A Risk-Based Optimization Framework For Security Systems Upgrades at Airports

by

Khaled M. Berbash

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Civil Engineering

Waterloo, Ontario, Canada, 2010

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners. I understand that my thesis may be made electronically available to the public.

ABSTRACT

Airports are fast-growing dynamic infrastructure assets. For example, the Canadian airport industry is growing by 5% annually and generates about $8 billion yearly. Since the 9/11 tragedy, airport security has been of paramount importance both in Canada and worldwide. Consequently, in 2002, in the wake of the attacks, the International Civil Aviation Organization (ICAO) put into force revised aviation security standards and recommended practices, and began a Universal Security Audit Program (USAP), in order to insure the worldwide safeguarding of civil aviation in general, and of airports in particular, against unlawful interference. To improve aviation security at both the national level and for individual airport, airport authorities in North America have initiated extensive programs to help quantify, detect, deter, and mitigate security risk. At the research level, a number of studies have examined scenarios involving threats to airports, the factors that contribute to airport vulnerability, and decision support systems for security management. However, more work is still required in the area of developing decision support tools that can assist airport officials in meeting the challenges associated with decision about upgrades; determining the status of their security systems and efficiently allocating financial resources to improve them to the level required.

To help airport authorities make cost-effective decisions about airport security upgrades, this research has developed a risk-based optimization framework. The framework assists airport officials in quantitatively assessing the status of threats to their airports, the vulnerability to their security systems, and the consequences of security breaches. A key element of this framework is a new quantitative security metric ; the aim of which is to assist airport authorities self-assess the

condition of their security systems, and to produce security risk indices that decision makers can use as prioritizing criteria and constraints when meeting decisions about security upgrades. These indices have been utilized to formulate an automated decision support system for upgrading security systems in airports.

Because they represent one of the most important security systems in an airport, the research focuses on passenger and cabin baggage screening systems. Based on an analysis of the related threats, vulnerabilities and consequences throughout the flow of passengers, cabin baggage, and checked-in luggage, the proposed framework incorporates an optimization model for determining the most cost-effective countermeasures that can minimize security risks. For this purpose, the framework first calculates the level of possible improvement in security using a new risk metric. Among the important features of the framework is the fact that it allows airport officials to perform multiple "what-if" scenarios, to consider the limitations of security upgrade budgets, and to incorporate airport-specific requirements. Based on the received positive feedback from two actual airports, the framework can be extended to include other facets of security in airports, and to form a comprehensive asset management system for upgrading security at both single and multiple airports.

From a broader perspective, this research contributes to the improvement of security in a major transportation sector that has an enormous impact on economic growth and on the welfare of regional, national and international societies.

Acknowledgements

First, I would like to thank my great God “Allah” for giving me the passion and the capacity necessary to successfully pursue, complete, and fulfill all the requirements for this thesis. As well, I would like to acknowledge the tremendous funding and support, and the privilege of pursuing my doctorate that was granted by the State of Libya. My studies have been enthusiastically administrated by the personnel in the Libyan Cultural Section in Ottawa so that I have been able to conduct this research peacefully at the University of Waterloo in Canada.

I would like to express my sincere thanks to all of my family members for the patience, encouragement, and support they have offered, which have inspired my endeavors to complete my Ph.D. program.

I offer my profound gratitude to my supervisors, Prof. Tarek Hegazy and Prof. Carl Haas, for the countless hours they have spent and the academic guidance they have provided throughout my research. Their innovative supervision and professional leadership were elements in the successful completion of this thesis. My thanks are also extended to my entire thesis defense committee: Prof. Michael McNerney, Prof. Ralf Haas, Prof. Keith Hipel, and Prof. Susan Tighe.

I would especially like to thank all the people from the Libyan Civil Aviation Authority for their outstanding assistance and for the information and data they have generously contributed this innovative research. In addition, special appreciation is due to the security officials at the Greater Toronto Airport Authority for their valuable contribution, feedback, and cooperation with respect to the validation of this research.

I am also very indebted to my colleagues in the construction research group in the Department of Civil and Environmental Engineering, the staff of the University of Waterloo, my friends, and all the other people who directly or indirectly provide help throughout my studies.

Finally, I would like to thank my wife for her heartfelt support, unbounded patience, and enormous encouragement throughout the last four and one-half years.

Waterloo, ON 2010

Dedication

To the soul of my great parents for all their unforgettable love, loyalty, and sacrifices that they have made to ease my life. To my wife and my sons, Mohamed, Adam, and Fayad, for the endless brightness, infinite emotion, and delightful passion they have added to my life and that kept me optimistic. To my brothers and sisters for the enormous spiritual support and encouragement they have provided. To my very dear home country, Libya, for the enormous assistance and opportunities I have been granted, which confidently paved my path throughout my Ph.D. studies.

Table of Contents

List of Figures

List of Tables

List of Equations

CHAPTER 1
INTRODUCTION

1.1 General

As pivotal links in the mass transportation infrastructure, airports have a substantial impact on regional and national economies. In Canada, it is estimated that the airport industry generates about CAN$8 billion annually and provides about 150,000 jobs (Gooch, 2007). In the USA, it is estimated that airports produce US$380 billion annually and provide 5.2 million jobs (Airports Council International-North America [ACI-NA], 1999).

Air transport is one of the busiest transportation modes, and it has experienced continuous and rapid growth over recent decades. Globally in 2006, the International Civil Aviation Organization (ICAO) reported that 2.1 billion passengers traveled though airports worldwide, and the international passenger traffic volumes rose 6.7% in 2006, while international domestic volumes rose 4.1%. Freight volumes also rose 3.0% and 5.4% for international and domestic cargo, respectively. Figures 1.1 and 1.2 show passenger and freight growth trends (ICAO, 2007).

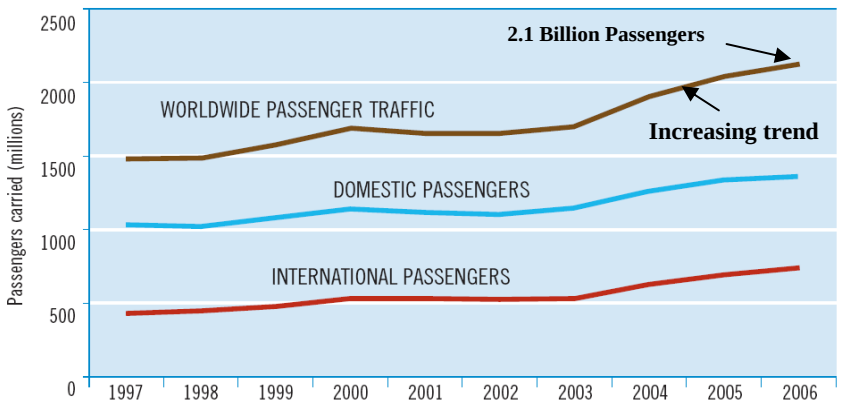


Figure 1.1: Passengers carried on Scheduled Air Services Worldwide, 1997-2006 (ICAO, 2007)

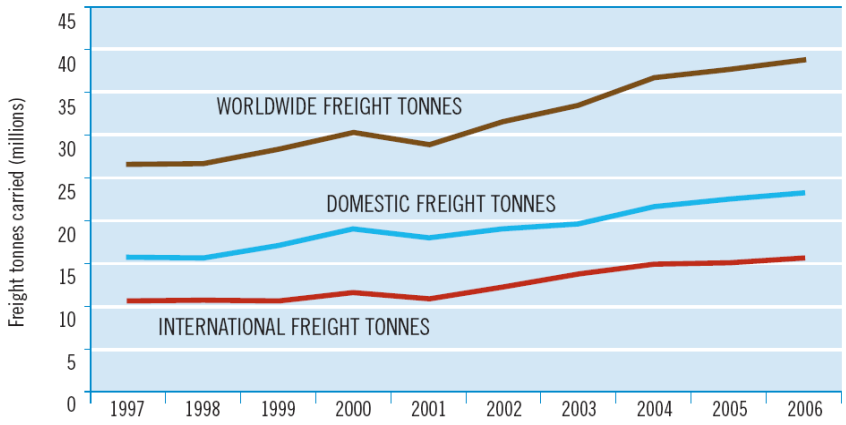


Figure 1.2: Tones of Freight Carried Worldwide, 1997-2006 (ICAO, 2007)

Similarly, the Airports Council International (ACI) predicted that "over the next 20 years, world passenger volumes will rise by 4.2 per cent annually…" and accordingly as illustrated in Figure 1.3, "Global passenger volumes will surpass the 5 billion mark by 2009 and reach 11 billion – or 30 million passengers per day –by 2027." (ACI, 2008)

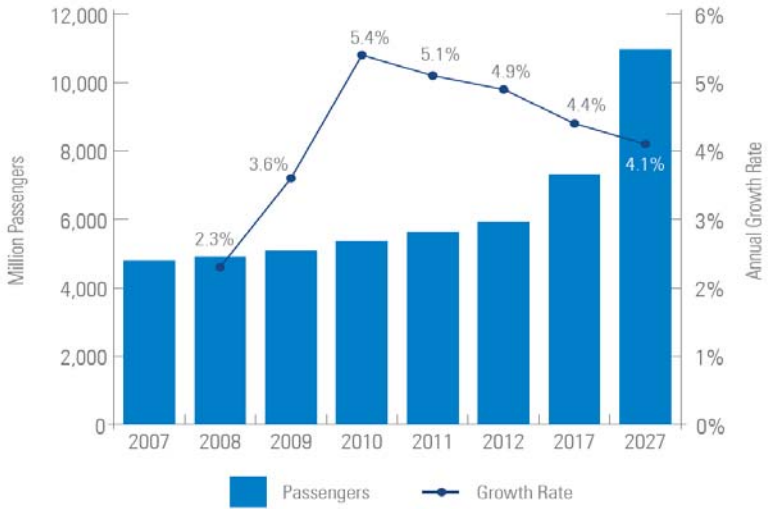


Figure 1.3: Global Passenger Traffic Forecast till 2027 (ACI, 2009)

At national levels the trend will continue, in North America in forecasts for future, in the United States alone, the Federal Aviation Administration (FAA) predicts that US airports will serve about 1.0 billion passengers annually by the year 2015 (Archibald, 2007).

