DOT/FAA/AR-99/95

Office of Aviation Research
Washington, D.C. 20591

Application of the FAATC Risk Management Process to the Airport Vulnerability Assessment and Analysis Project (AVAP)

Richard T. Lazarick

Aviation Security Research and Development Division
Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

June 1999

This report is approved for public release and is on file at the William J. Hughes Technical Center, Aviation Security Research and Development Library, Atlantic City International Airport, NJ 08405

This document is also available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161

U.S. Department of Transportation
Federal Aviation Administration

TECHNICAL REPORT DOCUMENTATION PAGE

PB2000-101748

1. Report No. DOT/FAA/AR-99/95	3. Recipient's Catalog No.
4. Title and Subtitle APPLICATION OF THE FAATC RISK MANAGEMENT PROCESS TO THE AIRPORT VULNERABILITY ASSESSMENT AND ANALYSIS PROJECT (AVAP)	5. Report Date June 1999 6. Performing Organization Code AAR-510
7. Author(s) Richard T. Lazarick	8. Performing Organization Report No.
9. Performing Organization Name and Address U.S. Department of Transportation Federal Aviation Administration William J. Hughes Technical Center Aviation Security Research and Development Division Atlantic City International Airport, NJ 08405	10. Work Unit No. 11. Contract or Grant No. DT059-96-D-00410
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration Associate Administrator for Civil Aviation Security, ACS-1 800 Independence Avenue, S.W. Washington, DC 20590	13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code ACS-1

15. Supplementary Notes
Report Prepared by:

Monica S. Grusche
Abacus Technology Corporation
5454 Wisconsin Avenue, Suite 1100
Chevy Chase, MD 20815

16. Abstract

This report summarizes Abacus Technology Corporation's experience in conducting risk/vulnerability assessments of airports in support of the Federal Aviation Administration (FAA) Airport Vulnerability Assessment and Analysis Project (AVAP). The report describes Abacus Technology's findings regarding application and effectiveness of the Risk Management Process developed for the FAATC and of the selected automated tool methodologies.

17. KEY WORDS Aviation Security; Security Surveys; Vulnerability; Threat; Countermeasures; Physical Security; Risk Assessment; Risk Analysis; Vulnerability Assessment; Vulnerability Analysis; Automated Tool.	18. Distribution Statement This document is available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 26	22. Price A03

TABLE OF CONTENTS

Page
Number

This page intentionally left blank.

1. INTRODUCTION

This report summarizes Abacus Technology Corporation's experience in conducting risk/vulnerability assessments of airports in support of the Federal Aviation Administration (FAA) Airport Vulnerability Assessment and Analysis Project (AVAP). The AVAP was initiated in response to a recommendation by the White House Commission on Aviation Safety and Security. The Commission's Final Report, presented on February 12, 1997, included a recommendation to conduct periodic vulnerability assessments of the nation's commercial airports. In response, the FAA William J. Hughes Technical Center (FAATC) issued Abacus Technology a Task to conduct risk/vulnerability assessments of Denver International Airport (DEN) and Detroit Metropolitan-Wayne County Airport (DTW).

The AVAP provided Abacus Technology an opportunity to test the Risk Management Process already under development for the FAATC. The Risk Management Process as used in the airport assessments is the result of nearly three years of research and development. It is described in detail in the FAATC Technical Report DOT/FAA/AR-99/, *Guide to the FAATC Risk Management Process*, March 1999. Abacus Technology applied the Risk Management Process to structure the vulnerability assessments conducted at the airports, as discussed in the *Airport Vulnerability Assessment Master Plan*, Abacus Technology Corporation, December 1997. The Abacus Technology Team assembled to conduct the airport assessments consisted of technical and operational security experts from Abacus Technology Corporation, Toyon Research Corporation, Security Design Sciences, and independent experts in the field of aviation security.

This report describes Abacus Technology's findings regarding application and effectiveness of the Risk Management Process and of the selected automated tool methodologies. Specific findings from the airports surveyed are presented in two security sensitive reports: the *Denver International Airport (DEN) Vulnerability Assessment Report* and the *Detroit Metropolitan-Wayne County Airport (DTW) Vulnerability Assessment Report*, Abacus Technology Corporation, September1998.

