

# **Development of An Analysis Tool For Performing Civil Aviation Security Risk Assessment**

Allan R. Hunt  
AKELA, Inc.  
5276 Hollister Avenue, Suite 263  
Santa Barbara, CA 93111

Karl F. Kellerman  
FAA Office of Civil Aviation Security  
800 Independence Avenue, S. W.  
Washington, DC 20591

Assessing the effectiveness of security measures within the aviation operating environment carries with it profound risk management implications. Remedial actions which result from these assessments affect the safety of airline passengers, airports, and aircraft and can significantly change the cost of doing business for the airline industry. Being able to quantify the risks to the civil aviation system allows the development of informed policies which balance the cost of corrective actions with the benefits of increased safety.

AKELA has developed an expert system program which enables users to examine and assess the three major elements of risk - threats, vulnerabilities, and assets - and then determine the impact of mitigating measures on overall security risk. Risk is determined quantitatively and measured in dollars thus allowing a common comparison between airports in widely varying operating environments. The program's expert system leads the user through a detailed vulnerability assessment which encompasses physical, operational, and technical elements of security in each of the major areas of an airport. A graphical user interface allows the user to see all of the vulnerability and risk assessment results at one time and provides a simple means of investigating the effects of implementing risk reduction measures which the tool recommends to the user.

The FAA has embarked on a program of using this tool to perform vulnerability and risk assessments at selected domestic airports as directed by the Vice President's Commission on Aviation Security.

## **1.0 INTRODUCTION**

Commercial aviation is an important part of the U.S. economy generating about \$300 billion in revenues, employing about 1 million people, and enplaning 500 million passengers each year. Increasing competition, and the trend toward lower fares are projected to increase the number of enplanements annually to 800 million by 2007.

At the same time, the threat of violence to aviation is estimated to be increasing. Incidents such as Pan Am 103 and more recently TWA 800 focus attention on aviation security and generate the impetus for improvements. However, implementing security improvements is often difficult because of differences between the government and industry over funding, effectiveness, and the impact on operations, passengers, cost, and revenues.

What is needed is a means of determining where in the aviation system the risks are greatest, prioritizing responses so the limited amount of money available is used most effectively, and tailoring the response on the basis of individual airport and airline needs.

The Civil Aviation Security Risk Assessment Program (CASRAP) was developed to help the FAA meet these needs. It has been designed as a tool to quantify security risk, to provide consistent assessments, and to support recommendations for specific improvements to the security of individual airports and airlines.

## 2.0 PROGRAM ORGANIZATION

CASRAP is a customized version of AKELA's Security Analysis Support System (SASSy) software. It is an analysis tool which has been structured to examine the three major elements of a security risk assessment. These elements are: 1) Assets - the tangible and intangible things that could be lost, 2) Threats - the potential causes of the loss of assets, and 3) Vulnerabilities - the weaknesses in security measures which allow threats to be successful.

Assets are important to this model because they have a quantifiable value. Without assets there is no risk because there is nothing to lose. Assets are threatened in ways which cannot be controlled. Threats choose when to act, where to

act, and how to act. While the threat can't be controlled, vulnerabilities can. Vulnerabilities are a direct result of the way in which security measures are implemented to protect assets.

Risk is defined in terms of dollar loss of assets. It is the combination of how often a threat will try to deprive us of our assets, the likelihood that each attempt will be successful, and the value of the assets lost. Each of these elements of risk is examined in detail by CASRAP.

Figure 1 shows a simple diagram of the architecture of CASRAP. As shown in the figure each of the elements of a CASRAP risk assessment interacts with SASSy's expert system and analysis algorithms. These algorithms make judgments about the frequency and severity of threats, attractiveness and value of assets, and adequacy of existing security measures. The SASSy user interface shows analysis results in easy to read charts.

### Threats

Quantifying the frequency of occurrence of the threat is usually the hardest element of a risk assessment. This is because what has happened in the past at a specific location is not necessarily a good indication of what might happen in the future. The occurrence of threat attempts is a statistical phenomenon. Trying to predict future attempts from past history at a location is a