While in Europe, in the UK for example, the Department for Transport (DfT) completed a comprehensive study, entitled "The Future of Air Transport," which predicted that the demand on UK airports in 2030 will range from 400 to 600 million passengers per year, as illustrated in Figure 1.4 (DfT, 2003).

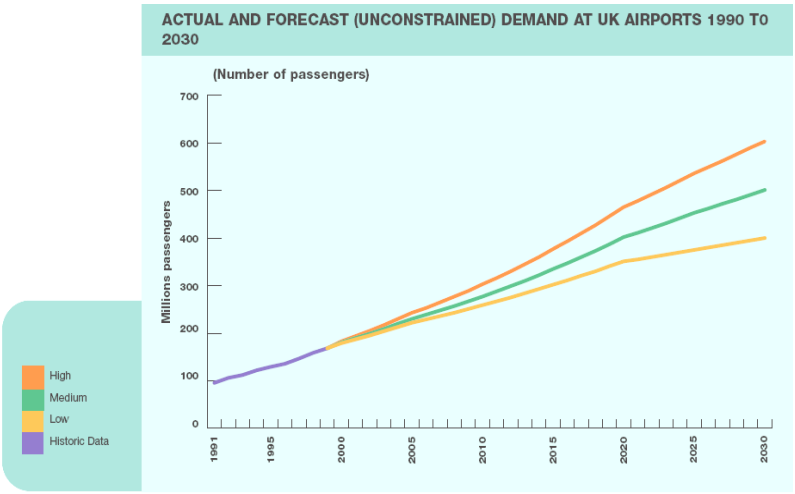
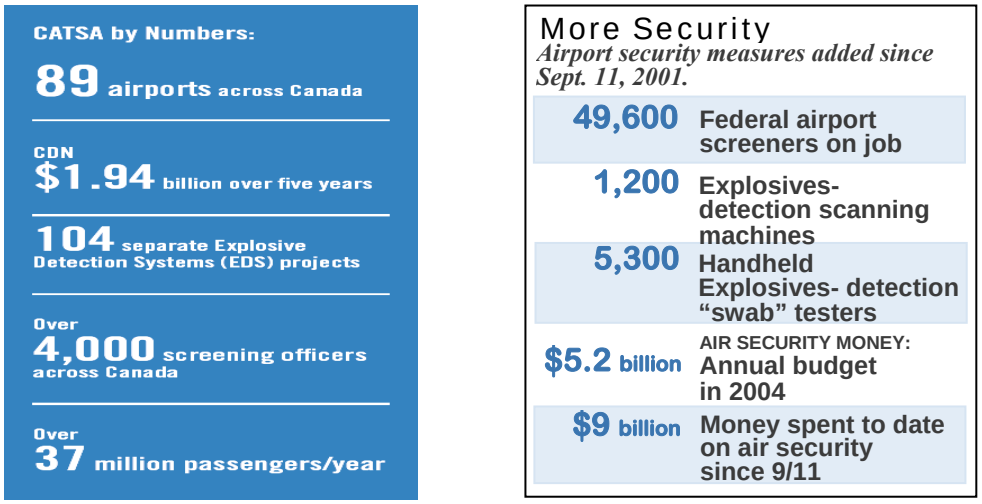


Figure 1.4: Future Forecasts of UK Airports (DfT, 2003)

Since the September 11 attacks, governments have spent billions of dollars to improve and maintain airport security systems. For example, in 2005, a total amount of $7.7 billion security initiative was declared by the Canadian government for security improvements. About $2 billion was allocated to the Canadian Air Transport Security Authority (CATSA) to deal with security issues at Canadian airports (McLaughlin, 2005). Similarly, in the USA alone, between 2000 and 2006, the federal government planned to fund US$60 billion in projects for airport development. A total of 15% of this amount was allocated for security projects at US airports (ACI-NA, 1999). The US Transportation Security Administration (TSA) also spent more than $5 billion over the same period to buy, maintain, and install explosives-detection systems (Darklord, 2008). In addition, The US Congress invested about $12 billion through the fiscal year of 2008 that was allocated through the Department of Homeland Security's Grant Program (Dillon et al., 2009).

Following the substantial increase in security screener jobs, as depicted in Figure 1.5 (a, b), and the use of the new system, called Computer Assisted Passenger Pre-screening System II (CAPPS II) in 2003 (Goo, 2003), the US Aviation Investment and Modernization Act of 2007 allocated US$1.5 billion to be spent over a three-year period in a newly established Aviation Security Capital Fund (Ash, 2007). Likewise, the Canadian Air Transport Security Authority (CATSA) spent about 2 billion dollars between 2001 and 2006 to enhance and develop security measures in the 89 publically accessed Canadian airports Figure 1.5 (b). The improvements included deploying 104 separate explosive-detection systems and hiring over 4000 screening officers for Canadian airports.



(a) Canada (CATSA, 2006) **(b) United States** (Goo, 2003)

Figure 1.5: Security Measures after 9/11

At the international level, the ICAO's Ministerial Conference adopted a comprehensive strategic plan to maintain aviation security worldwide. Then in September 2002, Annex 17, a revised version entitled "The Aviation Security," was published. The Annex 17 includes 74 security standards and recommended practices, which aim at standardizing and ensuring the preparedness of security systems at the national and airport levels (ICAO, 2002b).

Despite being one of the safest types of infrastructure, airports are extremely busy and considered to be among the most potentially vulnerable public assets; they are of paramount concern for governments around the world, especially after the events of September 11, 2001 (9/11) (Dillon et al., 2009; Enoma & Allen, 2007). As the Security Industry Association reported, "By the year 2016, the airlines will need to double their existing fleet size. In order to manage this staggering growth, improved security measures must be planned for today" (SIA, 2008). Thus, upgrading and enforcing security standards and procedures at airports have recently received enormous attention (Lippert and O'Connor, 2003), to ensure the preparedness and effectiveness of airport security systems (Francis et al., 2003).

1.2 Research Motivation

This research on upgrading security systems for airport networks has been motivated by the aspects explained in the following sections.

1.2.1 The Challenge of Assessing Airport Security

Prior to September 11th tragedy, aviation security did not rely on risk-based methodologies, and only introduced general measures to respond to airplane hijacking, bombing and accident events (Dillon et al., 2009 and Elias, 2008). Due to these events, governments worldwide and the aviation industry developed new security standards with more strict measures (Peterson et al., 2007). Internationally, the ICAO mandated that governments should issue guidelines and National Aviation Security Program (NAVSECP), in order to satisfy ICAO's Annex 17 security requirements. In the USA, The Department of Homeland Security (DHS) developed "a risk-based methodology to complement the overarching National Infrastructure Protection Plan (NIPP)." (Elias, 2008) One of the main objectives of the NIPP is "implementing a long-term risk management program." Likewise, in Canada and the European Community, in 2002, a Strategic

Aviation Security Plan and common civil aviation security rules were issued to be implemented by airport authorities (GSP, 2002) and (EP, 2002).

After the Sept. 11th attacks, the assessment of airport security risk assessment received growing interest to examine potential threats, vulnerabilities, and consequences. Although many airport authorities and researchers have initiated extensive programs and studies to help detect, deter, and mitigate airports' security risks, many still hinder objective assessment of airports risks (Dillon et al., 2009). In particular, further research is required to provide quantitative assessment guidelines for security upgrades.

1.2.2 Constraints on Security Funding

Providing and maintaining the necessary financial resources for airport security upgrades have become a crucial problem. Choosing the types of security upgrades and the allocation of resources over a planning horizon are also key challenges for decision makers, who are constantly pressured by budget constraints. Minimizing the costs of these upgrades, and maximizing the return on investment are the key objectives that are difficult to attain. To do this, effective tools are required to support airport officials' decisions. Other constraints include human factors, policies, technological developments, political considerations, and operational considerations (Antonni, 2002).

