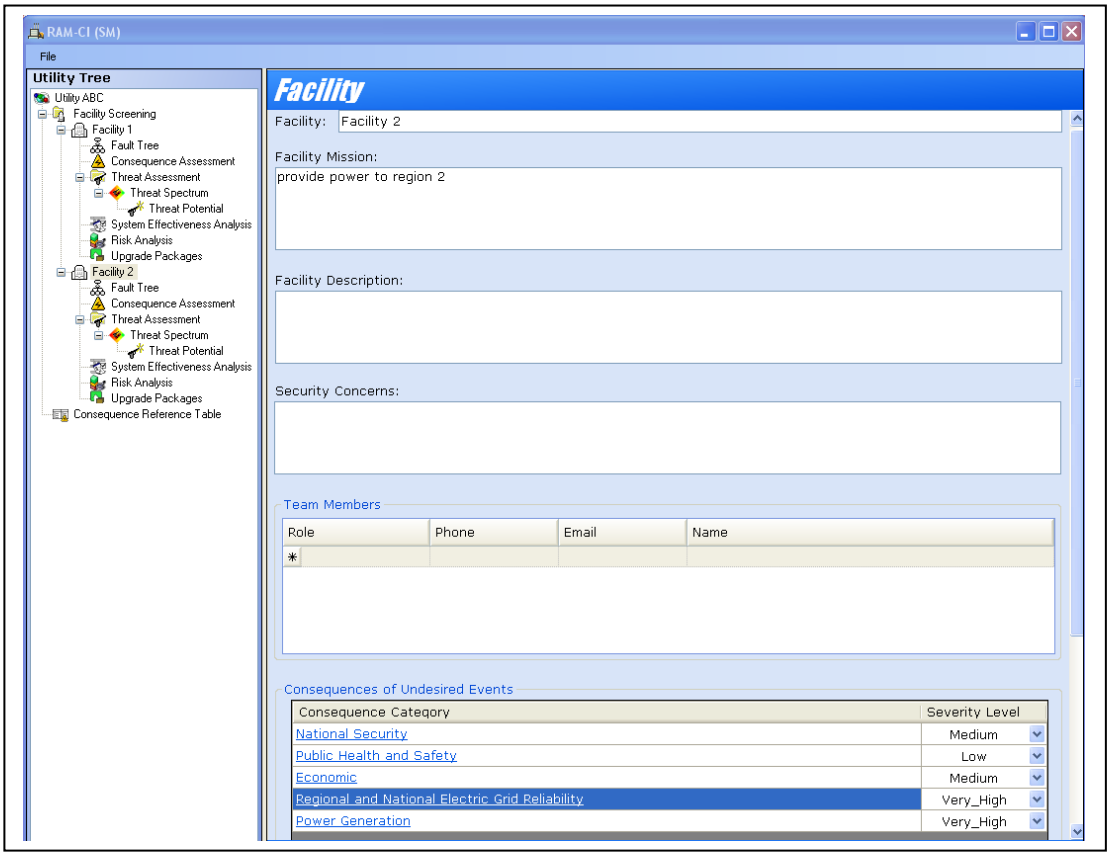

Figure 9. Input for Facility Description and Screening Criteria

The screening step provides an organization with the ability to list all their facilities. This step allows senior managers to prioritize the numerous sites or facilities within a certain area and identify those that may require a more comprehensive security risk assessment. From this step an organization can develop a prioritized list of facilities based on the input for the defined screening consequence criteria. The screening step is not necessary for a single facility, but the user must still enter the facility and the requisite information to continue with the automated prototype RAM tool assessment.

4. PLANNING

The next step in automated prototype RAM tool process is the planning step. In this step specific project information can be recorded. Later versions of the automated RAM tool will have input screens for some of the planning-related areas.

4.1 Management Roles and Responsibilities

Management's input is necessary in the initial assessment phase of the automated prototype RAM tool. A team of facility employees must be identified and assigned to participate in the process from start to finish. This assessment team should consist of at least one management-level representative, one or two highly experienced and knowledgeable senior staff members, a Supervisory Control and Data Acquisition (SCADA) or process control expert, and several operator-level employees. If existing facility personnel do not have experience with risk management and security assessment, the user should consider hiring or acquiring this expertise for the initial assessment effort. It is highly recommended that the user secure the agreement of the facility management team on mission objectives, prioritization of undesired events (and assets), the defined threat, and protection objectives before proceeding. This information is critical to the process and will drive the outcome of all remaining steps.

In the final stages of the assessment, the decision makers will be presented with a comprehensive draft report that characterizes the risk spectrum. The draft report includes many tables, details, and recommendations that rank the relative risks currently faced by the facility. This report should be reviewed by the appropriate management and staff and then critiqued for accuracy. This feedback is then incorporated into the final report.

The management team should oversee the development and implementation of an action plan based on the risks described in the final report. Management must make several major decisions about the approach and risk mitigation philosophy prior to the development of the final implementation plan. Future versions of the automated RAM tool may identify those areas within the RAM process that require management approval (e.g., adding text boxes for dated and signed comments).

4.2 Project Management

A security risk analysis undertaken for a CI facility is a limited-time project. Using project planning concepts to plan the analysis will provide a great deal of assistance to the project leader and the assessment team by ensuring that essential work is conducted and management's requirements and expectations are met. Planning is an important part of a successful analysis. The amount of time and resources the user spends will depend on the size and complexity of the analysis and the complexity of the facility itself. Sufficient time spent up front determining and documenting management's expectations is a requirement for a successful analysis.

4.3 Defining Protection Objectives

The automated prototype RAM tool provides a systematic structure for estimating relative levels of risk based on the defined threats. This information will be used for decision-making in implementing system upgrades to reduce risks deemed unacceptable to the facility. Early in the assessment process, the user should begin the discussion of possible protection goals for the security system with the facility management. Protection objectives will be further developed later after undesired events have been defined and the threats have been identified and characterized. Some example protection objectives that the facility may consider are:

1. Deter the adversary.
2. Prevent the adversary from causing undesired event(s) (i.e., disrupting the mission objectives).
3. Detect the adversary and mitigate the consequences of the attack.
4. Protect employees.
5. Collect information for later prosecution.
6. Increase redundancy in the operations.

Note that only objectives 2, 3, 4, 6, and 7 actually reduce the risk value by either increasing protection system effectiveness or reducing consequences in the risk equation. Objective 5 may reduce risk in the future by reducing the incidence, but this likelihood is difficult to predict and measure. Deterrents may work, but the ability to lower the risk is unknown and hard to quantify without the event actually happening.

Each increased level of protection has an associated cost; therefore protection goals may be resource-constrained. It is important to be specific and refer to the defined goals throughout the security risk assessment process, particularly when discussing upgrades. The user must constantly review the protection goals of the assessment. To reduce the risk, it is strongly recommended to improve the system effectiveness and/or design consequence mitigation measures that will stop an adversary from achieving their objective (i.e., prevent the undesired event) with a high likelihood of success. The facility will need to decide how well the PPS performs in accomplishing their protection objectives.

5. FACILITY CHARACTERIZATION

Facility characterization is the next step in the automated prototype RAM tool process. A significant part of a risk assessment is the site and asset characterizations, which consist of identifying existing protection features at a site or facility. Characterization includes the collection and distillation of data and documentation. For malevolent threats, one of the goals of facility characterization is to identify PPS components in the functional areas of detection, delay, and response and to gather sufficient data to estimate component performance against the defined malevolent threats. The PPS is characterized at the component and system levels; vulnerabilities to defeat by the defined threat are documented. Knowledge of previous safety analyses, process hazards analyses, or other studies are valuable. Data collection is the core of effective site and asset characterization; accurate data are the basis for conducting a reliable analysis of the ability of the protection system to meet its defined protection objectives.

For future releases of the automated RAM tool, various data collection screens will be available to the user to record information collected on the facility. The following sections provide a brief description of the different activities that would take place in this step.

5.1 Preparation for Site Characterization

It is absolutely essential that a site be fully understood in terms of constraints, performance parameters, operations, and the circumstances in which it exists. Information and data about all aspects must be obtained and reviewed. When collecting information a variety of sources should be used including drawings, policies and procedures, tours, briefings, reference material, and personnel interviews. The preparation phase for site characterization allows the facility to assess the operations from a systems perspective.

5.2 Risk Assessment Scope

The user must define the scope of the analysis for the facility. The user should review the system process diagrams, interview the facility operators and others who understand in detail how the system operates, review emergency operations plans, and consider the interdependencies with other critical infrastructures to help define the boundaries of the assessment (i.e., the user needs to define what will and will not be included in the analysis). The user will want to assess the ability of an adversary to cause disruptions using an interdependent infrastructure.

5.3 Security System, Policies, and Procedures

Part of the facilities characterization step includes documenting the PPS. This also includes an understanding of written and unwritten security policies and procedures for the facility. The presence, or absence, of well-documented, consistently applied, and thoroughly trained policies and procedures usually are an indicator of the organizational culture.

5.4 Regulatory Requirements

It is important to understand the nature of all regulations a facility may be expected or required to meet. In some cases the regulating organizations may have established standards and/or guidelines in the areas of physical and cyber protection.

5.5 Legal Issues

A thorough understanding of the legal issues to be considered when designing and assessing and upgrading a protection system should be gained. Legal issues can cover such areas as liability, employment practices, proper training for the response force, and deadly use of force by response personnel. The last item is particularly important with regard to the ability of any protective or response force being able to protect the facility, its assets, and the public.

5.6 Safety Considerations

Safety and security do not always have the same goals, although they are complementary functions. Both safety and security hold as goals to protect life, property, and business continuity. Both attempt to minimize vulnerabilities at the facility. Security events are caused by deliberate malevolent acts whereas safety events are random non-malevolent acts and natural events. Safety features and security features must be well integrated so that the protection system will be effective in normal, abnormal, and malevolent conditions. Major areas where security and safety intersect are in building and property area access and egress and emergency response (e.g., fire).

5.7 Generic Undesired Event Fault Tree

The user must understand the processes, functions, and/or operations that are in place to meet the facility's mission objectives, as these are the starting point in the fault tree analysis described in this section. The fault trees are developed to describe the entire system, at least at a high level. The main purpose of this high-level description is to identify all potential undesired events that can occur at the facility. The fault tree can be developed in more detail as necessary, allowing for deeper analysis.

The fault tree shown in Figure 10 illustrates the top levels for an undesired event for disruption of a facility's mission. The fault tree may have many different branches including those for malevolent, natural, or non-malevolent human-caused events. In addition to physical events, SCADA/process control events would also be included in the event fault tree if applicable. Sector-specific fault trees would be part of the sector-specific application for the automated prototype RAM tool. The user has the ability to modify the generic fault tree to fit the specific facility. Once completed, the site-specific fault tree should identify all undesired events and thus include the critical assets (or collection of critical assets) that must be protected to prevent the topmost undesired events on the fault tree from occurring (e.g., loss of mission). The site-specific fault tree can be used to model the relationship between mission and critical assets for malevolent threats. More information on fault trees is available in Attachment A.

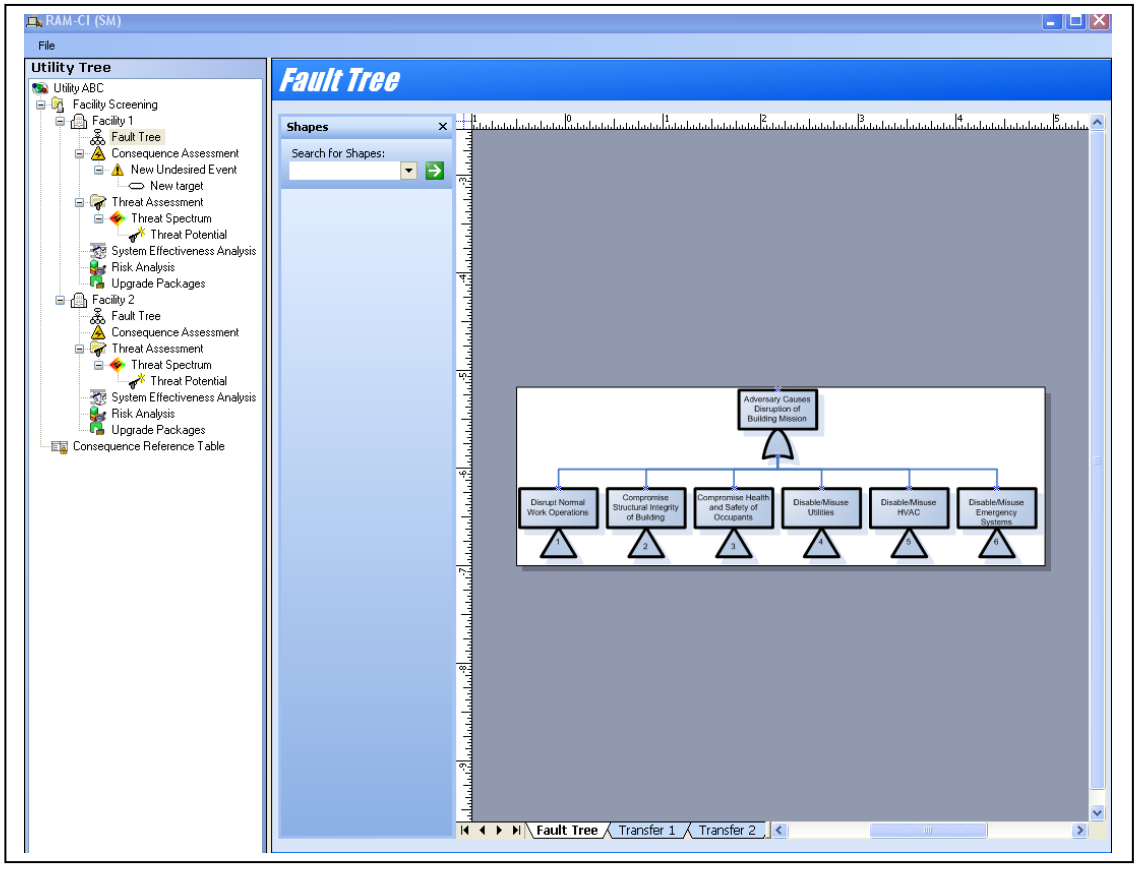

Figure 10. Example Fault Tree Screen

5.8 Asset Identification

Asset identification is the process of identifying assets and specific locations to be protected that if damaged or disabled would cause the topmost undesired events in the fault tree. In the automated prototype RAM tool, the specific targets will be linked to the identified undesired events. This will be shown as part of the consequence assessment step.

6. CONSEQUENCE ASSESSMENT

It is not possible or practical to protect all the assets owned by a facility. The criteria for selecting assets to protect will depend on the need to avoid undesired events and the capabilities of the adversary. The consequence assessment process uses the consequence of the undesired event to help determine which assets (or suite of assets) are at greatest risk relative to all the assets owned by the facility. In the consequence assessment step the user reviews and edits a consequence table, identifies undesired events using information from the fault tree, identifies potential targets that if attacked by an adversary could result in the undesired event(s), and determines the possible consequences for each of the undesired events.

6.1 Consequence Assessment

The first screen in the consequence assessment step provides a summary of any input developed from previous input. If this is the initial analysis, no consequence table will exist and the user will be directed to create a consequence reference table.

6.1.1 Consequence Measures

A consequence assessment determines a qualitative consequence value (i.e., very high, high, medium, low, or very low) for all undesired events identified during the assessment. If values for some of the undesired events are not readily available, expert opinion of the assessment team or other subject-matter experts (SMEs) can be used. Each undesired event can have several types of consequences and all must be captured. Once the consequence matrix has been established, an appropriate consequence value is assigned to each undesired event. The following consequence measures may be used for the consequence assessment:

- Loss of life,
- Serious injury,
- Loss of critical mission/operations,
- Duration of loss,
- Economic loss (to the facility, to the community),
- Psychological impact,
- National security impact, and
- Other as specified by the facility.

6.1.2 Consequence Reference Table

The screen in Figure 11 shows an example of a consequence reference table. For the automated prototype RAM tool, there is no default table available. (For certain CI sectors a default table may be provided.) The user creates the table by adding the different consequence measures, identifying the unit of measure (e.g., number of people killed, economic impact, or, in the case of qualitative measures, may just indicate *qual*), and then the values for the five severity levels (very low to very high). For quantitative values the range can be from 0 to any reasonable number. For qualitative values the range is from 1 to 5.

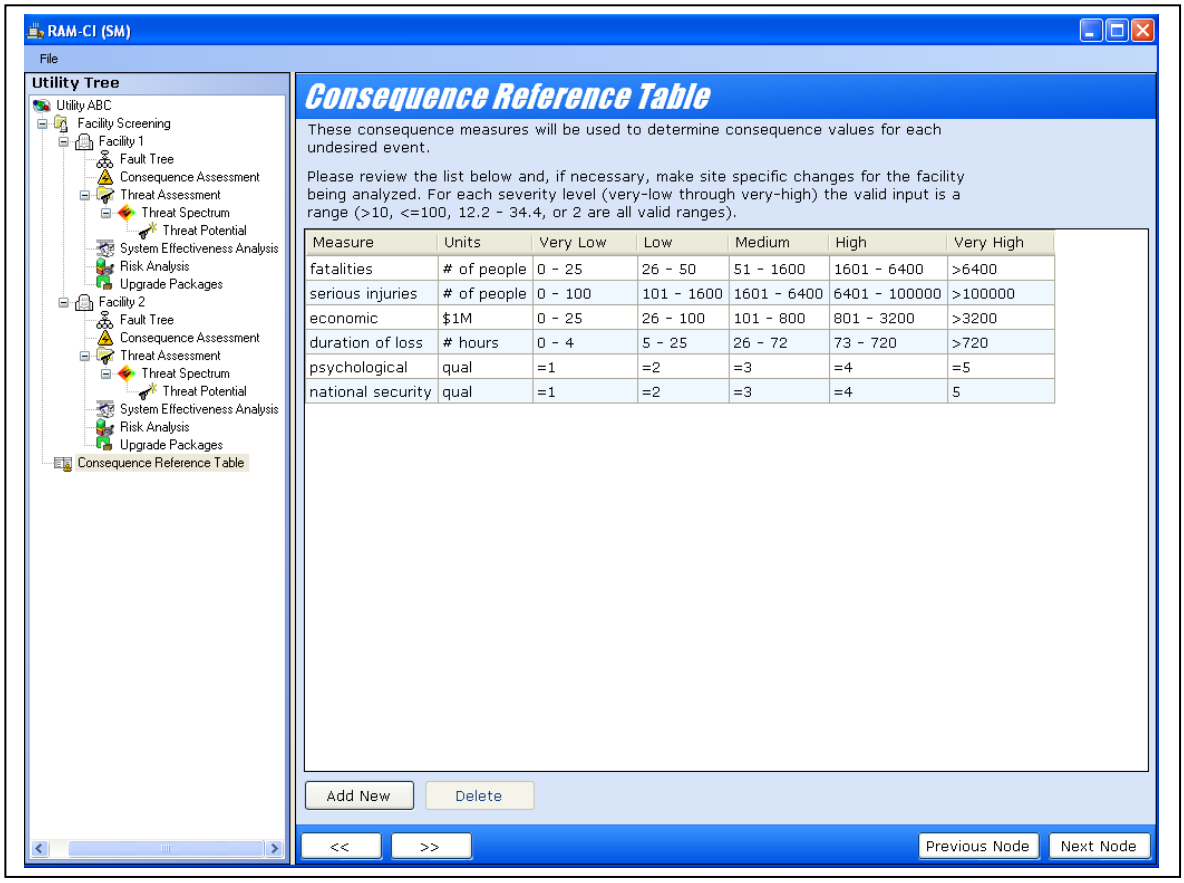

Figure 11. Consequence Reference Tables

6.2 Defining Undesired Events

The criteria for selecting assets to protect depend on the undesired events to be prevented and the associated level of consequence.

Consequence of the loss can cover a spectrum, from the unacceptable (e.g., disabling the entire facility) to the relatively less severe (e.g., theft of laptops). The process of consequence assessment uses asset identification and consequence of the undesired event to help determine which assets and asset locations should be protected and to what extent. The site-specific fault tree should be relied on to identify the undesired events (and assets) to be considered in the analysis.

Figure 12 shows the screen for the undesired event, related targets, and consequence assessment for that undesired event. The user reviews the fault tree and selects the top-level undesired event (or critical missions to be protected). The user then identifies the potential targets that if attacked by an adversary could result in the undesired event. This could be only a few possible targets or could be many possible targets in different locations. As part of the system effectiveness step, a path analysis will be performed for the undesired event, target, and threat.

The user will then determine the severity level of each consequence measure for a successful adversary attack by providing an estimate for the consequence measure. The user may use SME input or perform very specific analyses (e.g., blast effects, chemical dispersion, economic calculator) to determine these values.

