DRAFT

Report #05-023

Risk Analyst Workbench Design and Architecture

Orosz, M.

CREATE REPORT
Under FEMA Grant EMW-2004-GR-0112

August 31, 2005

Center for Risk and Economic Analysis of Terrorism Events
University of Southern California
Los Angeles, California

Acknowledgment

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), grant number EMW-2004-GR-0112. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the U.S. Department of Homeland Security.

Executive Summary

The CREATE Risk Analyst Workbench (RAW) is a software tool that provides modeling and analysis capabilities for the risk analysis and decision analysis steps of the CREATE Terrorism Modeling System (CTMS). RAW provides a mechanism for extracting data from external sources, building libraries of data for internal use and linking models to support other modeling steps. RAW guides the risk analyst through the steps of threat and counter-measure characterization, probability estimation, outcome definition, and scenario creation. It also provides tools for rating outcomes of threats, effectiveness of counter-measures, and prioritizing investments.

RAW will be executable in a classified, "official use only" or public environment. When security is needed, sensitive information, such as specific intelligence, may be restricted to authorized users. RAW is also being designed with the capability for networked analysis and distributed sharing of information, combined with information security when needed. By collaboratively integrating their models and data, analysts can perform far more complicated assessments, far more quickly, than previously possible.

This document defines the system requirements, the preliminary system software design, list of deliverables, and development plan.

Table of Contents

1 Introduction

The CREATE Risk Analyst Workbench (RAW) is a software tool that provides modeling and analysis capabilities for the risk analysis and decision analysis steps of the CREATE Terrorism Modeling System[1] (Figure 1-1). RAW also provides a mechanism for extracting data from external sources, building libraries of data for internal use and linking models to support other modeling steps. RAW guides the risk analyst through the steps of threat and counter-measure characterization, probability estimation, outcome definition, and scenario creation. It also provides tools for rating outcomes of threats, effectiveness of counter-measures, and prioritizing investments.

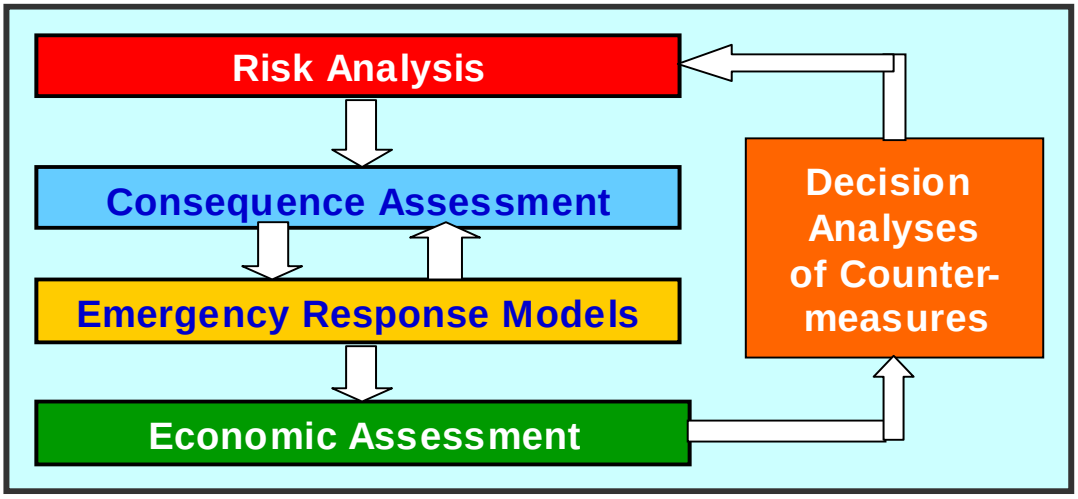

Figure 1-1 CTMS Four-step modeling system

This document defines the system requirements, the preliminary system software design, list of deliverables, and development plan.

2 The Problem

2.1 Current Homeland Security Risk Analysis Environment

Formal quantitative risk analysis has been an important tool for defending against mechanical system failure and project failure or delay. Many software packages have been constructed for aiding in analyzing project or mechanical system risk. Risk analysis is now being used for assessing the risks of terrorist attack. Terrorism is similar to mechanical systems in that, given an event, a chain of dependencies and consequences can be examined to estimate the likely outcomes and the value of mitigation efforts can

[1] Hall, R. (2005). "Assessment Guidelines for Counter-Terrorism: CREATE Terrorism Modeling Systems (CTMS) ," CREATE Report

studied. Unlike traditional mechanical system failure or project risk, terrorism is the result of intelligent attackers, making decisions about whether to attack, what to attack, when and how. Terrorists, unlike natural or mechanical threats, can observe some or all of the mitigation efforts of the defender and possibly adjust to them. Existing risk analysis packages generally lack a framework for capturing adversarial behavior. The estimation of consequences given a terrorist event may involve complex models of damage, human, physical, and economic. While some risk analysis software incorporates such models, the packages are frequently closed to adding models without significant programming.

Homeland Security risk analysis requires goal-driven interdisciplinary collaborations between researchers from multiple disciplines, including engineering, information technology, economics, and social and life sciences at multiple locations. Such collaborations might cross over all stages of risk analysis including scenario definition, model development, and result analysis.

Currently, a lack of a common framework prevents effective collaborations among researchers both locally and across the nation. The following are some of the problems that result from ineffective collaboration and connectivity among risk assessment researchers and data.

- Redundant scenarios. Multiple representations of the same risk scenario due to a lack of standards and collaboration among risk assessment researchers
- Mixed vocabulary. Scenario developers don't share the same vocabulary in their scenario definitions.
- Multiple models. Model developers develop models using different tools and languages (e.g., in-house developed, Analytica, MATLAB, @risk for Project, Crystal Ball, etc.,).
- Reduced usability: Running risk models developed by other researchers requires considerable effort to prepare, install, configure, and execute the model.
- Reduced availability. Limited access to available risk models developed by various researchers
- Limited model workflow generation capabilities. Due to the difficulties of running risk models developed by other researchers, composing and running a risk analysis workflow composed of chaining multiple models is difficult and is usually undertaken as a manual process.
- Limited data sharing. Output generated is not readily available to the risk analyst community. Users currently publish their results and view peer generated results in some informal way (via symposium publications, web pages or email communications), however, direct access to the data in a timely fashion is currently not available. In a dynamic environment where real-time information sharing is crucial, the current approach is not effective for sharing among a large number of researchers.
- Reduced situational awareness. Changing conditions (e.g., data, political, policy, etc.,) can render current and previous risk assessment decisions invalid.

2.2 Motivation/Vision of RAW

The goal of this work is to develop a Windows based software modeling system -- called the "Risk Analyst Workbench (RAW)" -- that provides modeling and analysis capabilities for the risk analyst and decision-maker. RAW provides a mechanism for extracting data from external sources, building libraries of data for internal use and linking models to support other modeling steps. RAW guides the risk analyst through the steps of threat and counter-measure characterization, probability estimation, outcome definition, and scenario creation. It also provides tools to the decision-maker for rating outcomes of threats, effectiveness of counter-measures, and prioritizing investments.

RAW will be executable in a classified, "official use only" or public environment. When security is needed, sensitive information, such as specific intelligence, may be restricted to authorized users. RAW is also being designed with the capability for networked analysis and distributed sharing of information, combined with information security when needed.

RAW is executed in the following steps:

1. Select problem type: Problems are divided into four broad classes: portfolios, programmatic investments and policies, targeted investments, and acting on intelligence[1].
2. Define Threat: A set of threats is defined according to the attributes defined by CREATE[1]. The user is asked to rate a threat according to various attributes, either subjectively, or by calling on data or models to support the assessment. RAW then guides the user in the creation of threat scenarios.
3. Define Counter-Measures: The user inputs, or selects, a set of alternative counter-measures to associate with the threats.
4. Matrixing Counter-Measures and Threats: RAW guides the user in rating the effectiveness of counter-measures relative to a set of defined threats. RAW assists the user in identifying sets of counter-measures that are most effective against a spectrum of threats.
5. Probability Generation: RAW interviews the user, or a collection of participating experts, to elicit probability estimates for alternate threat scenarios. RAW also searches relevant databases to locate information to support probability estimates. Using game theory derived models, RAW estimates changes in probabilities resulting for intervention strategies, to produce estimates of incremental change in risk.
6. Evaluation Based on a selected set of interventions, RAW estimates effectiveness according to multiple outcome measures. When desired by the user, RAW calls consequence, emergency and economic models to estimate outcome measures. RAW estimates effectiveness of interventions based on modeled scenarios, data libraries on prior analyses, and human judgments.
7. Exploration and Presentation: RAW provides a set of interactive graphical

displays to explore and compare alternative interventions. Users can change intervention strategies and visualize cost-effectiveness. Graphical displays will include:

- Display of terrorist scenarios and interventions in the staircase format
- Matrices and networked diagrams showing the matching between threats and interventions
- Icons showing relative effectiveness of interventions
- Maps showing areas affected by threats and interventions.

2.3 Survey of Existing Solutions

In the risk analysis and assessment field, there are many existing software solutions that model and assess risks ranging from mechanical failure of mission-critical machinery to the impact of earthquakes and other natural disasters on infrastructure (e.g., HAZUS[2]). Many of these models address a specific domain and, in many cases, focus on one or two areas of the risk scenario sequence (i.e., selection of target, obtaining the weapon, positioning of weapon or weapons, undertaking the attack, estimating the consequences, evaluating the impact, etc.,). For example, Foretell by DecisionPath[3] is used to assess the consequence of an event occurring (i.e., how much damage might occur) and the impact of possible responses (i.e., how can the level of damage be reduced?), however, the application doesn't address the risk of the event actually occurring.

Although many of these existing risk assessment systems were originally targeted for a specific domain and are limited to addressing specific events, they can be used in the terrorism risk assessment environment. For example, HAZUS (which consists of a set of tools and utilities to analyze the effects of earthquakes, floods, and wind damage for regions of the US) could be used in the terrorism risk domain. For example, an analyst could use components of HAZUS to help analyze the impact of damaged bridges and other infrastructure on the local and global economy.

In addition to existing risk analytical tools that are used or could be used to analyze risk across several different domains, there are a number of terrorism specific models that have been recently created. Many of these models are built around existing commercially available analytical tools and systems such as Analytica[4], Matlab[5], Crystal Ball[6], and @RISK[7] for Project Management. For example, research into dirty bombs and airport

[2] http://www.fema.gov/hazus/

[3] http://www.decpath.com/

[4] http://www.lumina.com/

[5] http://www.mathworks.com/

[6] http://www.decisioneering.com/

[7] http://www.palisade.com/

fortifications undertaken at USC's Center for Risk and Economic Analysis of Terrorism Events (CREATE) relies on models created using Analytical and @RISK.

In addition to commercially available software solutions that can be used to address terrorism risk, there are many custom-developed solutions that address specific areas of terrorism risk. One such solution is the Critical Infrastructure Protection Decision Support System (CIP/DSS) developed at Los Alamos National Laboratory[8]. CIP/DSS is a decision support system that allows the analyst to examine tradeoffs between the benefits of terrorism risk reduction and the costs of implementing counter-measures in protecting our nation's critical infrastructure (e.g., transportation, agriculture, public health, energy, etc.,). A key feature in CIP/DSS is the ability to model and track the propagation of terrorism events from one infrastructure sector to another (e.g., impact on banking & finance due to a disruption in telecommunications).

Another custom-developed system is the Simulation Analysis of Aviation Security (SAAS)[9] system developed at CREATE. SAAS is a simulation-based decision support tool that integrates multiple models and software components to enable emergency personnel to explore possible responses to threats to airports and commercial aircraft and to evaluate the risk and cost tradeoffs associated with various responses (e.g., cost of rerouting commercial aircraft to "fortified" airports, etc.,). One of the key goals of the SAAS project is to integrate multiple models into a "system" that allows a user to undertake risk analysis on different aspects of the external threats to aviation security.

Although many of the aforementioned risk analysis solutions do a very good job of addressing a wide array of domains and problems, they exhibit one or more of the following limitations:

- Models are closed and domain and/or scenario specific
- Models are difficult to use
- Lack of researcher collaboration support
- No standardization
- Limited decision support
- Limited situation awareness

RAW addresses these limitations by providing an infrastructure/framework in which multiple users collaborate and access multiple models and data to help carry out the entire risk assessment process as defined in the CREATE Terrorism Modeling System (CTMS)[1] (see Figure 1-1). RAW is not designed to replace existing tools and models. Rather, RAW is being developed to bring these tools (data and models) together into an integrated "system of systems" that allows for a more robust and on-going analysis of terrorism threats and responses.