1.2.3 The Need for an Efficient Decision Support System

To help decision makers meet the requirements for security upgrades, within the budget limit and other operational constraints, a decision support framework is strongly needed to assist decision makers in various tasks, including: (1) conduct a comprehensive security risk assessment of potential threats, vulnerabilities, and consequences, (2) examine the effectiveness of different

risk mitigation alternatives and their costs, and (3) optimally select the most cost-effective upgrade strategy. The risk-based optimization framework needs to employ a new quantitative metric within an optimization-based decision support system.

1.3 Research Objectives and Scope

The goal of this research is to provide decision makers in the aviation industry with a practical framework that helps optimize decisions about security upgrades for airport terminals. The focus of the research is on the Passenger and Cabin Baggage Screening System. The detailed research objectives are as follows:

1. Investigate the various airport security systems and related national and international security regulations.
2. Investigate various security upgrade options for passengers, cabin baggage, and checked-in luggage along with their costs and effectiveness to detect threats.
3. Develop a new quantitative metric to assess the security risks of various systems through a detailed assessment process of threats, vulnerabilities, and consequences.
4. Develop a decision support system for airport security upgrades that utilizes cost-effective countermeasures to minimize security risks.
5. Experiment with optimization techniques to determine the optimum security upgrade decisions.
6. Develop a computerized prototype and validate the system performance and usefulness to airport officials.

The proposed framework is applicable to the airport terminal Passenger and Cabin Baggage Screening System (PCBSS), with special focus on PCBSS physical measures that mitigate

security risks. It is assumed that the non-physical measures, such as policy issues and human and training related factors, equipment maintainability, etc, are applied satisfactorily. Integrating these factors will be a future challenge, and some initial suggestion for how to approach this within the framework proposed here are made in the final chapter of the thesis. The proposed methodology is applicable to all airport security systems within the PCBSS. It is noted that the research focuses on passenger terminals in international airports, which require more comprehensive security systems than domestic airports. The developed framework provides airport security officials with a practical tool for maximizing the security investment return, minimizing security risk, documenting their decision process, and meeting their specific constraints and security standards at the subsystem, system, airport and multi-airport levels.

1.4 Research Methodology

The research methodology that was employed to achieve the above mentioned objectives is illustrated in Figure 1.6. The methodology tasks are as follows:

1. **Airport Security Systems Review**: Conduct a comprehensive survey to investigate up-to-date security systems requirements and related risk assessments. Through this survey:
    a- Security systems (modules) and their important in-depth security aspects at international airports were investigated.
    b- Risk-based assessment methodologies and the rationale of quantitative risk analysis in terms of threats, vulnerability, and consequence were reviewed.
    c- Options for upgrading decisions were evaluated and quantified so that an upgrading mechanism could be selected for building the proposed upgrading framework.

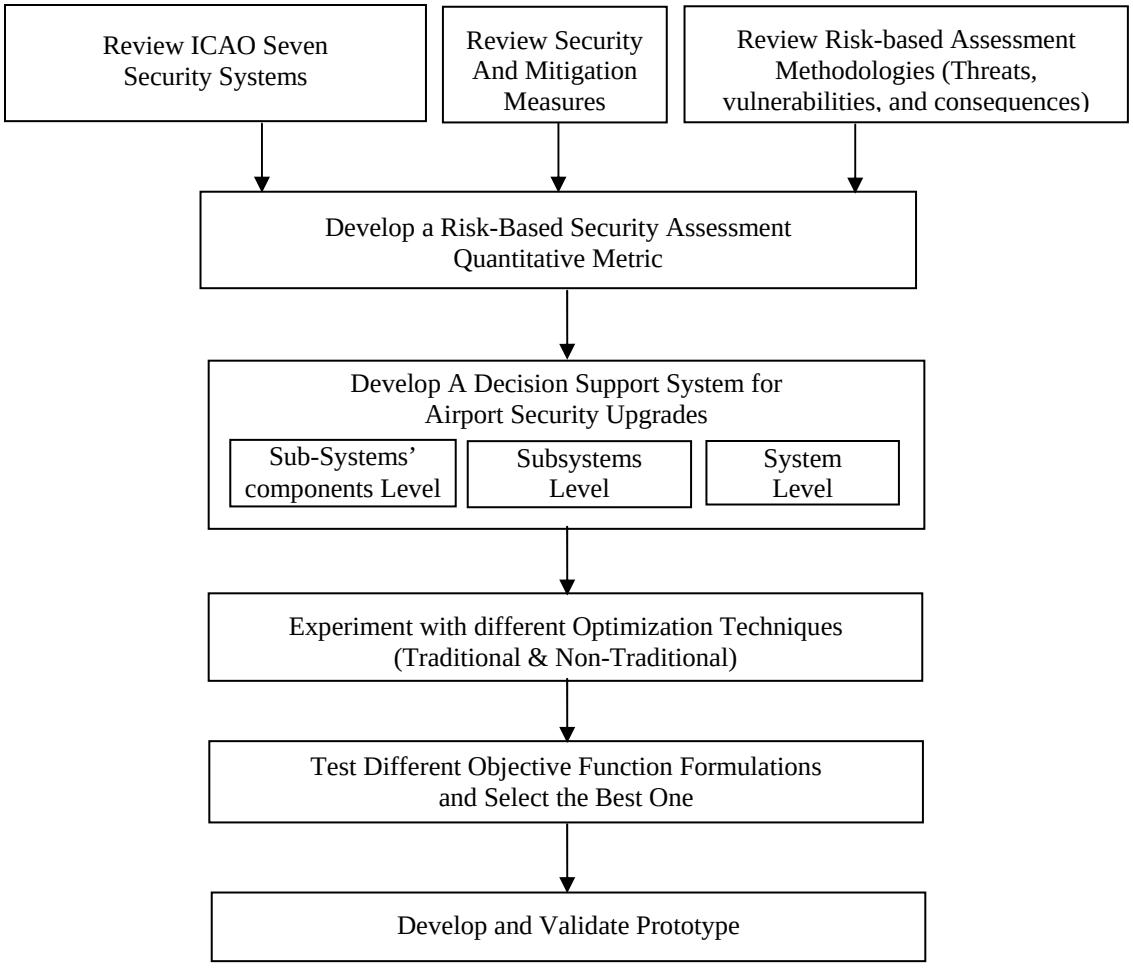


Figure 1.6: Research Methodology

2. **Development of a Security Risk-Based Quantitative Metric:** A new quantitative security risk metric is developed. The proposed development involves a quantitative metric to assess the effectiveness of airport security systems. The process for developing the proposed metric includes:

   a- Review ICAO's seven security systems (standards and measures), an international airport security program, and the current in place mitigation measures, if any, in order to create a list of security measures and their possible assessment schemes.

b- Investigate potential security risks dimensions in terms of airports' threats that the airport is subject to, existing vulnerabilities that could be exploited, and possible consequences that would result if an attack was a success.

c- Develop a security risk-based quantitative metric that incorporates the important security dimensions. The metric provides a hierarchal score as a Security Risk Index (SRI) at each security system components, system, and the overall airport levels. The SRI is used for building a decision support system for airport security upgrades.

3. **Development of a Decision Support System for Airport Security Upgrades**: The quantitative metric indices, upgrade decision options, and influencing constraints are incorporated to develop an optimization-based model. The developed model is tested for the Passenger and Cabin Baggage Screening System. Techniques such as, a simple ranking method, a mathematical optimization, and a non-traditional optimization technique are used to solve the optimization problem. Further enhancement involves testing different forms of objective functions. A computerized prototype has been built and tested to validate the potential functionality and practicality of the system.

4. **Prototype Development and Validation**: The developed framework has been validated through the following approaches:

   a- **Expert opinion**: The developed framework was presented during research meetings and interviews that were held with involved stakeholders, such as airport security officials, representatives of government security agencies, and airport authorities. The purpose of these meetings was to collect their professional feedback regarding application and operation efficiencies.

b- **Case Study**: A real-world case study at an international airport was conducted. The goal was to test the output of the developed system with respect to actual upgrading decisions and achieved security levels, and then to compare these results with the airport's accomplishments.