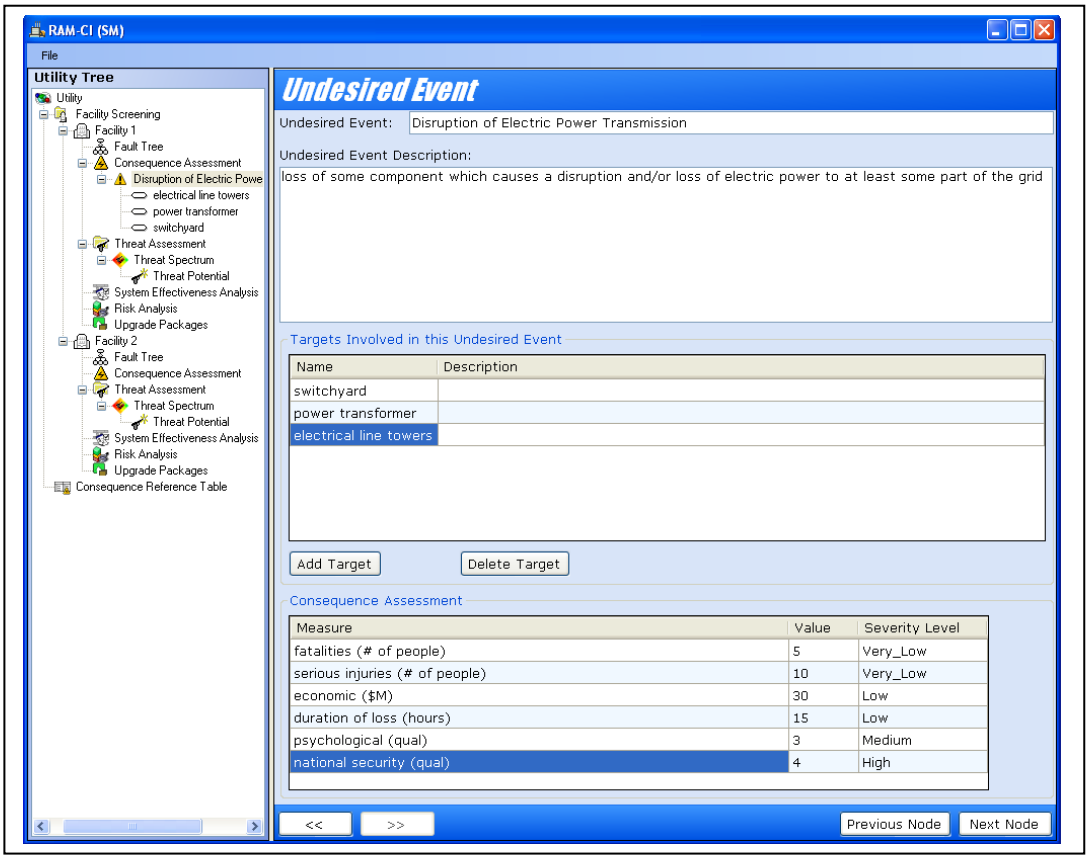

Figure 12. Undesired Event Screen

Figure 13 shows the summary screen for the consequence assessment. An overall consequence value is provided along with the values for the different consequence measures. If another undesired event and set of targets is developed by the user, the results for this undesired event and any others will be provided. The results from the consequence assessment will be used in the risk analysis step.

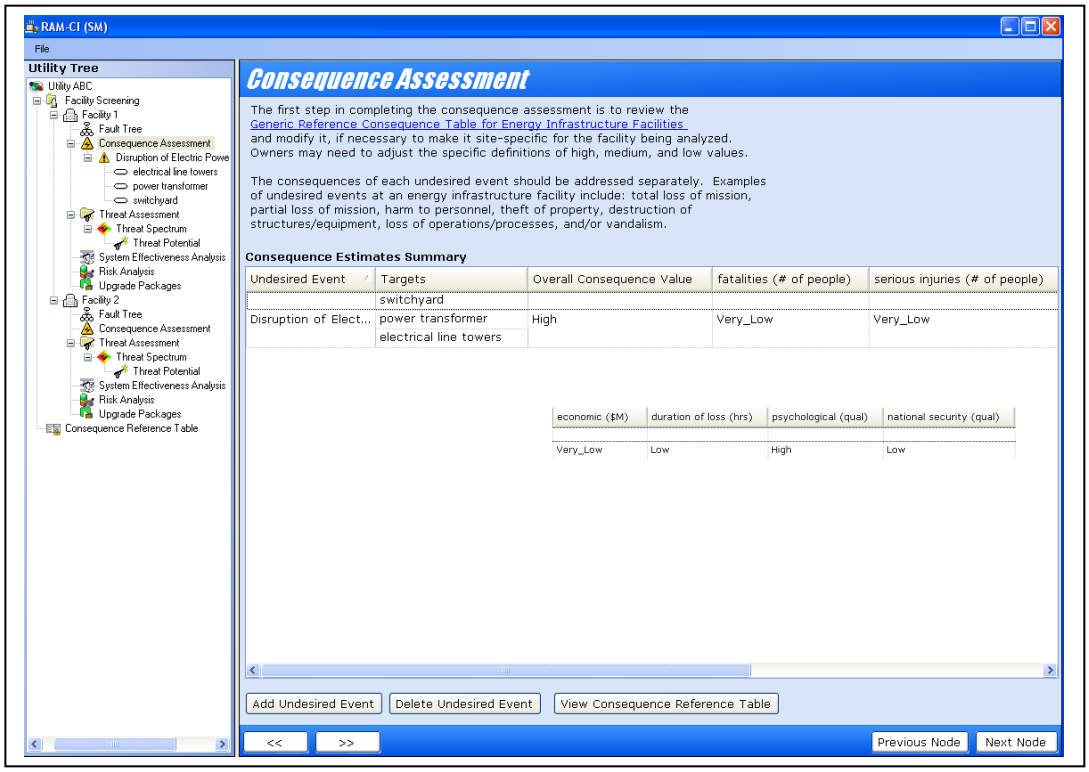

Figure 13. Consequence Summary

7. THREAT ASSESSMENT

The threat to a facility must be defined as part of determining the protection objectives: i.e., what does the site need to protect (target or targets) and from whom (threat)? The inputs to the threat assessment process are threat data from a variety of sources (local, regional, and national law enforcement or intelligence agencies). The user provides input that describes the characteristics of the adversary groups identified. For the malevolent threat, the description includes information about the potential actions, motivations, attributes, and physical capabilities of the potential adversaries. The threat definition for each facility may be comprised of a threat spectrum that includes all credible threats (outsider and insider).

7.1 Threat Characterization for the Malevolent Threat

A threat assessment helps identify and describe the types of adversaries (malevolent persons or groups) that may try to prevent a facility from performing one or more of its mission objectives. For the automated prototype RAM tool a generic threat spectrum is provided which can be the user for their facility. The choice of a threat spectrum is an important part of the assessment as it greatly impacts the results of the system effectiveness and vulnerability components of the risk analyses. The threat spectrum, which is comprised of the numbers of adversaries, their capabilities, and their tools, should be carefully researched and discussed before undertaking the assessment. During the risk analysis, the existing security systems are evaluated against the defined threats to determine their effectiveness at preventing the undesired events and to identify the vulnerabilities.

Collecting threat information, organizing it, evaluating it, and using it to determine which threat a particular facility will use for its analysis forms the basis of the threat assessment. This threat information will be used later to help develop adversary strategies and scenarios.

7.2 Defined Malevolent Threat Spectrum

The user must acknowledge that extremely high threat levels (e.g., very large improvised explosive devices, a large well-armed assault force) exist and without allocating enormous amounts of resources, there is little a facility can do to defeat these adversaries or prevent them from carrying out their objectives. However, it is strongly recommended that the facility complete the assessment with a terrorist-level threat to understand system vulnerabilities to high-level threats. Considering only lower-level threats may result in exclusion of high-consequence assets that could have devastating impacts to the facility if compromised.

After the threat information needed is identified, collected, and organized, some of the outsider and insider threats will be selected to represent the site-specific threat spectrum. It defines the credible attributes and characteristics of potential insider and outsider adversaries who might attempt malevolent actions against a facility. It is the maximum site-specific threat against which a facility will evaluate and design its protection systems. The site-specific threat spectrum should be carefully reviewed, discussed, and supported by management before undertaking the detailed system effectiveness and vulnerability analysis. It is also highly recommended that the user utilize the expertise of a specialist (local law enforcement, military agency, Federal Bureau

of Investigation, Environmental Protection Agency, Department of Transportation, etc.) to help formalize the site-specific threat spectrum.

For these reasons, the selection of the site-specific threat spectrum is a management-involved decision and may or may not reflect the actual threat to the site. This in no way diminishes the importance of developing the site-specific threat spectrum, but recognizes that real constraints may prevent a facility from achieving the level of security desired.

The first screen in the threat assessment step for the automated tool provides the user with the opportunity to select from a list of adversary groups for which default capabilities have been identified. Figure 14 shows this screen and, as an example, the selection of three different threat groups: ecological terrorist, criminal, and insider.

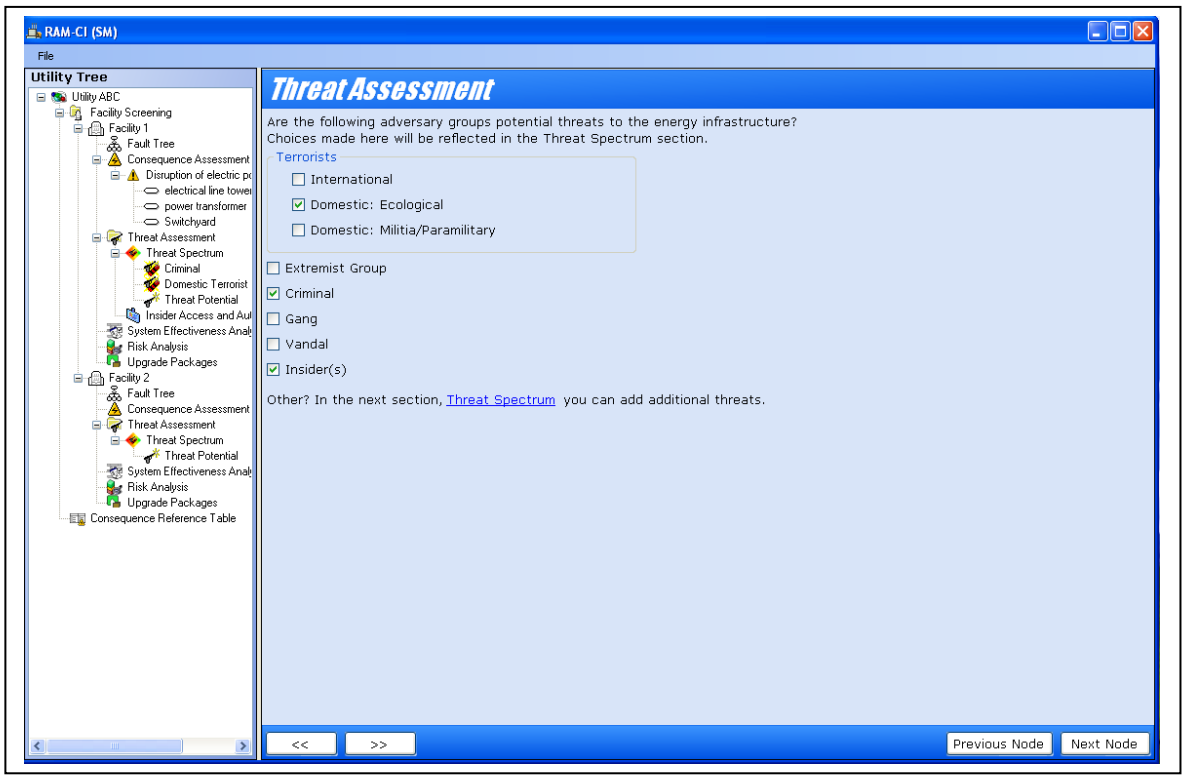

Figure 14. Selection of an Adversary Group

The user has the options to add additional threats, add information on the existing threat groups, or modify the attributes of identified threats. Figure 15 shows the screen for providing input for a specific threat group. The number and weapons of the adversaries are important when considering the success of the adversary in interactions with possible response forces (e.g., probability of neutralization [P_N]). The equipment and vehicles used by the adversaries are important when estimating the probability of interruption (P_I), which is accomplished in the system effectiveness analysis step (measuring the ability of the PPS to detect, delay, and respond).

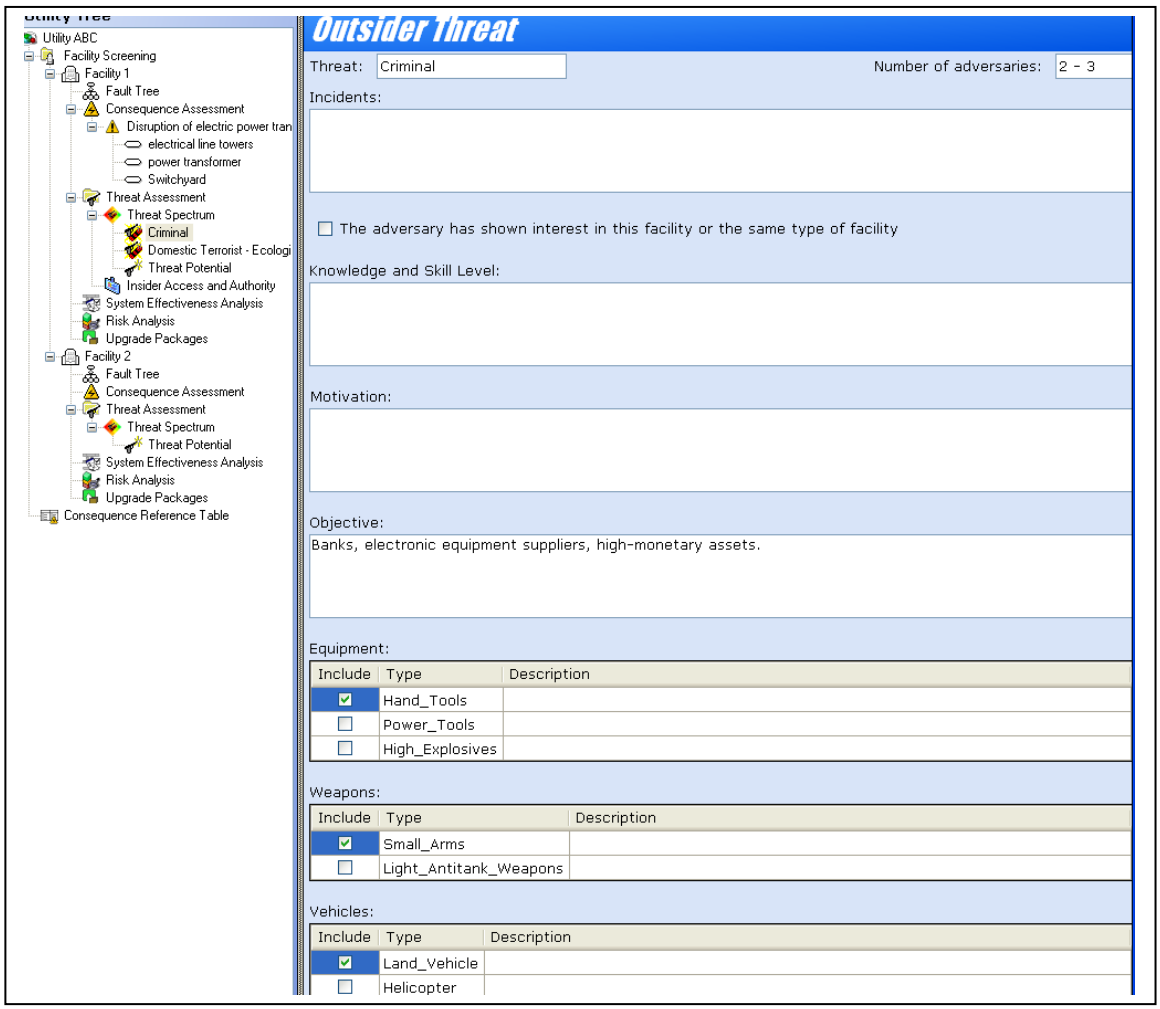

Figure 15. Input for Threat Group Attributes

The automated prototype RAM tool provides the user with the ability to identify specific job positions for personnel with authorized access and to define their authority level, their access to potential target location, and their access to security systems. Figure 16 shows an example of a list of personnel with authorized access. From this list the user may identify one or more groups to evaluate for possible insider adversary scenarios. Later releases of the automated RAM tool will allow the user to prioritize the insider positions and provide additional guidance in analyzing the insider threat.

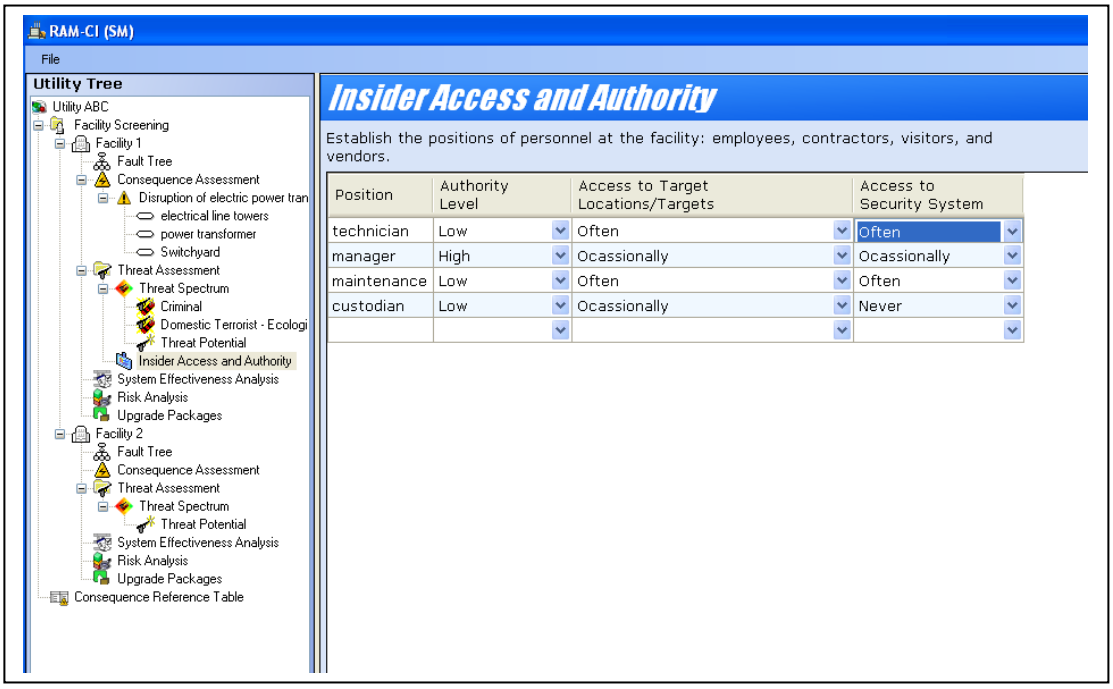

Figure 16. Insider Identification and Defining Access and Authority

Just as for the outsider adversary groups, the user has the ability to use a screen like that shown in Figure 15 to define the attributes of each of the insiders. After providing input for the outsider groups and/or insider, a summary is available showing the defined site-specific threat spectrum that will be used for the analysis (Figure 17).

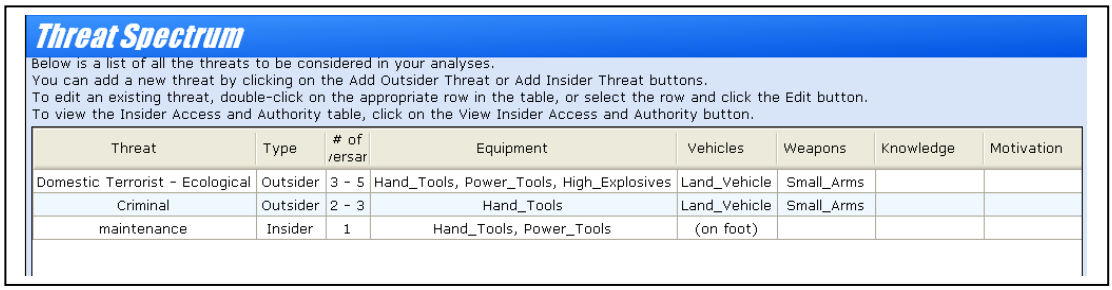

Figure 17. User-defined Threat Spectrum

7.3 Threat Potential

The automated prototype RAM tool allows the user to select that the attack will occur (e.g,. use conditional risk) or an option to calculate a threat potential that would estimate a qualitative value for the likelihood of attack term. Figure 18 shows one of the screens used as part of the determination of the threat potential. The user would identify the threat being considered and the undesired event. The user would then answer a series of questions on capability, historic interest, historic attacks, current interest in the site, current surveillance, documented threats, consequence, ideology, and ease of attack. Based on the responses to these questions, a threat potential is estimated for that specific threat. Threat potential has been used for prioritizing assets based on threat by some users of the manual RAM process.