[8] http://public.lanl.gov/bwb/do/c3deaa7498e3cda534456f844c69c4d6.pdf#search='CIP/DSS%20Sandia'

[9] Yao, K. and Kadam, S. (2005). "SAAS: Simulation Analysis of Aviation Security, Year One Interim Report," CREATE Report

3 Requirements

Table 3-1 defines the system requirements. The table lists the requirements along with an indicator of which year (or years) the requirement is addressed in the CREATE RAW development effort. In many cases, requirements are implemented over multiple years.

CREATE RAW Requirements

Date: 31 August 2005

= Year one requirements

System Requirements

No.	Sub No.	Requirement	Sub-Requirement	Details	Year Implemented			Comments
					Year 1	Year 2	Unfunded	
S1		Enable users to create scenarios/events (I.e., define the threat)						Enable users to create threat descriptions using a standardized approach
	S1.1		Guide user through the process		X	X		A standardized approach is used to guide the user through the risk scenario/event description
	S1.2		Support mulitple "risk scenario/event" categories		X	X		User will be able to select from several different risk scenario/event generation interfaces to enter a new risk scenario/event description
	S1.3		Support editing of existing risk scenarios/events		X	X		User will be able to edit an existing risk scenario (that he or she has access to)
	S1.4		Access to copies of existing remote (not local) risk scenario/event descriptions			X	X	Non-sensitive risk scenario/event descriptions are available to anyone on the CREATE RAW distributed network
	S1.5		Support creation of new risk scenarios using an existing description as a base		X	X		User will be able to create a new risk scenario by making a copy of an existing scenario/event and making the necessary changes.
S2		Enable users to specify counter-measures						Enable users to specify counter-measures to specific threats
	S2.1		Support a counter-measure to threat matrix - user defined		X	X		Matrix contains defines effectiveness of counter-measure's against a terrorism event. User supplied.
	S2.2		Support a counter-measure to threat matrix - external system supplied			X	X	Same as above - matrix populated by data from external sources. User can still override
	S2.3		Counter-measure matrix guides user in selection of counter-measures against a threat		X	X	X	RAW relies on counter-measure matrix to guide user in the selection of counter-measures for a given threat scenario/event. Guidance based on effectiveness of counter-measure.

Table 3-1a CREATE RAW System Requirements

S3		Support multiple problem types			X	X	X	User identifies the risk scenario/event as belonging to one of four classes: portfolios, programmatic investments and policies, targeted investments, and acting on intelligence
S4		Distributed Data Management						
	S4.1		Support both sensitive and non-sensitive data		X	X	X	Both sensitive (I.e., classified) and non-sensitive data will be stored, archived, and made available to qualified users. In year 1, only non-sensitive data will be addressed.
	S4.2		Share scenarios/threat event definitions		X	X	X	Non-sensitive risk scenarios/threat events are available to all users in the RAW distributed network. Sensitive risk scenarios/threat events are available to qualified users in the RAW distributed network.
	S4.3		Share results, input data, and models			X	X	Non-sensitive data and models are available to all users in the RAW distributed network. Sensitive data and models are available to qualified users in the RAW distributed network.
	S4.4		Notify users when data of interest is modified			X	X	Tag data, models, risk assessment results with name of user(s). When information changes, users (current and former) are notified.
S5		Support multiple terrorism risk assessment models						
	S5.1		Integrate existing risk models into the RAW framework			X	X	RAW will support access to existing risk assessment and consequence models.
	S5.2		Integrate new risk models into the RAW framework			X	X	Need tools/interface to allow seamless integration of new risk assessment models into the RAW framework.
	S5.3		Support building of composite models			X	X	Generate new models by selecting and "chaining" together multiple models (I.e., output from one model becomes input to another model.
	S5.4		Monitor execution of risk models			X	X	Display status of an on-going model processing.
	S5.5		Integrate/access remotely located risk models			X	X	User should be able to specify access to any threat assessment model available on the distributed RAW

Table 3-1b CREATE RAW System Requirements

S6		Integrate with GIS				X	X	
S7		Infrastructure						
	S7.1		Each workbench must operate in a stand-alone environment			X	X	User should be able to continue using RAW even though the workbench is disconnected from the RAW distributed network
	S7.2		Data on workbench re-synchronizes with the rest of the CMMD community when the off-line system reconnects with the distributed network			X	X	RAW tracks on-line/off-line status and how relevant the data is to the user's problem.
S8		Common look and feel GUI			X	X	X	
S9		Decision-Support Tools						
			Decision-support tools will be available to allow decision-makers/policy-makers to assess terrorism risk and mitigation strategies			X	X	In addition to models and data, RAW will also provide decision-makers with access to decision-support tools. These tools will allow users to analyze model output and other data sources to assess the risks of various terrorism events and the trade-offs between mitigation strategies

Table 3-1c CREATE RAW System Requirements

4 Design

4.1 CREATE RAW System Architecture

RAW is an infrastructure/framework in which risk assessment models, risk scenarios, and data from a variety of sources can be accessed, analysis undertaken, and results cataloged. Each workstation has a common look and feel human computer interface that allows the analysis to define risk scenarios, select risk models to be used, specify input data locations and formats, and define how and where the results are displayed.

As illustrated in Figure 4-1, RAW is a central-server based distributed system with one or more workstations (i.e., laptops, desktops, etc.,), each capable of on or off-line operations. RAW has access to both secure (e.g., classified, proprietary, etc.,) and non-

secure (i.e., open) data and models (Figure 4-2) that can be stored locally for off-line (stand-alone) operations.

Each RAW workstation contains the following capabilities/utilities.

- Scenario templates that guide the analyst in defining the risk scenario/event to be analyzed.
    - Create new scenarios from the templates
        - Target selection(s)
        - Weapon selection(s)
            - Guided via a weapon to target feasibility matrix
        - Counter-measure selection(s)
            - Guided via a counter-measure to threat matrix
        - Probability/feasibility of event(s) occurring
            - Default values will be provided
            - User can override
    - Create new scenarios from existing scenarios available either locally (to the workstation) or globally on the RAW distributed network
- Interfacing logic to existing risk assessment models and decision-support tools available either locally or globally on the RAW distributed network
- Communication protocol to allow new models and decision-support tools to be integrated into the CREATE RAW library
- Graphical interfaces to display results, alternatives, and current environment status
- Interface to the CREATE Geographic Information System (GIS)[10]
    - For mapping of results from analysis
    - For spatial and demographic information queries to retrieve critical data
    - To provide weapons, counter-measures, targets, and adversarial information
- Increased situational awareness through alert mechanisms that track data relevancy/currency
- Access to both secure/sensitive and non-secure/open data and models
- Data management services
    - Central-server based data archiving
    - Re-synchronization of data and status when off-line systems are brought back on-line (on the RAW distributed network)
    - Interfaces to non-RAW systems
        - XML
        - ODBC
    - Model parameter/interfacing configuration
    - Management of secure/non-secure data/models
    - Allow analyst to define access control list for proprietary scenarios, models, and assessment results and data

[10] Bowman, H. (2005) "CREATE Geographic Information System, Design and Architecture," CREATE Report

4.1.1 CREATE Geographic Information System (GIS)

As part of the development effort, an interface will be developed between RAW and the CREATE GIS[10]. The CREATE Geographic Information System (GIS) will provide tools for managing and displaying map-based data at each of the four steps in CTMS, particularly as they relate to managing data created and used by the CREATE analytical models. The CREATE GIS will provide:

- Data management: spatial and non-spatial, multi-user, server connected and detached
- Spatial analysis tools
- Map display and production
- Integration with the CREATE Risk Analyst Workbench
- Integration with analytic software developed by CREATE research teams
- Integration with commercial and government off-the-shelf software

CREATE RAW functions as a driver for creating scenarios for analysis and for undertaking risk assessment in support of the four-step CTMS model. Data produced from RAW will be available for mapping and possibly editing through the GIS, and RAW itself will have some map and spatial query functionality and access to spatial data sources. CREATE GIS will also have access to RAW data on weapons, adversaries, countermeasures and targets.