1.5 Summary

Airports are one class of a nation's vital transportation infrastructure and are key assets to a dynamic business environment. After the events of September 11th, security assessment research has focused on risk-based approaches. To help airport authorities with cost-effective decisions on airport security upgrades, this research proposes a risk-based optimization framework that focuses on the Passenger and Cabin Baggage Screening System, and proposes a risk-based optimization framework for airport security upgrades. The framework includes a quantitative security risk metric to assess the airports' threats, vulnerabilities, and consequences expressed in terms of Security Risk Indexes (SRIs). Based on those SRIs, the framework incorporates an optimization model to determine the cost-effective countermeasures that minimize security risks. Among the important features of the framework is that it calculates the level of security improvement using the new risk metric, allows airport officials to perform multiple "what if" scenarios, and considers security-upgrade budget limits and airport-specific requirements. Once the passenger and baggage screening system is tested, based on feedback from actual airports, it can be extended to include the other facets of security in airports, to form a comprehensive asset management system for airport-security upgrades. For both single- and multiple-level airports, the optimization model will have the potential to optimize and prioritize decisions about airport security upgrading projects so that they are both efficient and effective for the planning horizon.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

As a fundamental component of society's transportation infrastructure, airports are classified as one of the nation's vital transportation assets. Their importance arises from their role in rapidly transporting passengers, goods, and freight, and in providing services. This role universally facilitates trade and industrial international relations. Because they are dynamic business environments, they also affect local, national, and international development economic and influence global markets.

This chapter presents a detailed overview of civil infrastructure assets and their related management systems, along with examples of their advances, frameworks, tools, and techniques. Airport Performance Indicators were also addressed as a means to evaluate the level of service in airports. In addition this chapter documents an intensive review of development in aviation security, methodologies, simulation studies, and risk-based research on airport security and its management systems.

2.2 Civil Infrastructure Assets

Civil infrastructure assets are recognized as a key "fundamental foundation of societal and economic functions." (Mishalani and McCord, 2006) Generally, they can be grouped into seven function-related categories, as shown Figure 2.1: Recreational Facilities, Communication,

Buildings, Transportation, Waste Management, Water and Waste Water, and Energy Production and Distribution (Hudson et al., 1997). Each of these categories is divided into sub-categories. For example, the Transportation category includes Mass Transit, Intermodal Facilities, Air Transportation, Ground Transportation, and Waterways and Ports. Similarly, under each of these sub-categories there are a number of assets. Airports, which are the focus of this research, are one of the pivotal assets in air transportation infrastructure systems (Hudson et al., 1997).

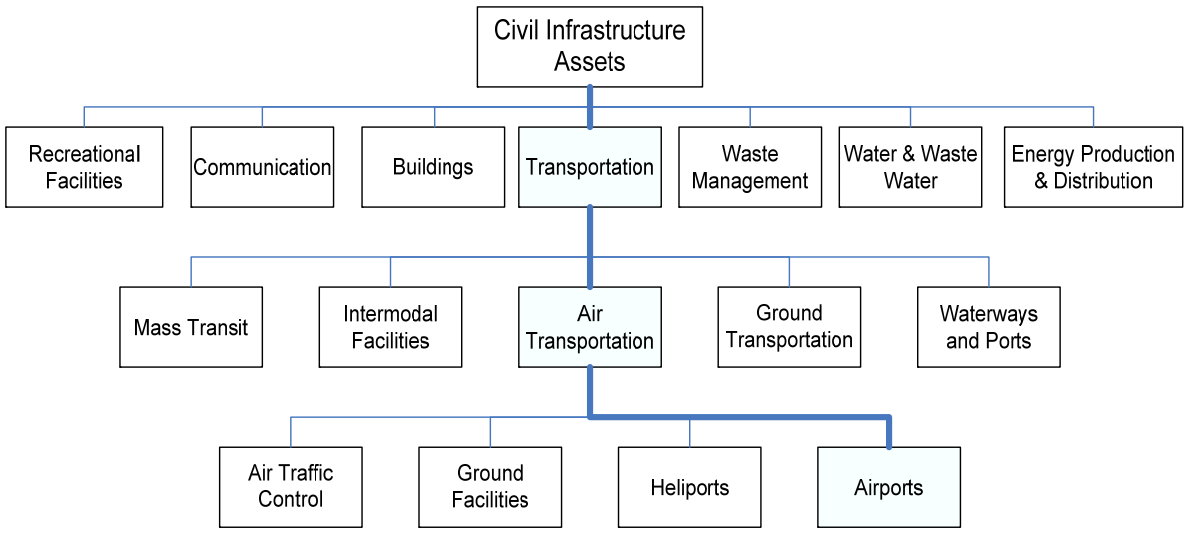
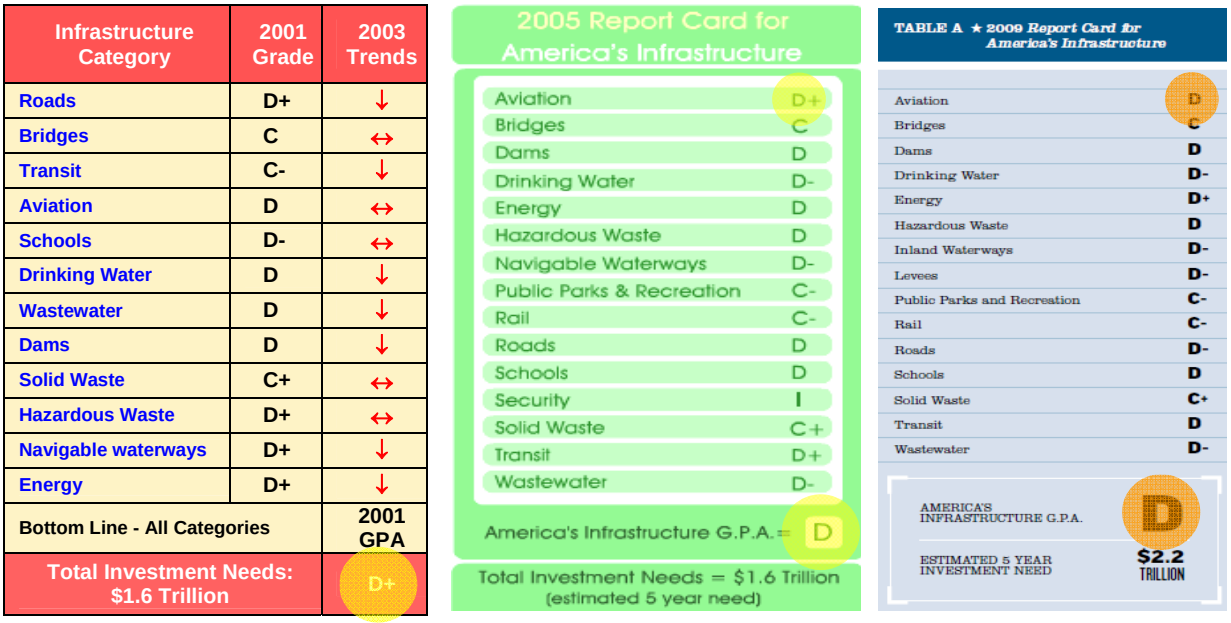


Figure 2.1: Civil Infrastructure Catégories (Based on Hudson et al., 1997)

All infrastructure assets in North America, and worldwide as well, are experiencing huge levels of deterioration, as shown in the American Society of Civil Engineers (ASCE) report cards of 2003, 2005 and 2009 (Figure 2.2). The 2003 report card shows a comparison with 2001. In 2005, aviation infrastructure was graded at a discouraging D+, as shown in Figure 2.2b. The ASCE report estimated total investment needs of $1.6 trillion to bring America's infrastructure to acceptable levels (ASCE, 2005). The discouraging continued to falls to D as shown in Figure 2.2c, as a result, the needed investments increased to $2.2 trillion (ASCE, 2009). Therefore, the condition of aviation infrastructure is not improving as a comparison of 2009, 2005 ASCE report

card with the 2003 demonstrates (Figure 2.2a) (ASCE, 2009). In 2005, ASCE graded the security of America's critical infrastructure at grade I and reported that "The information needed to accurately assess its status is not readily available to engineering professionals. This information is needed to better design, build and operate the nation's critical infrastructure in more secure ways. Security performance standards, measures and indices need to be developed and funding must be focused on all critical infrastructure sectors, beyond aviation" (ASCE, 2007).



Infrastructure Category	2001 Grade	2003 Trends
Roads	D+	↓
Bridges	C	↔
Transit	C-	↓
Aviation	D	↔
Schools	D-	↔
Drinking Water	D	↓
Wastewater	D	↓
Dams	D	↓
Solid Waste	C+	↔
Hazardous Waste	D+	↔
Navigable waterways	D+	↓
Energy	D+	↓
Bottom Line - All Categories		2001 GPA
Total Investment Needs: $1.6 Trillion		D+

(a) America's Infrastructure 2003 Progress Report (ASCE, 2003)

(b) ASCE Report Card on the America's Infrastructure (ASCE, 2005)

(c) America's Infrastructure 2009 Progress Report (ASCE, 2009)

Figure 2.2: ASCE Report Cards for Infrastructure

Airports are becoming even more demanding transportation infrastructure assets. The last three decades have witnessed very rapid growth and increased use of technological innovations. On the international level, the ICAO annual report of 2006 showed continued growth in air traffic of 4.1% worldwide (ICAO, 2007). At the national level, according to Transport Canada (TC, 2006), air traffic through Canadian airports continued to increase and hit a more than 5% growth rate for 2006. In a report published in December 2003 by the Department for Transport (DfT) of

the UK, the passenger traffic growth through UK airports is forecasted to reach 400 to 600 million by 2030, compared to 200 million in 2003 (DfT, 2003). It is obvious that the rapid increase in air transport demands will be a demonstrating trend in the aviation industry and will place high stress on the security systems at airports and their associated technologies.