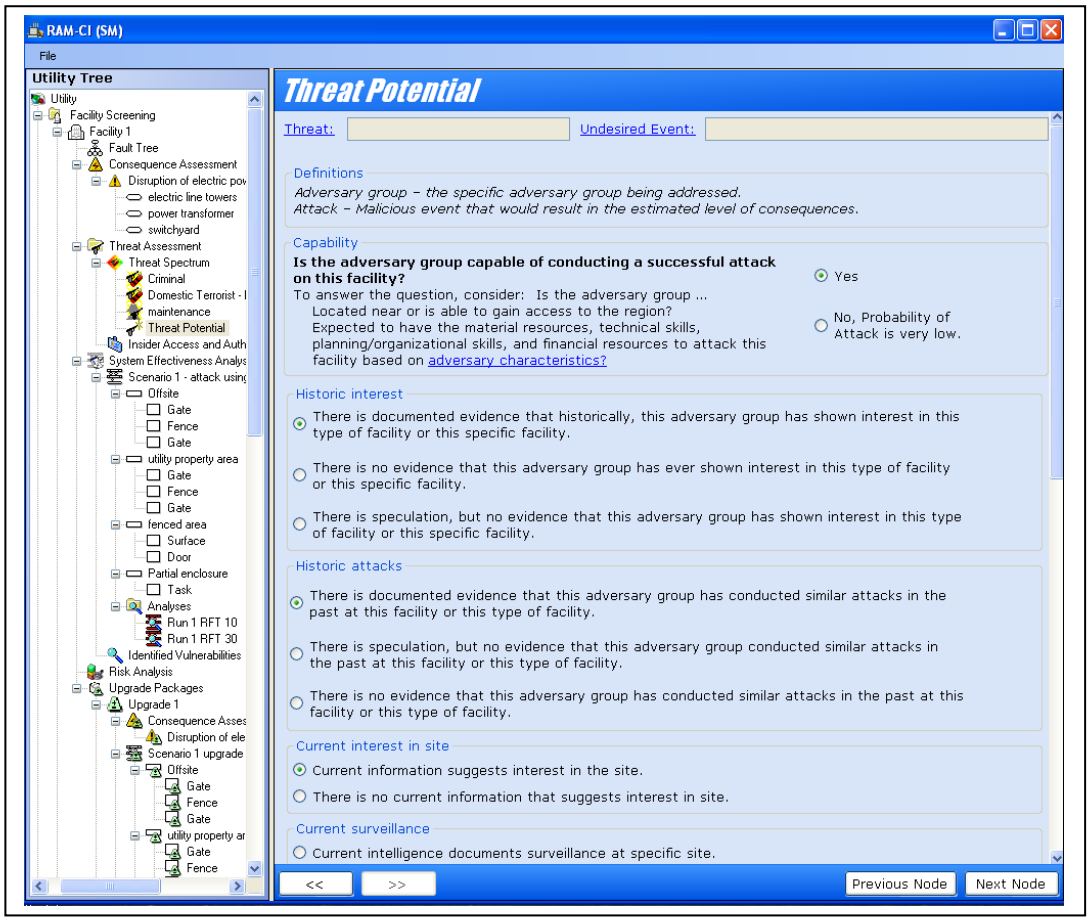

Figure 18. Estimate of Threat Potential

8. SYSTEM EFFECTIVENESS

Analyzing how well the protection system can protect against specific threats is part of the system effectiveness analysis. If the protection system effectiveness is judged to be low, specific vulnerabilities can be identified. The elements of system effectiveness (and vulnerability) analysis include:

- Understanding the performance characteristics of the protection system.
- Determining the attack scenario most likely to achieve the adversary's objective.
- Estimating system effectiveness against the defined threat based on worst-case attack scenarios.
- Identifying protection system vulnerabilities.

8.1 System Effectiveness Analysis Process for the Malevolent Threat

After the site survey and existing PPS is fully characterized (i.e., all performance data have been collected, organized, and evaluated), the next step is to define the scope of the system effectiveness analysis. The resources required to conduct the analysis are usually limited and the efforts should be focused on the events of significance. Combining the information previously gathered on the threat and consequences of the undesired events should lead the user to identify general malevolent activities that are of most concern. These malevolent activities primarily include those for which the defined threat has motivation and capability as well as for which the potential consequences are unacceptable. This limits the number of analyses required to evaluate the system effectively. The system effectiveness analysis usually focuses first on the highest level consequence events that are within the adversary's capability; however, all activities of significant concern should ultimately be addressed if sufficient resources are available. Initial observations and judgments about protection system vulnerabilities may also aid in selection of the malevolent activities to be analyzed. The site-specific fault tree should be reviewed to identify top-most undesired events and potential adversary strategies.

The system effectiveness results are based on analysis of the physical paths that adversaries can follow to accomplish the objective. The protection features (detection and delay) and safeguards (countermeasures) along the paths are important in determining the adversary attack scenario most likely to succeed. There are many possible combinations of ways to get to a target location and damage or destroy the asset(s); therefore all possible adversary paths should be considered.

The analysis process is based on developing and evaluating scenarios in which the adversary has a reasonable likelihood of being successful in causing the undesired events. The following are the steps leading to the determination of system effectiveness (and ultimately system vulnerability):

1. Define the adversary strategy and undesired events (refer to site-specific fault tree).

2. Build an ASD and identify all countermeasures in the system to protect against these adversary actions.

3. Incorporate the effectiveness values of each protection layer and path element in protecting against each defined threat.

4. Identify the most vulnerable paths by analyzing the effectiveness of detection and delay along the paths.

5. Develop potentially worst-case scenarios, evaluate response effectiveness, and determine system effectiveness.

6. Summarize system effectiveness (vulnerability) values for the worst-case scenarios for all threat and undesired events (assets) under consideration.

After completing the system effectiveness analysis, the user will examine the paths and scenarios with lower-than-desired system effectiveness (i.e., high vulnerability). The goal is to identify protection elements and system weaknesses to be considered in later discussions for protection system improvements.

Adversary objectives are identified for use in considering paths that the adversary could follow to access critical assets and cause undesired events. Considering PPS weaknesses and facility states (e.g., shut-down, middle of the night, holidays) and then considering the worst consequences that the adversary might cause by having access to the critical asset(s), the user derives the most potentially successful adversary strategy. The objective is a simple statement of what the defined threat is going to do to the asset(s) and roughly how it will be done (intention). It need not be path-specific because the next step determines the worst path.

In the automated RAM tool the user will be asked to identify and describe an adversary strategy. This will include selecting an undesired event and identifying the potential targets and the threats, as shown in Figure 19. Some targets may be more attractive to certain adversaries. The user has options to select multiple targets and/or threats and this may result in the need for more than one ASD.

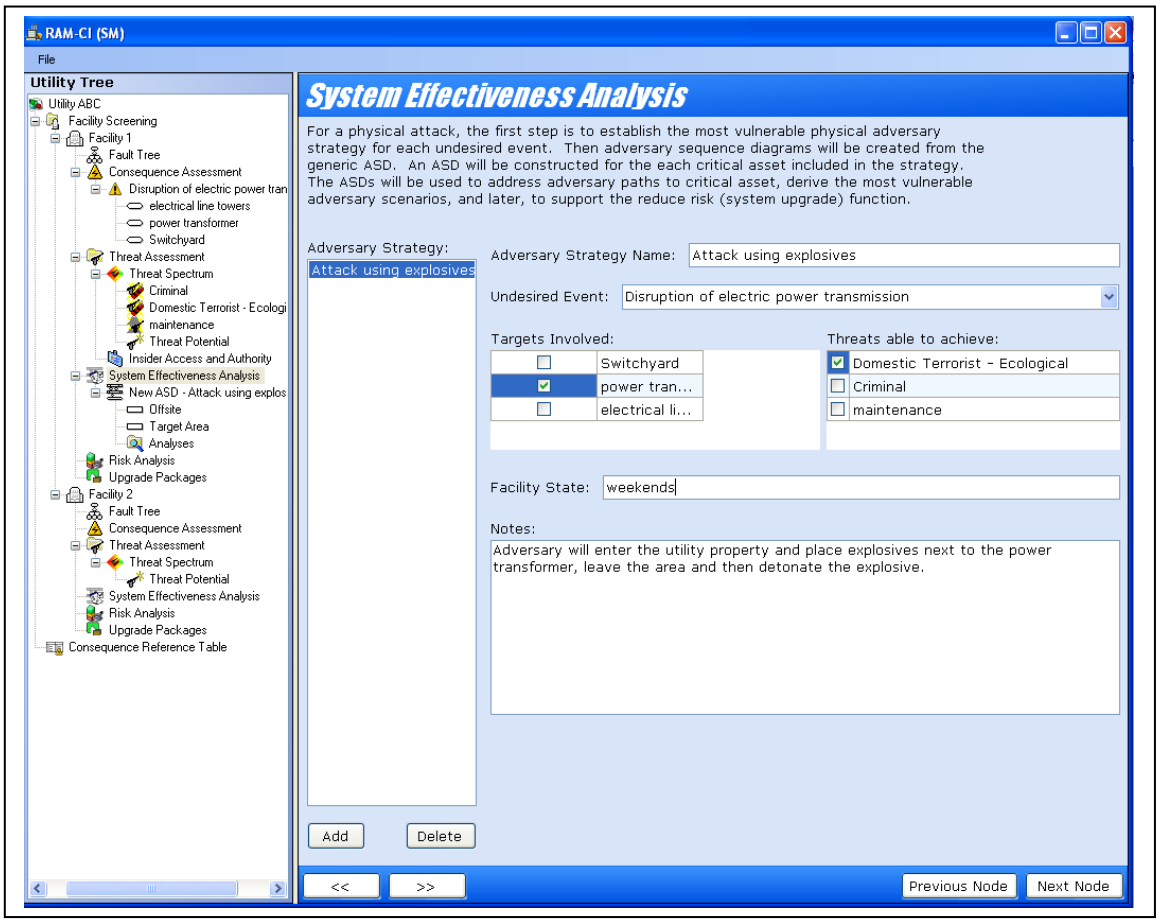

Figure 19. System Effectiveness: Defining Adversary Strategy

The physical paths that adversaries can follow to cause the undesired event and the PPS elements along the paths are important in determining the adversary attack scenario most likely to succeed. All possible adversary paths should be considered. As part of the automated prototype RAM tool, the user will likely create several ASDs. The user can now begin to create the ASD for the various undesired events/targets. The initial screen for developing the ASD, Figure 20, shows only protection layers for offsite, the target area, and the target with no paths elements between them. The user has the ability to add new layers or edit existing layers. The foot and tread symbols on the layer indicate that the adversary could travel either on foot or using some land vehicle across that layer.

After the layers are defined, the user adds path elements that connect the layers. When the editing the layer, the user can indicate if a vehicle can be used to travel across this area and the estimated distance across the area. The user can then identify the path elements that link the layers (Figure 21) and define the safeguards associated with the path elements. If for a given layer there are multiple path elements that have the same basic safeguard values (e.g., emergency doors), only one path element is entered into the ASD. If for a specific layer there are two similar path elements (e.g., gate), the user can color one of the elements as a means to indicate that the path elements have different characteristics.

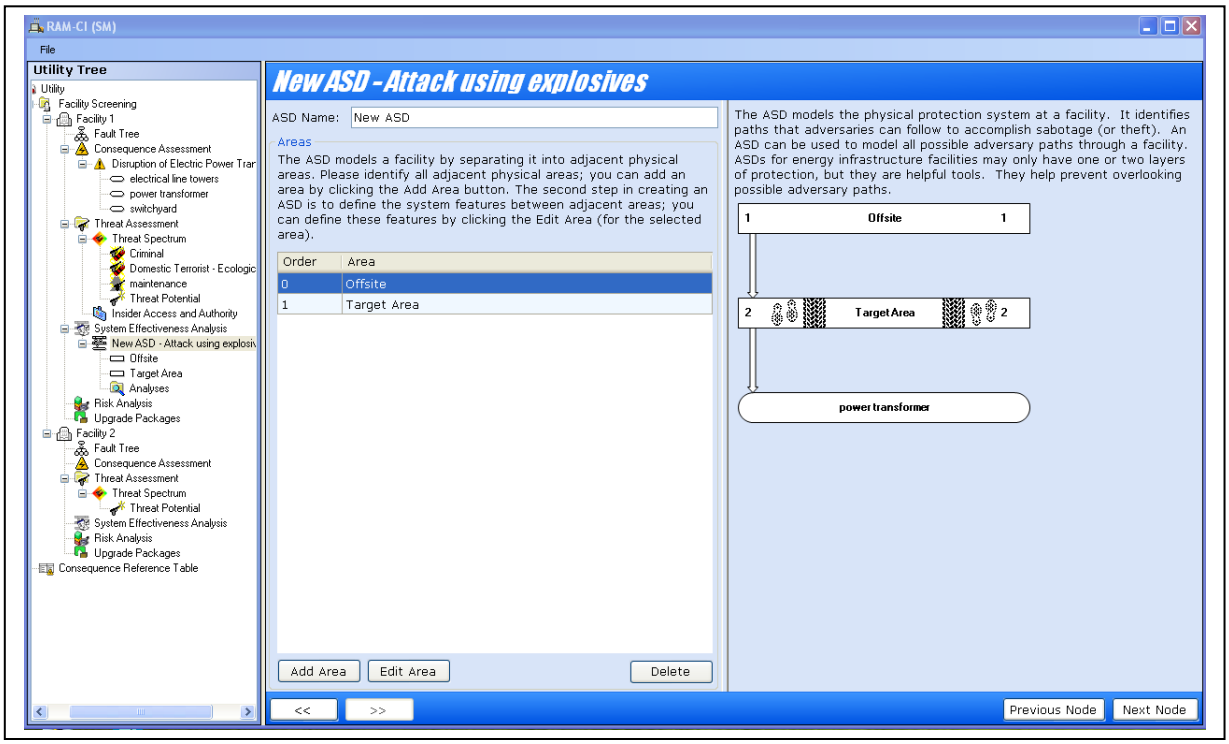

Figure 20. Initial Adversary Sequence Diagram Screen

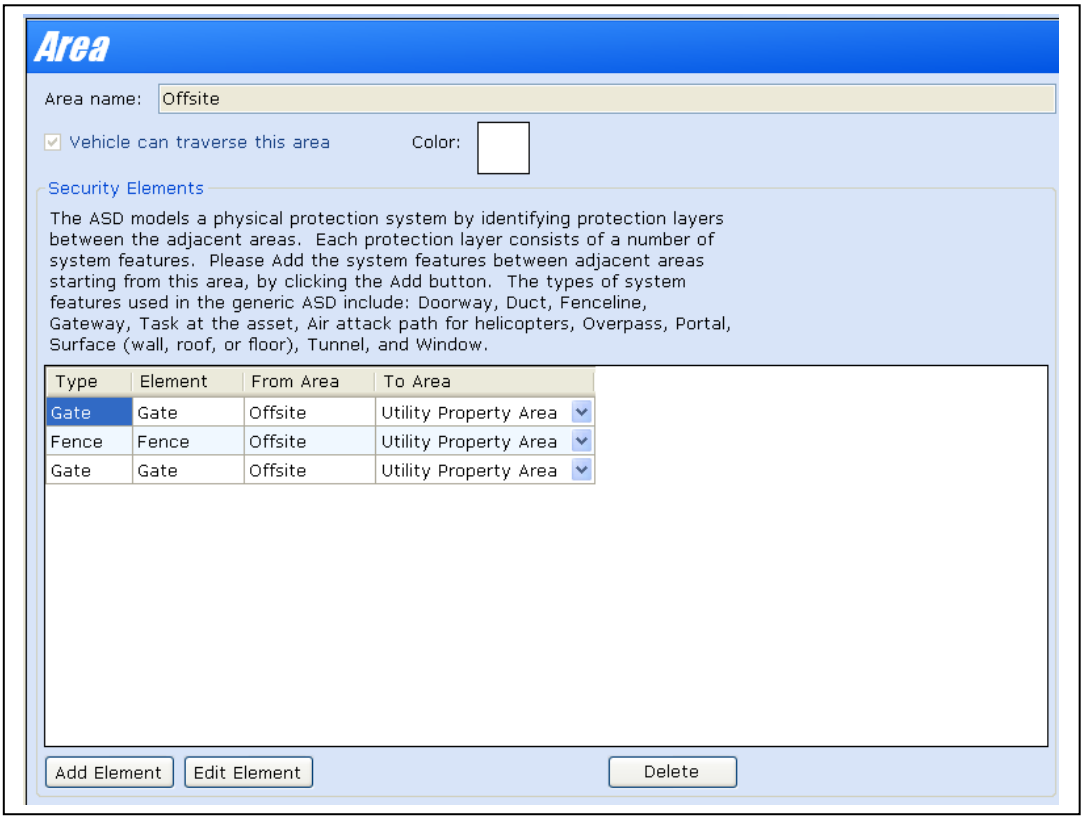

Figure 21. Selection of Path Elements Between Areas

8.2 Incorporate System Component Effectiveness Values

As part of the site survey and possible performance testing, the general characteristics of the protection measures (detection, delay, and response) present in the PPS were identified. The next step is to input the information and data collected for each safeguard path element in order to evaluate the effectiveness of the protection layers and path elements within the system. As part of developing the ASD the user will identify the features of the path elements (e.g., door construction, access control measures, sensors). Based on the user's input RAM software will select from a database the likelihood of detection for each element and the time for the adversary to compromise (bypass, traverse, etc.) these path elements. The values vary in the site-specific ASD for different threat groups with different capabilities and attributes.

In the automated RAM the user can identify what safeguard features exist for the path elements, Figure 22. The possible options vary depending on the path element but could include features for detection, contraband detection, security inspectors, and delay. For the safeguard selected the detection and delay value for that threat (e.g., for that set of tools, equipment and transport) are shown. The user can also identify the alarm assessment which exists for the PPS and if the communications lines are protected.

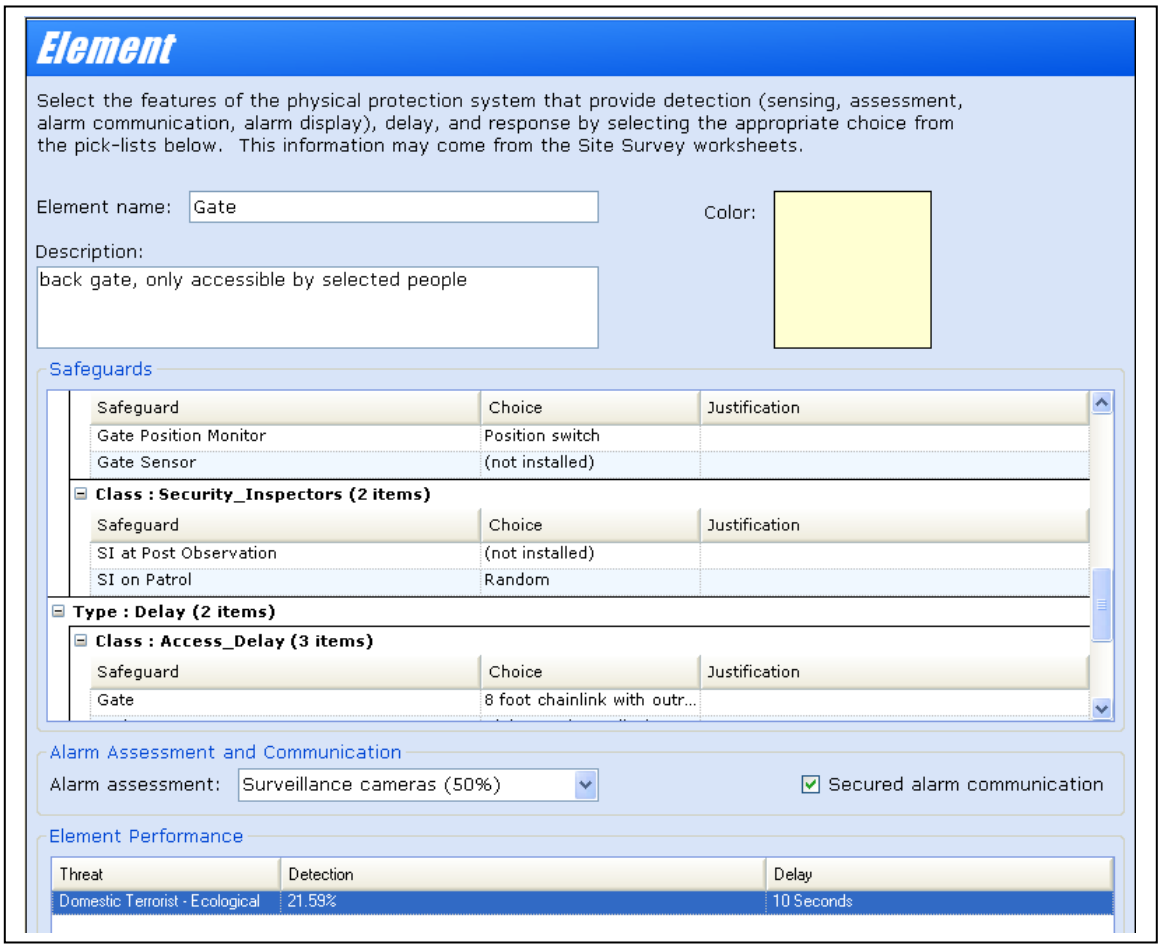

Figure 22. Defining Safeguard Features

After all of the safeguards have been defined for the path elements, the ASD is complete and ready to be analyzed. Figure 23 shows a completed ASD.