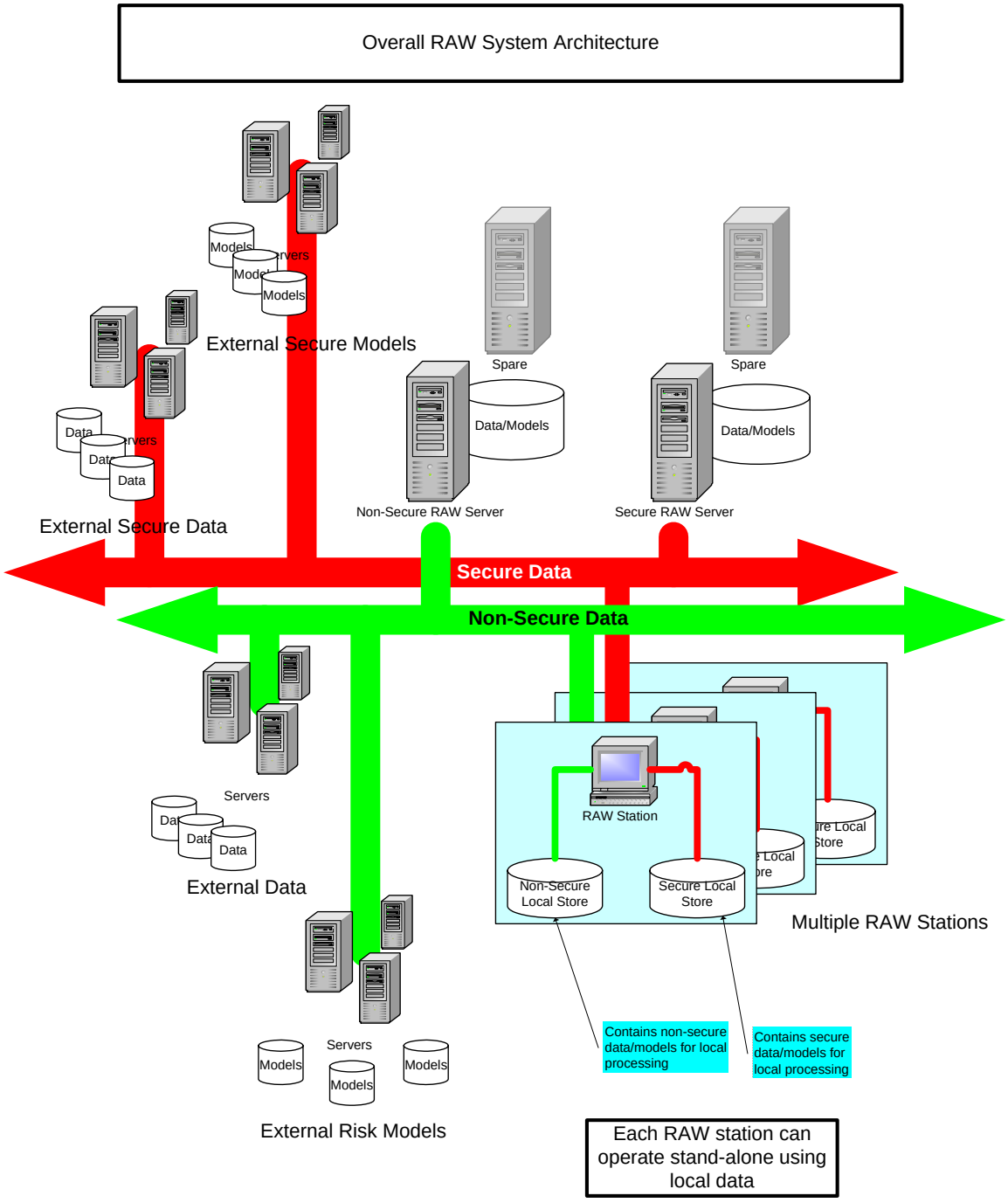

Figure 4-1 CREATE RAW Distributed System Architecture

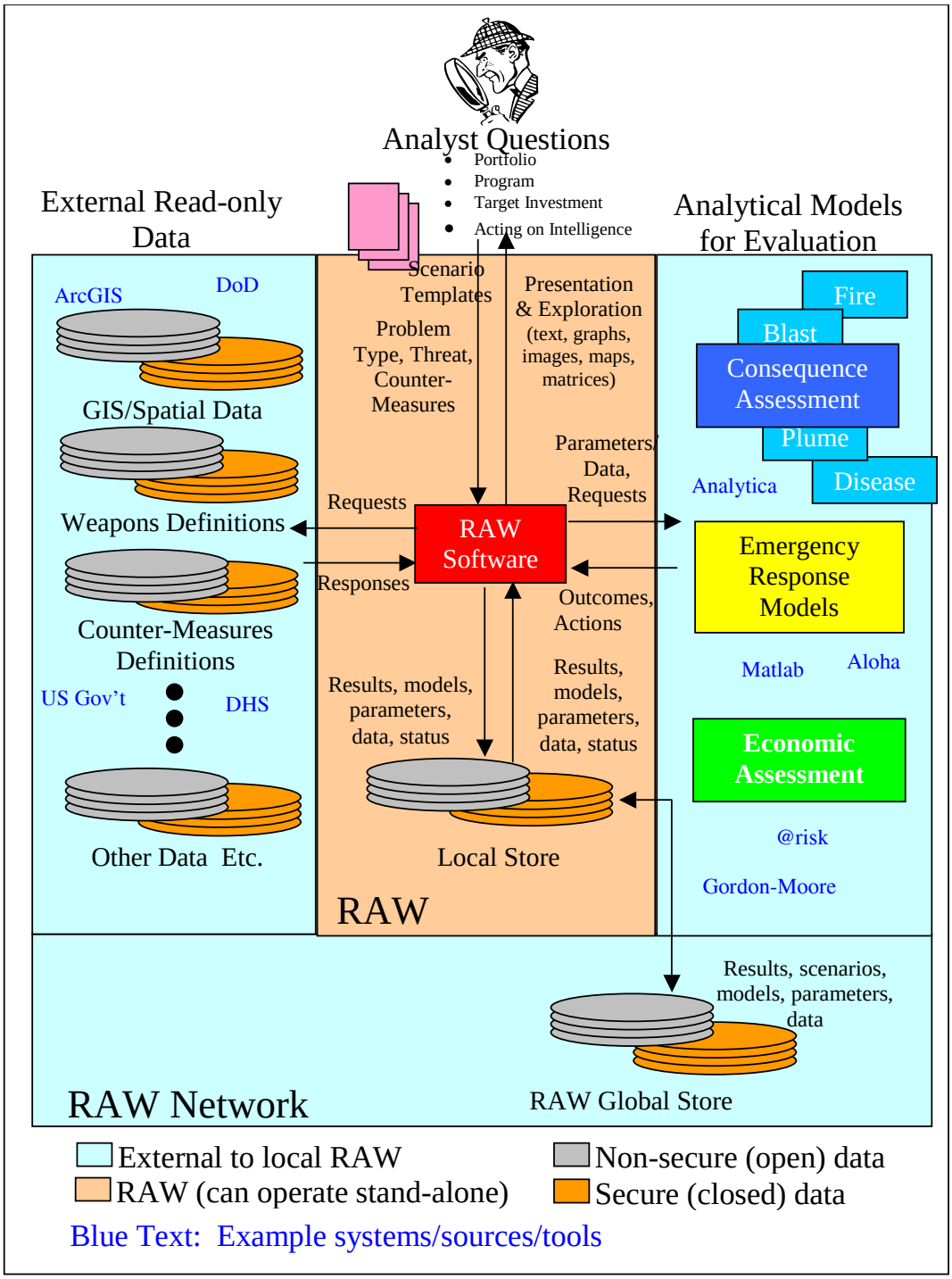

Figure 4-2 System Interfaces for a Single RAW Workstation

4.2 Preliminary Software System Design

4.2.1 Concept of Operations – Risk Assessment and Decision Support

The analyst and/or decision-maker undertakes a risk assessment through a sequence of steps (a process). Figure 4-3 illustrates the process followed by an analyst or decision-maker using RAW.

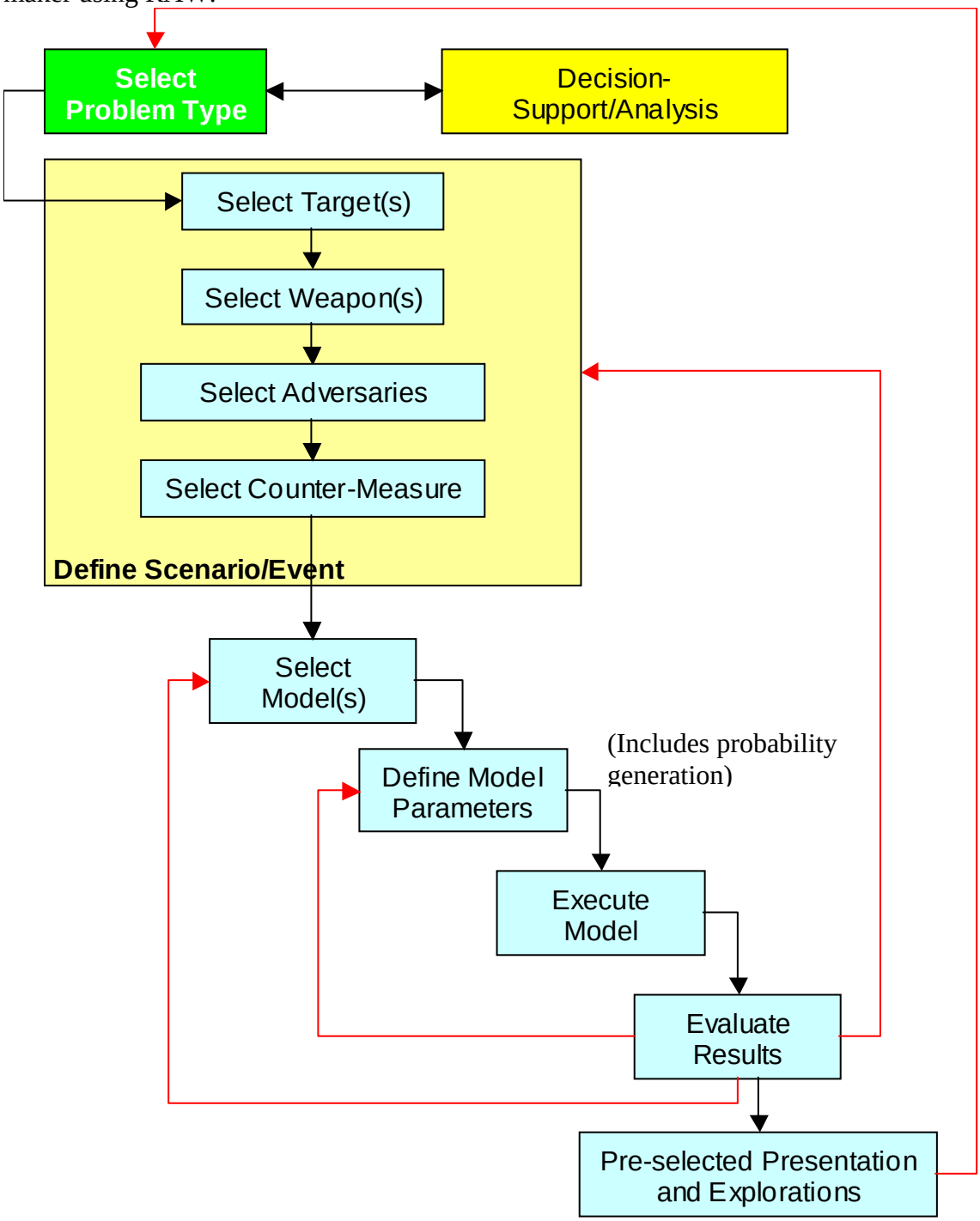

Figure 4-3 Concept of Operations – Risk Assessment

In Figure 4-3, the analyst starts off by first selecting the type of problem (green box)

being addressed (e.g., portfolio allocation, programmatic investments and policies, target investments, acting on intelligence). Portfolio allocation involves assessing the benefits and costs of allocating funds (e.g., DHS, etc.,) between one and/or more threat areas. Basically, a "trade-off" analysis is undertaken to assess the "payoff" in targeting funds to one or more threat areas. Programmatic investments and policies focus on determining what level of counter-measures and funding that should, as a general rule, be allocated to a specific category of threat (e.g., airport fortification, etc.,). Users selecting target investments are looking at assessing the level of protection (counter-measures) and funding that should be directed to a specific target (e.g., LAX). Finally, decision makers/researchers use RAW to assess the consequences of an event based on newly acquired intelligence (e.g., a MANPADs was recently sold on the black market to someone in LA – near LAX).

For most decision makers and, for some analysts/researchers, existing research results and recommendations already exist (yellow box in Figure 4-3) to aid in addressing the specified problem. Under these circumstances, the user extracts the necessary information and continues with the analysis/assessment using available decision-support tools. In situations where adequate existing information is not available in RAW (either locally or globally), the user undertakes a risk assessment by first defining the threat (or threats) of interest, the counter-measure(s) to be deployed, and model or models to undertake the analysts (Cyan boxes in Figure 4-3). In many situations, the analyst will use a combination of previously generated information/results and new information/results generated from RAW to arrive at a conclusion or recommendation.

The risk assessment process starts with the definition of the risk scenario/event. This involves selecting a target or targets, weapon(s), adversarial descriptions, and counter-measures (if any) as illustrated in Figure 4-3 (tan colored block). Risk scenarios/events are created either from scratch or from a modified copy of an existing scenario/event (i.e., create a new scenario by modifying a copy of an existing scenario). Once the risk scenario is defined, the analyst selects one or more mathematical models available through RAW that will be used to simulate the actual event (including consequences), the impact of the counter-measures, (optionally) the possible emergency responses and consequences, and finally (optionally) the economic consequences of the scenario/event occurring as defined in the CTMS (Figure 4-4).

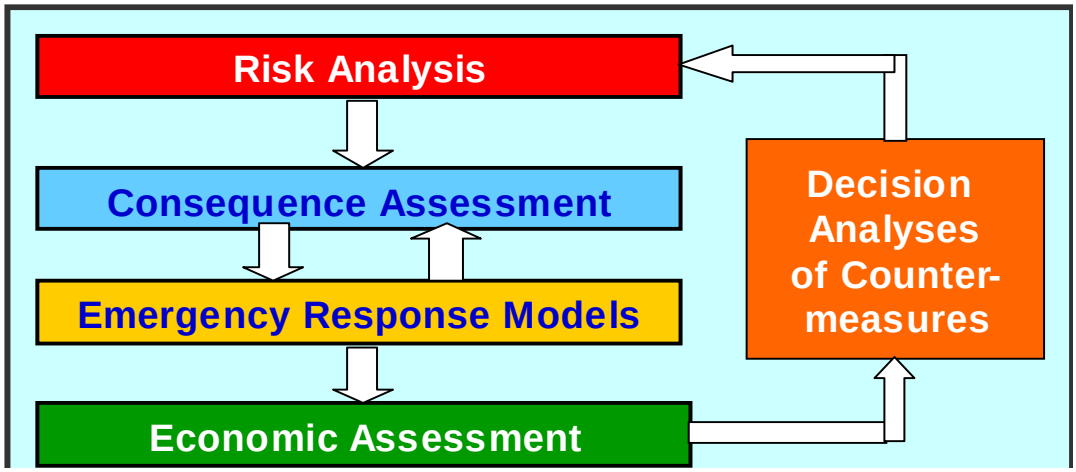

Figure 4-4 CTMS Four-step modeling system

With each selected model, the analyst can either rely on RAW pre-selected configuration parameters or provide customized values. Such configuration parameters include probability a chosen weapon can be acquired by a suspect, feasibility of weapon against selected targets, and feasibility of counter-measures to counter selected weapon(s). Once the parameters have been defined, the analyst can then run the selected model(s) and analyze the results.

When undertaking a risk analysis, the analyst will make many runs using different models and parameters, and different targets, weapons, and counter-measure combinations in order to compare the feasibility and "trade-offs" between different scenarios. These "what-if" exercises will produce a large collection of results from which the analyst or analysts can evaluate and generate recommendations/conclusions.

4.2.1.1 Probabilities and the Risk Analysis Process

Estimating probabilities is a difficult undertaking and subject to much scrutiny. Issues such as to where and how the data was derived and how current/relevant the information is can lead to questioning the validity of the model. In addition, it is conceivable that the probability of an event occurring is classified information that is on a "need-to-know" basis.

Under these circumstances, the normal RAW procedure is to provide "dummy" or "default" probabilities for specific events occurring. These "dummy" values will be reasonable approximations to allow the analyst (e.g., academic) to confirm the validity of the risk analysis "process" (i.e., model selection and configuration, scenario definition, etc.,) prior to undertaking an actual risk assessment. In other words, default values are used to allow the risk analyst to confirm or validate model selection, parameter assignments, and test scenario descriptions. Once validated, the analyst can then specify the actual – and possibly classified – probabilities prior to undertaking a risk assessment

session.

4.2.2 Concept of Operations – Administration

In addition to providing the interface and tools to allow a decision maker and/or risk analyst to undertake risk assessment, RAW also provides an administrative capability to allow a privilege user to undertake the following administrative operations:

- Integrate new models and decision-support tools into the RAW suite of available models
- Manage system-wide weapon-target and counter-measure to weapon feasibility matrices
- Manage weapon capability matrix
- Define user access lists
    - Define who can be part of the RAW network
        - User authentication procedures
    - Define what level of data (secure, non-secure, etc.,) user has access

4.2.3 Scenario/Event Templates

To guide the analyst in defining a new risk/threat scenario/event, templates of existing classes of risk events will be provided. When the analyst begins a threat definition, a list of risk scenario/event classes will be provided (list to be determined). The analyst selects the desired class and then is presented with the following two options:

- Create a risk scenario from scratch using the supplied template
- Create a risk scenario from a copy of an existing scenario.