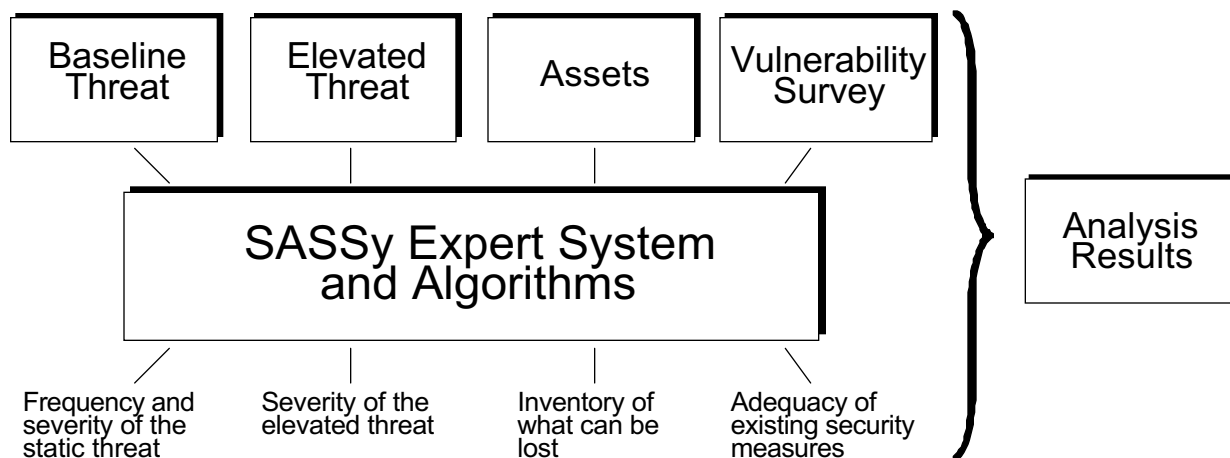


Figure 1 - Civil Aviation Security Risk Assessment Program Architecture

problem because the sample size is small and data may be incomplete. Past incidents are really a better indicator of vulnerability rather than the frequency with which threats occur.

In CASRAP there are two elements of threat: 1) baseline, and 2) elevated. The baseline threat analysis takes into account the underlying criminal threat which is always present in the airport environment. It is based on crime statistics compiled nationwide by the FBI and adjusted to reflect the local airport environment. This is an attempt to recognize that terrorists and bombs are not the only source of criminal activity which threatens the civil aviation system. Passengers, visitors, and employees have the right to be protected from murder, rape, robbery, and assault and it is not just terrorists who perpetrate these acts.

The elevated threat analysis increases the statistical probability of a specific terrorist act being perpetrated and is based on an assessment of intelligence information. It considers things such as the type of threat, threatener credibility, source reliability, and the current threat environment in making judgements about the level to which the threat statistics within CASRAP should be elevated.

### **Assets**

Assets are the focus of the risk assessment. They are divided into two categories - people and property. CASRAP knows which threats are applicable to which assets. An important part of the risk assessment is placing a value on each asset. This takes the form of specifying both a direct and indirect value associated with a single loss of each asset. Direct value is usually associated with the replacement cost of the asset. Indirect value is sometimes called an “opportunity” cost by economists. It is a cost incurred because the opportunity to use the asset is lost - for example, profit dollars not made because an airplane can not be flown. In a CASRAP analysis one can choose to omit or include indirect costs.

### **Vulnerability**

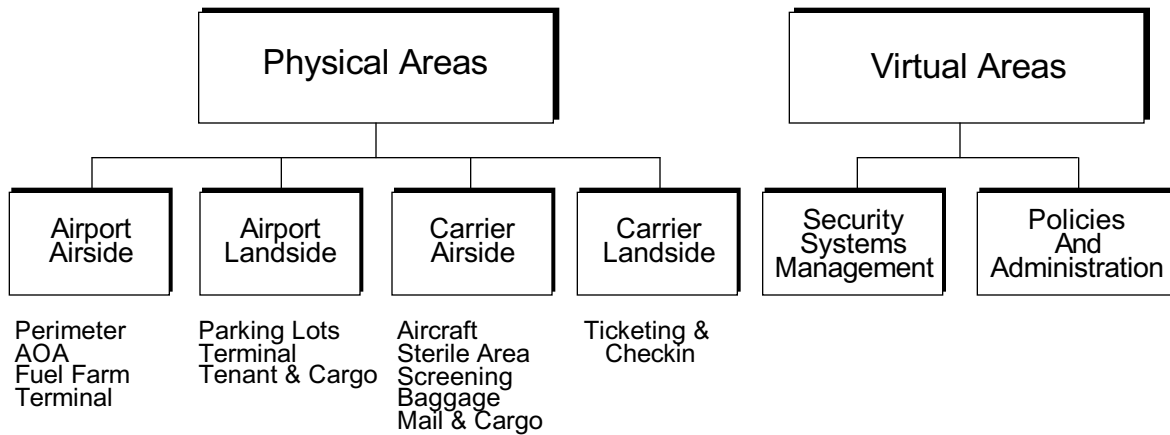
Vulnerabilities are the only element of risk over which we have some control. Vulnerabilities are built into a system through its design, the equipment that is used, the procedures that are followed, and the policies that are made. They are independent of the threat and are always there to be exploited even though there may have been no previous threat attempts.

Since there are so many different ways equipment, procedures, and policies can combine to protect assets, it usually takes a security expert to determine the vulnerabilities of a facility. An expert’s experience allows him to make judgements about the vulnerabilities in new situations. Traditional math model approaches to vulnerability analysis fall prey to this multiplicity of possibilities and generally fail in their attempt to describe overall system vulnerability except within the bounds of a very specific “known threat”.

Embedded in CASRAP is “expert system” software which does what a security expert does. It knows what questions to ask about equipment, procedures, and policies and makes judgements about vulnerabilities.

Underlying CASRAP’s expert system is an organized security assessment methodology which is shown in Figure 2. It relies on two concepts: 1) a facility can be divided into physical and virtual areas, and 2) there are elements which provide security functions in each area. Vulnerabilities are uncovered by making a systematic survey on an area by area basis of the elements which provide protection to the assets.