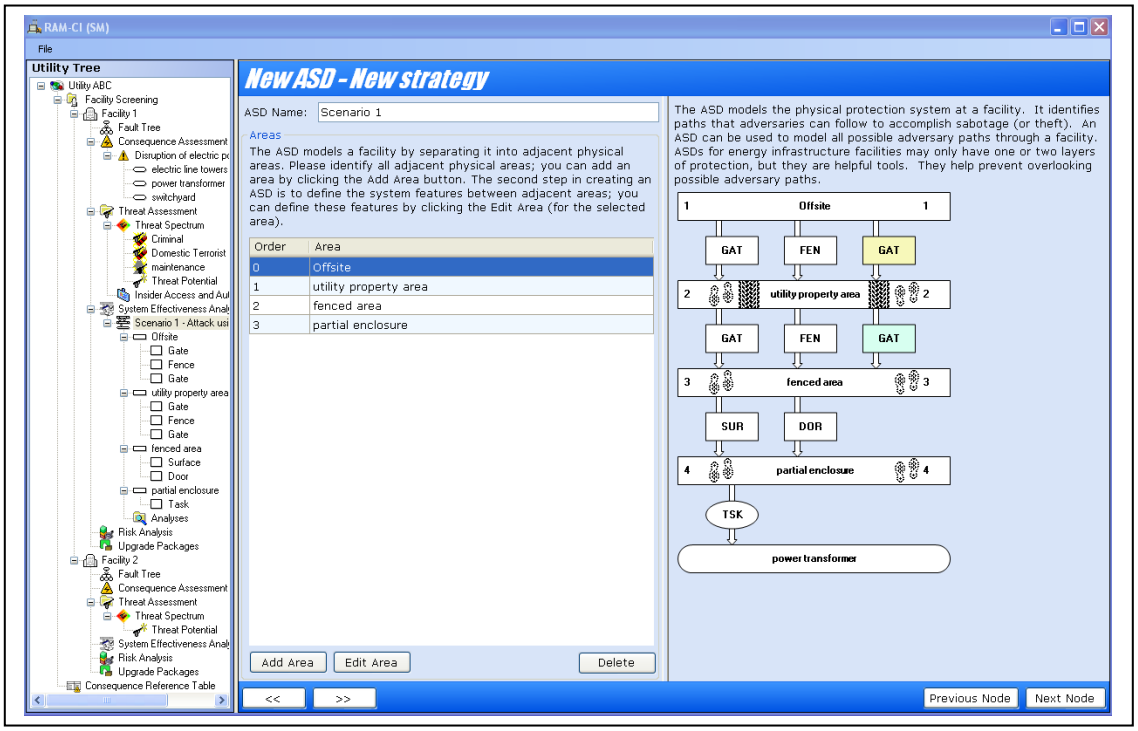

Figure 23, Completed Adversary Sequence Diagram

8.3 Develop Most Vulnerable Paths

After developing the ASD and defining the safeguard attributes for the path layers and elements, the user is almost ready to perform the analysis. The user will input the response force time(s) (RFTs). The RFT should be for the first security responders with the capability of defeating the adversary. This could include on-site security forces or local law enforcement. The ability to defeat the adversary threat depends on the capabilities of the adversaries as well as those of the responders. For a low-level threat the response force capabilities may be relatively low, whereas for a high-level threat a significant response may be required. The user can identify a possible most vulnerable path and calculate the P_I. To the right of the ASD, the P_I for the identified RFT is shown. By expanding that result the specific adversary path elements are listed along with the detection and delay values associated with that element. The user has the option to use the first selection or identify another path by clicking on the relevant path elements and performing the analysis again. In most situations there will be a few different path options that can lead to vulnerable paths. Several factors must be considered in judging which adversary paths might be the most successful:

- Protection system weaknesses are
  - Least-protected path (detection, delay, response),
  - Easiest system features to defeat, and
  - Worst consequences.

- Facility operating states that the adversary could use to an advantage include
  - Emergency conditions,
  - Minimal personnel on site,
  - Nighttime and weekends, and
  - Inclement weather.

As a general rule, until the adversary is detected, he will proceed with stealth, defeating delays in place and avoiding detection to the best of his ability. After the perceived point of detection by the adversary, he will move as quickly as possible taking the path of minimal delay because avoiding detection is no longer a consideration.

In the automated RAM tool, the user can either click on *Next Node* or in this case *Analyze* on the left-hand side to get to the analysis section. The user has the choice of adding a new analysis or editing an existing one. Figure 24 shows the screen with the ASD created for the adversary strategy. The user can name this analysis run and also enter a RFT.

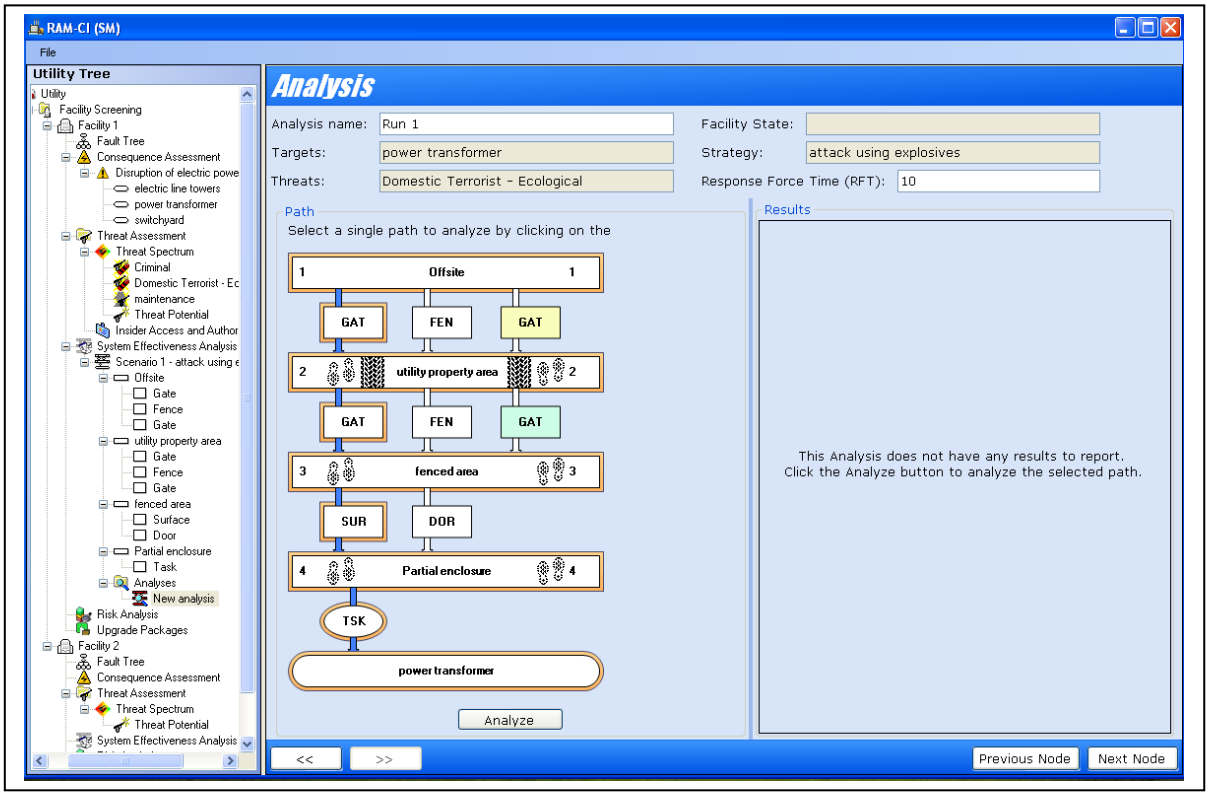

Figure 24. Initial Analysis Screen

After the user inputs the analysis name and RFT for this run, the user clicks the *Analyze* button below the ASD. The path selected by the software for that analysis is indicated by the colored frame around the areas and path elements used by the adversary. In the *Results* pane to the right of the ASD, the results of the analysis are shown. The P_I and delay time are shown. By expanding the results for that run (click on the + to the left of the RFT time), each of the steps used by the adversary is shown along with the transport and/or equipment

used and the detection and delay times associated with the area or path element. Figure 25 shows the results of the first analysis run.

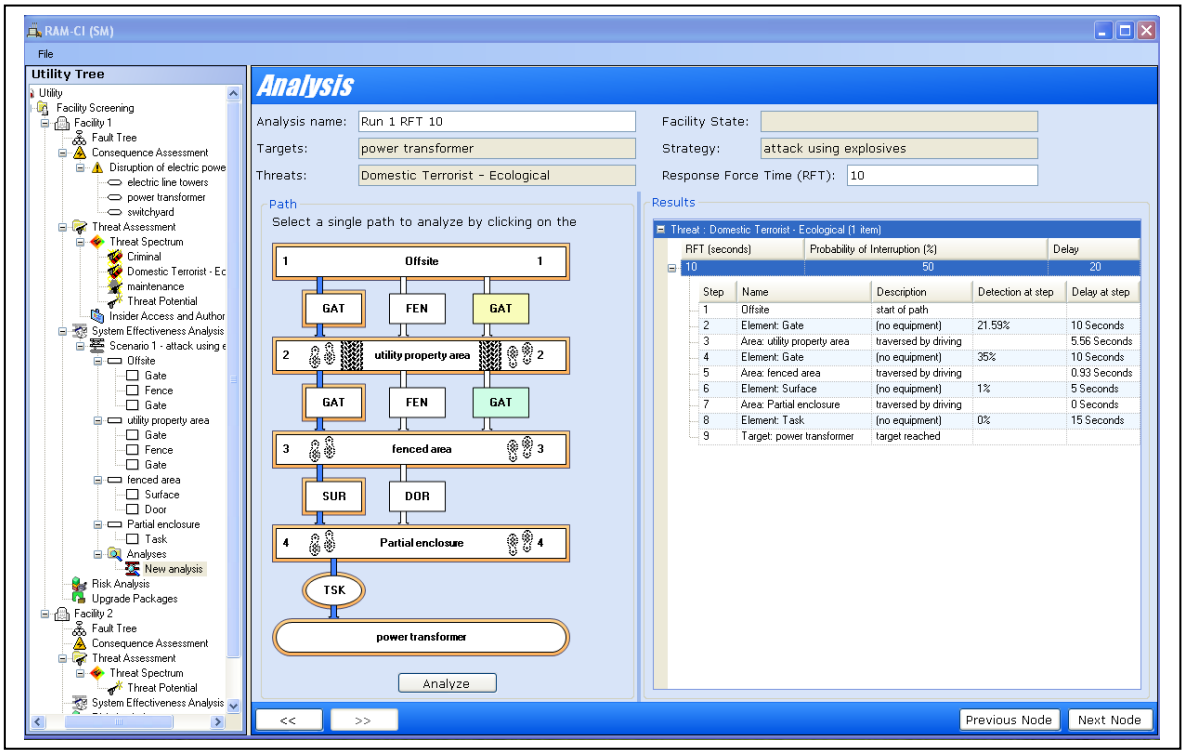

Figure 25. First Analysis Screen

The results from the first analysis are only one of the many possible adversary paths and does not necessarily represent the worst-case scenarios for the defined set of conditions (threat, RFT, target).

8.4 Develop Worst-Case Scenarios

The analysis of each potentially vulnerable path by the RAM software evaluates the interaction between the adversary and the protection system along the path using the following steps:

- Estimate at which step in the sequence detection will most likely occur.
- Estimate, based on the detection data from this and preceding steps, what the likelihood of detection is at that point.
- Add the delay times of each of the subsequent steps resulting in an estimate of the amount of time the adversary takes to complete his tasks after the point of detection.
- Compare this cumulative adversary task time to the RFT and determine whether the response force will be able to interrupt the adversary. If the RFT is longer than the cumulative adversary task time, interruption will not occur in time for the response force to prevent the adversary actions, resulting in a low or zero system effectiveness.

A judgment must be made about the likelihood of the response being able to stop the adversary from completing the necessary tasks to achieve the objective. This judgment will utilize the data about the adversary and response numbers, effectiveness, and capabilities. The likelihood of being able to stop the adversary is then subjectively combined with the likelihood of interruption to estimate system effectiveness.

The end result of this entire analysis is an assessment of the potentially most-vulnerable adversary paths and worst-case scenarios and the likelihood of the system being successful at preventing the adversary from achieving the objective. The user can click on different path elements to determine the worst case P_I, as shown in Figure 26.

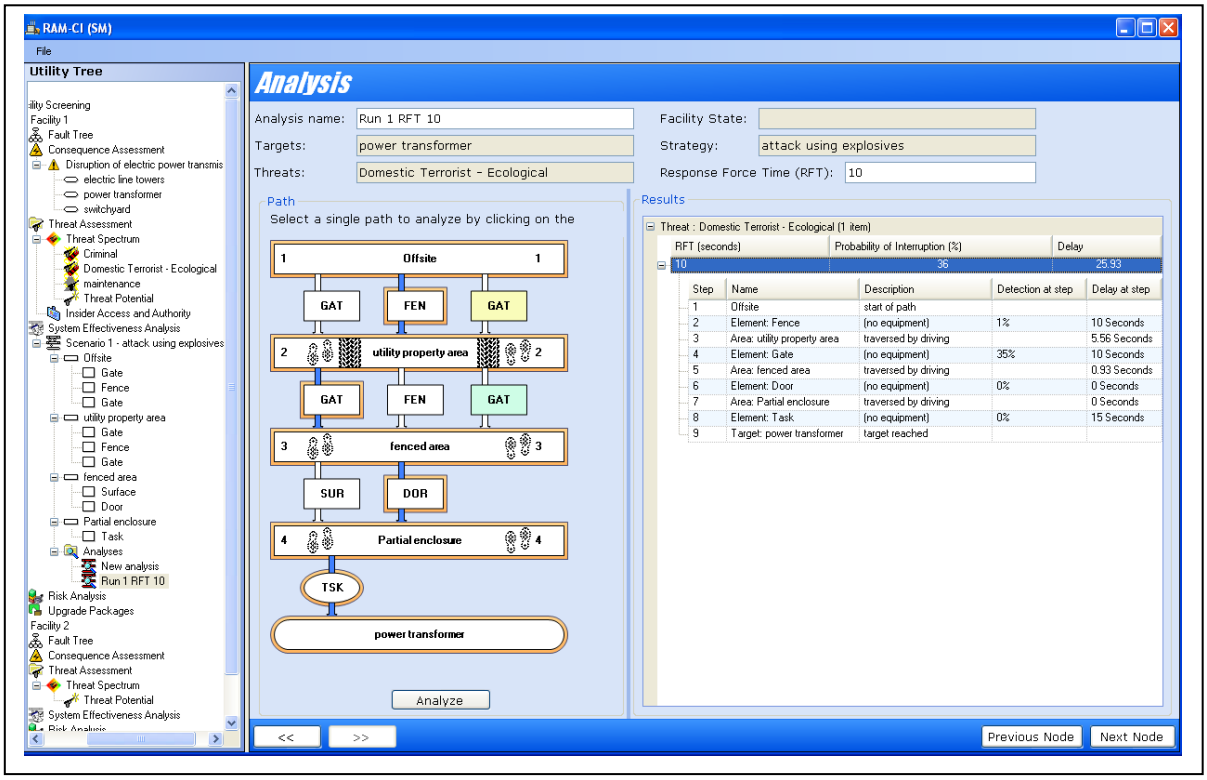

Figure 26. Possible Worst-case Scenario Results for a Response Force Time of 10 Seconds

The user can select and save different analysis runs by identifying the path elements and RFT. For the example shown in the initial analysis runs, the RFT is 10 seconds and the P_I is 36%. This is a very short RFT and basically means that the response force has to be outside and relatively close to the critical asset. This is probably not realistic for many CI facilities. Using an RFT of 30 seconds, which is also relatively short, the calculated P_I goes to 1%. For RFTs greater than 31 seconds, the P_I is 0%. Figure 27 shows the results for an RFT of 30 seconds.

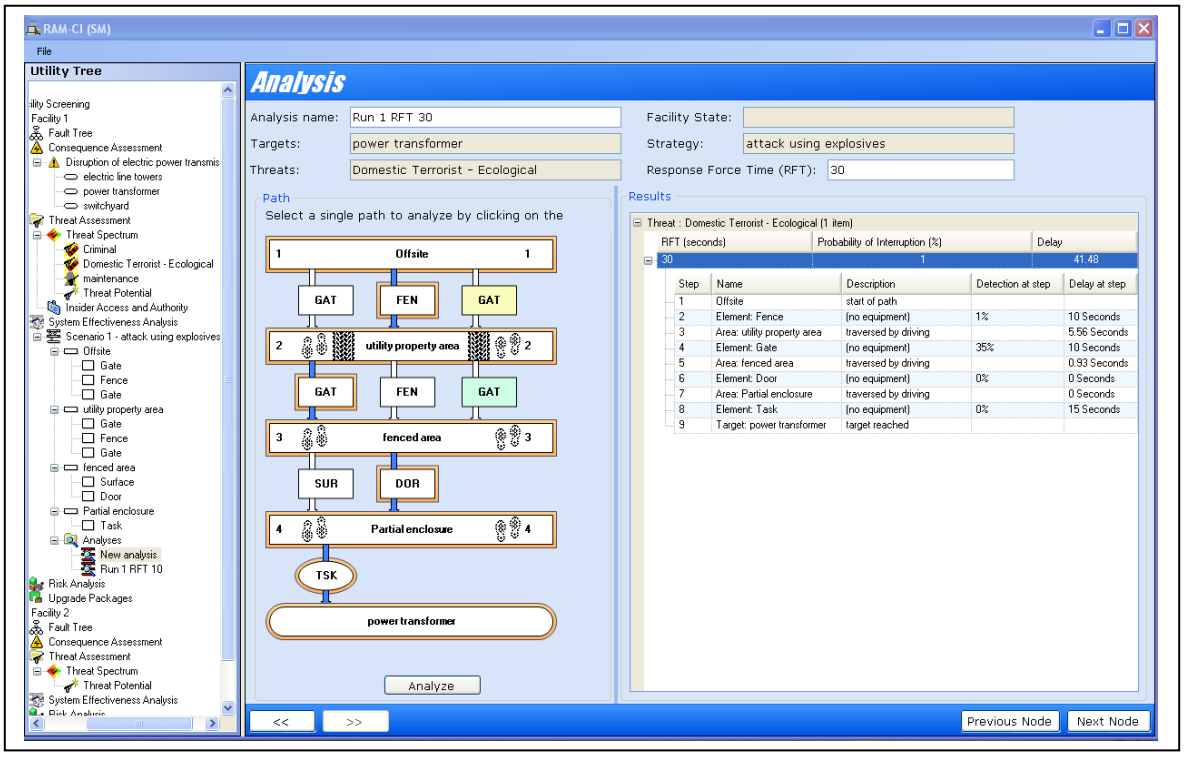

Figure 27. Possible Worst-case Scenario Results for a Response Force Time of 30 Seconds

8.5 Summarize Scenario Results

The previous discussions illustrated the process for analyzing a single scenario for a specific undesired event and threat. Several similar analyses must be performed for each undesired event (asset) and threat of concern (i.e., create an ASD, identify most vulnerable paths, develop worst-case scenarios, and estimate system effectiveness). After these analyses are completed and documented, a table is created that shows a summary of the results for the worst-case system effectiveness and also the values for the risk components and ris, as shown in Figure 28. The system effectiveness results are relative values. Also shown is the probability that an adversary can cause some level of consequence.

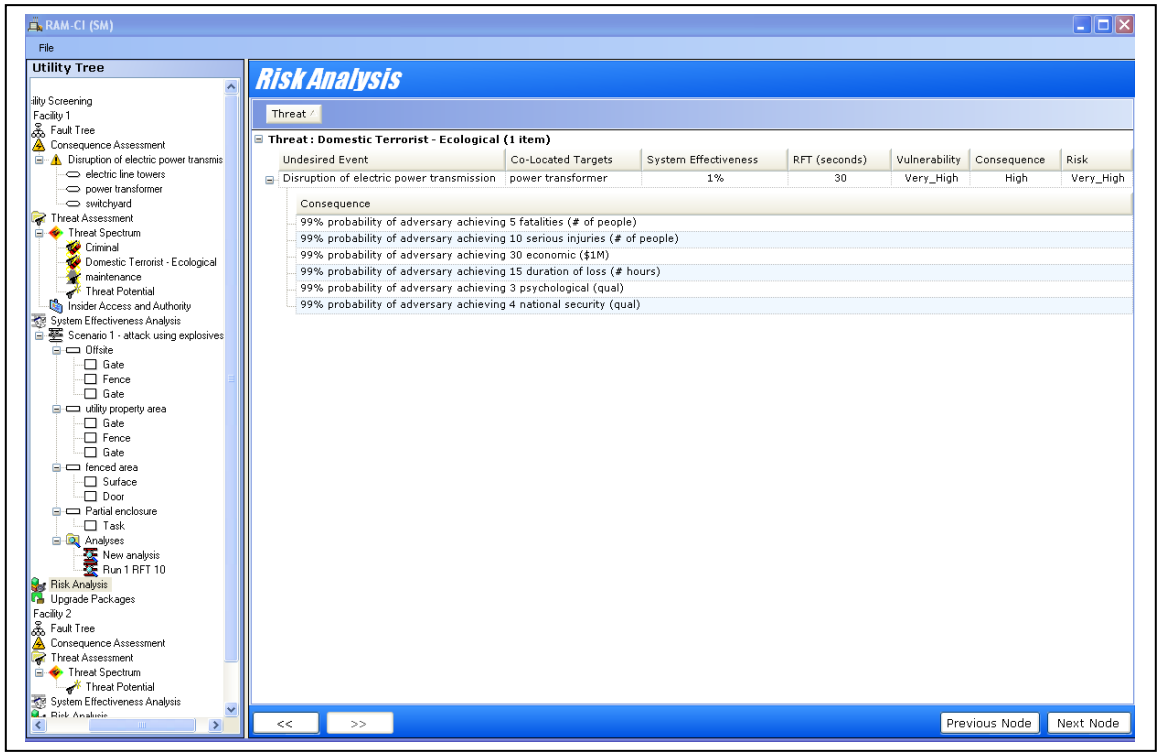

Figure 28. Risk Analysis Results Summary

8.6 Identify Physical Protection System Vulnerabilities

Examination of scenario results will identify which scenarios result in system effectiveness that is less than desired. For these scenarios, the details (system effectiveness and ASDs) should be reviewed to determine path elements and system weaknesses or vulnerabilities that could be the cause of the low system effectiveness (or high vulnerability) measure. At this point in the process, the user will only identify potential safeguards weaknesses and not propose upgrades. The user will need to review all the attack scenarios developed and for all worst-case scenarios, determine why they are worst-case scenarios. The user will identify for the different scenarios and adversary paths any weaknesses or vulnerabilities (Figure 29). These will be the vulnerabilities for the baseline case and will be considered during the upgrades step. The list of vulnerabilities will be grouped into the three PPS functions of detection, delay, and response. The input may be general or provide specific problems with a specific layer and/or path element.