In the first case, the analyst simply follows the template instructions and populates the template. In certain situations, the RAW software will provide default responses based on the current scenario definition. For example, if the target selected is a commercial airliner, the RAW software will pre-select a SA-7 shoulder-mounted MANPADs. In other cases, the RAW software will notify the analyst when incompatibilities arise. For example, if the target once again is a commercial airliner, the RAW software will notify the user that a dirty bomb has a low probability of bringing the airliner down. This interaction between analyst and the template software will continue until the threat is defined. In situations where a default value is not available, the RAW template software will prompt the analyst to provide a best-guess estimate.

In the second case, the RAW software will provide a directory tree containing existing scenario definitions that fit the particular scenario definition class selected by the analyst. This directory tree covers the availability of scenarios locally (to the workstation) as well as globally on the RAW distributed network (if the workstation is on-line). The user selects a candidate scenario, makes a copy (renames it), and then modifies the parameters as desired.

4.2.4 RAW Distributed Network

The RAW distributed network is a private distributed network (most likely implemented as a VPN) that only DHS researchers and decision makers can access. As Figure 4-1 illustrates, this private distributed network relies on two data paths, secure and non-secure. Secure means "for official use only" situations and not classified information typically reserved for internal DHS and DoD operations.

Regardless of whether accessing secure or non-secure information, the user must be an authorized user of the system. When accessing the system, the user will be required to log-in by supplying a user or account name along with a password.

RAW workstations will have the option of operating either on-line with access (if allowed) to all data and models available on the RAW network. RAW workstations can also operate off-line using only the data and models stored locally on the workstation (if the software is licensed for such operation). A status indicator will indicate when the RAW workstation is on or off –line.

Prior to operating off-line, the risk analyst must download (locally) the necessary data and models (if software license allows) that he or she will be using for a risk assessment exercise. To aid in determining where data, scenarios, and models reside (either locally or globally), the human computer interface will include an indicator flag that signals whether the desired data resides locally (on the current workstation) or on the network (in the central server).

When the off-line RAW workstation rejoins the RAW distributed network, a re-synchronization of data occurs. Analyst can only modify data that they have "write" access to. When the RAW workstation software detects the RAW distributed network, a comparison is made between existing software on the central-server and the local RAW workstation. Data that has changed, been deleted, or new data created on the RAW workstation are flagged and presented to the analyst for action. The analyst updates the central-server with the updated data, overwrites the local data by downloading the "original" data, or just does nothing (i.e., have a data mismatch between the central-server and the RAW workstation). In situations where "read-only" data on the central-server is more current than that on the local RAW workstation, the RAW software once again notifies the analyst. The analyst can either download the more current data (and possibility re-run risk assessments with the new data) or waive the download and continue operating with mis-matched data.

4.2.5 Enhanced Situational Awareness

A key feature in RAW is the ability to notify risk analysts when models and data used in a previous risk assessment have changed. An assessment is only as good as the models and data used to arrive at that assessment. If the underlying models and/or data used to generate the assessment change, the original assessment may be rendered invalid. To aid the analysts, RAW tracks the currency/relevancy of the models and data used for a given

assessment. If RAW detects that a "tagged" model or information source has changed status (i.e., been modified), RAW will notify the risk analyst. Notification will be in the form of non-intrusive text messaging and graphical icons.

4.2.6 Preliminary Software System Design – RAW Software

Figure 4-5a is the preliminary RAW workstation software sub-system architecture.

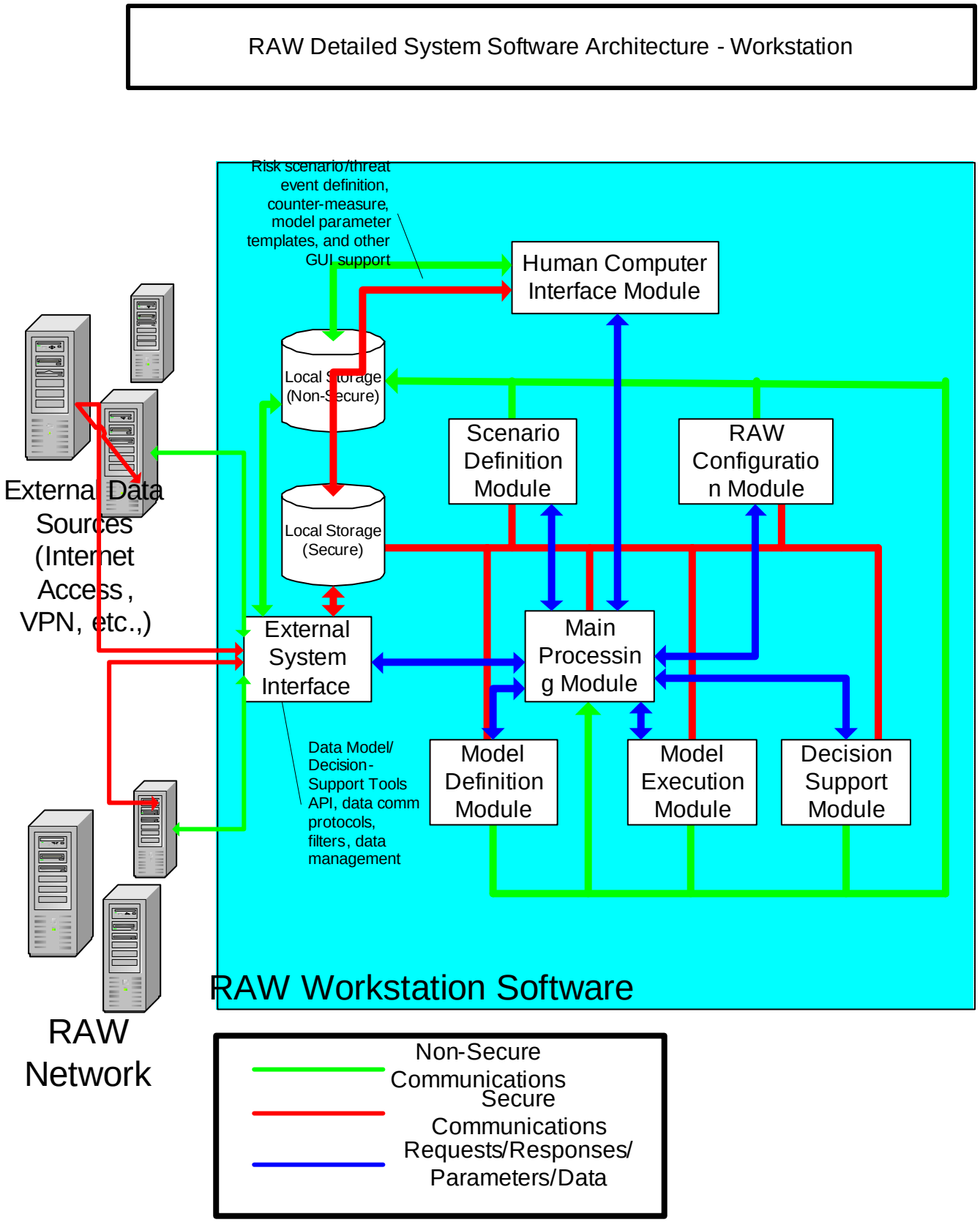

Figure 4-5a Preliminary RAW Workstation Software System Architecture

Figure 4-5b defines the preliminary software system process flow

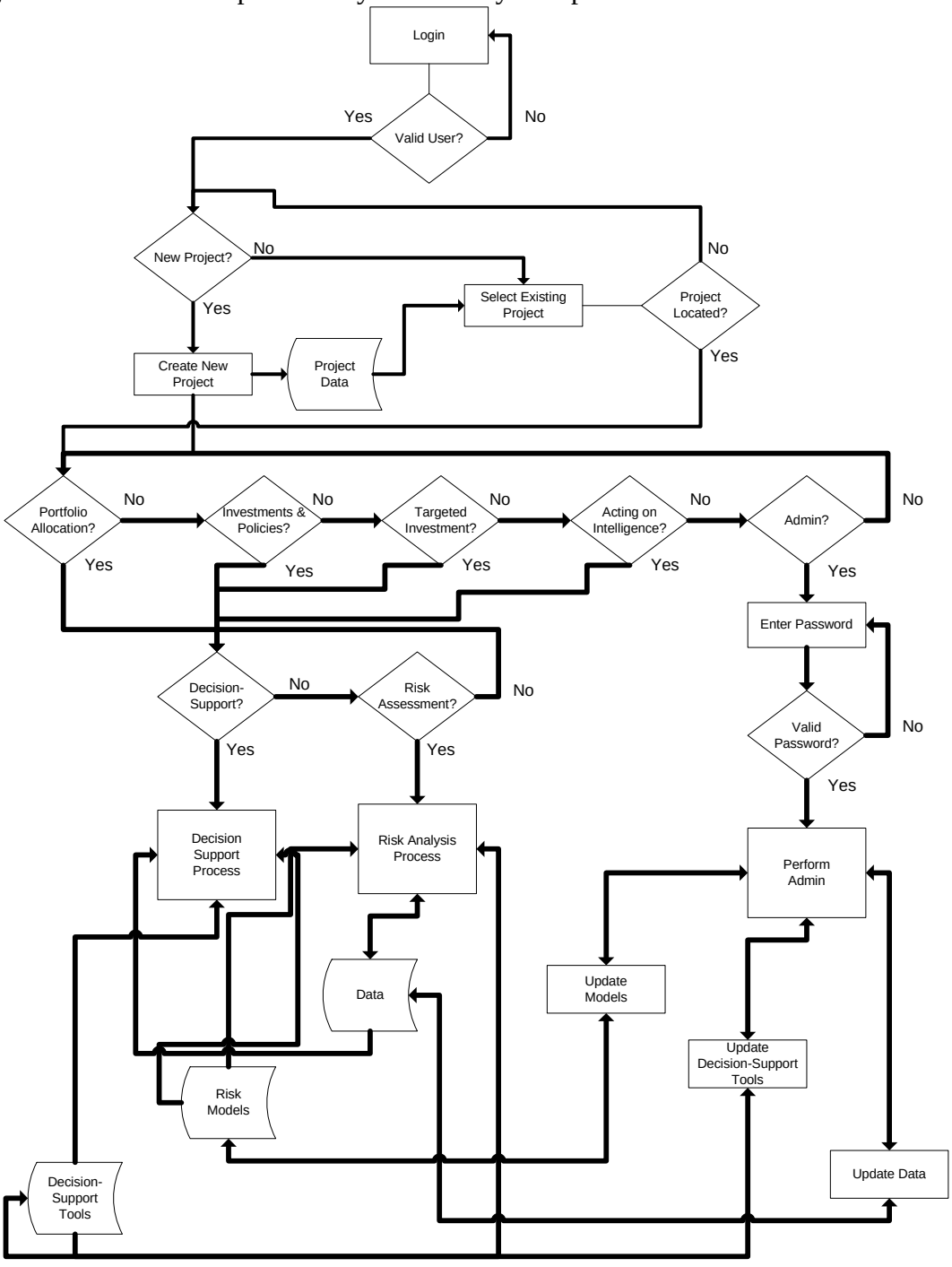

Figure 4-5b Preliminary RAW Workstation Software System Process Flow

4.3 Graphical User Interface

The following section defines the look, feel, and behavior of the RAW graphical user interface. This is a preliminary design specification and many of the GUIs are still being

developed or will change based on further analysis.

4.3.1 Login GUI/Problem Selection – Main GUI

A risk analysis session starts with the user logging in (Figure 4-6a), selecting a new or existing project (Figures 4-6b, 4-6c, and 4-6d), and type of problem to investigate (e.g., portfolio allocation, programmatic investments and policies, targeted investments, and acting on intelligence) to investigate (Figure 4-6e). In cases where the analyst was already working on a problem, RAW remembers the previous state of the software (i.e., which project and problem was being worked on, which models selected, scenarios defined, etc.,) and provides the analyst with a direct link to the project in question.

