*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**

DRAFT

# 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 ..... 4**

**2 THE PROBLEM ..... 4**

2.1 CURRENT HOMELAND SECURITY RISK ANALYSIS ENVIRONMENT ..... 4
2.2 MOTIVATION/VISION OF RAW ..... 6
2.3 SURVEY OF EXISTING SOLUTIONS ..... 7

**3 REQUIREMENTS ..... 9**

**4 DESIGN ..... 11**

4.1 CREATE RAW SYSTEM ARCHITECTURE ..... 11
*4.1.1 CREATE Geographic Information System (GIS) ..... 13*
4.2 PRELIMINARY SOFTWARE SYSTEM DESIGN ..... 15
*4.2.1 Concept of Operations – Risk Assessment and Decision Support ..... 15*
*4.2.2 Concept of Operations – Administration ..... 19*
*4.2.3 Scenario/Event Templates ..... 19*
*4.2.4 RAW Distributed Network ..... 20*
*4.2.5 Enhanced Situational Awareness ..... 20*
*4.2.6 Preliminary Software System Design – RAW Software ..... 21*
4.3 GRAPHICAL USER INTERFACE ..... 23
*4.3.1 Login GUI/Problem Selection – Main GUI ..... 24*
*4.3.2 Decision-Making/Policy-Making and Risk Analysis ..... 28*
*4.3.3 Decision-Support/Analysis GUI ..... 28*
*4.3.4 Threat/Scenario development GUI ..... 28*
*4.3.5 Model Definition ..... 35*
*4.3.6 Evaluation/Analysis ..... 35*
*4.3.7 Exploration/Presentation ..... 35*
*4.3.8 Administration ..... 35*

**5 TECHNICAL CHALLENGES ..... 37**

**6 DELIVERABLES AND DEVELOPMENT PLAN ..... 38**

**7 CONCLUSION ..... 38**

# 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.

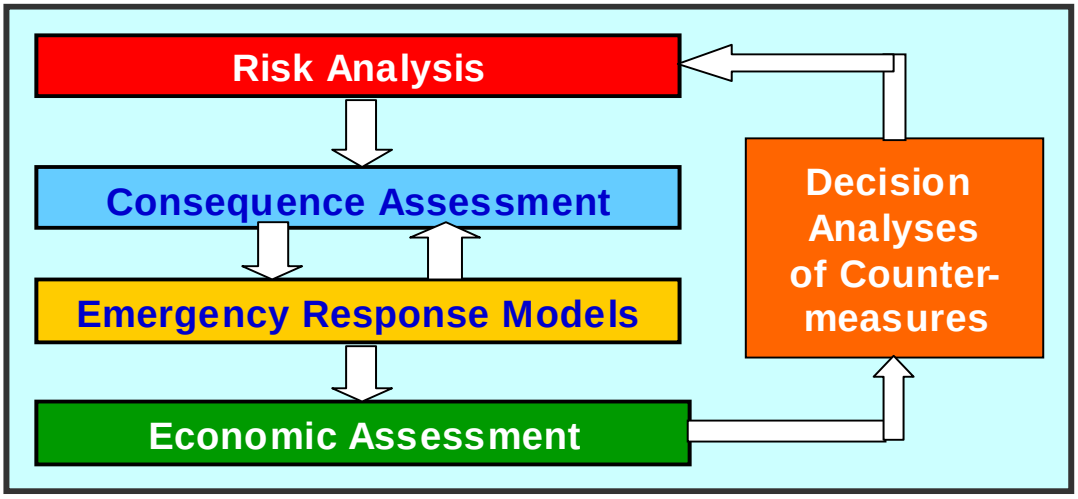


Figure 1-1 CTMS Four-step modeling system

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