As shown in Figure 2, CASRAP has defined four physical areas and two virtual areas. We define physical areas within a facility because that is where the assets we are trying to protect are located. A virtual area has no assets, however, elements of a virtual area have a direct impact on the protection of all assets.



**Figure 2 - CASRAP Security Assessment Organization**

Since there are many elements which provide a security function, we group them into physical, procedural, and policy categories. By surveying each area with respect to each of the security functions we make sure that nothing is overlooked.

**Risk**

CASRAP’s risk calculation puts together all of the threat, vulnerability, and asset value information to produce a quantitative risk result expressed in dollars. Showing trade-off results in dollars allows all results to be compared on a common basis.

There are two dollar results shown for each calculation. The first is Annual Loss Expectancy (ALE) which uses the expected frequency of threat attempts and the average cost of a loss to calculate an annual expected loss. ALE is calculated as if there were no security measures in place and represents a probability of success of 1.0 for threat attempts. This results in a worst case calculation and becomes the standard or baseline which is used to judge the effectiveness of your actual security measures.

The second calculation is Risk. It uses the same expected threat frequency and average cost of a loss numbers as the baseline ALE calculation, but it also factors in the effectiveness of the particular

security measures in place. What those security measures do is reduce the probability of success of the threat to some number less than 1.0. This is your vulnerability and is determined by CASRAP’s expert system.

Comparing the Risk number to the ALE number gives a direct measure in dollars of the effectiveness of your security measures. The difference between the two numbers is the amount of potential dollar loss your security measures prevent. The cost of providing your security measures can be compared to the annual potential loss prevention to show you the cost effectiveness of your security.

Having this common baseline makes it possible to compare all proposed changes in security measures to one another to determine which will provide the greatest risk reduction. The cost of implementation and the resulting risk reduction, together, show how cost effective a proposed security measure is, and can be used as the basis for informed decision making.

**3.0 CASRAP FUNCTIONS**

The graphical user interface for CASRAP is organized around a set of windows which let users exercise any CASRAP function at any time. The windows are accessed from the button bar or from the menu bar shown in Figure 3. There are



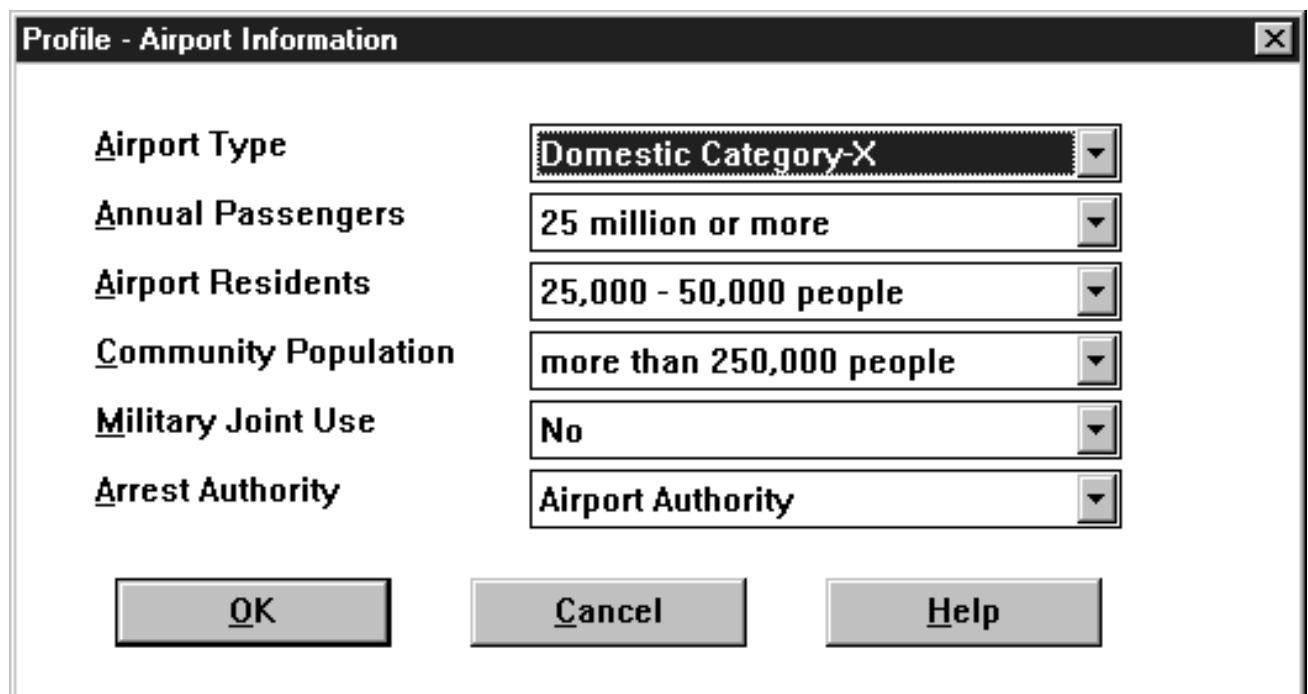
**Figure 3 - CASRAP Menubar**

six major functions - Profile1, Profile2, Threat, Assets, Survey, and Analysis. The first three are associated with defining the baseline and elevated threat.