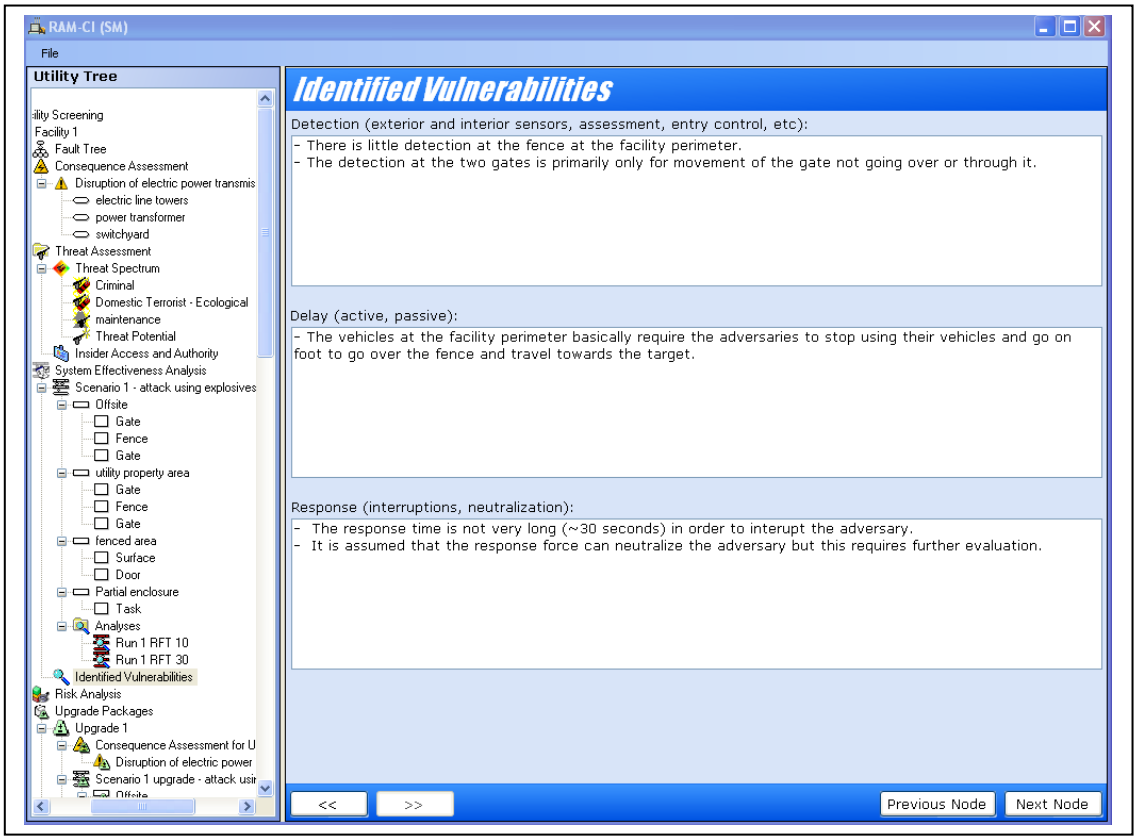

Figure 29. Identified Vulnerabilities for Baseline Analysis

9. RISK ANALYSIS

In order to make cost-benefit decisions, the system effectiveness/vulnerability and associated risk of the current (or baseline) protection system must be known. Without this information it becomes a difficult challenge for senior management to make effective cost-benefit decisions, because it is essential to know the reduction in risk (due to PPS upgrades and consequence mitigation) and the associated cost. A risk analysis for malevolent threats uses the quantitative and/or qualitative values estimated for threat potential, existing system effectiveness estimates, and the associated consequence values to calculate the risk value for each undesired event (critical asset)/threat pair.

9.1 Conditional Risk

If the user opts to use conditional risk so that risk for each threat/undesired event (asset) pair under consideration can be compared across the entire utility infrastructure, then the risk determined in the automated RAM prototype tool will use a qualitative analysis approach and estimate a conditional risk:

Conditional Risk = *function* (Vulnerability, Consequence)

Therefore, the risk analysis (for malevolent threats) will consider only vulnerability (system effectiveness) and consequence.

9.2 Relative Risk

If the user opts to estimate the threat potential, then the automated RAM prototype tool will estimate a relative risk:

Relative Risk = *function* (Threat, Vulnerability, Consequence)

The threat potential may vary in different geographic regions as well as for different CI sectors. In addition, there remains considerable uncertainty when estimating the likelihood of a malevolent event. Therefore, the relative risk value determined probably cannot be used to make comparisons across wide-ranging infrastructures.

9.3 Estimate Risk Values

When a conditional risk approach is applied, it is only through system effectiveness (vulnerability) and consequence that risk can be affected. This represents an important consideration because system effectiveness includes those activities, equipment/hardware, technologies, people, procedures, etc., that a facility can employ to reduce the risk of occurrence of an undesired event (i.e., loss of critical asset or assets). Likewise, consequence includes mitigation efforts related to operations that can be undertaken (e.g., facilities, equipment, procedures, emergency response, etc.) to create redundancy or a contingency.

These two terms in the risk equation represent ways to reduce risk. It is important to remember that system effectiveness considers the PPS and if the facility cannot prevent the adversary from causing the high-level consequence but can implement mitigation measures, then the consequence value would be affected.

At this point in the RAM process the user has determined vulnerability (system effectiveness) and consequence and has assigned qualitative values (very low, low, medium, high, and very high). Those qualitative values will be used to determine conditional risk for each undesired event/threat pair. Figure 30 shows the table used in the automated RAM to calculate a conditional risk. This table is common to all RAMs developed by SNL and was derived using the risk equation (i.e., numerical values were converted to qualitative values). The summary table provides the qualitative values for C, V, and R for each threat/undesired event pair. In this case the threat potential would be considered very high (VH). A different table would be used when the threat potential was not VH.

		RISK VALUE				
VULNERIBILITY	*VH*	VL	L	H	VH	VH
	H	VL	L	M	H	VH
	M	VL	VL	M	M	H
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
		VL	***L***	***M***	***H***	***VH***
		CONSEQUENCES				

Figure 30. Conditional Risk Table

Figure 31 shows the risk analysis summary table in the automated RAM prototype tool. Shown in this screen would be the baseline results for all threats, undesired events, and analysis runs performed. The values for risk and each of the three risk components are shown, as well as the percent system effectiveness and the potential consequence of a successful adversary attack. The value for the risk components was determined in earlier

steps. The value for threat potential would be *very high* (conditional risk) unless the user selects to estimate a threat potential value.

In addition to showing the qualitative values for risk and its components, the system effectiveness is also shown (e.g., 1%). The percent probability of adversary success (1 – system effectiveness) for achieving one of the consequence measures is also provided.

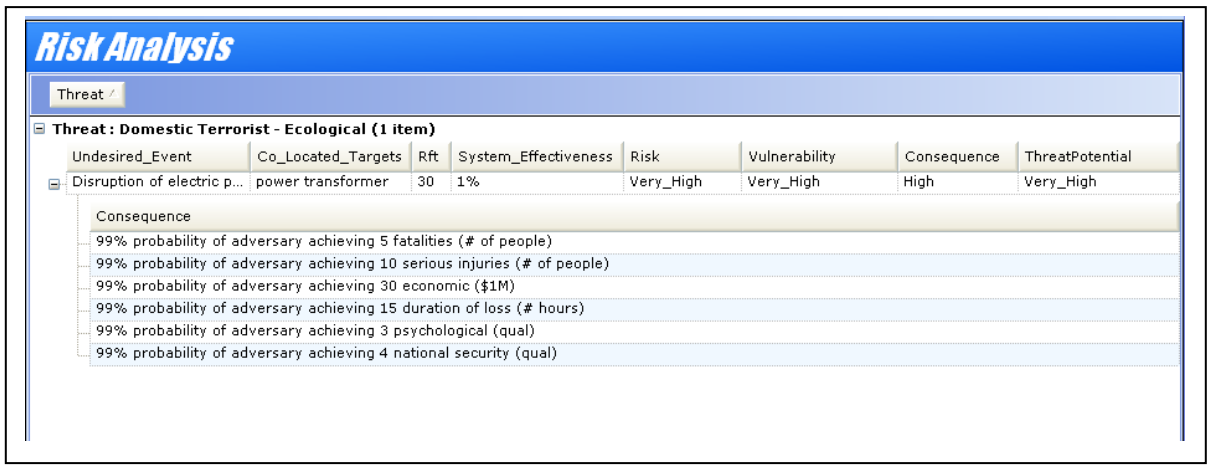

Figure 31. Risk Analysis Baseline Summary Results

9.4 Determining Whether Risk Is Acceptable

Before proceeding to recommending upgrades, the facility's senior management must decide whether the risk levels are acceptable. It is the responsibility of the facility's owner/operator and senior management to define and establish the security risk threshold for the site and its facilities/assets. It is important to recognize that there will be a limited amount of resources available to meet the protection objectives established for a facility. Therefore if the threat to a facility is high and only limited resources are available to protect the facility against a lower threat, then additional risk must be acknowledged and accepted by the facility owner/operator.

A different system performance will be required against different threats. Because system effectiveness is dependent on the threat, there will be different system effectiveness (vulnerability) values and therefore different risk values for different threats and undesired events. As the threat becomes more capable or sophisticated, the security system must also perform better. This analysis can serve as the justification for additional funds to reduce risk further or can serve as the basis for longer-term plans to increase security over a number of years. The goal of the risk assessment is not to spend as much money as possible, but rather to help senior decision-makers allocate the available funds most effectively to reduce security risk to the facility. If the results indicate an unacceptable high-risk exposure, additional funds must be made available to increase security system effectiveness (decrease vulnerabilities) and/or reduce consequences.

The risk assessment part of the automated prototype RAM tool is now complete and the next step is the risk management portion, in which the user considers possible risk reduction upgrades, formulates possible recommendations, analyzes the different courses of action, and determines the effects on system effectiveness and/or consequences. Risk will be re-analyzed to determine how much risk can be reduced by either increasing system effectiveness (i.e., reducing vulnerabilities) and/or reducing consequences.

10. RISK MANAGEMENT

If the baseline analysis indicates that the system risk is too high and the protection objectives established cannot be achieved, the user can suggest upgrades that will address the PPS vulnerabilities or ways to reduce the consequences. Sometimes these upgrades are specific technical recommendations (although those decisions are usually left to the security system conceptual design team), but often the recommended upgrades are functional improvements that can be achieved by increasing performance at certain locations. (The ASD can be very helpful in identifying those locations.) The organization of proposed risk reduction measures may vary but will likely include one set of upgrade options for the PPS and the interaction of detection, delay, and response features and another set of upgrade options for the consequence mitigation measures, such as back-ups, spares, redundancy, and emergency response plans.

In the automated prototype RAM tool, when the user clicks on *Upgrade Packages* in the *Utility Tree* on the left side of the window, the program copies the baseline information and makes it available for the upgrade analysis. Normally the user would create several upgrade packages for the decision makers to review. The user would go to the first upgrade screen and name the upgrade package, provide the rationale for the upgrade, and indicate what the upgrades may be included for any PPS measures (Figure 32). The user would also provide input on estimated costs for the upgrade and qualitative input (very low to very high) on impacts to operations, schedule, public opinion, and any other anticipated impact. The cost estimate provided by the user in the automated RAM prototype tool would include the initial costs for purchase and installation. Later releases of the automated RAM tool will provide more guidance for costs and impacts.

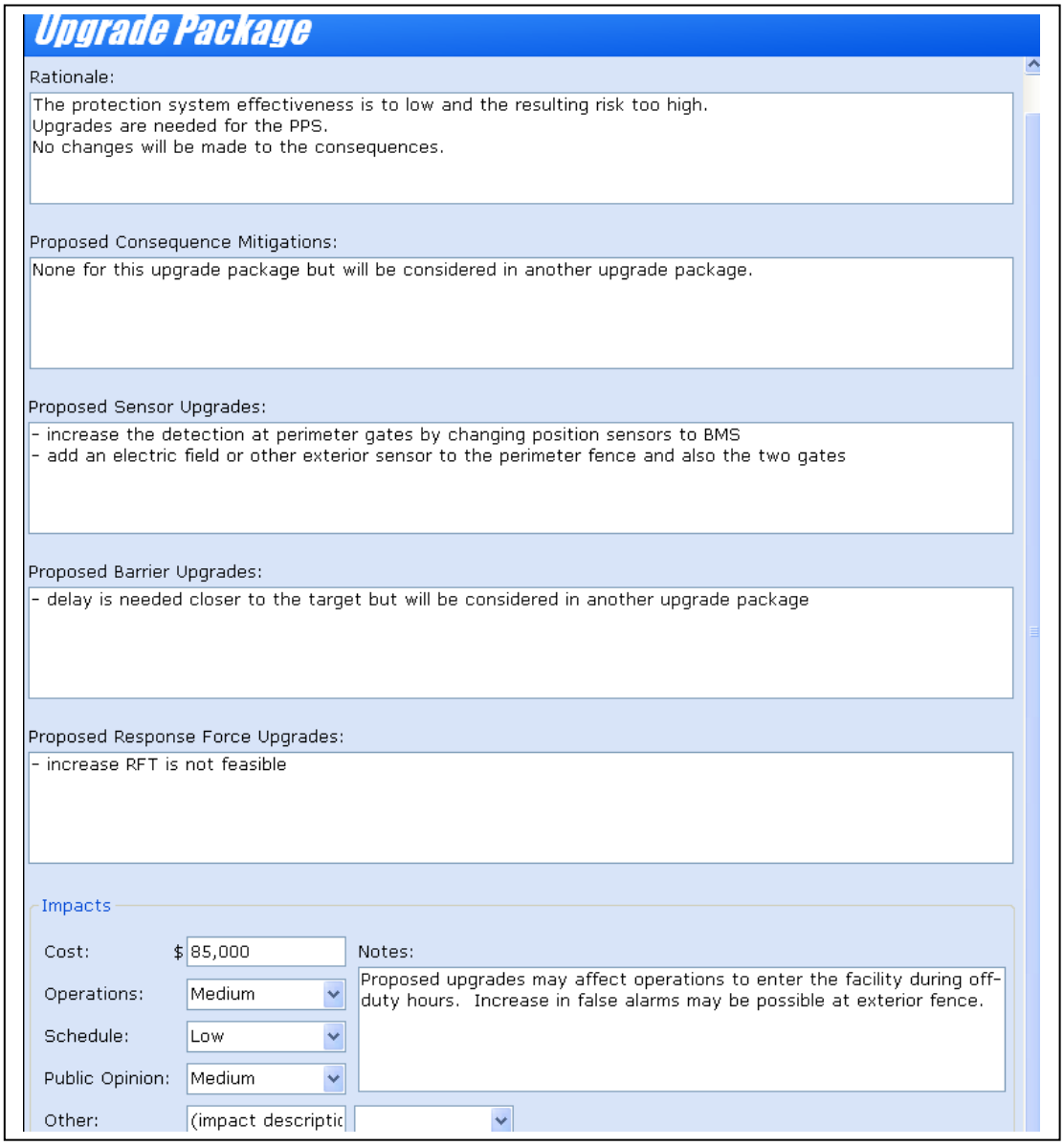

Figure 32. Upgrade Package 1 Input

10.1 Risk Reduction

Risk can be reduced by increasing the system effectiveness (decreasing vulnerability) or by decreasing consequences or both. Upgrades that reduce risk should be considered for each undesired event with an unacceptably high risk level. The basic elements of risk reduction include:

- Improvements in the security policies and procedures,
- Consideration of upgrades to prevent the undesired event (PPS upgrades), and
- Consideration of upgrades to reduce the consequences of the undesired event (mitigation measures).

10.2 Protection Objectives

The risk calculations performed for the baseline security system will determine whether the protection objectives have been achieved. If not, the user will proceed with developing upgrade suggestions to lower risk. Upgrades will differ depending on the protection objectives, operational states, and the design and operations of the facility. As noted in the previous section, it is important for the user to focus resources on the undesired events with the highest consequences.

10.3 Potential System Upgrades for Physical Protection System

Users of the automated RAM tool are cautioned not to interpret upgrade analysis as a simple process of inserting PPS upgrades and completing the analysis. Functional performance improvements must be considered to be achievable by the user. Reasonable improvements must be considered when conducting the upgrade analysis. The selection, installation, maintenance, and integration of PPS components as they exist at the facility have a major impact on performance estimates. Thus it is extremely important to use performance-based data that reflect actual performance at the site both for the baseline analysis and the upgrade analysis.

As a result of the baseline analysis (system effectiveness/vulnerability and risk), the facility owner/operator and senior management will need to determine whether risk levels are acceptable or there is a need to identify PPS upgrades to improve performance against the defined threat (i.e., the threat spectrum).

10.3.1 Security Policy and Procedures (General Guidelines)

The entire risk-reduction program for any facility hinges on performance. Performance of the system is heavily dependent on policies, procedures, and training. Critical areas for the user to examine include how well security, operational, and emergency response plans are documented; how well employees are trained on the plans; and how exercises are conducted

to reinforce the training. The presence or absence of well-documented, consistently applied, and thoroughly trained policies and procedures can be an indication of the corporate culture—a culture that will likely require change to implement higher levels of security.

10.3.2 Upgrade Analysis Process for the Physical Protection System

The process used to analyze upgrades to the PPS is:

- Review all worst-case scenarios for all defined threats to determine what proposed upgrades might impact all vulnerable paths.
- Identify potential upgrades for the PPS (upgrades to detection, delay, and response).
- Revise the ASD with upgraded likelihood of detection and delay time values.
- Determine new system effectiveness values.
- Identify potential upgrades for reducing consequences.
- Identify new consequence values.
- Recalculate risk and compare to baseline risk.

Each step of upgrade analysis process will be described in detail in the following sections.

10.3.3 Review Worst-Case Scenarios

The ASD helped identify the most-vulnerable paths with the lowest system effectiveness for the current protection system. Analyzing the PPS using the defined threats and then developing worst-case scenarios by identifying the weakest paths is the preferred approach to ensure that credible paths are not overlooked. Worst-case scenario analysis is conducted to determine whether the system has vulnerabilities that could be exploited by the range of threats defined in the site-specific threat spectrum using varying tactics. Using each scenario (for each threat/undesired event pair), a task-by-task or layer-by-layer description is developed. Each description should be detailed enough to provide a scenario timeline and contain enough information that performance estimates for alarm-sensing, assessment, communication, delays, and response can be made. The worst-case scenarios are used to define the adversary attacks that test the limit of the PPS effectiveness.

The user reviews the worst-case scenarios and the list of identified vulnerabilities (Figure 29) to determine what proposed upgrades would impact as many of the vulnerable paths for the range of threats. Typically, proposed upgrades must impact most or all scenarios in order to be cost-effective solutions.

10.3.4 Identify Potential Upgrades for the Physical Protection System

The baseline analysis demonstrates whether functional upgrades are needed to improve system performance against the range of defined threats. This report shows only a few examples for illustrative purposes; in real time the user would have conducted numerous analyses for every defined threat and high-consequence undesired event. However, it may be desirable to consider scenarios that are most likely or provide at least a reasonable upper limit for the threat and undesired events. The user evaluates detection, delay, and response

information to propose upgrades that could potentially impact most of the vulnerable paths for each defined threat. The user then proposes upgrades and documents those along with the rationale for recommending the upgrades.

10.3.5 Develop Upgrade Options

Often the goal for most sites is low cost and high return on installed upgrades. Therefore the user will need to organize the list of upgrades into option packages. Option packages allow the facility owner/operator and senior managers to quickly evaluate risk reduction and cost-benefit tradeoffs and therefore make cost-effective decisions about system upgrades. The protection features can be grouped into packages (options) and evaluated to allow comparisons among packages.

10.3.6 Revise the ASD With Upgraded Protection System Values

Users of the automated RAM are cautioned not to interpret upgrade analysis as a simple process of plugging in high performance estimates and completing the analysis. These functional performance improvements must be judged to be achievable by the user (or by other security subject-matter experts). Use of performance estimates that are not achievable using existing technology or procedural changes is not recommended and would not contribute to a defendable analysis. Performance-based values should be based on actual operations at the facility for various operating states (operational, non-operational, emergency, adverse weather conditions, etc.) and defined threats.

The next step in the upgrade analysis is to revise the original (baseline) values for the areas and path elements. For simplicity's sake, only those system components with value(s) that change(s) as a result of the proposed upgrades are identified. All other physical protection data for system components remain the same. Once the user verifies the changes (e.g., changes to the areas/layers, revised values for the probability of detection, delay times, response times, and response effectiveness), the revised ASD is ready to be analyzed.

For a full analysis every ASD developed for each critical asset should be reviewed to ensure that the proposed protection system upgrades affect all paths for all threats and operating states. It is important that the most-vulnerable paths for the upgraded system are adequately protected. Similarly, all paths should have adequate and comparable delay. Some designs will place delay features at a critical path element resulting in all paths being affected. An effective PPS will have balanced protection, protection in depth, and no single points of failure. Reviewing the ASDs after revising the affected safeguard values prevents the user from overlooking penetrations that require protection.