2. APPLICATION OF THE RISK MANAGEMENT PROCESS

The Abacus Technology Team applied the Risk Management Process previously developed for the FAATC to conducting its airport risk/vulnerability assessments. The Abacus Team approach was discussed in detail in its *Airport Vulnerability Assessment Master Plan*. The Risk Management Process is the product of nearly three years of research and development effort. The Airport Vulnerability Assessment Project (AVAP) provided the first practical test of the process. The process proved flexible enough to be applied in the airport assessments conducted for the AVAP. It worked well in efficiently analyzing the airport security situations. The process flow and description fit the airport analysis completely.

The process is shown below using the IDEF0 (Integration DEFinition for Function Modeling) modeling technique. In the IDEF0 method, boxes represent activities in a process. The left side of an activity box is reserved for inputs (things that are transformed into outputs by the activity), the right side for outputs (transformed inputs), the top for controls (constraints or rules that dictate the conditions of the transformation), and the bottom for mechanisms (tools, people, and systems that are used during the transformation). Each activity can be decomposed into sub-steps, creating a multilevel hierarchical diagram of a process.[1]

Figure 2-1, below, shows the parent of 19 detailed charts that define the process. The process consists of five primary steps depicted in Activity Boxes A1 through A5. In the AVAP, most of the preliminary and follow-on activities to the conduct of the risk/vulnerability assessments (Assess Risk, Activity A3) at the airports were defined either by the White House Commission on Aviation Safety and Security or by the FAA in response to the Commission's recommendations. These activities—Establish Risk Management Strategic Plan (A1), Formulate Approach (A2), Select and Implement Countermeasures (A4) and Monitor Countermeasure Effectiveness and Changes in Risk Factors (A5)—are important steps toward managing overall risk. The Abacus Technology Team described the application of these steps, even if they were determined and/or conducted by an outside entity. The application of the Risk Management Process activities in the surveys of DEN and DTW airports in the AVAP is described in Sections 2.1.1.1 through 2.1.1.5 below.