Pushing the Profile 1 button brings up the window shown in Figure 4. There are six elements of airport information which the user selects with list buttons. Each item has several choices. CASRAP uses this information primarily to determine the baseline threat frequencies and local population to which they apply. The Profile 2 button initiates a series of questions the user must answer about the environment around the local airport. An example question from this profile set is shown in the Query window of Figure 5. These questions are used to determine the threat environment in the airport operating area and to decide whether there is an increased likelihood of terrorism activities because of these

environmental factors. Profile 1 and 2 results are combined and used by CASRAP to predict the actual frequency of the threat.

The Threat button brings up another window with list buttons shown in Figure 6 which is used to enter intelligence information associated with a specific elevated threat condition. This information is used by CASRAP to adjust the baseline threat frequency to account for a higher probability of occurrence represented by the specific terrorist threat. Since specific threats occur infrequently, CASRAP allows the user to turn the elevated threat on or off. This is done with the lightning bolt button on the button bar of Figure 3. Toggling the lightning bolt button allows the user to see (when using the Analysis function) the resultant change in risk (\$) to the various areas of the airport and to investigate the impact of changing specific security measures in response.



**Figure 4 - Airport Profile Information Window**

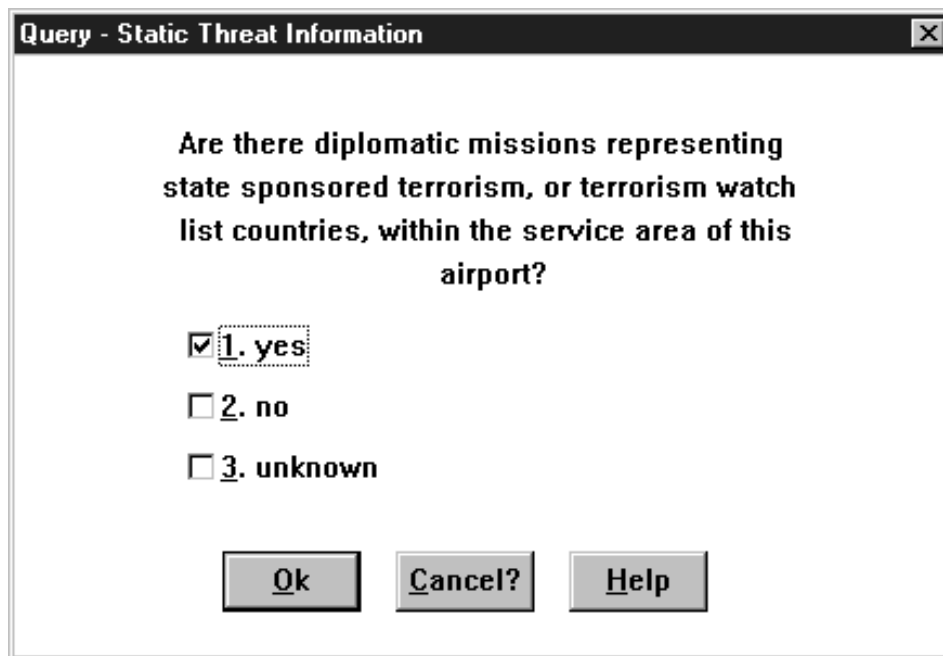


Figure 5 - Airport Local Environment Information Window

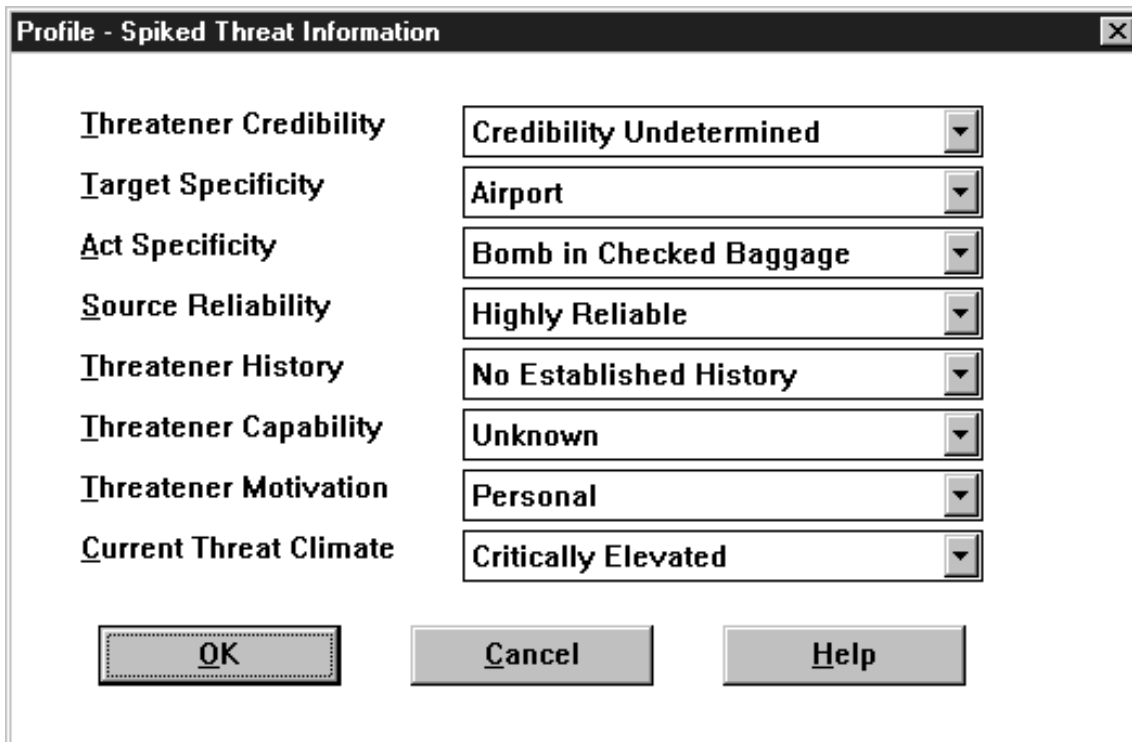


Figure 6 - Elevated Threat Information Window

The Assets button is used to input an inventory of airport assets which are at risk. Pressing this button brings up a window with predefined classes of assets as shown in Figure 7. The Area list button allows selection of the specific physical area in which the assets reside. An asset is selected by checking the box next to it. Direct and Indirect values for the one time loss of each asset are selected by using the list buttons.

The Survey button is used to start the vulnerability assessment portion of CASRAP's risk analysis by reviewing the specific security measures in