The user can make different changes to the path areas/layers and path elements and then analyze and review the impact to P_I. The user can continue this what-if approach until a reasonable set of upgrades is identified. An upgrade package will normally contain only a small number of possible upgrades.

In the example that has been used in this report, only one scenario with one threat and one target are analyzed, so the selection of the worst-case scenario is relatively simple. From Figure 27 and from the baseline list of vulnerabilities, it can be seen that there are two issues

with regard to the PPS. One is that the outer facility perimeter has a very low probability of detection. The other is that after the first point of significant detection, there is little delay.

The gates at the perimeter already have a relatively inexpensive position switch, so this sensor element could be improved for the two *gates*. At the *fence* any number of possible detectors could be used to improve the detection. The outer perimeter has an aircraft cable to stop vehicles and so, based on the path analysis, it appears that that the adversaries are dismounting and continuing on foot once they reach the fence. For the delay to be considered effective, it must be inside a perimeter with sensors and therefore it needs to be added after the point of significant detection. The only place where additional delay could be realistically added for an adversary on foot is the path element, *door*, which represents an opening between the metal walls around the transformers. In this case a metal grated door could be added to slow down the adversary. These two possible improvements will be shown as separate upgrades and the results provided in the following section.

10.3.7 Reanalyze the Most-Vulnerable Paths and Worst-Case Scenarios

Using the revised data a new P_I is calculated and the baseline worst-case scenario is revised. This information will be used in the subsequent upgrade analysis process. Once again a judgment must be made about the likelihood of the response being able to stop the adversary from completing the necessary tasks to achieve the objective. This judgment utilizes the data about both the adversary and upgraded response capabilities. The same questions as for the baseline analysis are used to determine system effectiveness/vulnerability.

In Upgrade Package 1 shown in Figure 33 an improved position sensor was added to the gate and a fence sensor was added to the outer perimeter fence and the gate. The resulting improvement for P_I was from 1% to 41% for the adversary path shown.

In the automated prototype RAM tool any number of possible upgrades can be considered until the best ones are determined. The process described above is continued for the entire threat spectrum and suite of critical assets to identify possible upgrades and to estimate the improvement in P_I. These results (which become new system requirements for upgrade designs) can be provided to security system designers, who will determine which specific equipment/technologies or other upgrades will provide the required performance. These specific design details are generally addressed in a follow-on activity to the risk assessment and often captured in a conceptual design project or phase. Once the analysis is completed, it is important to present both the baseline and upgrade system effectiveness/vulnerability analyses to establish the need for PPS improvements and demonstrate the return on investment as a result of implementing the upgrades.

For Upgrade Package 1 the user can evaluate different adversary paths and/or make other changes to the path elements. For this upgrade if the adversary decides to enter the facility property area through one of the two *gates,* the P_I is reduced to 35%. If the adversary decides to enter the fenced area through the *fence,* the P_I actually goes to 0%.

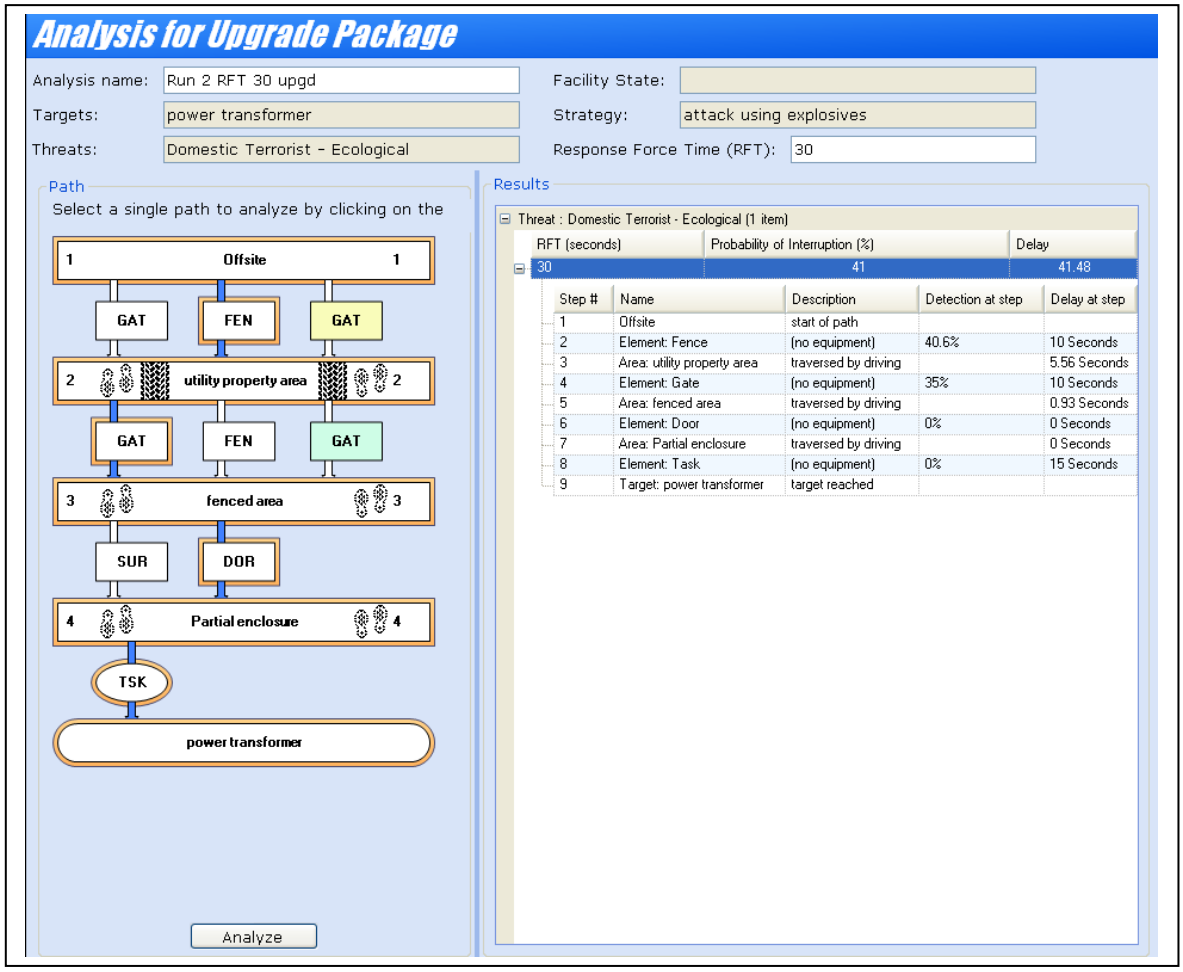

Figure 33. Upgrade Package 1 Results for Physical Protection System Upgrades

In Upgrade Package 2 the improvement in the detection at the outer perimeter is included and in addition, the original door (which was modeled as being open) is upgraded to a metal grated door. The delay value is changed in the path element, *door*. The result, shown in

Figure 34, is that the P_I improves from 1% to 61%. If the adversary uses the *fence* path element to enter the fenced area, the P_I improves to 71%. Because significant detection already is present before the adversary reaches the *door*, the adversary's tactics are to minimize delay; little detection at the *wall* and *door* around the transformers makes no difference.

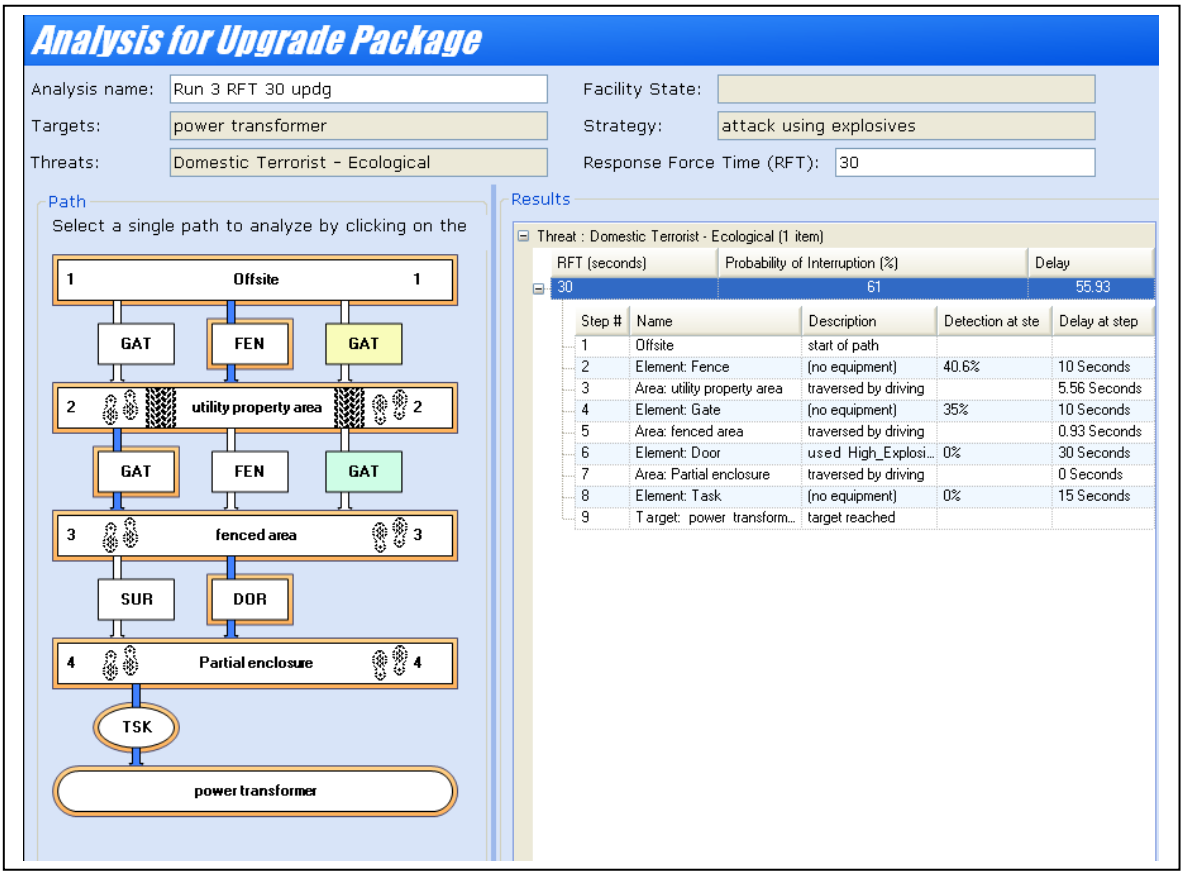

Figure 34. Upgrade Package 2 Results for Physical Protection System Upgrades

10.4 Potential System Upgrades for Reducing Consequences

If it is deemed impossible (or too costly) to prevent the adversary from achieving the objective, the protection objective may become to reduce the consequences caused by the undesired event. Mitigation measures (consequence-reduction measures) should then be considered for each undesired event. These measures, either action by people, technologies, or hardware that function to reduce the consequences of the undesired event, affect the consequence value, C.

The user evaluates the proposed consequence-mitigation measures upgrades to determine the impact on consequences. For the automated prototype RAM tool, the user can make changes in the consequence values and the new input will be used to calculate risk. If the decision is to eliminate a potential target (e.g., remove a hazardous chemical from the site), there no longer would be a risk for that target. In the example used in this report, the user decided to obtain a spare transformer that could be installed within 72 hours. For this consequence-reducing measure, the user goes to the *Undesired Event for Upgrade Package* screen and updates the values of the appropriate consequence measure metrics. Shown in Figure 35 is the input for this measure. There was no change to fatalities and serious injuries. The economic impact went from $30M (low) to $25M (very low). The user calculated the duration of loss

for the baseline case incorrectly; rather than 15 hours, it should have been 15 days or more. The duration with this upgrade was 72 (medium) hours. The psychological impact remained the same and the national security impact went from high to low. After making the changes the overall C value was reduced from high to medium.

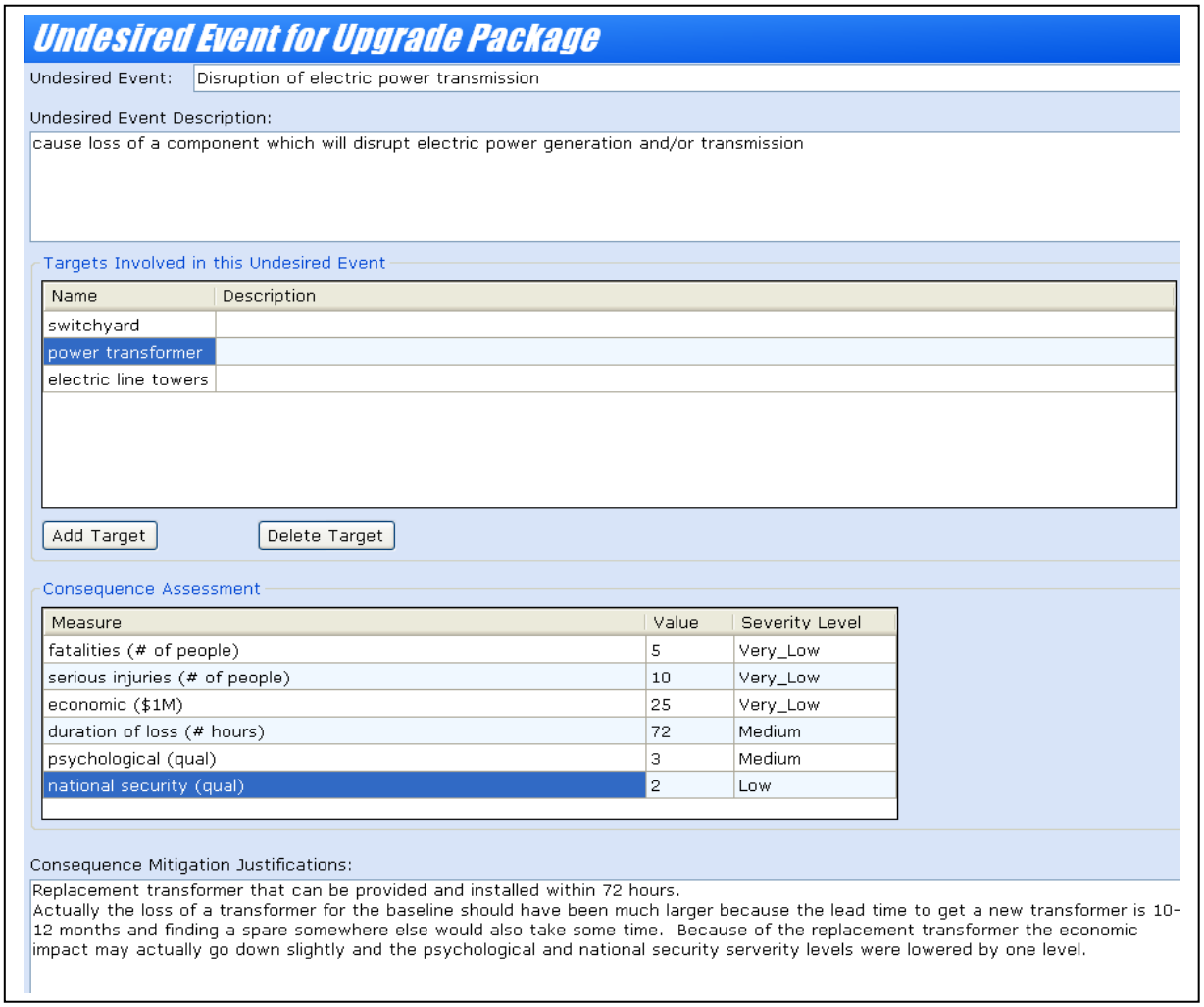

Figure 35. Upgrade Package 3 Results for Consequence Mitigation

10.5 Recalculate Risk and Compare to Baseline Risk

The obvious question is whether the proposed upgrade package(s) will lower risk values and, if so, how much. First, the protection system effectiveness (vulnerability) for the upgraded system must be estimated. The same risk analysis process used in the baseline case will be applied to the upgraded system. Consequence values associated with each undesired event also should be reviewed to determine the effects of the proposed consequence-mitigation measures. The risk associated with the upgrade package(s) can then be calculated.

The user will review the baseline risk summary for all threats and undesired events (loss/destruction of asset or assets). The only way to verify whether the proposed upgrades will reduce risk is to examine the upgrades in the context of the adversary attack scenario. If the proposed upgrades contribute to moving the PPS towards timely detection, then the PPS effectiveness will increase. The user must reanalyze the PPS upgrades to determine whether the upgrades will effectively lower risk. Similarly, consequence values associated with each undesired event should be reviewed to determine the effects of the proposed consequence-mitigation measures. Finally, the risk values for the baseline system can be compared to that of the upgraded system to determine the amount of risk reduction. If risk values are still unacceptable, the upgrade process can be repeated. When risk values fall in the acceptable range (the threshold is determined by the facility owner/operator), consideration may be given to the other impacts imposed on the facility or system as a result of the upgrades (e.g., cost, operations, schedule, or public opinion).

10.6 System Upgrades to Deter Adversary

The deterrence function of a PPS is difficult to measure and reliance on successful deterrence can be risky (especially for the higher threat levels); therefore, it is considered a ***secondary*** function of the PPS. Deterrence is an attempt to increase the perception level for the security system; i.e., it discourages an adversary from attempting an attack by making a successful attack appear very difficult or impossible. Deterrence may be accomplished by adding visible security features (e.g., increased lighting, warning signage, fences, cameras, or security officers) or by adding surveillance equipment or features that provide identification for prosecution evidence. It would be a mistake to assume that because an adversary has not challenged a system, the effectiveness of the system has deterred such challenges. Further, certain threats are not going to be deterred and some level of prevention or mitigation is still required. For the automated RAM tool, deterrence is not considered in calculating risk.

10.7 Upgrade Analysis Summary for the Malevolent Threat

The final step is to reanalyze system effectiveness (vulnerability), consequences, and risk as a result of upgrades to the protection system and/or reduction in consequences. An upgrade analysis process began with reviewing and revising worst-case scenarios (most-vulnerable paths) and ASDs based on proposed upgrades and the use of performance-based data (qualitative and quantitative). System effectiveness/vulnerability and consequences were re-evaluated and compared to the baseline results to demonstrate the impact of the upgrades.

There is no one right way to reduce risk and every facility has unique operational features and constraints. When the list of upgrades is complete, the user should then take a systems-level view of the entire operation to determine what might be done system-wide to lower risk. Before blindly going down the list of high-consequence facilities/assets and embarking on improvements, the user should spend time working what-if scenarios to determine the best system-level improvements. The user might recommend doing nothing with a few high-consequence facilities/assets because improvements elsewhere in the system will lower the risk across the utility when completed. After developing the upgrade packages in the

automated RAM tool, the user will be able to review the risk for the baseline results as well as the different upgrades. Figure 36 shows a summary for the risk for the baseline and the re-calculated risk for the different upgrade packages. This screen includes the results for all threats, undesired events, and analysis runs performed. The value for risk and each of the three risk components are shown, as well as the percent system effectiveness and the potential consequence of a successful adversary attack.

In this example, Upgrade Packages 1 and 2 result in lower vulnerability values and a risk value that has been lowered by one level and two levels for a RFT of 30 seconds, respectively. For Upgrade Package 3, only the consequence component has been changed; therefore the baseline vulnerability remains the same and the risk remained very high. As a result the overall risk is high. In this case the user accepts the potential loss of a power transformer (the vulnerability is not really relevant) and the overall risk value would be medium or lower.