The increase in air transportation demand will be accompanied by a rising number of regional and super-jumbo jets. These jets have to be accommodated with compatible infrastructure and security provisions (ASCE, 2005). In parallel with the expected expansion at airports, projected air traffic growth, and increased funding requirements, the security systems in airports must also increase. To meet these challenges, funding by national governments is critical. In the USA, for example, ASCE recommended that the "US Congress must reauthorize funding for the Airport and Airway Trust Fund and enact an increase in user fees as necessary for continued funding of the Airport Improvement Program." Consequently, the US Federal Government allocated $5 billion in 2006 for the Transportation Security Administration to spend on improving and upgrading security systems at the 450 commercial airports across the USA. On the other hand, ASCE, in its 2005 Report Card for America's Infrastructure, stated that "The National Plan of Integrated Airport Systems estimates that over the next five years (2005-2009) $39.5 billion will be needed to meet the infrastructure demands of all segments of civil aviation" (ASCE, 2005).

2.3 Infrastructure Management Systems

Decision makers need to keep infrastructure at an acceptable service level, consider their limited funds, prioritize their decisions, and satisfy planning time frames and other practical constraints at both single and multiple levels. In response to this need to consider all the multiple, complex

factors involved in decisions, infrastructure management systems have emerged (Flintsch and Chen, 2004).

2.3.1 Advances in Infrastructure Management Systems

Since the mid 1960's, significant research has been undertaken by industry and academic scholars with the goal of developing systems to evaluate, manage, and upgrade infrastructure assets. As stated in the 2000 report of the US General Accounting Office, well-managed infrastructure systems will positively increase the productivity and competence of economies at the national level (GAO, 2000). Managing these assets requires the integration of engineering principles with sound business applications and thorough economic knowledge. "A management system has been proposed as a solution for balancing growing demands, aging infrastructure, and constrained resources in the transportation sector." (Federal Highway Association [FHWA], 1999) An asset management process involves the use of planning and programming schemes as well as management systems. A generic asset management framework that was introduced and used by the US's FHWA is shown in Figure 2.3 (FHWA, 1999).

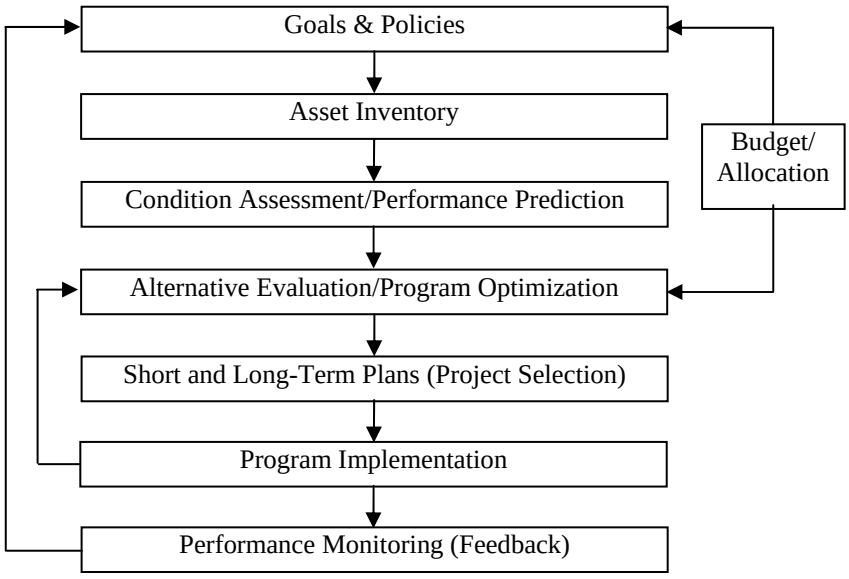


Figure 2.3: Generic Asset Management Framework (FHWA, 1999)

The system incorporates a broad database of asset inventory, condition assessment performance prediction modules, and rehabilitation possibilities. Several modules and decision support tools are integrated in order to analyze, compare, and select the most cost-effective solution. This framework, and many similar ones proposed in the literature, assures that these solutions will meet overall goals, efficient performance levels, and user expectations (Flintsch and Chen, 2004). In general, asset management systems can support decisions not only at the individual asset level (e.g., an airport) but also at the network, or multiple assets, level (e.g., a network of airports). These two levels of management are strongly merged and are influenced by external decision-making factors, constraints, and a shared data-base, as shown in Figure 2.4 (Hudson et al., 1997).

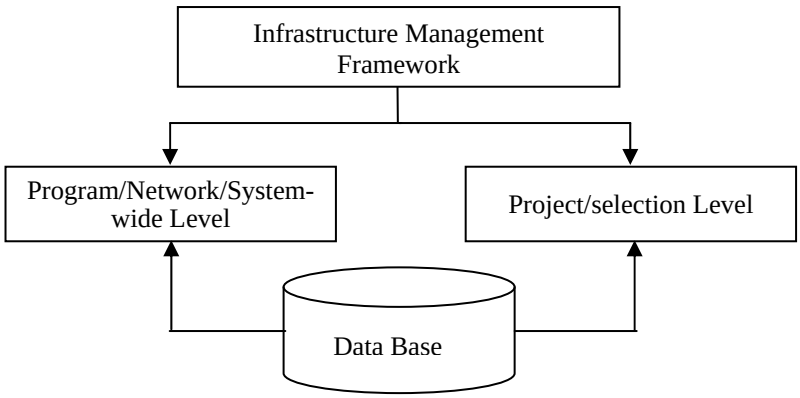


Figure 2.4: Infrastructure management framework in principle (Hudson et al., 1997)

Since airports are critical infrastructure assets, they will require expansions in facilities, services, and funding. These expansions will make it harder to maintain the security of the diverse components of airports: passenger terminals, cargo terminals, catering, aircraft maintenance, air traffic control and navigation aids, runways and taxiways, aprons, buildings, hotels, commercial and industrial concessions, etc. As a result, an overall framework for airport infrastructure management and security upgrades is a necessity.

Figure 2.5 illustrates applied tools and techniques that infrastructure decision support systems most often employ (Flintsch and Chen, 2004). As Figure 2.5 shows, management systems can be divided into two main branches. The first includes recent techniques to support decision systems, and the second includes applied decision support techniques. Each of these branches is further divided into main divisions. These divisions can again be subdivided into detailed levels. For example, decision support techniques include performance assessment, needs analysis, and tradeoff analysis, while tools and techniques include traditional approaches and soft computing techniques.

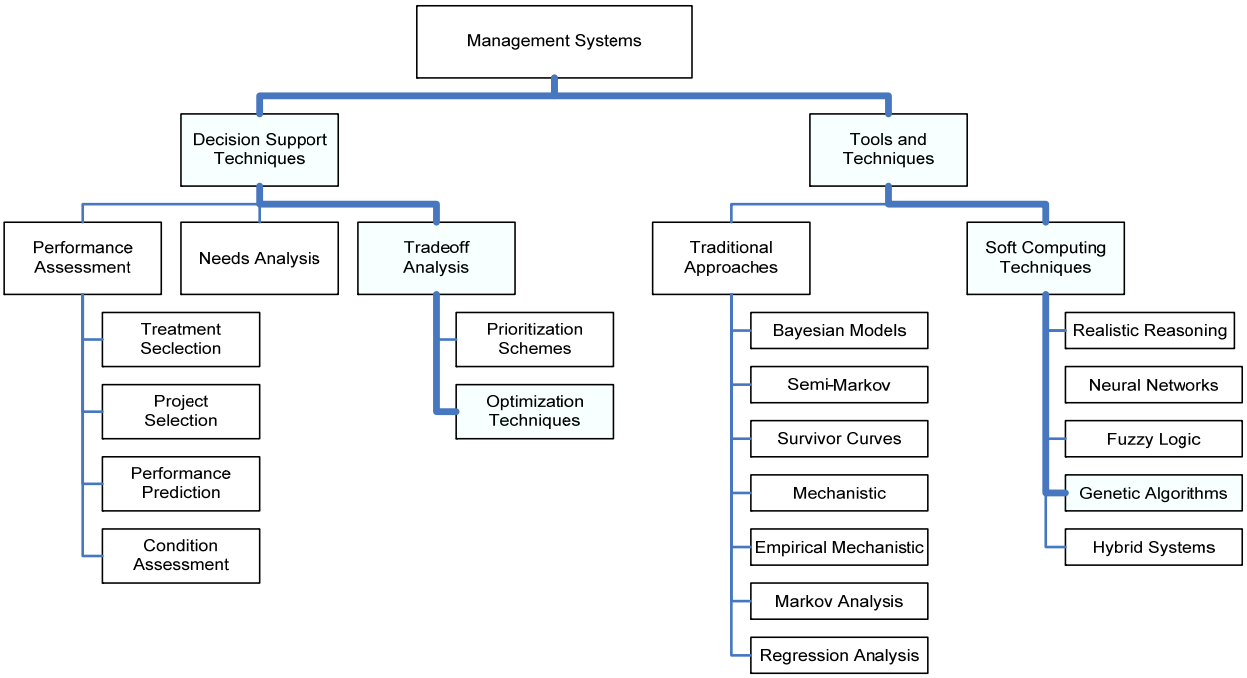


Figure 2.5: Infrastructure-related tools and techniques

Mishalani and McCord (2006) reported that much advancement has been carried out in "infrastructure condition assessment; deterioration modeling; and optimal maintenance, repair, and reconstruction." Recently, sophisticated tools such as soft computing have been introduced. Soft computing techniques are among the most promising tools because they have extremely promising capabilities of enhancing the current processes, procedures, and techniques of