place. Selecting Survey brings up two columns of buttons as shown in Figure 8 which show the Areas of the airport and the Security Components of each area. The number of buttons shown in the components column is sensitive to which button in the Area column has been selected. A vulnerability assessment is conducted by first selecting the Area for assessment and then selecting a security component. As soon as a Component button is selected, CASRAP's expert system begins asking questions about the specific security component. These questions are presented to the user through the Query window

The screenshot shows a window titled "Asset Selection" with a close button (X) in the top right corner. At the top, there is a dropdown menu labeled "Area" with "Airport Airside" selected. Below this, there are two columns of dropdown menus labeled "Direct" and "Indirect". To the left of these columns is a list of asset categories, each with a checkbox. The assets and their corresponding values are as follows:

Asset Category	Direct Value	Indirect Value
<input checked="" type="checkbox"/> Human Assets	\$10K	\$100K
<input type="checkbox"/> Buildings		
<input checked="" type="checkbox"/> Vehicles	\$20K	\$20K
<input checked="" type="checkbox"/> Heavy Equipment	\$20K	\$50K
<input checked="" type="checkbox"/> Portable Equipment	\$2K	\$20K
<input checked="" type="checkbox"/> Fuel Farms	\$10M	\$10M
<input checked="" type="checkbox"/> Aircraft	\$1M	\$1M
<input checked="" type="checkbox"/> Control Tower	\$1M	\$10M
<input type="checkbox"/> Avionics Equipment		
<input type="checkbox"/> Utility Systems		
<input type="checkbox"/> Communications System		
<input checked="" type="checkbox"/> Navigational Aids	\$20K	\$50K

At the bottom of the window, there are three buttons: "OK", "Cancel", and "Help".

Figure 7 - Asset Definition and Valuation Window

Areas	Components
Security Systems Management	ID Media
Policies and Administration	Security Officers
Airport Airside	Key Controls
Airport Landside	Intrusion Detection
Air Carrier Airside	Access Controls
Air Carrier Landside	Design and Construction

**Figure 8 - Vulnerability Survey Window**

shown in Figure 9. Many questions asked depend on the answers given to previous questions. After each set of questions has been answered CASRAP places a check mark in the appropriate Components button and makes its judgement about the effectiveness of the security measures.

Pressing the Analysis button shows the results of CASRAP's calculations in a series of four windows. These windows are in bar chart format as shown in Figure 10 and show the vulnerability of each airport area, the vulnerability of the security components in a specific area, the risk associated