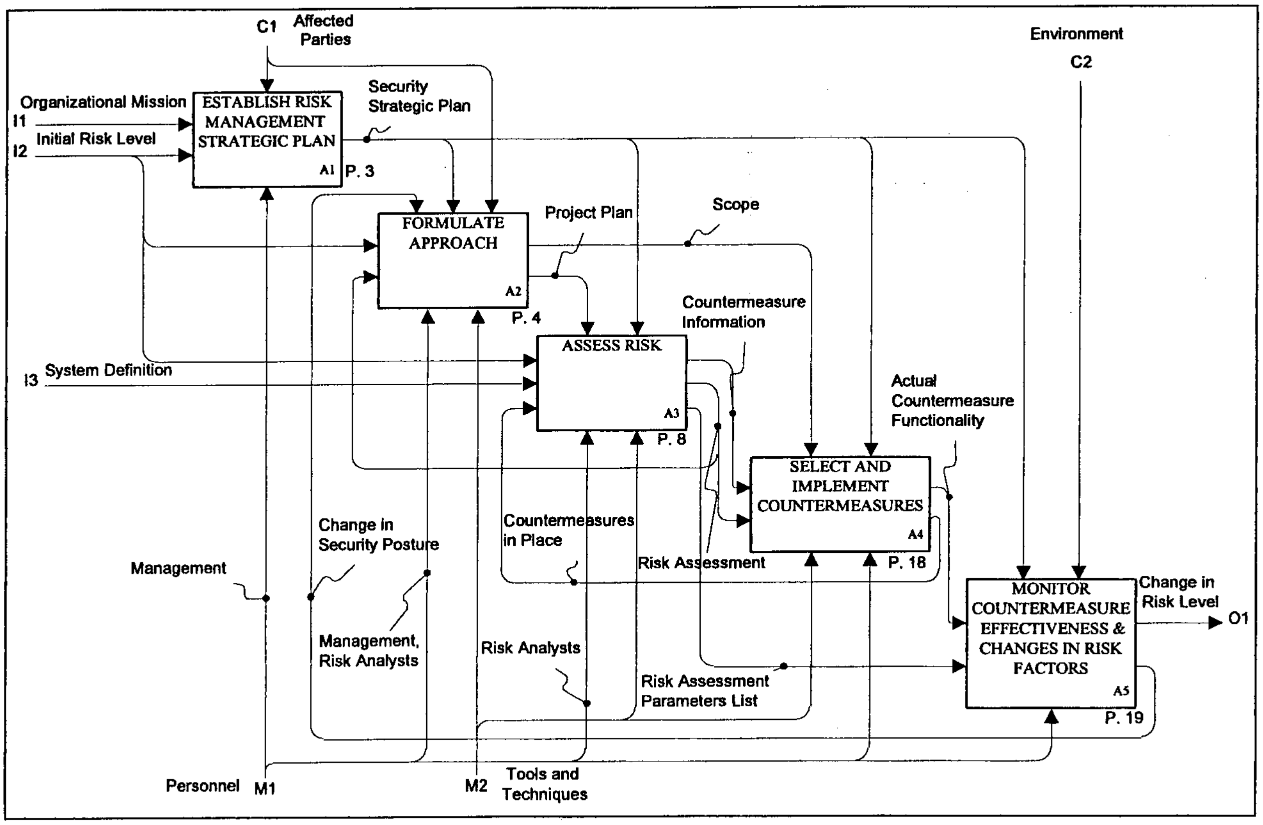

Figure 2-1. The Risk Management Process

[1] For a more detailed description of the IDEF0 modeling technique and description of the FAATC Risk Management Process, refer to the FAATC Technical Report DOT/FAA/AR-99/, *Guide to the FAATC Risk Management Process*, March 1999.

2.1 Establish Security Strategic Plan (A1)

To establish a security strategic plan (A1), it is necessary to establish objectives, authority, and coordination. The White House Commission on Aviation Safety and Security, through its recommendation to "conduct (quantitative) airport vulnerability assessments and develop action plans," established the strategy for the airport assessments performed under the AVAP. The Abacus Technology Team found that it was helpful to restate the security strategy in formulating its own approach and methodology to conducting the airport assessments.

2.2 Formulate Approach (A2)

The diversity of the airport system is such that there are many competing interests; therefore, the Formulate Approach (A2) step for an airport environment must address complex issues. An airport consists of a variety of facilities, assets, and organizations with various missions and areas of responsibility. Formulating the approach (A2) includes defining the scope and boundaries of the system, selecting the analysis approach and tools, and planning the project. The FAA statement of work (SOW) defined the scope and boundaries for this project. Predetermined FAA threat scenarios identified in the SOW governed the establishment of protection goals, an element of the scope.

The overall project budget, another element of the scope, was established in September 1996 when Congress appropriated funding to the FAA to conduct these assessments. Abacus Technology selected a combined qualitative and quantitative methodology and corresponding tools for its analysis approach. Both quantitative and qualitative approaches were used in order to uncover and measure the vulnerabilities inherent in the system while controlling the costs associated with conducting the analysis. The use of a combined qualitative and quantitative analysis approach was also essential in structuring the assessments and consolidating the objectives of multiple organizations.

Various software tools also aided the process. The Abacus Technology Team selected RiskWatch® to automate the survey instrument developed by Abacus Technology and the Security Assessment Model (SAM) to perform the quantitative vulnerability analysis. Additional tools used in the sensitivity analysis of risk were @Risk® (by Palisade Corporation) and REP/PC (by Decision Sciences Corporation). The Application of the Selected Tools is discussed in greater detail in Section 3.

2.3 Assess Risk (A3)

The Assess Risk (A3) activity step is the heart of the analysis. Vulnerability analyses (Evaluate Vulnerability, Activity A32), like those required for the AVAP are a component of risk assessment. The Assess Risk step consists of:

- Collect Data (A31)
- Evaluate Vulnerability (A32)
- Evaluate Risk (A33)

The Assess Risk process steps as applied to the Abacus Technology Team assessments of DTW and DEN as part of the AVAP are discussed in Sections 2.3.1 through 2.3.3.