infrastructure management (Mishalani and McCord, 2006). Flintsch and Chen (2004) summarized in a comprehensive review various soft computing techniques, their applications, and a listing of the scholars who utilized them in different types of infrastructure (Table 2.1). In this table, it is clear that a significant number of scholars have utilized these evolutionary techniques in main areas of application, such as asset performance, needs analysis prioritization schemes, and optimization techniques. It is also obvious from the table that Artificial Neural Networks (ANN), Fuzzy Logic Systems, and other Hybrid Systems were widely used in condition assessment tasks, whereas genetic algorithms (GAs) are reported as the most employed optimization technique.

Table 2.1: Summary of Soft Computing Applications in Infrastructure Management
(Based on Flintsch and Chen, 2003)

Soft computing Technique	Asset performance		Needs analysis		Prioritization Schemes	Optimization Techniques	Scholar Reference
	Condition Assessment	Performance Prediction	Project Selection	Treatment Selection			
Artificial neural networks	11	8	1	2	1	1	Pant et al. (1993), Kaseko and Ritchie (1993), Hajek and Hurdal (1993), Fwa and Chan (1993), Eldin and Senouci (1995), Flintsch et al. (1996), Razaqpur et al. (1996), Cattan and Mohammadi (1997), Huang and Moore (1997), Alsugair and Al-Qudrah (1998), La Torre et al. (1998), Owusu-Ababia (1998), Shekharan (1998), Wang et al. (1998), Van der Gryp et al. (1998), Martinelli and Shoukry (2000), Lou et al. (2001), Farias et al. (2003), Felker et al. (2003), Fontul et al. (2003), Lee and Lee (2004), Lin et al. (2003), Sadek et al. (2003), Yang et al. (2003)
Fuzzy logic systems	7	1	1	1	1	2	Elton and Juang (1988), Zhang et al. (1993), Grivas and Shen (1995), Prechaverakul and Hadipriono (1995), Shoukry et al. (1997), Wang and Liu (1997), Fwa and Shanmugam (1998), Cheng et al. (1999), Saitoh and Fukuda (2000), Bandara and Gunaratne (2001)
Genetic algorithms		2			1	6	Fwa et al. (1996), Liu et al. (1997), Pilson et al. (1999), Shekharan (2000), Miyamoto et al. (2000), Chan et al. (2001), Hedfi and Stephanos (2001), Ferreira et al. (2002)
Other hybrid systems	6	1		2			Ritchie et al. (1991), Chou et al. (1995), Taha and Hanna (1995), Martinelli et al. (1995), Abdelrahim and George (2000), Chiang et al. (2000), Chae and Abraham (2001), Liang et al. (2001), Flintsch (2002)

Numbers represent scholars who used the specific technique

2.3.2 Examples of infrastructure management systems

Pavement management systems (PMS) and bridge management systems (BMS) were among the earliest developed infrastructure management systems. They have emerged as a result of the infrastructure agencies' focus on finding a balanced approach to infrastructure management (Flintsch and Chen, 2004). Other infrastructure management systems have been developed to suit the needs, criticality, function, and nature of other asset systems. Some of the applied infrastructure management systems are highlighted in the following sections.

MicroPAVER Pavement Management System: MicroPAVER is a state-of-art technology for pavement management that was initially developed in the late 1970s for the management, maintenance, and rehabilitation (M&R) of the enormous pavement inventory of the US Department of Defense (DOD) (MicroPaver, 2007). As described by the US Army Corp of Engineers, "MicroPAVER uses inspection data and a pavement condition index (PCI™) rating from zero (failed) to 100 (excellent) for consistently describing a pavement's condition and for predicting its M&R needs many years into the future." In general, in addition to the calculation of a pavement condition index, a Pavement Management System (PMS) includes a rehabilitation analysis that helps optimize budget-constrained decisions for the rehabilitation program, and predicts the effect on the condition of the network. Decision makers can use any PMS to optimally allocate their funds, in order to achieve the objectives of their M&R programs (Corazzola and Poli, 2003). In 1993, the American Society for Testing and Materials (ASTM) adopted the PCI™ for airports as an ASTM standard (MicroPaver, 2007).

MicroBUILDER: MicroBUILDER is known as an engineered management system (EMS) for buildings. It was developed by the US Army Corp of Engineers as multitalented software for

optimally managing M&R plans and their building projects at different facilities. The software merges benefits of the engineering technologies, asset management systems, condition assessment and modeling techniques, and analysis methodologies (Karim, 2003). The main feature of MicroBUILDER is that it uses a subcomponent condition index (CI), which is a numerical index between 0 (failed) and 100 (excellent). The Construction Engineering Research Laboratory (CERL) indicates that the CI has been incorporated into inspection procedures and data base analyses supporting M&R planning for civil works facilities. An advantage of CI is that it can be used in conjunction with cost curves to determine condition deterioration curves, which will then predict cost-effective multiyear repair budgets at various CI scores over the M&R planning horizon in accordance with each facility's circumstances. The MicroBUILDER has the potential to be integrated with other seismic risk assessment systems, engineered management systems, GIS, etc. (CERL, 2007).

MircoROOFER: This software is similar in function and features to MicroPAVER and MicroBUILDER. It was developed to help building engineers assess the condition of built-up or single-ply roofing systems for the purposes of minimizing expenditures on M&R work orders for roofs based on condition index (CI) procedures for assessing the overall roof CI, while increasing the level of roof stock safety and serviceability (Morcous and Rivard, 2003). The MicroROOFER program use a process compiled from three components: the establishment of a network inventory database, condition inspection using an objective and repeatable rating system, and network-level and project-level management to select the optimum M&R strategy (Karim, 2003).

Other Management Systems: CarteGraph Systems Inc., a software developer for management systems, offers a number of asset management packages, including BRIDGEview, SIGNview,

SIGNALview, and PAVERMTview. The main purpose of all these packages is to help the managers of facilities efficiently and cost-effectively manage, maintain, and repair their assets.

2.3.3 Airport Management Systems

A number of management systems have been developed for airports, and computer-based versions are enormously in use, especially in Canadian, US, and Caribbean airports. For example, among infrastructure management systems that Lester B. Pearson International Airport uses are Airport Maintenance Management System (AMMS), Restoration Program, and Greater Toronto Airport Authority (GTAA) High Performance Building Policy (Karim, 2003). The features and capabilities of these systems are explained in following sections.

Airport Maintenance Management System (AMMS): The purpose of AMMS, as with other infrastructure management systems, is to plan, organize, direct, and control maintenance projects, allocate funds, and optimize maintenance strategies. Among the main capabilities of this system are maintenance task life-cycle analysis; workload and resources balancing and budget development during the planning period for current and upcoming fiscal years; and resource and cost tracking for active work orders by the month, quarter, etc. The system can operate in automated mode, or users with different access level can provide a Master Work Order with related health and safety checklists (Karim, 2003).

Restoration Program: Restoration is a management program that enables decision makers to sustain targeted levels of service for their facilities through the program's ability to systematically manage predefined replacement activities (LBPIA, 1985). Based on the facility's

funding rate, the program can predict the most appropriate replacement timing and associated funds. The program is designed to help officials make decisions at the macro level, such as long-term planning for 10-20 years, or at the micro level, such as short-term planning for 1-4 years (Karim, 2003).

GTAA High Performance Building Policy: This policy deals with the capital and operational costs encountered over a facility's physical and fiscal lifecycles and with the related benefits of high-performance buildings. Based on the four levels of performance as determined by Leadership in Energy and Environmental Design (LEED), which is a Green Building Rating System developed by the U.S. Green Building Council (USGBC) in 1994, GTAA was advised to adopt the silver level, which allows optimum returns with respect to tradeoffs of the funds employed. LEED certification is issued based on a set of required "Prerequisites" and a variety of "Credits," which will determine the level at which the candidate building is qualified. The four levels of certification are listed in Table 2.2 (USGBC, 2007; Karim, 2003).