**Query - Select one item only ...**

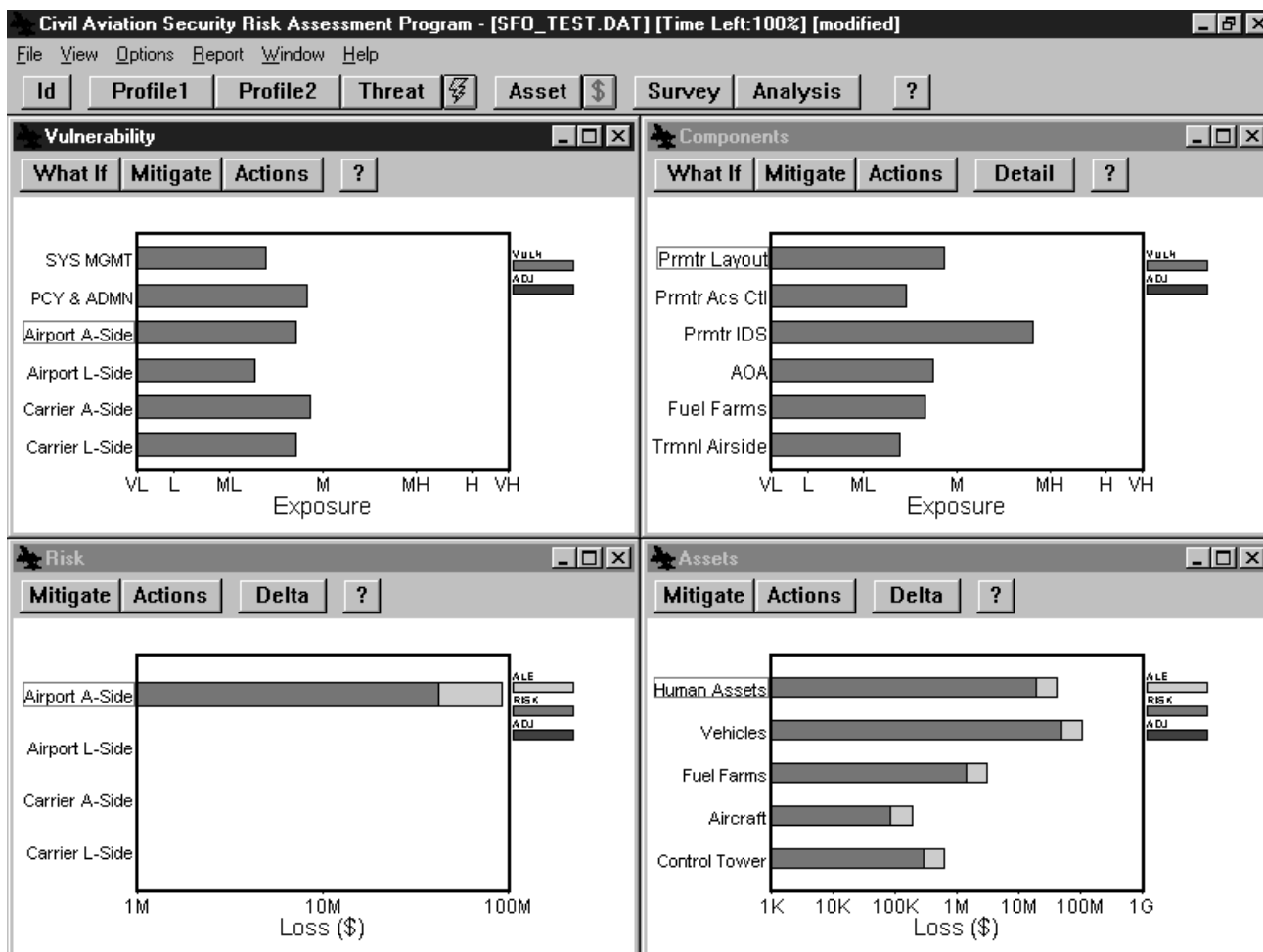
**Does the office of airport security control the issue, control and display of vehicle and personal identification media?**

1. Yes

2. No

**Ok**   **Backup**   **Cancel?**   **Help**

**Figure 9 - Vulnerability Survey Query Window**



**Figure 10 - CASRAP Analysis Window**

with each airport area, and the risk associated with the assets in a specific area. Vulnerability results are expressed in terms of exposure on a Very Low to Very High scale. Risk results are expressed in terms of dollars. The risk windows show both the ALE, as explained in Section 2, and the actual risk. Comparing risk and ALE shows quantitatively the value of your security measures.

The analysis windows have four additional buttons: What If, Mitigate, Actions, and Detail. The What If and Mitigate buttons allow you to see how changing security measures changes risk. Pressing the What If button lets you review the status of your survey of security measures as shown in Figure 11. You can see the effect of changing some of your security measures by

changing the answers to your survey questions. CASRAP calculates how much difference it makes and shows the result as an adjustment in the analysis graphs as shown in Figure 12.

Pressing the Mitigate button lets you see what CASRAP recommends as ways of improving security as shown in Figure 13. Selecting from the list will cause CASRAP to calculate the improvement and show the result as an adjustment in the analysis graphs as shown in Figure 14.

The Actions button keeps a history of the What If and Mitigation changes made. The Detail button shows more information on the vulnerabilities and attributes associated with a specific security component.