2.3.1 Collect Data (A31)

Abacus Technology created a survey instrument to collect qualitative and quantitative asset and countermeasure data for the airport vulnerability assessments. RiskWatch® was used to organize the questionnaire and direct questions to the organizations involved with the scenarios. For the quantitative analysis, each threat scenario was modeled from a component and systems viewpoint. Initial quantitative models for each scenario at the airport were developed from airport layouts and airport security documentation collected before the on-site data collection effort, and were then modified after the site visits. From the operational data collected, a complete description of vulnerable paths and quantification of airport-specific sensors and procedures was recorded.

The FAA focus on the security of aircraft and passengers guided the determination of critical assets. The Abacus Technology conducted an analysis to determine which airport assets, if compromised, would directly affect the security of aircraft and passengers. The Abacus Technology Team then established the dependencies between those assets for input into the vulnerability analysis. Because only a risk sensitivity analysis and not a detailed risk assessment was conducted, only rough order of magnitude estimates of asset costs were determined for input into the risk calculations.

Data on the operational performance of security equipment at most airports are extremely scarce, very expensive, and potentially disruptive to acquire. Data from security equipment testing performed by the FAATC, not taken in an operational environment, are classified and were not available or directly usable for the Abacus Technology airport vulnerability analyses. Consequently, the information gathered on countermeasure performance was combined from many sources, including non-classified airport and FAATC documents and personnel, security equipment manufacturers, industry publications, and direct observation at the airport. Even with the combination of sources, the data available on most equipment was not sufficient to be able to identify probabilistic performance curves to replicate the operational setting of the airport. Therefore, when probabilistic methods were employed, assumptions concerning the shape and nature of the probabilistic curves were used in cases where there was an insufficient amount of statistically valid data to generate them. Engineering judgment was used to ensure that the uncertainty was properly accounted for and that the information was complete.

For political and security reasons, the FAA precluded the collection of airport-specific or local threat data; therefore, the Abacus Technology Team did not collect specific threat information at the airports. Only general threat information contained in a document entitled "Threat to Civil Aviation," provided by the FAA, and publicly available information concerning threats to the U.S. were considered during the preparation of the threat situation at the airport.

2.3.2 Evaluate Vulnerability (A32)

The Abacus Technology Team conducted quantitative vulnerability assessments. A quantitative vulnerability assessment is a representation of the current system from a *bottom-up* perspective—that is, it starts with a mathematical (e.g., fault-tree, logic tree) or graphical-path (e.g., simulation) model of the current security system. The goal of a quantitative vulnerability assessment is to represent the physical, operational, and procedural layout of the system as accurately as possible and then analyze the system's behavior.

Both a qualitative review at the airport and extensive modeling of the critical parameters that affect system vulnerability were used to define the quantitative analysis. The first step of the vulnerability analysis was to enumerate the paths to the targets based on data collected in the site surveys. For each threat scenario, a series of specific paths were chosen to represent the worst case (most vulnerable) set of paths. These paths are derived from the qualitative assessment of the unique facilities and procedures in place at the airport. In the modeling of each security system related to the paths, critical parameters[2] were determined, which have the most affect on overall system performance and therefore determine system vulnerability. The site surveys determined the following critical parameter inputs to the quantitative models:

- Distance from the target;
- Numbers and types of barriers;
- Sensors along the path that may be used to detect an intruder;
- The effectiveness of the assessment procedures, and
- The potential for responding to the event.

The quantitative analytical models for each threat scenario were then developed using the Security Assessment Model (SAM), a computerized simulation modeling tool. SAM was also used to analyze the likelihood of event success, prioritize vulnerable paths, analyze countermeasure performance/cost tradeoffs, and plan cost-effective security systems that include detection mechanisms, barriers, and response forces. The model employs a series of "shells" to describe the path along which an aggressor travels. At each shell, mechanisms (e.g., sensors, procedures, alarms) detect and/or assess the threat (i.e., person, weapon, or explosive device) and a response force reacts to the threat detection.