Table 2.2: LEED Levels of Performance (LEED)

Level	Premium Percentage	Non-Innovation Points
Certified	$0 %, no premium	40-50%
Silver	$0-4% capital cost premium	50-60%
Gold	5%-15% capital cost premium	60-80%
Platinum	15%-25% capital cost premium	over 80%

Based on the Hudson et al. (1997) definition of unitized facilities, an airport is a good example of such facilities, making use of the following infrastructure management systems: MicroPAVER MicroBUILDER, Airport Maintenance Management System (AMMS), Restoration Program, GTAA High Performance Building Policy, and other systems. These systems are used by some

airport authorities either separately or integrated to some extent within the airport's environment. Managing different airport facilities and utilizing these systems effectively and efficiently are the core challenges that face airport authorities around the world. One of the critical systems that airport authorities must make every effort to manage well is security because security measures in each facility must be sufficient to protect the aviation industry in general, and airports specifically, from actions of unlawful interference, and to mitigate threat levels in order to realize reliable aviation security and a safe industry environment at the international and national levels (ICAO, 2002b).

2.4 Airport Performance Indicators

Another research direction with respect to airport security is to develop indicators and indexes to evaluate and measure performance. Through interviews and research workshops and from other sources such as the internet and the media, Enoma and Allen (2007) investigated performance measures for UK airports safety and security issues and developed a list of five potential key performance indicators: breach of security, evacuation in the case of emergency (fire, bomb threat, and acts of terrorism), hysteria control, attack on airport facilities or installations, and destructive or criminal behavior by a passenger on board an aircraft.

Developing performance indicators has been a major topic in different areas. Tangen (2003) presented a review of the currently used performance measures in the manufacturing sector, and discussed the five common types of performance objectives: cost, flexibility, speed, dependability, and quality. These objectives were proposed by Slack et al. (2001) as important

indicators to consider in performance evaluation. Examples of financial and non-financial indicators are listed in Table 2.3.

Table 2.3: Examples of Current Used Performance Measures (Based on Tangen, 2003)

Measure Type	Measure Form	Drawbacks	Reference
Financial measures	- Profit margins - Return on assets - Return on equity	- Lack of relevance to the control of production. - Pressure to maximize short-term result. - Quantify performance in financial terms. - Weak in reflecting department's unique characteristics and priorities. - Not applicable to the new management techniques. - Don not penalize overproduction and do not adequately identify the cost of quality.	Ross et al., 1993; Zairi, 1994 ; Maskell, 1991 ; Crawford and Cox, 1990; Ghalayini et al.,1997; Maskell, 1991; Ghalayini et al., 1997; Bitichi, 1994
Activity-based costing	- Cost-drivers	- Not proven to provide accurate product costs. - Can not gauge adequately manufacturing performance relative to a competitive strategy.	Kaplan and Cooper, 1998; Hill, 1995; Neely et al., 1997; White, 1996; Maskell, 1991
Traditional productivity measures	- Partial productivity measures	- Can be useful if the workforce is a dominating production factor. - Considers only one production factor.	Sumanth, 1994; Suh, 1990; Bernolak, 1997; Grossman, 1993; Sumanth, 1994
	- Total productivity measures	- Difficult to understand and to measure. - Not always accurate because of difficulties in calculating such measures in practice,.	
Time-based productivity measures	- Ratio between value-adding time and total time	- Can not be classified as a real productivity measure, since total time does not provide information about the consumed resources in the production process.	Arnold, 1991; Jackson and Petersson, 1999; Flapper et al., 1996
Non-cost performance measures	- Source of data ± internal or external - Type of data ± subjective or objective - Reference ± benchmark or self-referenced - Orientation to process ± input to some process or outcome of some process	- Most do not offer much help in developing insight into the relationships between performance objectives.	White, 1996
Intrinsic dimensions	- Decision type ± strategic/tactical/ operational - Aggregation level ± overall/partial - Measurement unit ± monetary/physical/ dimensionless		Flapper et al., 1996

In describing the current situation of airport performance research, Benoit (2006) states that "performance measurement in air transport security is hampered by the fact that comparative and empirical data on specific performance measures, benchmarks and targets being used in other jurisdictions is largely unpublicized and unavailable." In addition, "few formal industry standards [have] yet [been] developed against which nations can gauge their proficiency in areas such as screener attrition, infiltration testing and training levels."

Pitt et al. (2002) claimed that operational efficiency of any facility is highly weakened by incompatible selected type technology. As the contemporary generations of airport and aviation industries are relying primarily on the new emerging technologies to operate efficiently and manage their infrastructure assets and facilities effectively, the task becomes more challenging to achieve prescribed objectives in terms of performance, quality, and security as illustrated in Figure 2.6. As a result, the facility design and configuration are the key factor achieving these objectives. For example, poor design and inadequate configuration with respect to deploying baggage screening machines and passenger conveying system to enhance security measures will produce long waiting queues, and consequently will result in delays and low performance rates (Pitt et al., 2002). Accordingly, the continuous delays will generate crowds and possible violent passenger activities and may lead to more security breaches. Table 2.4 summarizes more examples on aviation and airport performance indicators.

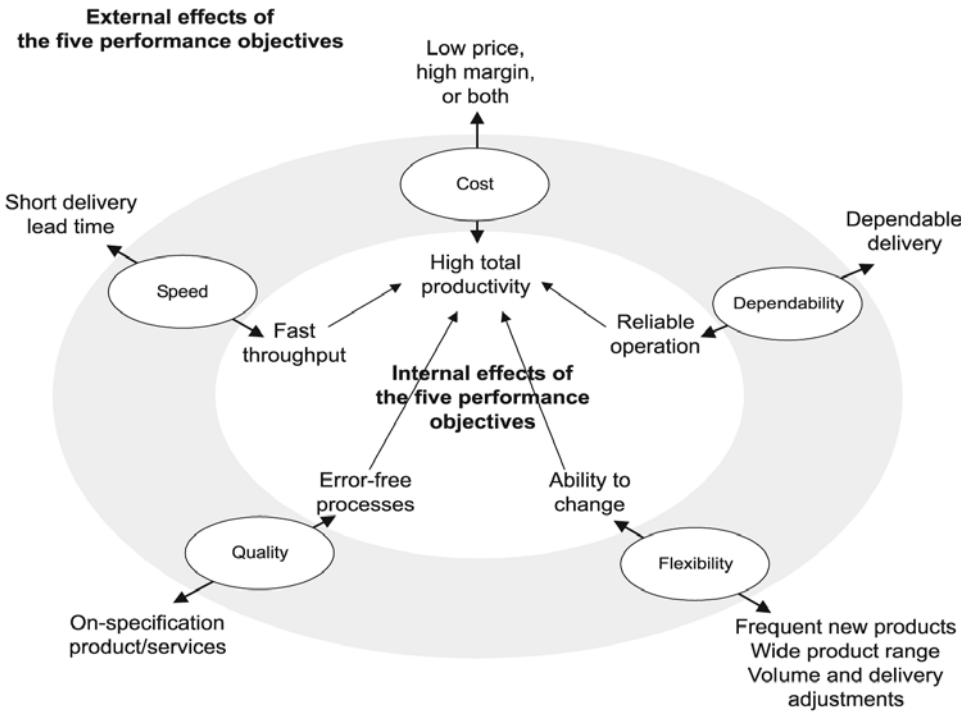


Figure 2.6: Desirable Performance Objectives (Pitt et al., 2002)

Table 2.4: Examples of Airport Performance Indicators Research

	Title	Author	Type	Objective	Methodology / Work Program	Output / Product	Comments
Performance indicators and measures	Developing key performance indicators for airport safety and security	Enoma, A. and Allen, S. (2007)	Case-study approach (empirical investigations)	Develops and tests a set of key performance indicators for airport facility management, with particular focus on safety and security.	Literature review; interviews of key airport personnel; workshops and observations; questionnaires; internet; and other media.	A potential list of key performance indicators for airport safety and security.	The paper addresses a good approach for measuring relative performance of airport safety and security and the role of facility management in achieving that level of performance.
	A Study of Performance Measurement in Canadian Air Transport Security	Benoit, L. E. (2006)	Case-study approach (empirical investigations)	Researches, discusses and analyzes the existing performance measurement criteria currently in use by the Canadian Air Transport Security Authority.	Interviews and telephone conversations with persons responsible for various aspects of performance measurement within both CATSA and TC.	A findings report that suggested analysis of the issue of performance measures and the identification of gaps and/ or recommendations.	Much of the critical information with regard to key performance targets, the frequency of evaluation, and the qualitative target levels, is classified "Secret."
	Safety performance evaluation models: a review	Adebiyi, K. A., Charles-Owaba, O.E. and Waheed, M.A. (2007)	Literature review	Considers different approaches and modeling of safety performance evaluation.	Review and synthesis of literature.	Ten major safety performance evaluation approaches are identified; based on the approaches, quantitative and qualitative models have been proposed.	Several research questions remain to be answered related to the impact of these provisional safety performance measures. Frequency co-efficient, severity co-efficient, and safety program performance models have potential applications in the security field.
	Aviation Security: Efforts to Measure Effectiveness and Address Challenges	Berrick, C. (2003)	Governmental report	Describes the TSA's efforts to measure the effectiveness of its aviation security initiatives and addresses key challenges to further enhance US aviation security.	Empirical investigations.	A list of opportunities to help ensure useful annual plans and applied practices for the effectiveness of the aviation security system.	Encouraging efforts to develop the information and tools needed to measure the effectiveness of aviation security performance are of greatest need.