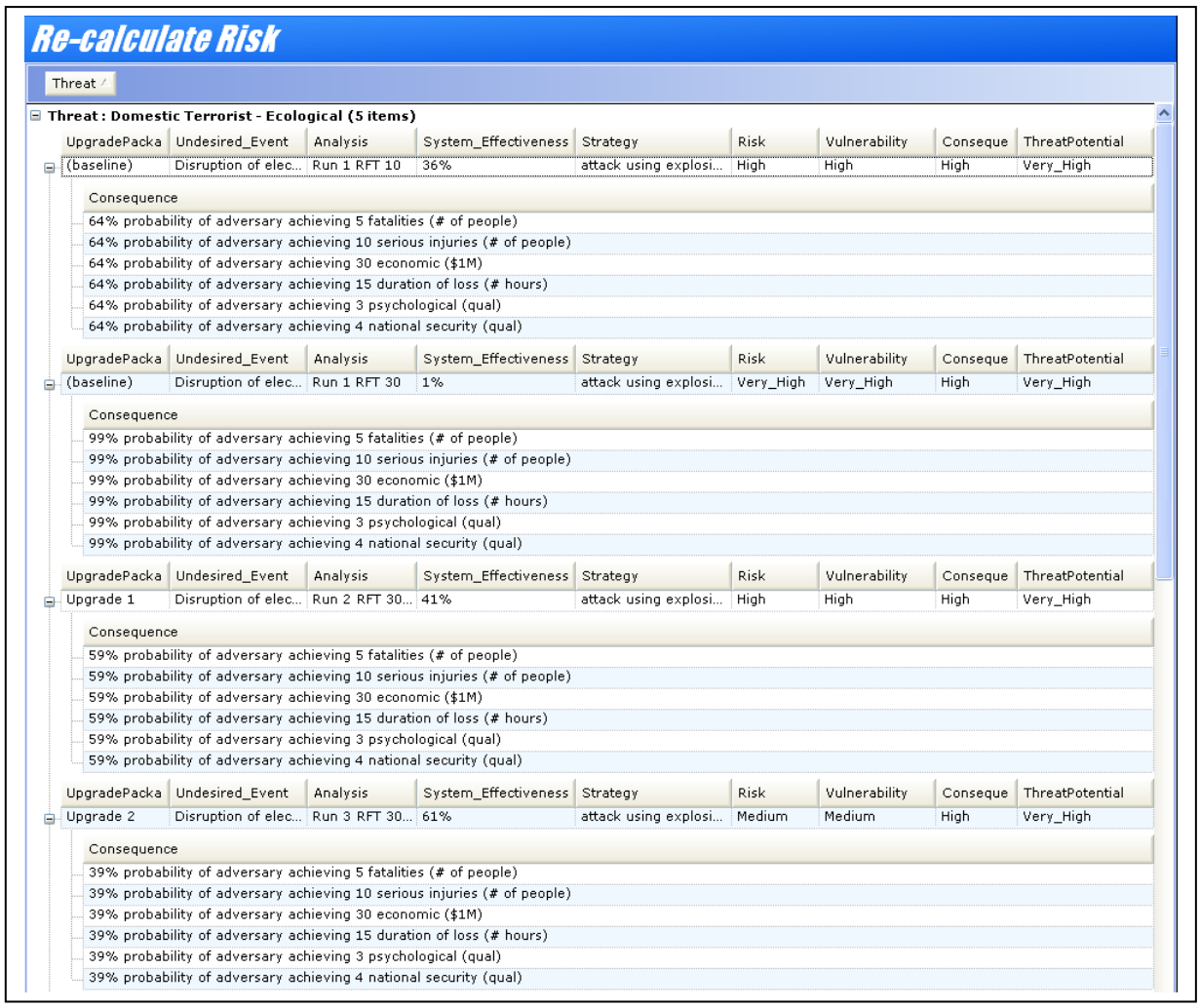

Figure 36. Summary Risk for Baseline and Upgrades

10.8 Evaluate Costs and Impacts

An upgrade for the protection system may impact several areas of the facility including costs, operations, schedules, and public opinion. The purpose of this section is to help the user identify costs and evaluate the impacts of alternative upgrade packages.

10.8.1 Costs

Because resources for security enhancements are limited, it is important that facility owners/operators have a methodology for making sound decisions regarding the allocation of limited resources among competing uses in general and specifically between alternative protection and mitigation strategies for dealing with the defined threats. Ideally such a methodology would allow the aggregation of costs and benefits across different threat scenarios and also allow comparison with other investments. Probably the single most important impact of upgrading the protection system is cost. For this reason one or more proposed packages may be evaluated in an attempt to optimize the cost versus benefit. After costs are estimated for each proposed upgrade package, cost information can be included in the upgrade package information. In the automated RAM tool, the user has the ability to provide input on costs for the proposed upgrade options.

10.8.2 Operations

Implementation of an upgrade package could have a negative impact on operations if it imposes significant changes or disruptions in normal operational practices and processes. An estimate is made of the impact imposed by the upgrade package(s) on operations, functions, and processes. In the automated RAM tool,, the user can describe and define the impact values for VL, L, M, H, and VH.

10.8.3 Schedules

Implementation of an upgrade package could have an impact on operational schedules if it imposes significant delays in normal operations. An estimate must be made of the impact on operational schedules imposed by the upgrade package(s). In the automated RAM tool, the user can describe and define the impact values for VL, L, M, H, and VH.

10.8.4 Public Opinion

Public opinion or political relations can be a factor for some upgrade packages. Credibility and acceptance by the public is an important aspect to the facility. An estimation of the impact on public opinion imposed by the upgrade package(s) must be made. In the automated RAM tool, the user can describe and define the impact values for VL, L, M, H, and VH.

10.8.5 Other Concerns

Upgrade packages could cause other concerns that are site-specific. Some of these could be impact on facility reliability, ratepayer vs. taxpayer issues, political sensitivities, etc. The user should identify any other sensitive issues that could be affected by upgrading the protection system or mitigating consequences. In the automated RAM tool, the user can describe and define the impact values for VL, L, M, H, and VH.

In the automated RAM tool, the user will provide qualitative input on operations, schedule, public opinion, and other potential impact areas and also provide a quantitative estimate of the initial costs, as shown earlier in Figure 32.

11. RISK ASSESSMENT REPORTING

After the completion of the automated RAM process, the last activity is reporting the results. Currently the automated RAM tool does not provide the user with a specific format. This section presents suggestions on how to organize the final security risk assessment report. The final report represents the efforts of the entire assessment team and becomes the basis for future risk-reduction efforts. Providing a well-considered, systematically organized final report accomplishes several goals including:

- Documents entire process including definitions and decisions.
- Makes it easy for others to follow the methodology.
- Contains an Executive Summary for management review.
- Creates a defensible end product.
- Streamlines the ability to update the assessment when conditions change.
- Provides a professional product.

The final report format presented here is an example. The content and format may be dictated by the CI sector.

11.1 Protection of Information

The information from the automated RAM assessment would be helpful to potential adversaries, as would any materials produced to support the analysis and the mitigation activities called for in the final report. It is the responsibility of the facility to define the process necessary to prevent this information from being improperly disseminated.

The organization of the final report is shown in Figure 37. It shows the primary subject areas in each chapter of the report as well as specific topic details within each chapter. The report flowchart also shows that after completion of the risk analysis, the facility management team is faced with a decision step: Is the calculated risk acceptable? (Is it below the threshold established by the facility owner/operator?) If the calculated risk is acceptable, then the application of the automated RAM tool is complete. If the calculated risk is not acceptable, then the application of automated RAM tool must be iterated. Note that the process is repeated until upgrades have reduced the risk and the established protection objectives are met.

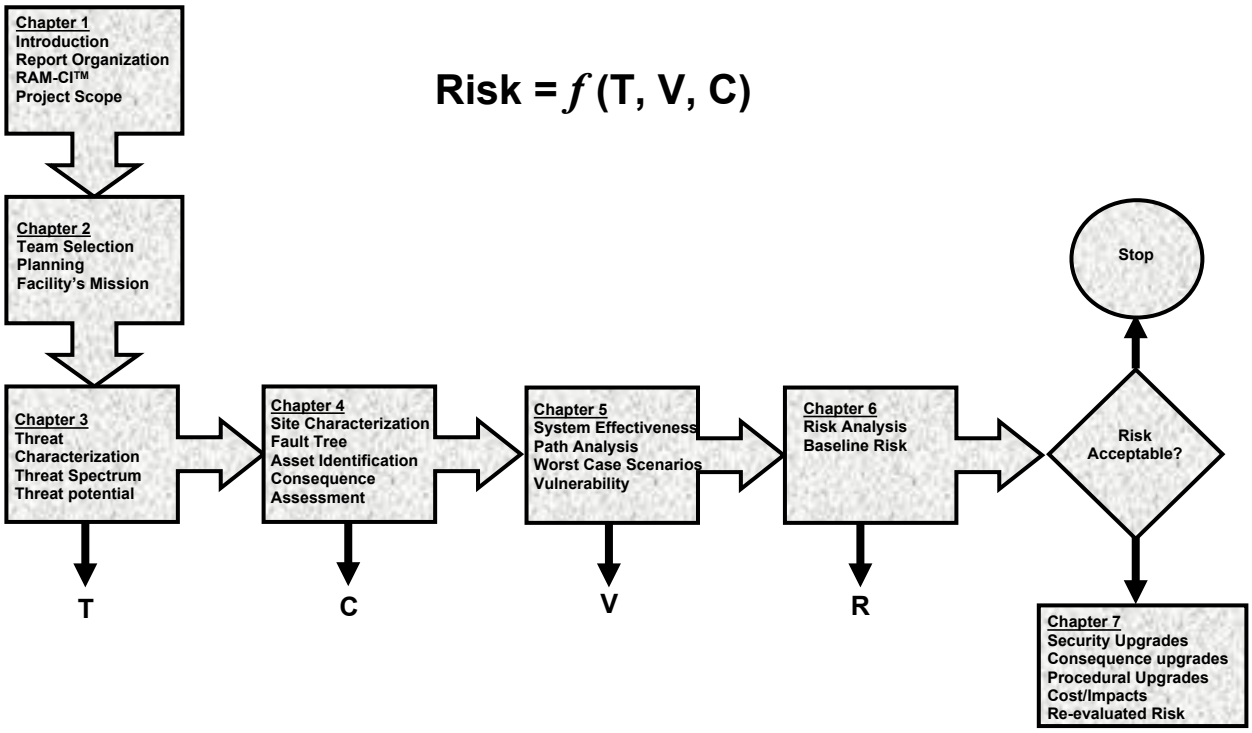

Figure 37. Organization of Final Report

11.2 Results Format

The format for a final report was not developed for the automated RAM prototype tool. The format for the final report, as well as the information potential users would want for presentations and briefings will be determined for the next release of the automated RAM tool.

12. SUMMARY

12.1 Conclusion

The primary product of this effort is a prototype automated security RAM tool for critical infrastructures. It leverages SNL's unique capabilities in security risk analysis and VA-based tools. The automated RAM prototype tool provides a sound scientific and technical framework with which to evaluate the total security risk at particular site or facility. The automated RAM tool provides a user-friendly, systematic, and comprehensive risk-based tool for CI sector and security professionals. It provides users with a rigorous approach to assess and manage security risk, identify vulnerabilities, and help to evaluate possible risk-reduction measures.

Although the automated RAM tool is still considered a prototype, it is a functional tool that follows the basic RAM steps. It is both a risk assessment and a risk management tool. The automated RAM tool has an optional high-level screening step in which the user can identify and prioritize facilities based on a defined set of consequence criteria. The planning provides a means for the user to document assessment goals, scope, team composition, and other items; define the facility's missions; and determine the facility's protection objectives. The facility characterization step includes the collection of facility information, a site-specific fault tree with which possible ways to cause undesired events are developed and potential targets are identified.. In the consequence assessment step, the user develops a consequence reference table, identifies the undesired events and the targets which, if attacked, may cause the undesired event, and provides input for each of the consequence criteria to define the severity level for the undesired events. The threat assessment step provides the user with the ability to identify both outsider and insider threats and define their motives, objectives, and capabilities. If sufficient information is available, the user can also develop an estimate for the threat potential. The system effectiveness step for the automated RAM tool includes a comprehensive approach that is unique among the many risk-based tools available. The user first defines the adversary strategy and targets. An ASD, which is a graphical representation of the facility that includes layers/areas and path elements between the layers, is then developed. Using an SNL database derived from many years of testing and SME reviews, each of the safeguard attributes for each of the elements is defined. A path analysis is then conducted to determine the worst-case paths and system effectiveness against those paths. A list of possible vulnerabilities is also identified for the PPS functions of detection, delay, and response. A risk value is then calculated and the probability that an adversary would cause an undesired event and consequence is provided. The risk assessment is now complete and a decision must be made as to whether the risk is acceptable. If the risk estimate is unacceptable, the automated RAM tool provides the user with the ability to identify possible risk-reduction measures and evaluate their impacts. Upgrade packages can be developed and the associated changes in risk, cost estimates, and impact to operations, schedule, and other areas can be provided to the decision makers. The final step in the process is reporting the assessment results, which will be developed in later releases of the automated RAM tool.

The automated RAM tool provides a comprehensive, risk-based, systems view, and rigorous automated capability. The automated RAM tool also supports the goal of the NIPP to "build a safer, more secure, and resilient America by enhancing protection of the Nation's critical CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by adversaries to destroy, incapacitate, or exploit them …" (2006). In particular, it provides processes for combining consequence, vulnerability, and threat information to yield a comprehensive and systematic risk assessment and management capability that can be applied to all CI/KR sectors. It meets the requirements for risk assessment methodologies outlined in the NIPP and supports national objectives identified by DHS and other federal agencies. It will provide an enhanced capability to address the determination of security risk in the different CI/KR sectors.

The automated RAM tool provides a proven risk-based systems approach to help decision makers in making cost-effective security decisions based on a rigorous systematic process. It is an integrated systems engineering approach. It provides the level of detail necessary to identify the vulnerabilities and possible risk-reduction measures. Finally, the RAM process and data used are repeatable, traceable, and defensible.

12.2 Capabilities and Future Development

The primary focus of the automated RAM tool is the evaluation of malevolent threat to the facility. Some of SNL's manual RAM and VA tools also include consideration of natural threats, human-caused non-malevolent threats, threats to cyber and process control systems, and the capabilities to apply blast effects analysis, chemical dispersion analysis, economic analysis, selected GIS capabilities, and other sector-specific areas analytical tools. These capabilities could be added to future releases of the automated RAM tool.

The development efforts have focused primarily on making all steps in the automated RAM process functional, rather than developing features such as the user interface, help sections, and additional information. The general layout of the automated RAM tool follows the RAM process and is relatively easy to navigate and perform the necessary operations. With additional resources the automated RAM tool can be adapted to meet the specific needs of the CI sectors/areas and additional capabilities can be added as required. The automated RAM tool has been tested on hypothetical facilities only.

The automated RAM tool:

- Provides users with a rigorous approach to assess and manage security risk, identifies vulnerabilities, and helps to evaluate possible risk-reduction measures.
- Uses a fault tree to model ways to cause undesired events and a PPS database to analyze for vulnerabilities.
- Uses a fault tree to identify assets that need to be protected.
- Provides a risk-based approach that is science-based and yields values for the three risk components that are repeatable and traceable.

- Uses site-specific information to determine consequences for each undesired event.
- Determines PPS effectiveness and identifies protection system vulnerabilities using adversary path analysis and safeguard performance data for identified path elements.
- Helps user to identify vulnerabilities for contingency planning, develop possible courses of action, and evaluate impacts on operations, safety etc. The tool can be used to design new (effective) protection systems.
- Meets DHS NIPP risk assessment methodology criteria and can become RAMCAP (Risk Analysis and Management for Critical Asset Protection)-compliant.
- Provides an approach that adapts easily and can be tailored to meet the needs of different CI sectors.

12.3 Availability of the Automated Risk Assessment Methodology Tool

The automated RAM tool is still a prototype and is not yet available to potential users. Currently SNL is communicating with different federal agencies and CI sectors to identify requirements for potential application to different CI sectors. The automated prototype RAM tool can be used in its current version to evaluate some different CI sector facilities. The intent is to use the basic automated RAM framework and adapt it to meet the needs of different CI sectors.

The focus during the development of the automated RAM prototype tool was to make it a functional tool. The user interface, instructions to the user, help sections, and the user's guide will be developed, based on input from potential users. A training course is also planned to support the automated RAM tool; this course could also include sector-specific instruction.

The automated RAM tool has been copyrighted as SNL intellectual property. More information about the automated RAM tool, other SNL RAMs, and contact information can be found on SNL's RAM web page at http://www.sandia.gov/ram/.

REFERENCES

Biringer, Betty E., Matalucci, Rudolph V. and O'Connor, Sharon L., 2007. *Security Risk Assessment and Management*, John Wiley & Sons, Hoboken, NJ.

Garcia, Mary Lynn, 2008. *The Design and Evaluation of Physical Protection Systems*, Edition 2, Reed Elsevier (Butterworth-Heinemann), Boston, MA.

Garcia, Mary Lynn, 2006. *Vulnerability Assessment of Physical Protection Systems*, Reed Elsevier (Butterworth-Heinemann), Boston, MA.

Freeman, J. W., Darr, T. C., and Neely, R. B., 1997. *Risk Assessment for Large Heterogeneous Systems*, IEEE Proc. 13th Annual Computer Security Applications Conference, pp. 44-52,

Modarres, M., 1993. *What Every Engineer Should Know About Reliability and Risk Analysis*, Marcel Dekker, Inc., New York, NY.

Sandia National Laboratories, October 2002. Risk *Assessment Methodology for the Water Utilities (RAM-W™*), version 2*,* Sandia National Laboratories, Albuquerque, NM.

Sandia National Laboratories, February 2002. *Risk Assessment Methodology for Electric Power Transmission (RAM-T™)*, Sandia National Laboratories, Albuquerque, NM,

Sandia National Laboratories, September 2007. *RAMCAP-Compliant Risk Assessment Methodology for Water and Wastewater Utilities (RC-RAM™), version 1.0,* Sandia National Laboratories, Albuquerque, NM

U.S. Department of Homeland Security, 2006. National Infrastructure Protection Plan

DEFINITIONS

Adversary – **A** person performing malevolent acts in pursuit of interests harmful to the facility; an adversary may be an insider or an outsider.

Adversary path – An ordered collection of actions against a target that, if completed, results in successful theft or sabotage.

Adversary scenario – A detailed description of how the adversary strategy is accomplished (including task times).

Adversary strategy – An overall plan used to achieve the adversary's objective under advantageous conditions.

Adversary strategy, most vulnerable –The adversary strategy to which the security system is most vulnerable. The *most vulnerable adversary strategy* is the one most advantageous for the adversary to pursue.

Adversary tactic –The employment of available means to prevent a system feature from accomplishing its purpose. The feature may be part of the security system or a critical asset.

Analysis – The separation of an intellectual or material whole into its constituent parts for individual study. In the context of risk management, a broad, unconstrained consideration of risk and its component factors aimed at improving the ability to make informed decisions.

Assessment – The application of a method or methodology to measure or produce a decision-support product, with specific constraints in scope.

Asset – Any people, facility, physical system, cyber system, material, information, activity, or intangible attribute that has positive value to an owner or to society as a whole and requires protection.

Baseline risk – The estimated existing level of risk for an organization's critical asset(s) and defined threat.

Collusion – An attack in which adversary types collude, as in outsiders working with insider(s).

Conditional Probability – The probability of an event, such as in an event tree branch, that is determined based on the assumption or condition that a previous event has occurred. At any node of an event tree, the sum of the conditional probabilities associated with each of the events or branches immediately following that node should equal 1.

Conditional Risk – A measure of risk that focuses on consequences, vulnerability, and adversary capabilities, but excludes intent. It is used as a basis for making long-term risk-management decisions. The adversary capabilities, countermeasures, and residual vulnerability are often combined into a measure of likelihood of adversary success.

Consequence – The outcome of an event occurrence, including immediate, short- and long-term, direct, and indirect losses and effects. Loss may include human casualties, monetary and economic damages, and environmental impact. Loss may also include less tangible and therefore less quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness, or other impacts.

Consequence Management – Consequence management is predominantly an emergency management function and includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by an unwanted event.

Covert attack – A stealthy attack.

Countermeasure – An action, device, or system used to eliminate, reduce, or mitigate risk by affecting an asset, threat, or vulnerability. Security countermeasures are intended to reduce the probability that an attack will occur or, if an attack does occur, to reduce the probability that the attack will succeed in causing a failure or significant damage.

Critical assets – Those assets that are essential to meeting the mission objectives. Security systems are intended to assure that the mission continues to be performed despite malevolent intervention by humans. Identification of the critical assets is necessary before designing, evaluating, or upgrading a security system for their protection.

Critical detection point (CDP) – The final detection point that allows effective response force function.

Defend – The use of security countermeasures to prevent an adversary from succeeding in an attack or other threatening activity.

Delay – The element of a physical protection system designed to impede adversary penetration into or exit from the protected area.

Deny – The use of security countermeasures to prevent an adversary from succeeding in an attack or other threatening activity.

Detect – The determination that an unauthorized action has occurred or is occurring; detection includes sensing the action, communicating the alarm to a control center, and assessing the alarm. Detection is not complete without assessment.

Deter – The use of security countermeasures to discourage an adversary from attempting an attack by inducing fear, uncertainty, or doubt about the successful completion of the attack.

Emergency Response – A response to emergencies, including both natural disasters, such as fire, flood, earthquakes, and the like and human-induced events, such as civil commotion, adversary attacks, and the like, in order to protect lives and limit damage to property and impact on operations.

Facility – This term is commonly used to describe a fixed manufacturing site or installation. However, the more general term *asset,* as used in this document, includes facilities as well as other types of assets.

Fault Tree – A graphic, logical representation of the relationships among the mission objectives of the facility and the critical assets that support the objectives. A fault tree is built from the adversary's point of view, describing events that cause the facility to fail to meet its objectives by misusing, disabling, or destroying critical assets. From the point of view of energy infrastructure security, every event on the tree is an undesirable event.

Frequency – The rate of occurrence of an event measured in terms of the number of a particular type of event expected to occur in a particular time period of interest.

Insider – A person who, by reason of official duties, has knowledge of operations and/or security system characteristics, and/or position that would significantly enhance the likelihood of successful bypass or defeat of positive measures should that person attempt such an action.

Intent – An adversary's goals and the value that the adversary would ascribe to achieving these goals through a particular means, as determined by expert judgment. In terrorism, intent can be associated with symbolic goals, *i.e*., attacks against cultural symbols or against targets where there was a prior failure, with types or categories of assets as targets, *e.g*., buses in Israel, or U.S. embassies, or with the demonstration of an adversary's capability; *e.g*., certain weapons of mass destruction (WMDs).

Likelihood – A description of the chance of the occurrence of a particular event.

Methodology – An organized, documented set of procedures and guidelines for one or more processes, such as assessment or design. Many methodologies include a record-keeping feature for documenting the results of the procedure, a step-by-step approach for carrying out the procedure, an objective set of criteria for determining whether the results of the procedure are of acceptable quality, and the reasoning associated with the process.

Mitigation (Consequence Mitigation) – Pre-planned and coordinated actions or system features that are designed to reduce or minimize the damage caused by attacks (consequences of an attack); support and complement emergency forces (first responders); facilitate field-investigation and crisis-management response; and facilitate recovery and reconstitution.