Analysis matrices were used to model the threat scenarios and shells in SAM. SAM calculates the probability of impeding or preventing an aggressor from perpetrating the threat event, or Probability of Intercept (P_i), at each shell. Three essential values, the Probability of Detection (P_d), the Probability of Assessment (P_a), and the Probability of Response (P_r) are required to determine P_i. Detection measurement performance data, cost data, and shell description provide the input parameters to calculate P_i. The cost, Probability of Detection (P_d), and Probability of Assessment (P_a) established for the sensors, procedures, and personnel are based on data gathered during the assessment.

[2] The determination of critical parameters was based on Pareto's law, also known as the 80/20 rule. Parato's law asserts that not all system elements have the potential for affecting system performance by a significant amount. In most cases, just a few variables will account for the largest variation in results. This phenomenon is also called the law of the significant few and insignificant many.

SAM uses two types of logical operands, called AND-gates and OR-gates, to combine the P_is of various countermeasures along a path. AND-gates and OR-gates define the way detection sensors and procedures function together. In most cases, the countermeasures deployed for each successive shell are combined using an OR-gate. The P_i increases if one "OR" more sensors are able to detect an object in the same shell (or at the same time in the process). The P_i decreases as successive shells are combined (one sensor "AND" then another type of sensor is deployed). This decrease in P_i results from the fact that each sensor has some probability of failing to detect the object. This probability of failing is additive through each shell.

A minimum to maximum ranging methodology was used to calculate P_i to reflect the inherent uncertainties properly. These uncertainties include sensitivities of the equipment in detecting the threat, skill level of the operator in assessing the threat, and uncertainties of response personnel in responding to the threat. Better testing and analysis using SAM and related tools will decrease the range of uncertainty, although the results shown in the analysis provided a valuable insight to security vulnerabilities.

In the process of assessing the proposed countermeasures, the lowest cost equipment option with the highest P_d and P_a was selected for analysis. The number and subsequent cost for equipment is heavily dependent on the throughput of the equipment, which involved operational issues outside the scope of the analysis. These issues drive how many machines will be required to maintain acceptable passenger and baggage flow. False positive alarms have a dramatic effect on throughput. For convenience, the entire cost of personnel and equipment at each shell was used to calculate the annual and lifecycle cost for the path. No distribution of cost to other paths (i.e., other gates along the concourse) that share the cost was attempted.

Intercept, for the purposes of the analysis, was defined as successfully detecting, assessing, and setting a response action into motion. Interception did not consider the *success* of the response. For example, the response to an armed aggressor may be initiated, but the success of the resulting firefight is not assured. Assuming that the response to an incident will be effective after intercept has occurred, vulnerability (V) in the quantitative analysis was set equal to the likelihood (L_p) that a path will be successful, $V = L_p$. Therefore, L_p is equal to one minus the probability of intercept (P_i), that is, $L_p = (1-P_i)$, therefore $V = (1- P_i)$. That is, the more difficult it is to intercept an aggressor (P_i is low), the more vulnerable the path (V is high).

2.3.3 Evaluate Risk (A33)

A vulnerability assessment determines the weaknesses in a system given that the perpetrator *will* attempt to achieve the undesirable event, i.e., the likelihood of event occurrence is considered *one* (100 percent probability). A risk assessment uses the information gained from a vulnerability assessment and also includes an assessment of event likelihood and event impact. A threat analysis is performed to determine event likelihood, i.e., the probability that a particular threat scenario may be perpetrated against a particular asset within a given timeframe. An impact analysis is performed to determine economic and/or social, political, and other indirect costs based on asset valuation. The result of an impact assessment is frequently expressed as an economic factor based on replacement cost and other financial assumptions.

The conduct of a risk assessment was not required for the AVAP; however, the Abacus Technology Team went a step beyond the required vulnerability assessments in its analysis to conduct risk sensitivity analyses. Since airport-specific threat information was not available, Abacus Technology used expert opinion and decision science methodologies to perform the risk sensitivity analysis. By using range estimates, and understanding how sensitive the results are to critical data elements and their density functions, it is scientifically possible to make decisions based on limited data and expert judgment. An expert panel of aviation security specialists was assembled for the risk sensitivity study. The panel used available data, including the "Threat to Civil Aviation Security" information provided by the FAA, concerning acts of terrorism to formulate their opinions. Similarly, the panel used historical aviation accident and terrorist event data to determine broad impact range assumptions. Then in a Delphi study, panel members created a range-estimate of likelihood and impact factors for each defined threat scenario.