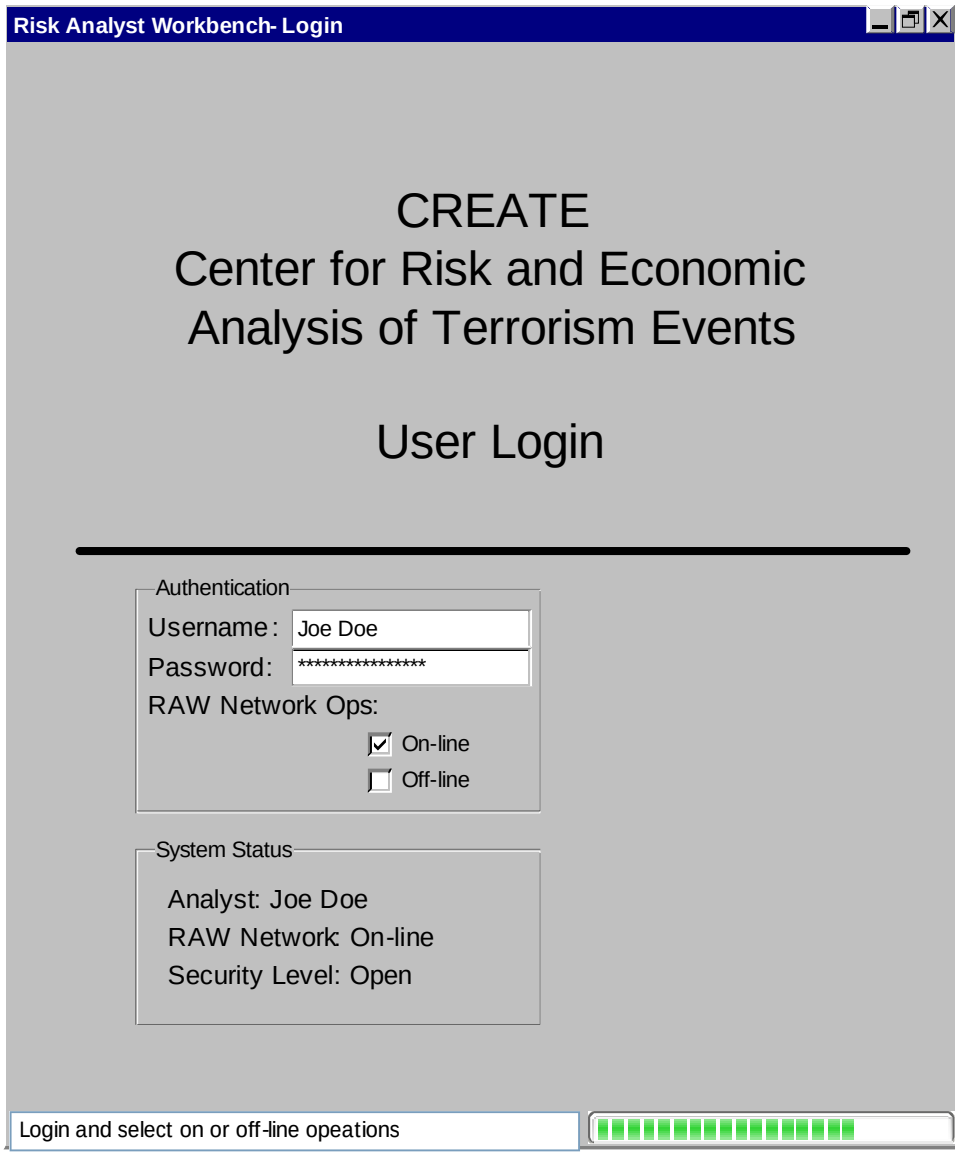

Figure 4-6a Login GUI

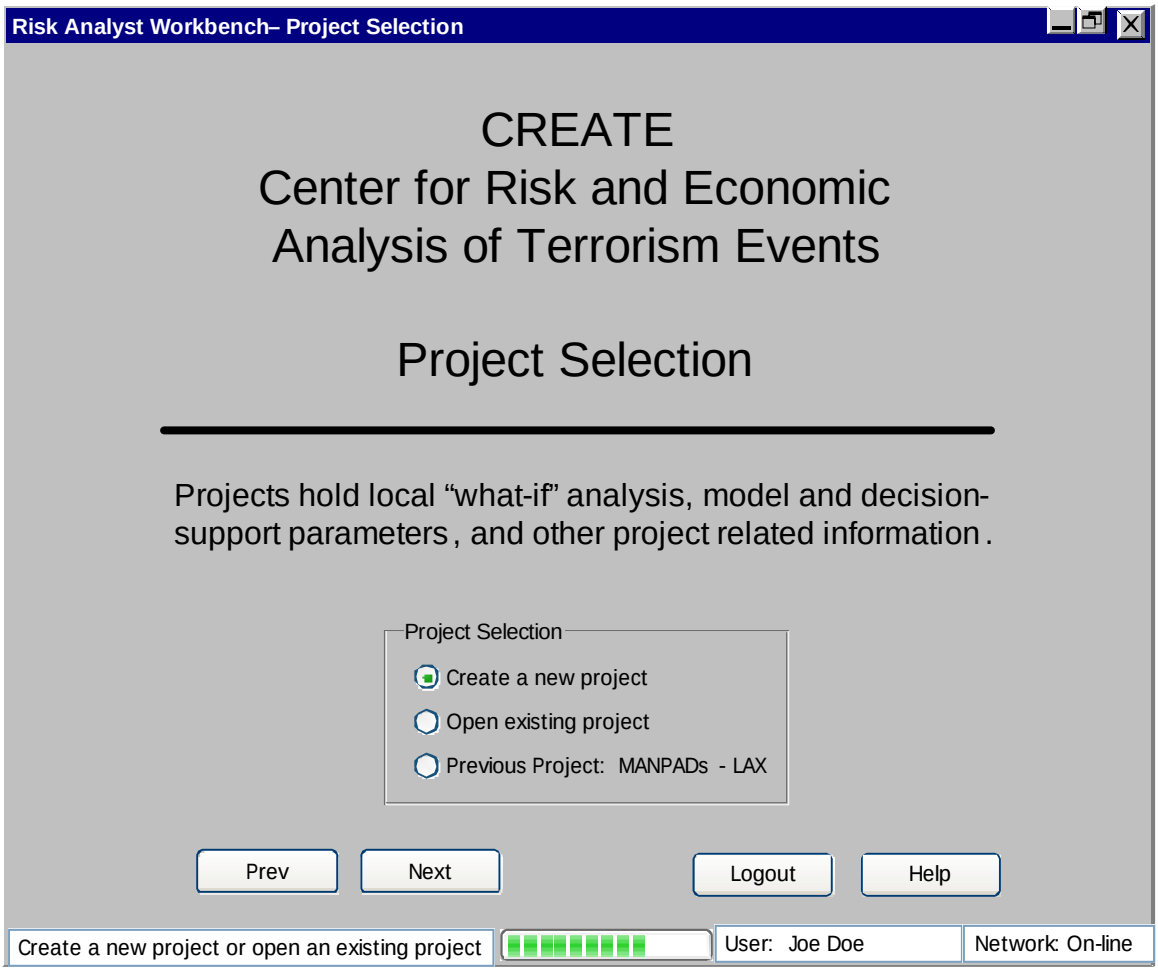

Figure 4-6b Project Selection GUI

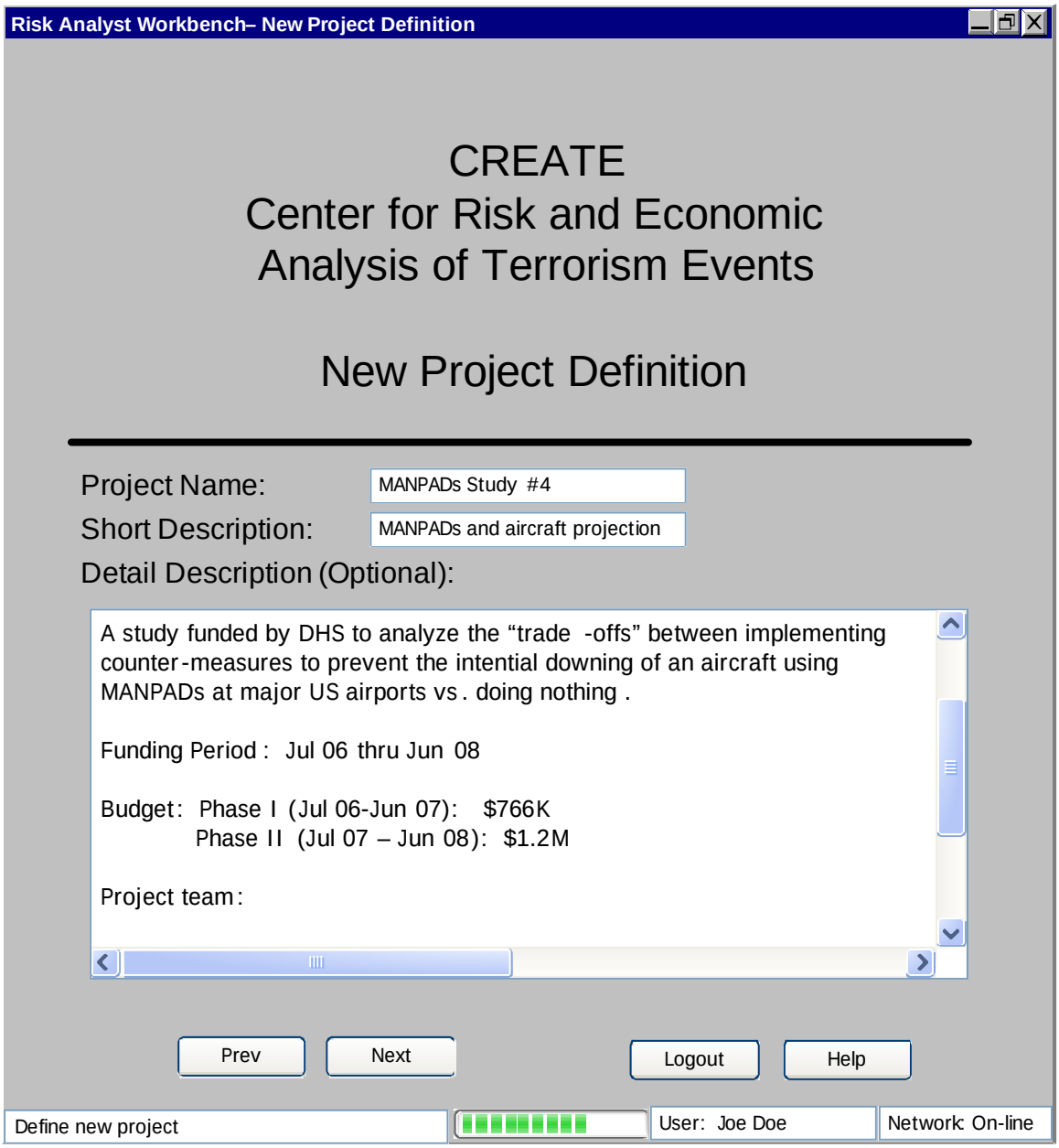

Figure 4-6c New Project Definition GUI

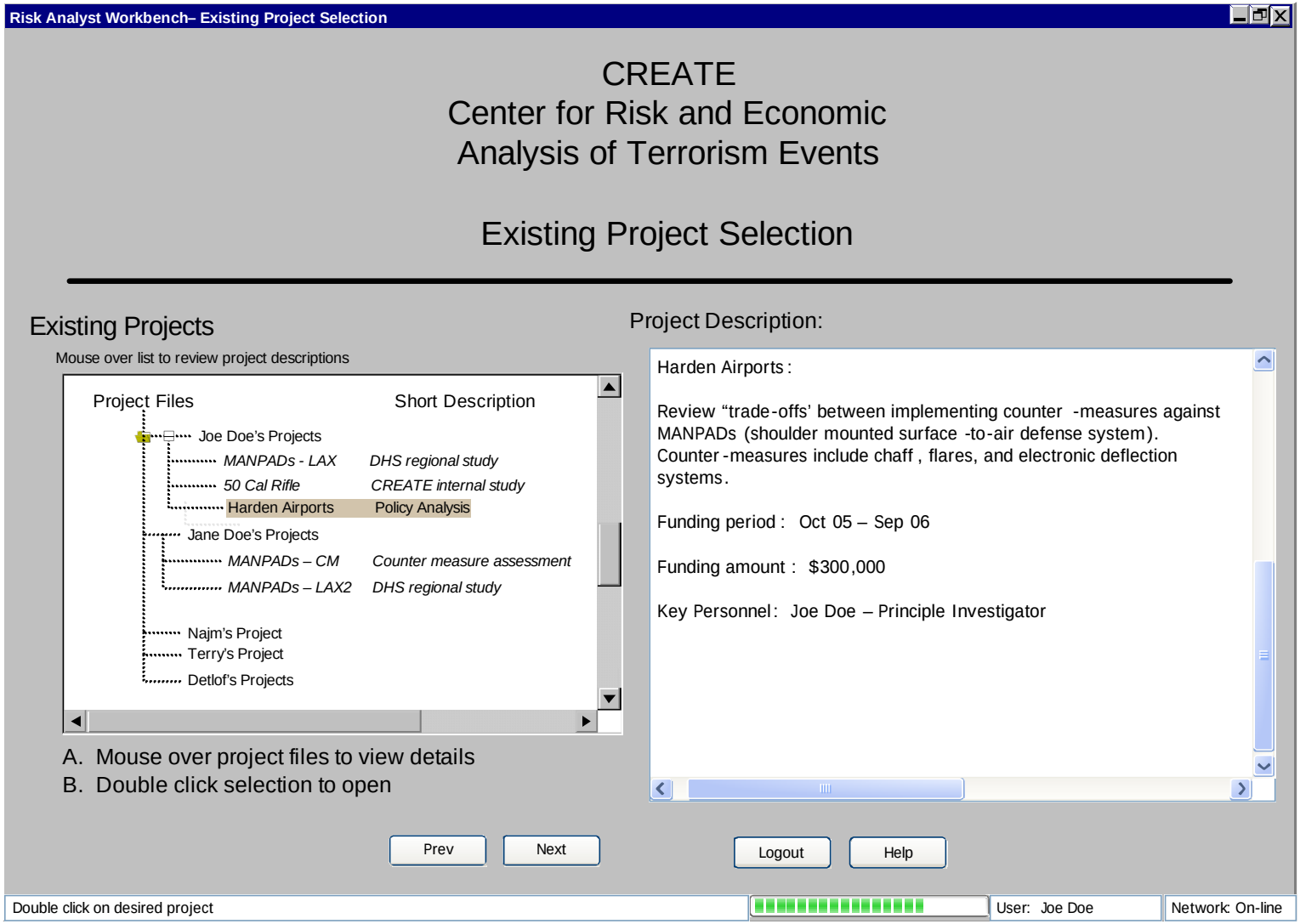

Figure 4-6d Existing Project Selection GUI

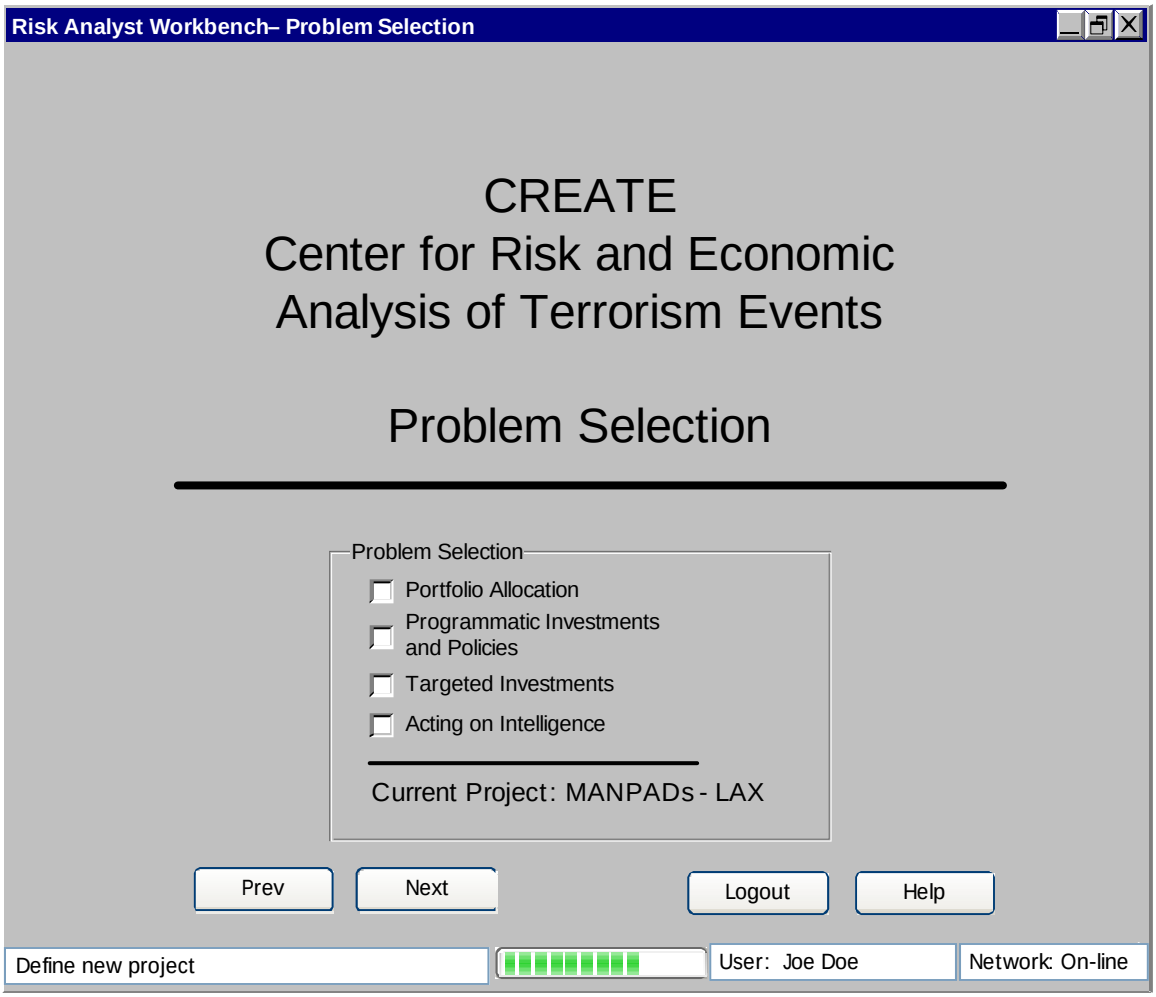

Figure 4-6e Problem Selection GUI

4.3.2 Decision-Making/Policy-Making and Risk Analysis

Once a project and problem area have been selected, the user has access to a variety of decision-support tools and risk models to evaluate "trade-offs" and courses of action to prevent or mitigate a terrorist event. GUI is to be defined.

4.3.3 Decision-Support/Analysis GUI

This GUI provides decision-makers access to decision-support tools and data to evaluate and undertake "trade-off" analysis. Much of the analysis relies on existing risk assessments. The analysis will use the RAW network to access existing analysis and results. GUI is to be defined.

4.3.4 Threat/Scenario development GUI

This graphic user interface (GUI) allows the user to modify or define a risk threat/scenario. The key function of this interface is to help the user frame the question that is to be answered/analyzed. This is typically the most difficult stage of the risk

analysis process.

The risk threat/scenario is modified or defined by selecting the Threat/Scenario Definition tab in the main RAW interface (Figure 4-6). The following risk scenario selection interface is presented (Figure 4-7).