Non-malevolent threat – For this methodology a non-malevolent threat is either (1) a weather-induced or -related event (e.g., hurricane, intense precipitation, storm surge), (2) a physical phenomenon-induced event (e.g., seismic event), (3) an accident-induced event (e.g., transportation accident, accidental toxic gas or material release, pipeline accident), or (4) a wildlife-induced event (e.g., insects) that has the potential to disrupt the operations of a facility. In other words there is no malicious intent associated with the event that has the potential to disrupt facility operations.

Outsider– A person who does not have official business with the facility or has not been granted routine access to a program, operation, facility, or site; a person who is not authorized to enter a protected or vital area.

Overt attack – An attack in which open force is used.

Path – Route taken by an adversary from offsite through areas and path elements to reach the target and, optionally, to return offsite. A path is part of a scenario.

Performance test – A test that confirms the ability of a system element (or total system) to meet an established requirement (i.e., has required sensitivity). For a security system, as an example, this may mean measuring or collecting performance data on security response times under various conditions to ensure the system meets minimum required response times. Tests may be limited scope (test only one element) or may be full performance and measure the entire system.

Physical Protection System or PPS – Provides notification that a malevolent act is being attempted (detection), makes it difficult and time-consuming for an adversary to complete the malevolent act (delay), and allows a security force enough time to stop the adversary (response).

Probability – A measure of the likelihood, chance, or odds that a particular outcome or consequence will occur. A probability provides a quantitative description of the likelihood of occurrence of a particular event. This is usually expressed as a mean value between 0 and 1, with an associated minimum and maximum range. However, probability can also be expressed in qualitative terms (*e.g*. low, moderate, high), if there is a common understanding of the relative meaning of the qualitative terms among the stakeholders. The probability must be associated with a specific outcome and either a defined time frame (*e.g.*, range of probability that a threat occurs in one year) or set of trials(*e.g*., range of probability of detecting a particular type of intrusion given 10 attempts or range of probability that a consequence mitigation action is successful given a demand).

Protection System – A security system that includes both aspects of a physical protection system and operational design system.

Qualitative– Concepts that cannot be communicated through a natural metric, such as national security consequences or judgments of potential interactions between adaptive humans. Such concepts must sometimes be stated descriptively and specifically, but wherever possible should be couched in a measure that allow comparisons. Qualitative measures can be linguistic, *e.g*., high, medium, low or quantified, *e.g*., a scale of 1 to 10.

Qualitative Risk Assessment – An appraisal of risk that uses linguistic terms and measurements to characterize the factors of risk. If possible qualitative assessments should be couched in terms of a consistent measure that allows comparisons between assets. Qualitative measures can be linguistic, *e.g.*, high, medium, low, or quantified, *e.g*., a scale of 1 to 10.

Quantified – A quantitative measure that uses numbers as a proxy for language. This enables greater accuracy in communication of things that fall within ranges and facilitates the use of mathematical formulas to combine the elements of risk.

Quantitative – Concepts that are easily communicated through a natural metric, such as numbers of lives, dollars, frequency, etc.

Quantitative Risk Assessment – An appraisal of risk that uses numerical measures to describe factors in the analysis. If possible, quantitative measures should be used to allow clear, defensible, and accurate comparisons between assets.

Response – The element of a physical protection system designed to counteract adversary activity and interrupt the threat.

Response force – The guards and external agencies that respond immediately to counter the threat of an adversary.

Response time – The time between the verification of an alarm and the interruption of an attack.

Residual Risk – The amount of risk remaining after the net effect of risk-reducing actions are taken. The residual reflects the impact of threats that are not deterred, consequences that are not avoided through devaluation, and vulnerabilities that are not reduced through countermeasures.

Risk – The potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences. It is measured as the combination of the probability and consequences of an adverse event, i.e., threat. When the probability and consequences are expressed numerically, the expected risk is computed as the product of those values with uncertainty considerations. In security, risk is based on the analysis and aggregation of three widely recognized factors: threat, vulnerability, and consequence.

Risk Analysis – A flexible and loosely structured method for studying the nature of, and relationship between, the components of risk in order to understand the likelihood of loss. Risk analyses are typically broader in scope than risk assessments and should consider the uncertainty of the information upon which they are based. A risk analysis can involve risks to multiple assets or geographic regions or explore risks that affect the nation broadly.

Risk Assessment – A structured method for characterizing the risks to an asset based on a review of identified threats, vulnerabilities of the available protection system, and the consequence-mitigation measures. Risk assessments provide the basis for rank ordering of risks usually at the asset level, and help establish priorities for the application of countermeasures.

Risk Management – The deliberate process of understanding risk and deciding upon and implementing action, e.g., defining security countermeasures, consequence-mitigation features, or characteristics of the asset ?, to achieve an acceptable level of risk at an

acceptable cost. Risk management is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned or accepted value.

Risk reduction – Risk is reduced by preventing the undesired event, by mitigating the consequences of the event, and by protecting against the DT using PPS improvements.

Scenario – Outline of events along a specific path by which the adversary plans to achieve his objective.

Scenario, most vulnerable – The scenario that takes the greatest advantage of the vulnerabilities of the security system.

Site – A geographic location providing a particular function or purpose.

System – An integrated combination of people, property, environment, and processes that work in a coordinated manner to achieve a specific desired output under specific conditions. As used in this document, a system encompasses the set of one or more assets and their associated environment, e.g., threats, vulnerabilities, consequences, and buffer zone attributes?, that are being considered in a risk analysis.

Target – An asset or one or more systems, subsystems, or other endeavors within an asset that a threat is intended to disrupt, damage, or destroy.

Terrorism – Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intending to influence an audience (Title 22 of the Untied States Code, Section 2656f(d)).

Terrorist – An agent of a sub-national group who uses premeditated, politically motivated violence against non-combatant targets, usually intended to influence an audience (derived from Title 22 of the United States Code, Section 266f(d)).

Threat – Any indication, circumstance, or event with the potential to cause the loss of, or damage to, an asset or population. In the analysis of risk, threat is based on the analysis of the intention and capability of an adversary to undertake actions that would be detrimental to an asset or population.

Threat Analysis – The study or assessment of threats including adversary capability, intent, and incidents that may be indicators of adversary activities.

Uncertainty – A measure of knowledge incompleteness and inconsistency due to inherent deficiencies in acquired knowledge. Also, a characterization of the degree to which the state of a system is unsettled or in doubt, such as the uncertainty of the outcome. In a quantified risk assessment, uncertainty is a representation of the confidence in the state of knowledge about the models and parameter values used.

Upgrade– Modification of an existing physical protection system to improve the system's effectiveness.

Vulnerability – Any weakness in an asset's or infrastructure's design, implementation, or operation that can be exploited by an adversary. Such weaknesses can occur in building characteristics; equipment properties; personnel behavior; locations of people, equipment, and buildings; or operational and personnel practices.

Vulnerability Analysis/Vulnerability Assessment – A systematic examination of the ability of an asset, including current security and emergency preparedness procedures and controls, to withstand a threat. A vulnerability analysis may be used to compute the probability that a particular attack will succeed; compute the probability of significant damage, destruction, or incapacitation of all or part of an asset resulting from a given threat; identify weaknesses that could be exploited; and predict the effectiveness of additional security measures in protecting an asset from attack.

Weapon of Mass Destruction (WMD) – Generally, a WMD is any weapon capable of inflicting a large number of deaths immediately or over a period of time. Examples are chemical, biological, radiological, or explosive weapons.

ATTACHMENT A: FAULT TREE

Generic Undesired Event Fault Tree

The user will need to focus on those parts of the operation that must be functional for the facility to meet the mission objectives and that will be used as a starting point in the fault tree analysis described in this section. The fault trees are developed to describe the entire system, at least at a high level. The generic undesired event fault tree is applied to the specific facility or asset that is being assessed. The main purpose of constructing a fault tree is to identify all potential undesired events that can occur at the facility. If any potential WMD events are identified, they should be included in the analysis. The fault tree can be developed in more detail as necessary, allowing for more detailed analysis.

The event fault tree shown in Figure 38 illustrates the top levels for an undesired event of loss of a facility's mission. The malevolent branch has been expanded to consider several possible ways the facility could lose mission capability through a malevolent event. A similar set of activities could be developed for the natural/non-malevolent branch. In addition to physical events, SCADA/process control events could also be included in the event fault tree.

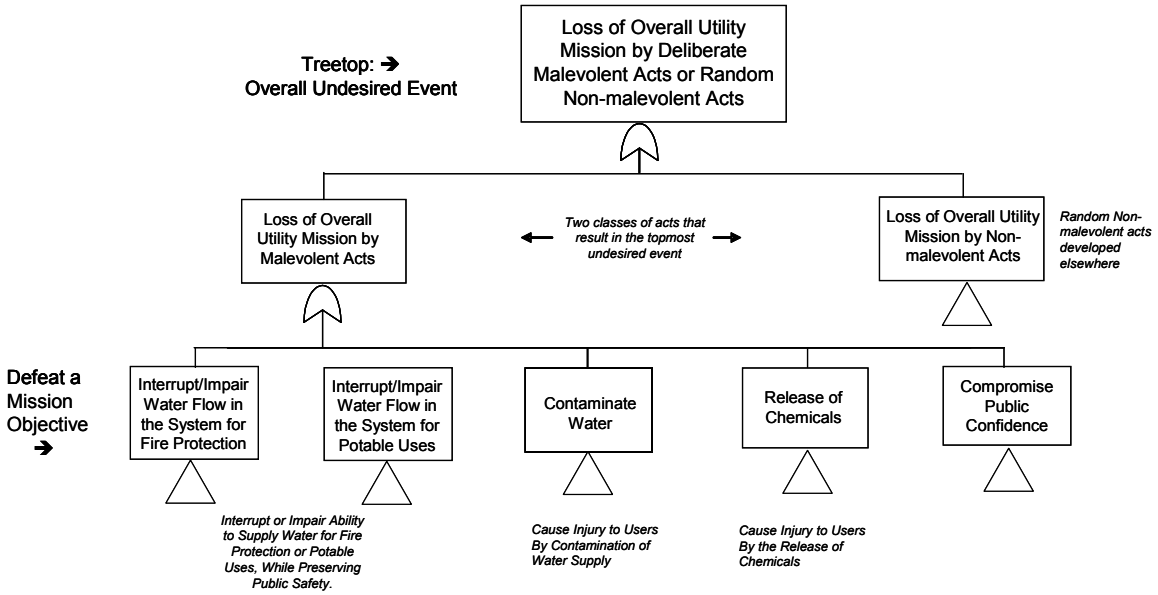

Figure 38. Upper Levels of Generic Undesired Event Fault Tree

Introduction to the Fault Tree

The entire fault tree is constructed from the adversary's point of view. It describes how the overall mission and mission objectives of a facility system can be defeated. The most generalized events are found in the upper layers of the tree. As the causes of these events are developed deeper in the tree, adversary strategies and the targets of attacks are revealed. The events can be numbered in outline format beginning at the second layer and proceeding downward. The upper levels of the generic undesired event fault tree are described in this attachment.

Upper Levels of the Generic Undesired Event Fault Tree
The upper levels of the generic undesired event fault tree are shown in Figure 38. They depict the topmost undesired event (the overall mission of the facility) and the mission objectives (written as undesired events) are found on the second level of the fault tree. In this example the undesired event may occur through malevolent or non-malevolent/natural acts. The event fault tree and subsequent discussion are for malevolent acts. An analogous set of events would exist for the non-malevolent/natural events.

Treetop – Defeat Overall Mission
The overall goal of the adversary is stated in the topmost event (treetop): the adversary seeks to *defeat the mission of the system by deliberately, malevolently causing an undesired event*. The treetop is the first layer of the tree. Every event on the tree is undesired from the viewpoint of the facility (but desirable from the adversary's point of view).

Layer 2 – Classes of Acts That Would Result in Loss of Overall Mission
In layer 2 the fault tree splits into two possible acts that could cause the loss of the overall mission. It is important for each facility to develop a site-specific malevolent and non-malevolent branch because it may have different undesired events and critical assets associated with it than the malevolent branch. Information from the non-malevolent branch will be used in the non-malevolent vulnerability and risk analyses. The discussion in the following sections pertains to the malevolent branch of the tree.

Layer 3 – Defeat Mission Objectives
The third layer of the fault tree consists of events that cause the defeat of mission objectives of the facility system. In the example a mission objective of the facility is to continuously maintain a flow of water to their customers; therefore Undesired Event 1 is *Interrupt or impair water flow in the system.*

Layer 4 – Attack a Major Stage of the Facility
The third layer of the tree partitions Events 1 and 2 into attacks on a major stage of the facility. The development of Event 1 could, for example, follow the progress of water through the facility from source, through pretreatment and treatment, to distribution to the customer. The undesired events at this level address attacks made at these stages to interrupt or impair water flow. The development of Event 2 could address a contamination act before distribution, where pretreatment or treatment occurs, or in the distribution system.

Layer 5 – Adversary Strategies and Critical Assets
The fifth layer of the tree shows diverse adversary strategies to cause each fourth-layer event. At this level of development and deeper, assets are identified that are critical to the operations of the facility. For example, at this level events could address such assets as critical pump systems, critical valve systems, process control system, critical pipelines or conduits, etc.

Process for Customizing the Fault Tree
The two activities that may be necessary when customizing the generic fault tree to create a site-specific facility are pruning and grafting. To apply the generic fault tree to a specific facility, it may be necessary to delete (prune) irrelevant strategies and/or assets and modify descriptions to match the specifics for that facility. Similarly, for those features (mission

objectives, undesired events, assets, etc.) not shown on the fault tree, add (graft) them at the correct location and develop them in enough detail to understand what an adversary might do to compromise that specific feature.

The user will continue working through the fault tree until a customized version is created for the specific facility being analyzed.

Protecting Fault Tree Information

The resulting fault tree is site-specific and thus provides sensitive information regarding disruption of a function/mission. The fault tree is a roadmap that provides detailed information an adversary can follow to cause the topmost events on the fault tree. Protection of the site-specific fault tree is of utmost importance.

ATTACHMENT B: ADVERSARY SEQUENCE DIAGRAMS

The first step in creating an ASD is either to use existing layouts or draw the facility and then identify possible adversary paths (Figure 39) and identify the concentric areas (adjacent physical areas) through which the adversaries must pass as they proceed from offsite to the critical asset. In between these areas are layers that bound each area and through which the adversary must pass. In these layers are physical protection elements (detection elements or delay elements). An ASD includes protection layers indicating every way that the adversary may pass from one area to the next; these must include all possible areas. An example of the path layers for an ASD for a hypothetical Treatment Plant 2 is shown in Figure 40. The ASD with the path elements is shown in Figure 41.

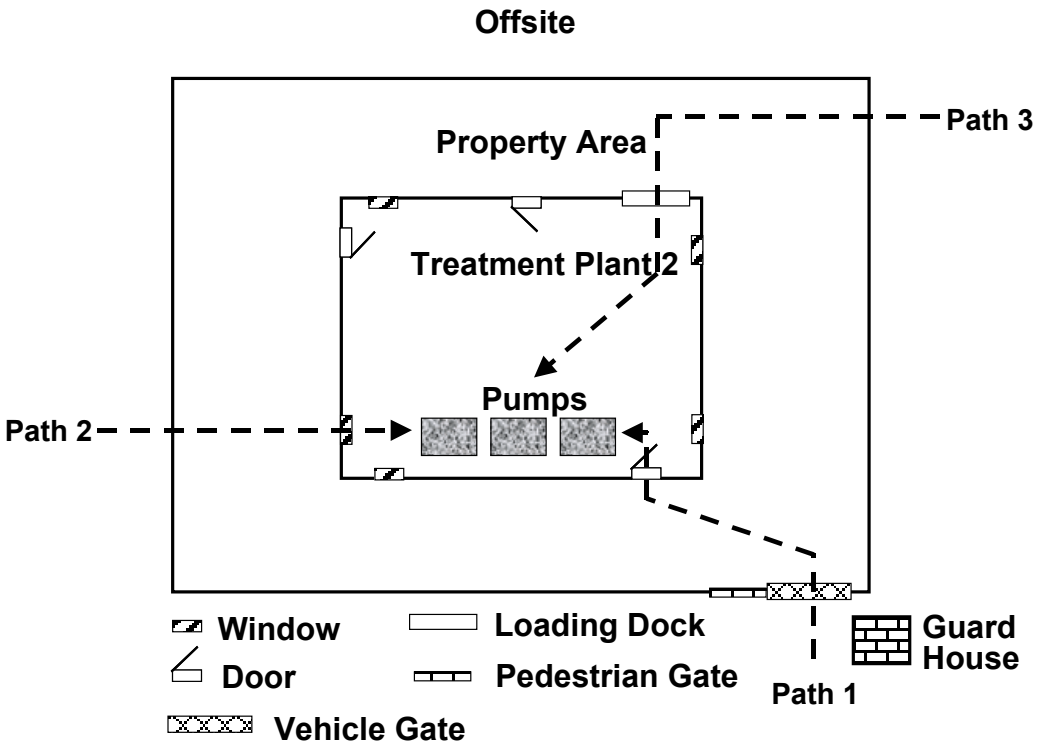

Figure 39. Adversary Path Development for an Example Facility

For Treatment Plant 2, there are four path elements between Offsite tand the Property Area and five path elements between the Property Area and the Treatment Plant 2. If many elements share the same characteristics, they are modeled as one path element on the ASD (e.g., all pedestrian doors are represented as Door). The final single step occurs when the adversary is in the presence of the critical asset and takes the necessary time to complete the task. There may be detection and delay elements associated with the final task.

The physical paths that adversaries can follow to cause the undesired event and the PPS and operational design features along the paths are important in determining the adversary attack scenario most likely to succeed. All possible adversary paths should be considered.

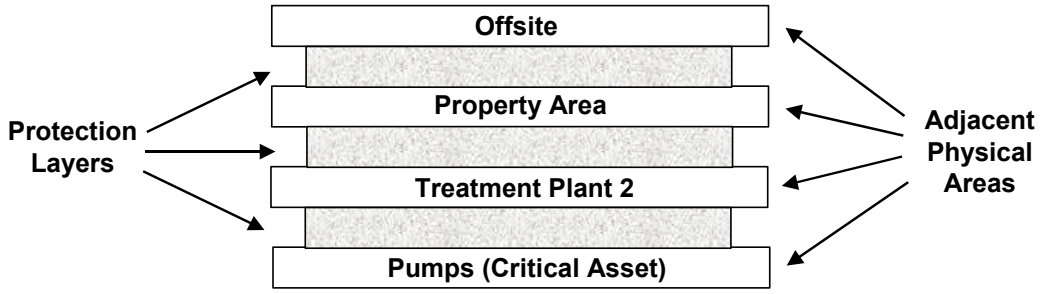

Figure 40. Example Protection Layers for an Adversary Sequence Diagram

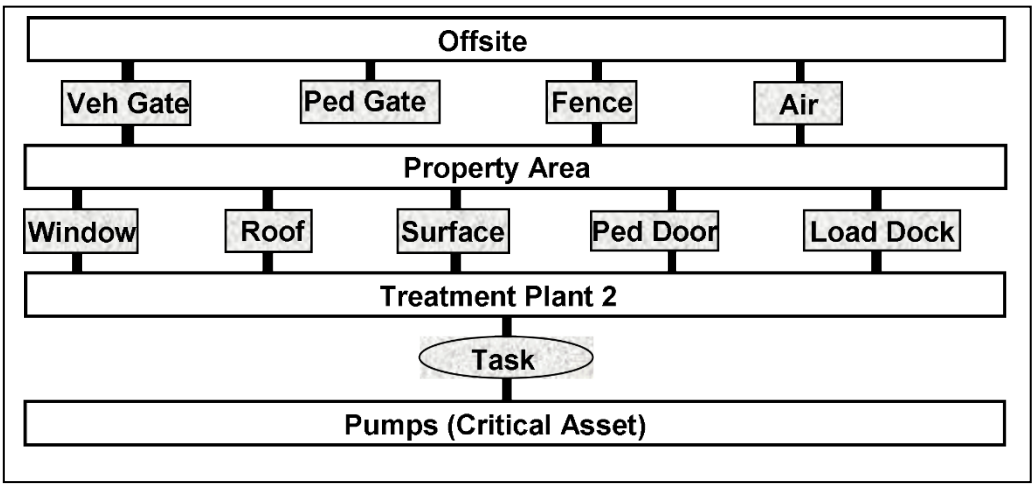

Figure 41. Example Adversary Sequence Diagram

There are many paths that an adversary could take to get to the asset. In this simple example three paths are shown, but there are numerous possible paths:

- They could use many ways to get into the Property Area.
  - Through, over, or under the pedestrian or vehicle gates
  - Through, over, or under the fence
- They could then use many ways to get into the building to sabotage the pumps.
  - Through the door (pedestrian or loading dock)
  - Through the window
  - Through any of the building surfaces (walls and roof)

There are many possible combinations of ways to get to the asset and sabotage or damage it. An ASD is needed to visualize all the possible paths. The ASD will aid the user in postulating worst-case paths. Note that ASDs are used to determine physical paths only. (ASDs are not used for cyber paths).

Distribution

Internal:

1	MS 0759	Cal Jaeger, 6411
1	MS 0759	Nate Roehrig, 6411
1	MS 0759	Teresa Torres, 6411
1	MS 0759	Betty Biringer, 6411
1	MS 0899	Technical Library, 9536 (electronic copy)