In most cases, assumptions were made as to how the various countermeasure components (e.g., sensors, barriers, humans) reacted together in a system. The use of probabilistic component models reduced the need to run costly and non-statistically valid tests on-site. System performance was modeled by performing Monte Carlo simulations to determine how each component operated in the system. In this way, it was possible to determine which components had the greatest effect on the vulnerability exhibited by the overall system. This same methodology was used to test the effects on the results of various assumptions for P_d and P_a.

The result of the Monte Carlo simulation, which included the output of the SAM analysis for the vulnerability range by scenario, was used to prioritize the recommendations for corrective action to be taken by the airport. The resulting risk values were relative in nature, i.e., each threat scenario was compared to the others to determine which scenarios are most sensitive to increased risk factors. The cost-benefit estimates were not normalized (e.g., cost per passenger) and therefore, no conclusions were drawn as to precise cost-benefit issues. For example, if one risk value is twice as high as another, it does not follow that exactly twice the expenditure in corrective countermeasures is warranted. This study produced a prioritization of actions to be taken to reduce vulnerability.

2.4 Select and Implement Countermeasures (A4)

Essential to the vulnerability assessment is a method for the selection of appropriate and cost-effective countermeasures. The first step was to define the available alternatives. For the airport assessments, the FAA confined the scope of countermeasure alternatives to those already existing or available within two years. The Abacus Technology Team performed a cost/benefit analysis of countermeasures based on the relative vulnerability of the scenarios and available countermeasure installation, operations and maintenance, and lifecycle costs. Alternatives were ranked by factors such as cost and relative effectiveness against specific threats. The selection of suggested preventive measures is based on this step.

2.5 Monitor the System (A5)

Although this step was not within the scope of work defined in the AVAP project, the monitoring of countermeasure effectiveness and the changes in risk assessment factors is an essential element in the overall risk management process. Effective security management requires constant vigilance. It is recommended that airport vulnerability assessments will be conducted periodically to evaluate the impact of new environmental and other changes over time.

3. APPLICATION OF THE SELECTED TOOLS

Several computerized software tools were used to assist in this analysis. The two primary tools were RiskWatch® and the Security Assessment Model.[3] Additional tools used in the sensitivity analysis of risk were @Risk® (by Palisade Corporation) and REP/PC (by Decision Sciences Corporation). REP/PC is a DOS/PC based tool. It was not practical to use in its current level of development. The decision science concepts used in REP/PC were implemented in a @Risk model developed specifically for this project. Therefore, a detailed discussion of the REP/PC tool will not be presented in this section. The use of RiskWatch, SAM, and @Risk are discussed below.

3.1 RiskWatch

RiskWatch is an expert system-based, qualitative analysis tool that has been highly successful in the computer industry. RiskWatch catalogs and analyzes information on asset and loss value; potential threats (i.e., agents of damage/destruction); and safeguards (countermeasures). RiskWatch links threats to asset and loss categories to determine the effect of incidents, i.e., threat events. As was planned and documented in the Abacus Technology *Airport Vulnerability Assessment Master Plan*, the Abacus Technology Team did not employ the full capabilities of RiskWatch. The tool was used exclusively for qualitative data collection and not to conduct vulnerability or risk analysis.

The Abacus Technology Team had generated a set of over 400 questions based on previous security assessment work for the FAATC and tailored the questions to the AVAP threat scenarios. These questions were entered into a RiskWatch template for use at airports to assist in the organization of the survey database into question-specific categories. The intent was to focus the assessments prior to conducting site surveys to ensure efficient and comprehensive on-site data collection.