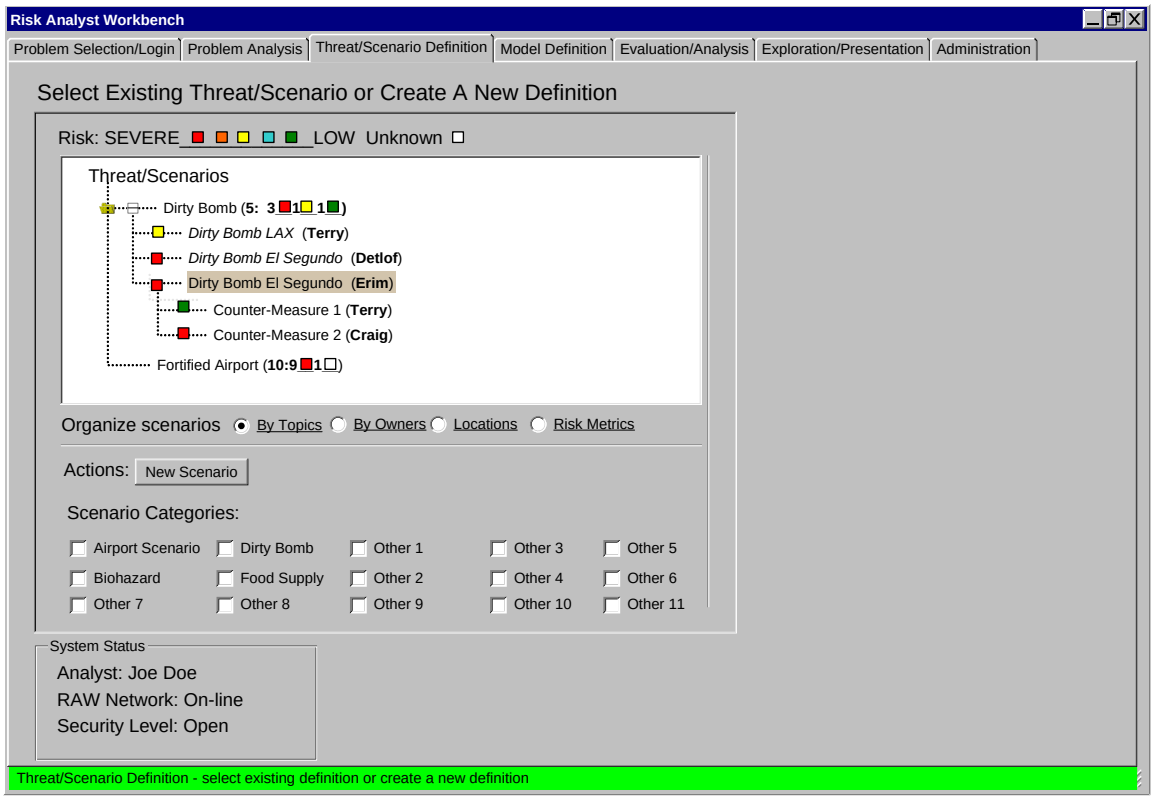

Figure 4-7 Threat/Scenario Selection/Creation

For existing scenarios, the user navigates the scenario space using a scenario tree. The scenario tree is structured (configured) based on the selected "organize scenarios" criteria. If "By topics (or classes)" is chosen, the tree is structured by scenario topics (see Figure 4-7). If "Risk metrics" is chosen, the tree is structured by "scenario clustering", and so on.

4.3.4.1 New Scenario Definitions

To create a new threat/scenario definition, the user either selects and edits an existing scenario and saves the definition under a different name or creates a new scenario from scratch. To create a definition from scratch, the analyst selects one of the fifteen "typical" scenario categories (Figure 4-7) and then selects the "New Scenarios" button. These typical scenarios exhibit similar behavior and performance. The following interface (Figure 4-8) is presented (whether selecting an existing scenario or creating a new definition).

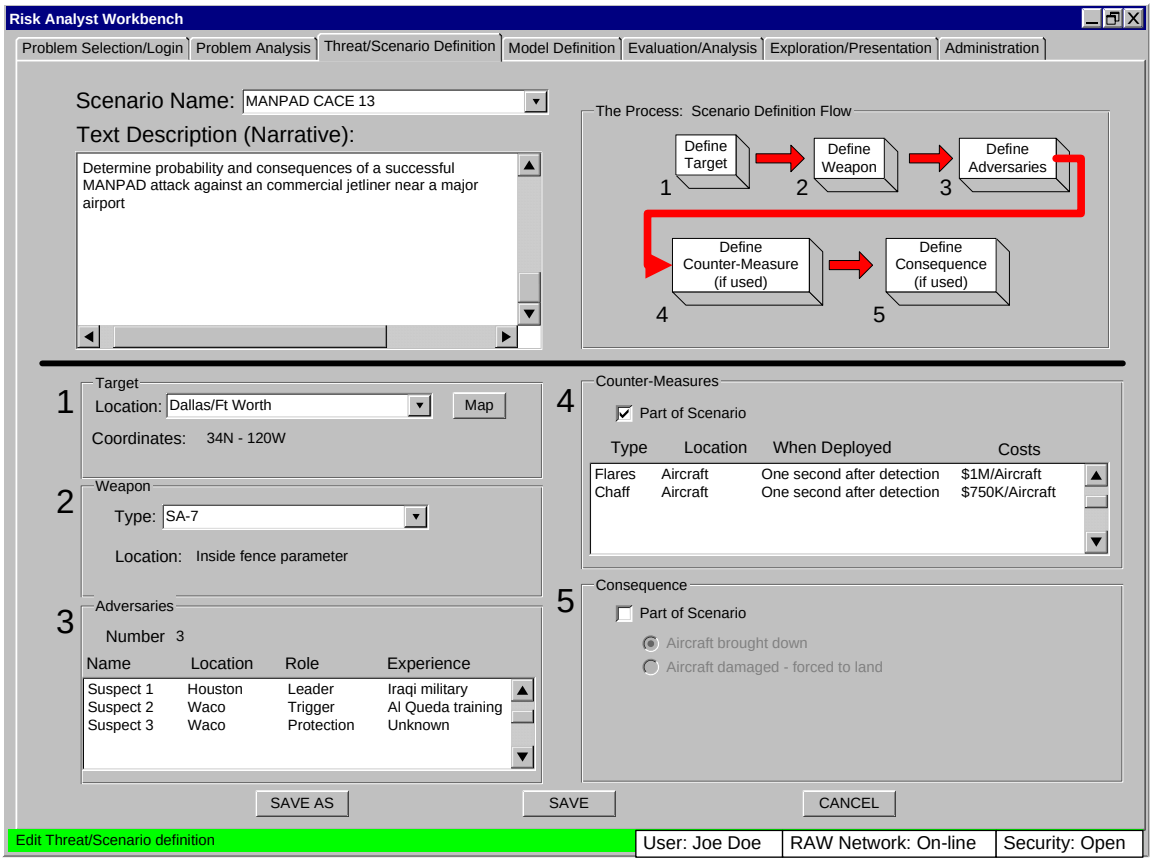

Figure 4-8 New Threat/Scenario definition

The risk scenario definition starts by entering a new scenario name followed by a brief narrative of the project (Figures 4-8 and 4-9). The analyst can either enter a new name (for a new definition) or select from a list of scenarios recently edited. This feature is intended to allow the analyst to go back and forth between scenario definitions without the need for having to go through the scenario selection interface (Figure 4-7).