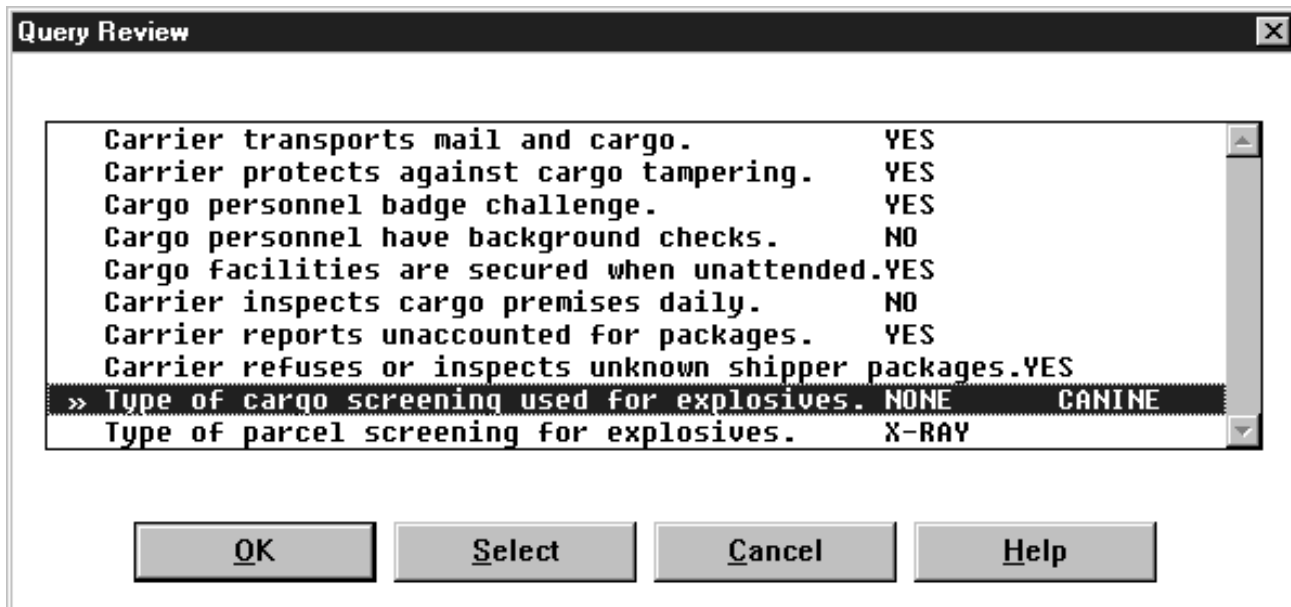


Figure 11 - What If Window

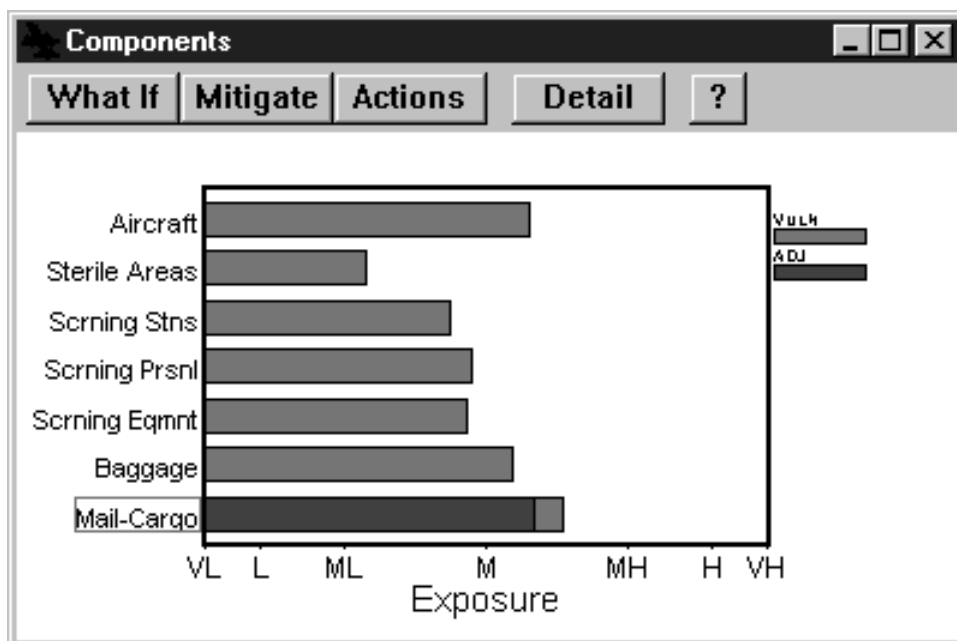


Figure 12 - What If Results Window

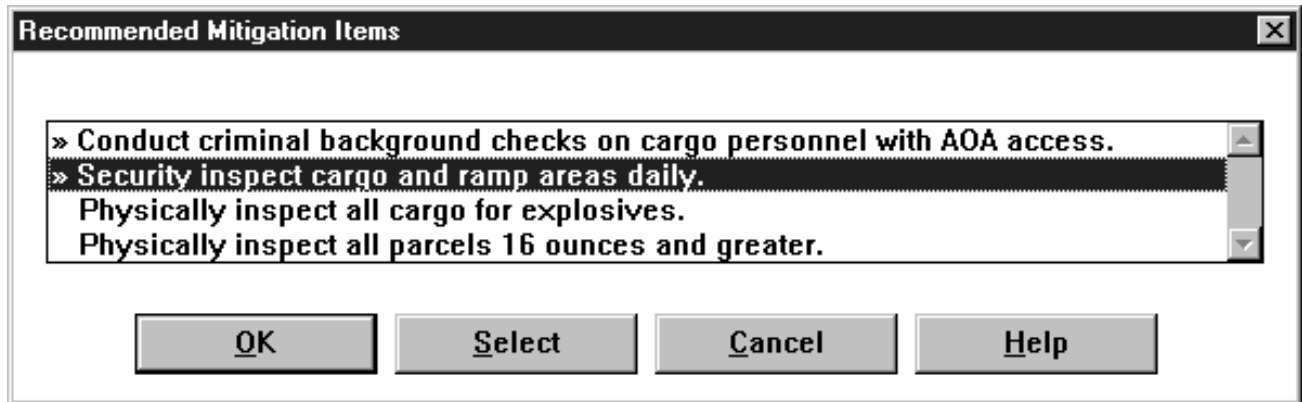


Figure 13 - Mitigation Window

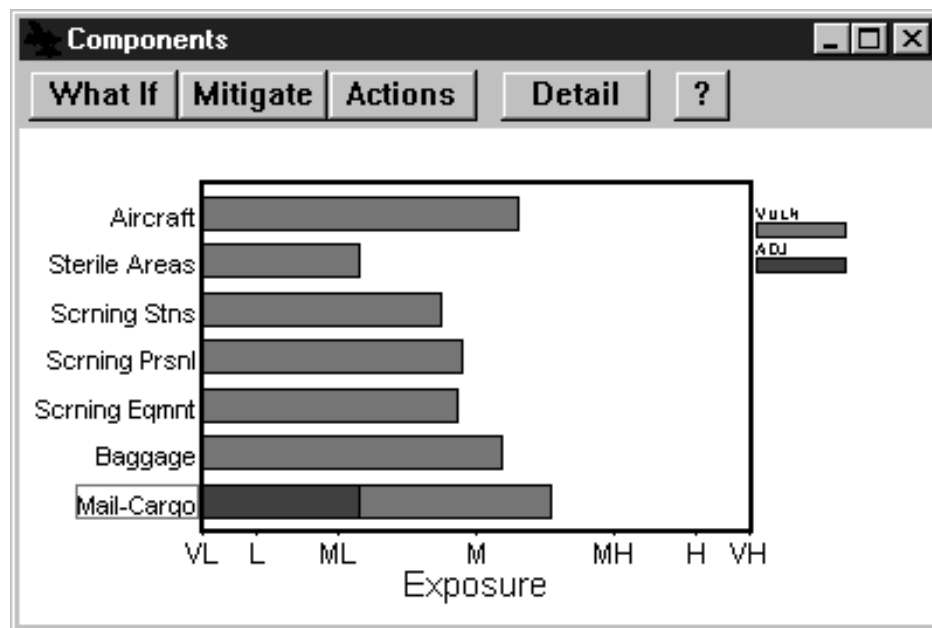


Figure 14 - Mitigation Result Window

CASRAP's windowed interface makes it easy to navigate among its major functions, shows results of the entire assessment on one screen so that problems are easy to spot, and lets the user see results of potential changes to security in real

time. This interactive interface lets the user control the analysis process, rather than being controlled by it, thus allowing both a wider range of analysis and consideration of options than traditional math model approaches.

#### 4.0 FIELD TEST EXPERIENCE

CASRAP has been used by the FAA in a set of preliminary field tests to determine how it can be integrated with its regulation and policy making functions. While the testing to date has gone slowly and its scope has been limited, there are some preliminary conclusions which can be made.

Field testing is being accomplished in parallel with an assessment function which was mandated by the White House Commission on Safety and Security. One way in which this function is performed is jointly with a team of FAA and FBI people. The last time we did it we took CASRAP along to see how it fit into the process.

Normally we do physical inspection first. Since a manual vulnerability inspection had recently been performed at Newark, we tried to use CASRAP to validate both the Newark results and the CASRAP model - in one step. We found out that CASRAP asked too many questions that no one knew the answers to. It used some terminology unfamiliar to the team. The FBI people were skeptical of the threat numbers. The team's tendency was to want a None of the Above or Not Applicable answer to almost every question until we actually began to think about it.