The ultimate intention of using RiskWatch, however, was to create a basis for developing a full-fledged qualitative airport risk assessment tool based on quantitative analysis. To determine vulnerability in the AVAP assessments, expert opinion weighted by the on-site observations was used to create unique P_d and P_a values to be input into the quantitative model. Abacus Technology's intention was to automate that process with the use of expert-system software (such as RiskWatch) techniques to record and reapply the expert knowledge. Programming of a

[3] SAM was originally developed by Mission Research, Inc. under contract to the Naval Facilities Engineering Security Center. The primary developer, Larry Pietrzak, worked for Toyon Research, Inc. and on the Abacus Technology Team at the time of the AVAP assessments.

comprehensive airport survey instrument and the expert knowledge required to relate survey elements and possible responses to threats, assets, and countermeasures into an expert system automated tool would improve the speed of the assessment and ensure repeatability.

Such a software development effort was beyond the scope and budget of the AVAP assessments; however, the Abacus Technology Team attempted to customize RiskWatch for use at airports. Abacus Technology purchased the development version of the software that included a physical security template and the ability to modify weights and relationships normally transparent to the user. The tool requires the analysis team to predetermine the asset, loss, threat, and vulnerability relationships (with factors for relative importance and impact). This set of relationships is tested using questionnaires directed toward informed personnel. The determination of vulnerability and risk are related to the answers of the questions as compared to a threshold value programmed into the tool.

In order for RiskWatch to provide usable results for an airport environment, needed sets, values for and relationships between assets, losses, threats, and vulnerability need to be established and tested. In working with RiskWatch, the Abacus Technology Team identified two main limitations of RiskWatch which make it somewhat cumbersome for airport use. The use of functional categories allows the user to establish specific question sets tailored to different types of users. In an airport environment, these categories might be established as security screeners, airport operations personnel, law enforcement, tenants, and other security-related elements. The survey questions overlap in many categories. While this does have the benefit of accommodating various types of users with different levels of knowledge, it can also be confusing, making the program more difficult to adapt.

A related limitation of RiskWatch which makes it cumbersome for users is the lack of a capability to nest questions. The only way to limit the number of questions any particular user sees is through the use of the functional categories. However, the user still has to answer all of the questions within the category or categories assigned to him or her. Without the ability to "nest" questions, and if a user answers negatively to the presence of an intrusion detection system, he or she would not be asked a series of follow-up questions about how that system operates. Additionally, in RiskWatch, the user would be forced to answer negatively to the follow-up questions, thus falsely increasing the overall vulnerability results.

3.2 Security Assessment Model

The White House Commission on Aviation Safety and Security, i.e., the Gore Commission, specifically recommended and appropriated funding to conduct the next round of vulnerability assessments quantitatively. Based on a study conducted by the Abacus Technology Team for the FAATC (Technical Report DOT/FAA/AR-95/60, *Catalog Of Automated Risk Assessment Tools - Airport Security*, July 1996), only a handful of tools fit the definition of a quantitative analytical tool. One such tool is the Security Assessment Model (SAM). SAM follows quantitative analytical methods similar to those of Sandia National Laboratory alluded to in the Gore Commission report (ASSESS). SAM also contains cost/benefit calculation modules, a comprehensive range of countermeasure information, and a wider range of modeling techniques (roving security personnel). For these reasons, the Abacus Technology Team chose the SAM tool to use in the airport vulnerability assessments.

The premise upon which probabilistic vulnerability and risk assessment is based, as previously stated, is to model the real world environment, procedures, operations, and technology surrounding each scenario. This means that each system is dissected, reviewed, and security failure modes determined. Points of unintentional (or intentional) system circumvention need to be determined and modeled. After the models are designed and developed, they must be tested to ensure that they properly reflect the operational performance of the system being studied.

To develop a detailed model for security systems is an extremely costly and complex task. Although the Abacus Technology Team added some graphical user interfaces to SAM to make it easier for an analyst to input data and manipulate scenarios, inexperienced users would still require in-depth training to create SAM models and conduct analysis. In addition, modifying the DOS-based code in SAM to translate it to a Windows environment proved to be a more complicated task and required more resources than anticipated.