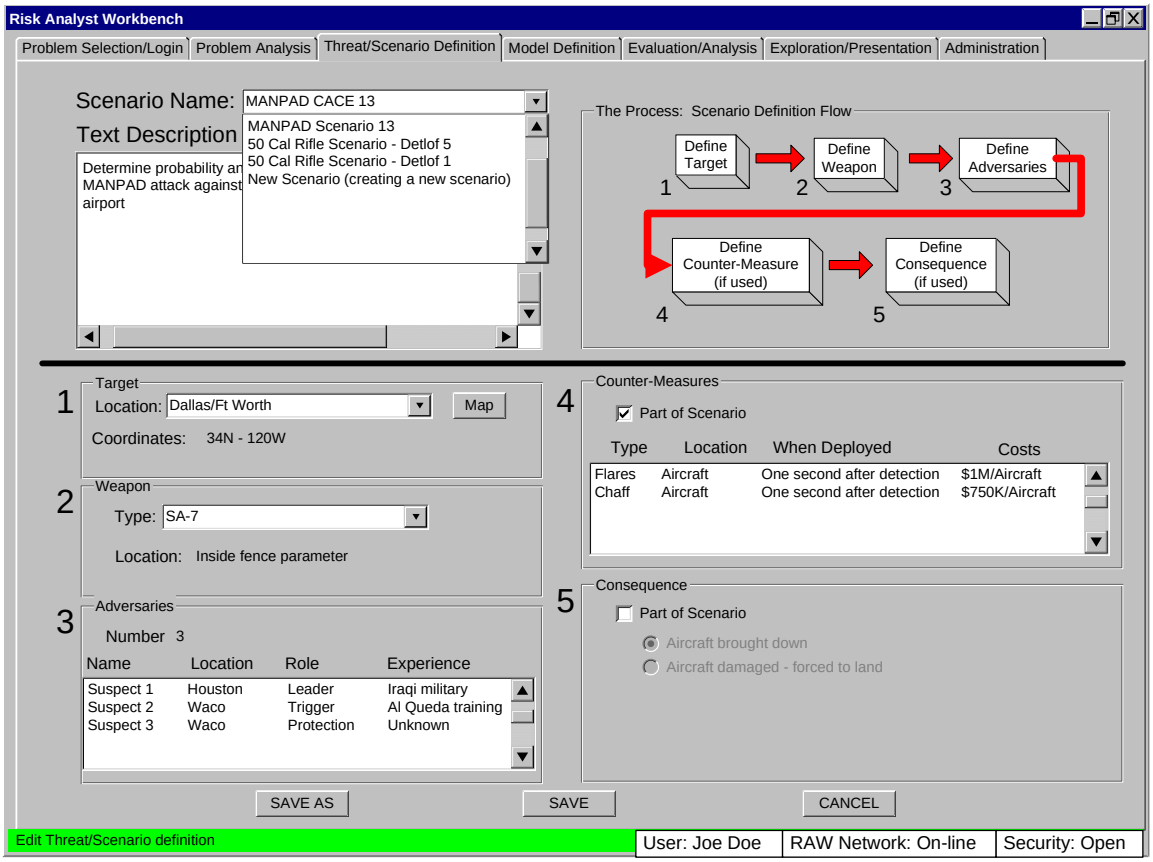

Figure 4-9 Scenario Name

4.3.4.2 Risk scenario definition process

In the upper right corner of Figure 4-9 is a “Scenario Definition Flow” diagram. This diagram defines the steps (in order of listing) necessary to define an airport risk scenario (one of the fifteen scenario “categories”). For the airport risk scenario, the user first defines the target; followed by anticipated weapons, list of adversaries, counter-measures deployed (if any), and consequences if the attack is successful.

Targets can be either a predefined in a combination list (Figure 4-10) or can be selected from a GIS generated map (Figure 4-11)

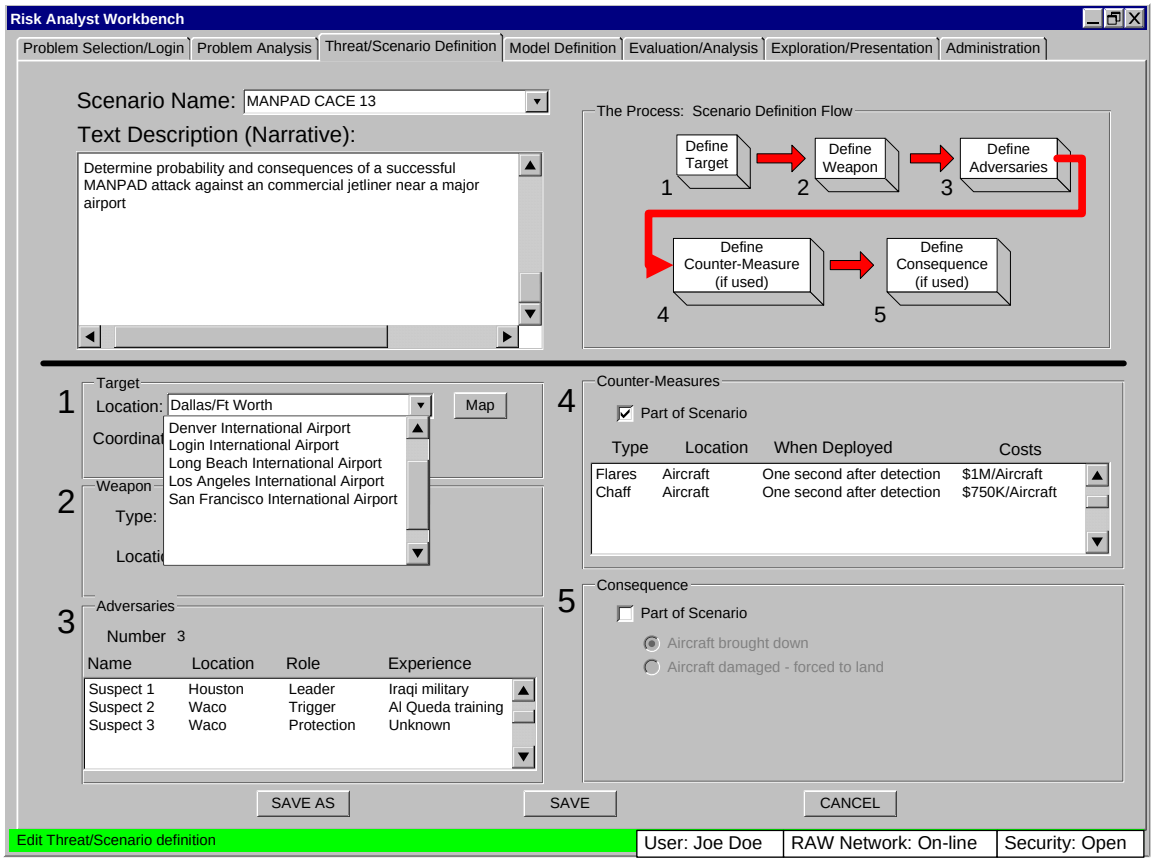

Figure 4-10 Selecting a target

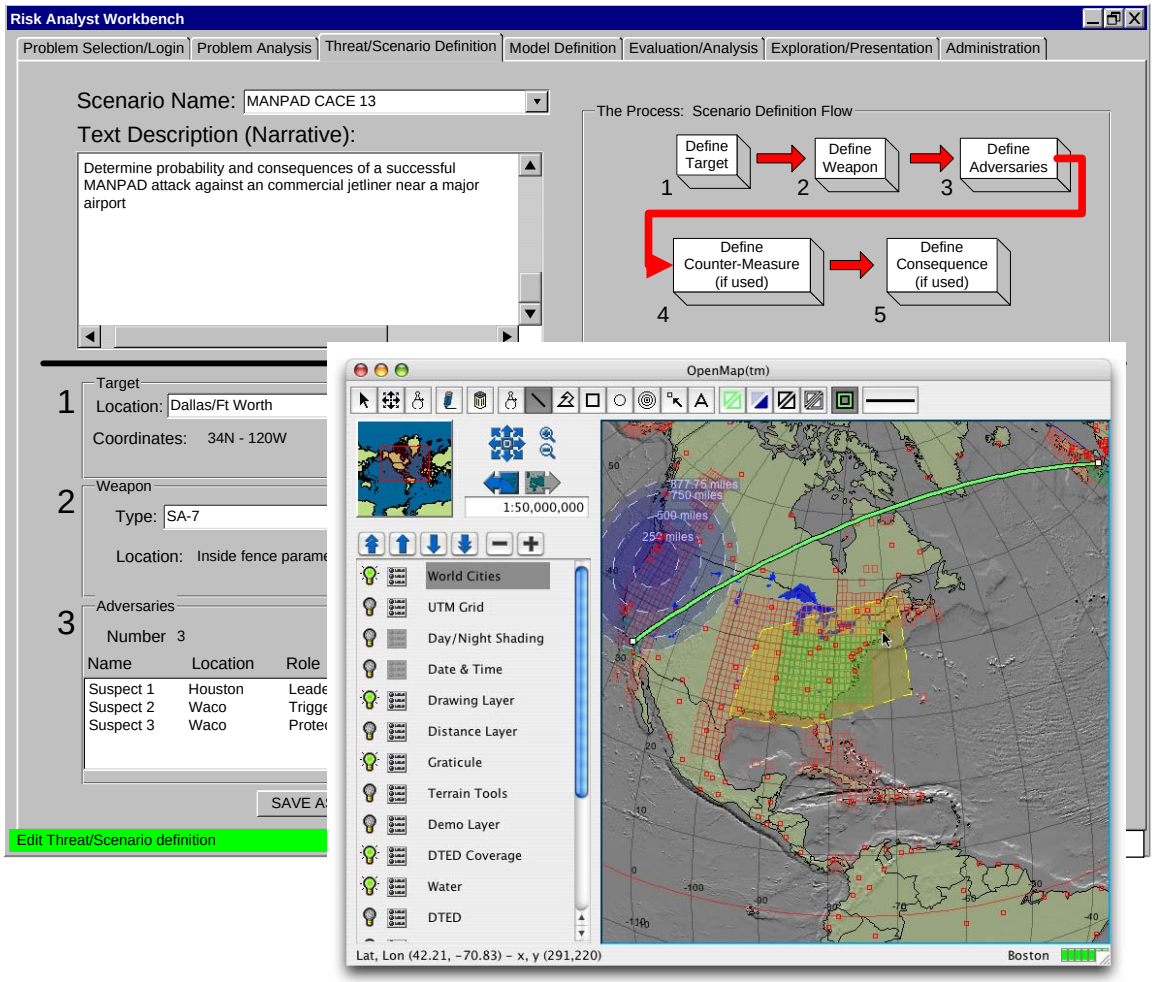

Figure 4-11 Selecting a target from a GIS generated map

The second step in defining an airport risk scenario is to define the weapon system(s) used. The user selects the desired weapons package from a pull-down list (Figure 4-12). The software provides a list of terrorism weapons, however, new systems can be added via the interface.

Once a weapon system is selected, the RAW software will prompt the analyst to define the attributes associated with the selected weapon system (Figure 4-13). RAW will provide default attribute values, however, the analyst can change the values as desired.