Asset values caused a lot of consternation. It was not clear to any of us how much the underlying mathematics of the model would do. For instance, should we put in the total replacement value of the asset if the "threat" would only destroy a small portion of it? (The answer is "no".) Some prior instruction or a handbook would be helpful in this area.

The consensus was basically that CASRAP did seem to do a reasonable job of making an assessment and provided consistency so that we could compare one place to another. It did highlight

areas of deficiency and gave some direction to what we should do about it. However, it was hard to change from the traditional pad and paper approach to a fully automated computer based approach.

Finally, there needs to be a way of rolling up multiple airlines at a single airport so that we can get a better overall picture. Multiple terminals and multiple airlines at each terminal (JFK, for example) present even more of a challenge. We don't have any way of doing that now.

#### 5.0 CONCLUSION

CASRAP captures the information needed to perform a quantitative risk assessment of airports and air carriers in a concise and easy to use format.

Its Threat function recognizes that there are differences in airports and their surrounding environments and tailors its results accordingly.

Its Assets function focuses attention on assets that need to be protected and forces consideration of the value of what could be lost.

Its Survey function performs disciplined and consistent vulnerability assessments making sure that nothing is overlooked.

Finally, its Analysis function highlights problem areas, recommends ways of improving them, and allows the investigation of changing security measures in response to changing needs.

Protecting the flying public from terrorism and acts of violence requires that technology and policy work cooperatively. Analysis clarity and insight help create policy wisdom. We believe that CASRAP will help provide the FAA with that analysis clarity and insight.