Detailed equipment and human performance and operational data are necessary for accurate assessments. Actual operational data from a single test, or spot testing, is not a statistically valid means for determining system capability. Therefore, while a "Red Team" approach may test the boundaries of a system, enough test results to actually "prove" system capability would be very expensive. In a complex environment like the airport environment, this type of rigorous analysis is not always practical.

One way around collecting detailed data is to use decision science techniques and observations to make the best use of the data that is available. For the AVAP assessments, the Abacus Technology Team collected data and examined previous studies and assessments that have been conducted by the FAA and the aviation industry related to airport security, human factors engineering, and aviation research and development. The data was incorporated into the SAM quantitative models by using range estimate techniques and biasing the sensitivity of the results to critical data elements and their density functions. In this manner, it is possible to make decisions based on limited data and expert judgment. Shortly after beginning the analysis, the Abacus Technology Team found that only a limited testing and operational data set was available. Because of the limited data, the Abacus Technology Team felt that a more qualitative vulnerability and risk assessment approach to airport analysis would be more practical in the future. The cost of data collection would be prohibitive in performing any more than just one to three threat scenarios in a fully quantitative analysis, given the funding and resources allocated to the task.

3.3 @Risk

The science of probabilistic mathematics defines models of potentially random and non-deterministic events. The science of statistics defines the methods and practices of testing and determining the reliability of results that lead to the theoretical limit-values used in probability theory. For each threat scenario analysis in the AVAP, a decision sciences approach to defining risk was used and Monte Carlo simulations run using @Risk. Mean values and upper and lower bounds of vulnerability levels were calculated for each threat scenario vulnerable path using SAM. A rough order of magnitude figure representing impact in dollars was determined using expert knowledge (see Section 2.3.3). These values were input into @Risk which, using basic Monte Carlo methods, sampled repeatedly from built-in sampling distributions for each defined element and generated a composite estimate of risk for each threat scenario. The result of the Monte Carlo simulation was used to prioritize the recommendations for corrective action to be taken by the airports.

4. SUMMARY AND LESSONS LEARNED

The first practical test of the Risk Management Process proved it flexible enough to be applied in to the airport assessments conducted for the AVAP. The process flow and description enabled the Abacus Technology Team to analyze the airport security situations effectively. However, the use of detailed quantitative tools suggested by the White House Commission on Aviation Safety and Security is less pragmatic in the airport environment than in the more controlled operational environments for which the tools were designed. The following is a summary of the Abacus Technology Team's lessons learned through the application of the Risk Management Process and the selected tools, RiskWatch, SAM, and @Risk:

1. Performing a risk assessment is the only way to truly prioritize and recommend actions based on the results of the vulnerability analysis.

2. There was insufficient operational data to conduct a purely quantitative assessment.

3. The Abacus Technology Team augmented the limited quantitative data available with qualitative assessments of threat situations to determine quantitative inputs with uncertainty parameters. For consistent, repeatable analysis and to reduce uncertainty, the qualitative translations must be further explored and tested.

4. Quantitative models required significant mathematical characterization for each scenario. In order to conduct meaningful analysis in some cases, certain statistical data may be necessary for calculations, e.g., security screening.

5. While the Risk Management Process was found to be complete, certain key inputs such as the selection of tools and methodologies and the protection of definition and plans can dramatically effect the level of effort required to follow through and complete this process in a consistent and thorough manner.

6. The best approach to evaluating large and complex systems with many threat scenarios would be to establish and test the qualitative to quantitative input factors in the methodology. Then repeatability and accuracy could be maintained while conducting the data gathering and analysis steps as well as developing the mathematical models of scenarios.

The complex and dynamic nature of the airport security environment and the scarcity of operational data do not lend themselves easily to the repeated application of scenario-driven, quantitative vulnerability assessment tools like SAM and ASSESS[4]. These methods are useful for providing baseline data, but not for performing airport security assessments and what-if analyses on a regular basis. For repeatable analysis, the Abacus Technology Team believes that a qualitative risk assessment tool based on quantitative airport analysis baseline would provide the most efficient use of limited airport security resources.

[4] The tool developed by Sandia National Laboratory for nuclear power facilities and referred to in the Commission's final report.