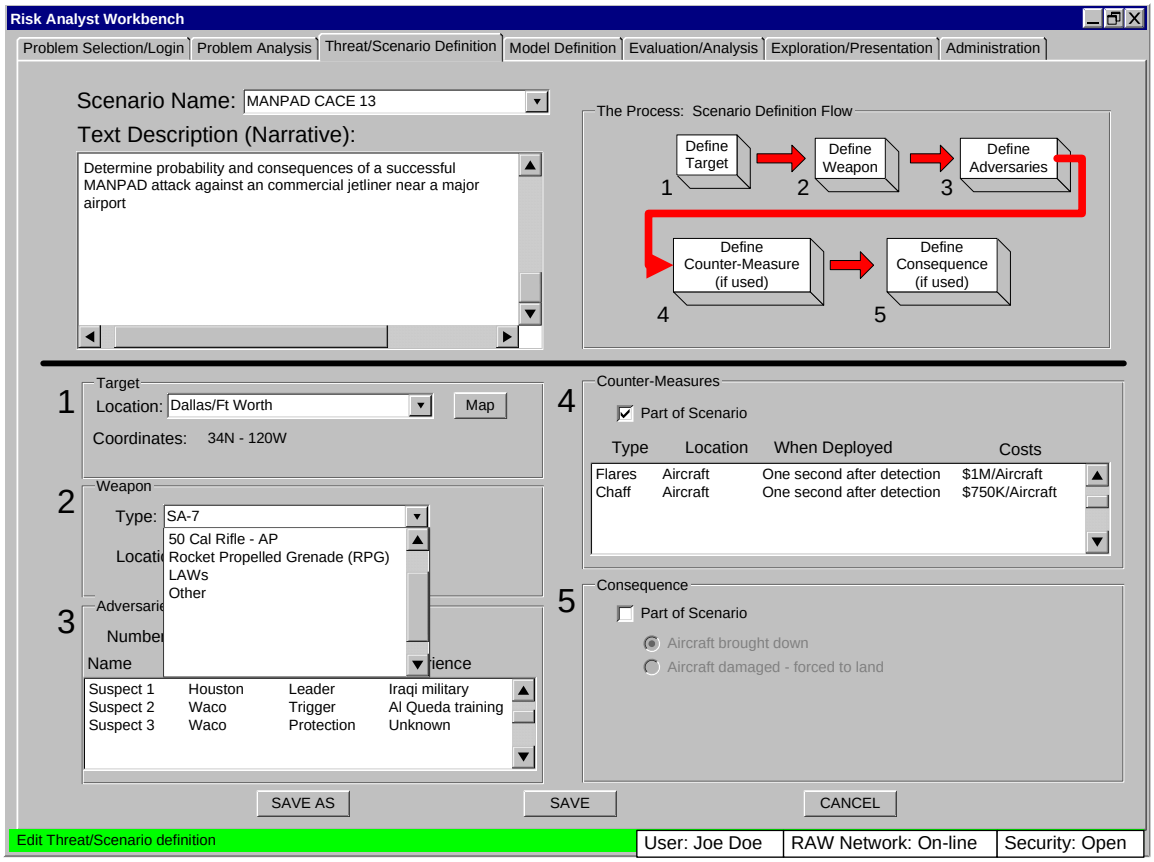

Figure 4-12 Weapons selection

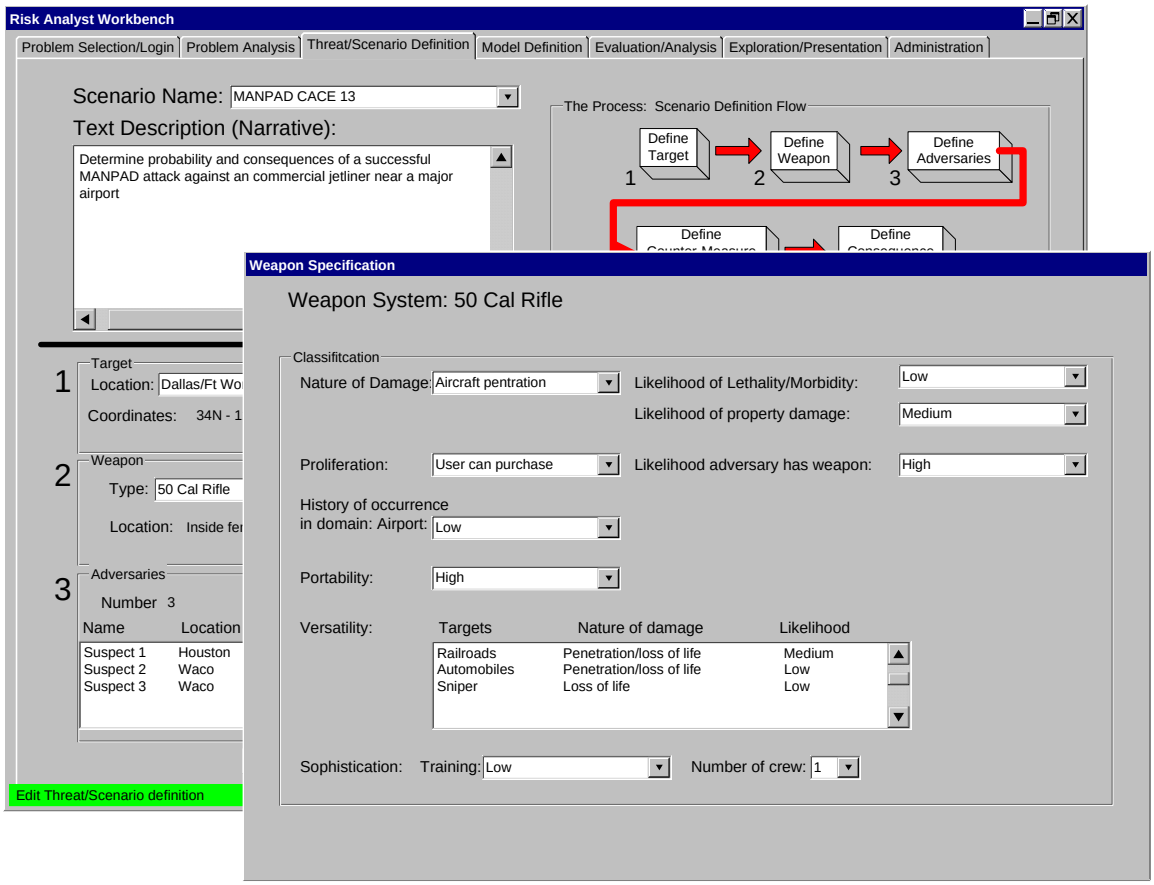

Figure 4-13 Weapon Attributes

4.3.5 Model Definition

This interface is yet to be defined.

4.3.6 Evaluation/Analysis

This interface is yet to be defined.

4.3.7 Exploration/Presentation

This interface is yet to be defined.

4.3.8 Administration

This interface is used to configure the default operation of RAW. Weapon types and capabilities, target specifications, personnel profiles, and counter-measure classifications can be added and/or updated via the “Admin” capability.

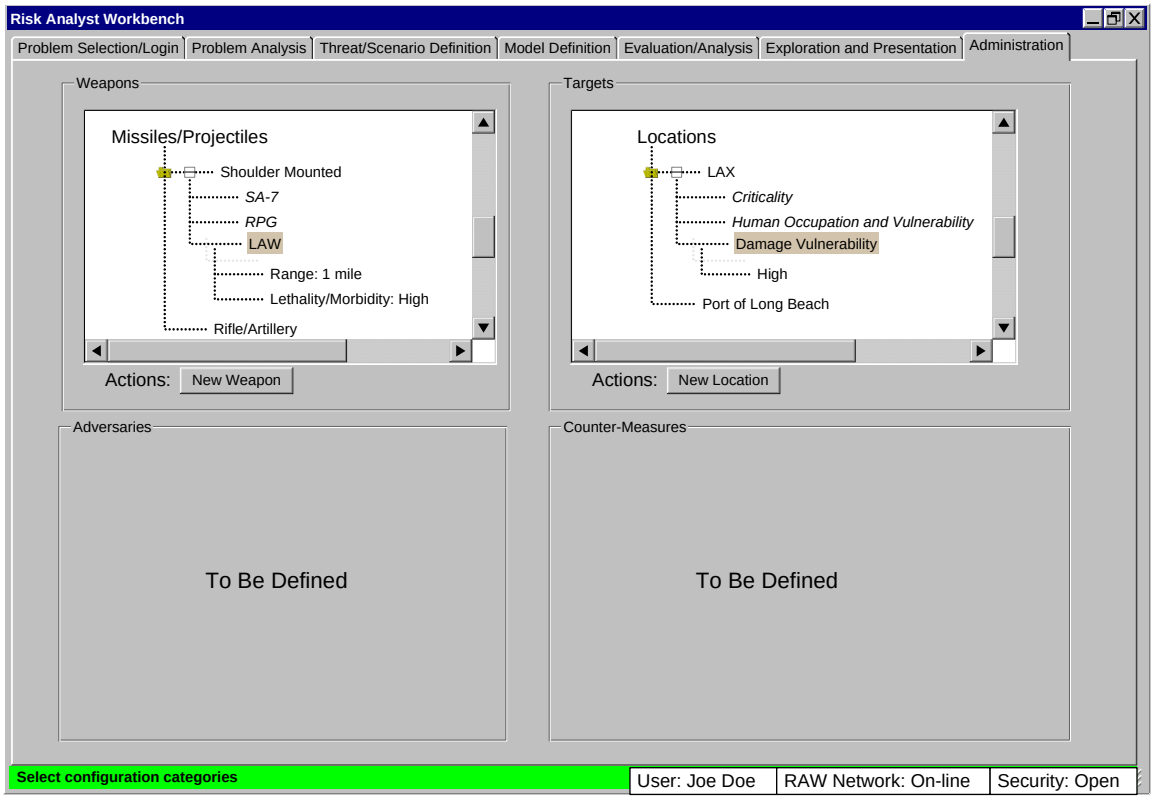

Figure 4-14 Possible Weapons Capability Definition Admin Interface

4.3.8.1 Weapons Classifications

For each potential weapon (including biological and chemical), the "admin" interface is used to classify the weapon in terms of the following attributes.

- Nature of damage
- Proliferation
- Historical occurrence
- Portability
- Versatility
- Sophistication

4.3.8.2 Target Classifications

For each potential target (structures, people, valuable assets), the "admin" interface is used to classify the target in terms of the following attributes.

- Criticality
- Human Occupation and Vulnerability
- Damage Vulnerability
- Symbolism
- Protection

4.3.8.3 Individuals Classifications

For each potential individual involved with undertaking the terrorism act, the "admin" interface is used to classify the individual in terms of the following attributes.

- Persistence
- Education and sophistication
- Commitment
- Mobility
- Motivation
- Scope and scale

4.3.8.4 Counter-Measure Classifications

For each potential counter-measure used to thwart a terrorism act, the "admin" interface is used to classify the counter-measure in terms of the following attributes.

- Point of intervention
- Direct costs
- Indirect costs
- Participants

5 Technical Challenges

The following are the technical challenges to successfully developing and deploying the CREATE Risk Analyst's Workbench (RAW):

- Ability to divide all possible risk scenarios/events into classes so that scenario/event templates can be developed
- Developing an API for interfacing risk models to RAW
  - What parameters are required and how should they be passed?
  - What is the expected input? Expected output?
- Tracking the authors and access levels of data and models
  - Who created the data/model and who (access level) can access this information on the global RAW distributed network?
  - How current is the data/model?
  - How recently has the data changed since last used?
- Human-Computer Interface. Development of the necessary templates, model interfaces, and configuration management interfaces to allow for an analyst to undertake risk assessment.
- Decision support tools required to aid analyst in defining the problem.
  - Weapon recommendations
  - Counter-measure recommendations

- Data management challenges
  - Keeping secure/sensitive data separate from non-secure/open data
  - Stand-alone/local operations and re-synchronization of data after workstation is back on-line.

6 Deliverables and Development Plan

The goal is to get a working prototype operational by Aug 2006. The prototype will contain the following capabilities:

- Human-computer interface that allows the user to define risk scenarios/events, select models and configuration parameters, and undertake unlimited "what-if" exercises to evaluate threats and counter-measures and generate recommendations.
  - Prototype will be limited to models developed by USC CREATE
    - However, will take advantage of opportunities to interface with models from other DHS Centers of Excellence if available.
  - Support for specifying weapons to target feasibility, weapon system capabilities, and counter-measure to weapon capabilities.
- RAW distributed network limited to the USC CREATE community
  - However, will take advantage of opportunities to interface with other DHS Centers of Excellence if available.
- Risk scenario/event definition templates that cover the majority of threats likely to be investigated by the DHS research and policy making community
- API to allow integration of models into RAW
  - Includes communication protocols

The following is the development plan:

- Jan – Jun '05: Requirements Analysis and Preliminary Design – Done
- Jul – Sep '05: GUI prototyping and preliminary system design development
  - Includes initial review of several GUI prototypes with USC CREATE research staff
- Oct '05 – Mar '06: Prototype development and testing of initial architecture
  - Development of CREATE RAW library interface
  - Development of initial GUI sub-system
  - Includes alpha testing with USC CREATE research staff
- Apr – Jul '06: Beta tests with USC CREATE research staff
  - Includes debugging
- Aug '06: Generate final report for year 2
  - Prep for on-going effort

7 Conclusion

The CREATE Risk Analysts' Workbench (RAW) helps risk analysts assess potential strategies for countering terrorist threats. RAW will allow the integration of different risk, consequence, emergency response, and economic models in a common user and data set management interface. The user interface allows for creation and specification of new scenarios and models for analysis, management of existing scenarios and data, and sharing of scenarios and data among multiple analysts. By collaboratively integrating their models and data, analysts can perform far more complicated assessments, far more quickly, than previously possible.