2.5 Development of Aviation Security

Since the 1960s, aviation safety and security have developed rapidly (TRB, 2007) and have caught the attention of governments around the world (Enoma and Allen, 2007). Hijackings of airplanes and bomb threats caused major distress for airport authorities in the 1970s and 1980s (SIA, 2008; NAS, 1996). On December 21, 1988, a famous incident shook the aviation industry. Pan American's airplane was blown up over the town of Lockerbie in Scotland. Such incidents motivated the International Civil Aviation Organization (ICAO) to play a significant role in promoting and implementing new security standards and recommended practices. These standards are vital because airport authorities continually confront very demanding, active changing industry and market circumstances (Fry et al., 2005). Lately, the events of 9/11 put airport security systems, standards, and current procedures at the center of attention (Frederickson and LaPorte, 2002) Vulnerability of airports was emphasized further following the July 7, 2005, London bomb attacks (Enoma and Allen, 2007).

ICAO is one of the United Nations' specialized agencies. ICAO's main mission is to support and encourage cooperation between its 190 member states. According to the 1944 Chicago convention that created the ICAO, ICAO is "responsible for establishing international standards and recommended practices and procedures, covering the technical, economic and legal fields of international civil aviation operations, and is ultimately responsible for promoting the safety, regularity and efficiency of international civil aviation" (ICAO, 1944). Over the years, the Chicago convention has been enhanced by the appending of 18 different Annexes that govern civil aviation activities, technical requirements and regulations, standards, and recommended practices for achieving the safety and security of global civil aviation. Following repeated

incidents of high-jacking and the blowing up of airplanes, the ICAO in collaboration with its member states introduced the following international conventions:

1. Convention on "Offences and Certain Other Acts Committed on Board Aircraft," Tokyo, September 14, 1963
2. Convention on "The Suppression of Unlawful Seizure of Aircraft," The Hague, Netherlands, December 16, 1970
3. Convention on "The Suppression of Unlawful Acts Against the Safety of Civil Aviation," Montréal, September 23, 1971
4. "Montréal Protocol on the Suppression of Unlawful Acts Against the Safety of Civil Aviation," Montréal, February 24, 1971
5. Convention on "Detection of Plastic Explosives," Montréal, March 1, 1991

To put these conventions into force, the ICAO published Annex 17; entitled "Aviation Security," in order to standardize aviation security measures, procedures, and practices worldwide. The first version of Annex 17 was issued in 1974 (Drury, 1998). To date, eleven amendments have been added to Annex 17. It defines civil aviation security as "a combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference." Currently, Annex 17 contains 74 individual standards that state minimum mandatory security requirements and 19 recommended practices to help achieve that goal (ICAO, 2002d).

2.5.1 Universal Security Audit Program (USAP)

In the aftermath of the tragic attacks on September 11, 2001, the ICAO general assembly adopted resolution A33-1 that calls for the establishment of a universal program to audit aviation security arrangements and practices in all international airports worldwide. The resolution

recommended the ICAO Secretary General reviews and consults the audit program that was being used by the European Civil Aviation Committee. As a result, to help implement the new security standards, the Universal Security Audit Program (USAP) emerged as a comprehensive process for auditing aviation security. USAP was approved by ICAO's Council in June 2002. In November 2002, mandatory security audits were launched. The program helps enhance security by identifying deficiencies in member states' security systems, at national and airport levels (Table 2.5), by urging action for resolving any such deficiencies. The program is also intended to promote greater understanding of systemic security issues and build confidence in aviation security around the world (ICAO, 2002d).

Table 2.5: USAP's Security System Categories at the Airport Level (ICAO, 2002a)

Level		Module	Security System Category
ICAO Security Systems	National Level	I	Organization and Administration
		II	Co-operations with other States
	Airport Level	III	Organization and Administration
		IV	Access Control
		V	Passenger and Baggage Screening
		VI	Hold Baggage Security
		VII	In-Flight Security
		VIII	Cargo and Catering
		IX	Responses to Unlawful Interference and Contingency Arrangements

The tragic events of 9/11 resulted in the expedition of the adoption of USAP as a way to promote global aviation security through periodic auditing of the airports of the member states in order to determine their status with respect to implementing ICAO's Annex 17 Standards (Zuzak, 2003). USAP's audits are conducted at both the national and airport levels in order to evaluate both a state's aviation security capabilities and the actual security measures in place (ICAO, 2002d). Since its launch in June 2002, USAP has proven to be the basis of a strengthening of civil aviation security systems at the global, national, and airport levels (Zuzak, 2003). Therefore, for

the purpose of developing the proposed research framework, USAP's seven security modules at the airport level (Table 2.5) are adopted as the main components of the proposed framework for analysis and development.

2.5.2 Security Systems in Airports

The security devices in an airport are deployed in various configurations based on the security dimensions; the requirements of stakeholders; and other factors, such as operation and maintenance costs, passenger flow, operational space, and other architectural requirements. For example, Rao and Keith (1999) stated that advanced technology explosive-detection systems (ATs) can be set up in different patterns in passenger terminals, such as the lobby, the lobby/curbside area, and the bag room. Recently, ICAO recommended that each member state establish a national-level government agency to enforce Annex 17 standards (Zuzak, 2004). According to Annex 17, USAP classifies the airport security systems into nine categories. The first two relate to "National Level" security arrangements, while the remaining seven deal with security concerns at the "Airport Level" (Table 2.5) (ICAO, 2002a). Each category includes a number of modules, which should be audited and evaluated by the USAP audit team according to the status and complexity of each airport. For the purposes of this research, the focus is the seven systems at the airport level along with their subsystems.

For each of the seven security systems (modules), USAP identifies a number of ICAO standards to be audited. Figure 2.7 is an illustration of a typical audit cycle, which takes about nine months. The audit process challenges airport authorities to align their processes to be compatible with ICAO standards. As shown in Figure 2.7, audit visit takes about 16 days, with the final audit report sent two months later. The audit report is a detailed text-based document that contains the

auditors' observations, comments, and recommendations about every security system in the airport visited.

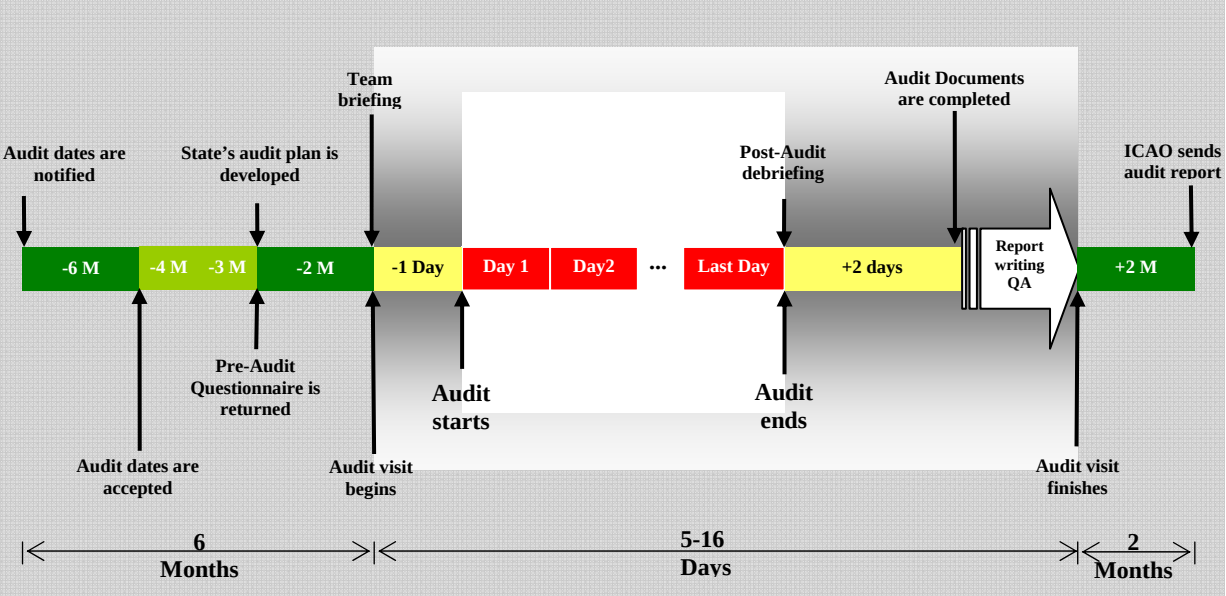


Figure 2.7: Typical ICAO Audit Cycle (based on ICAO, 2002d)

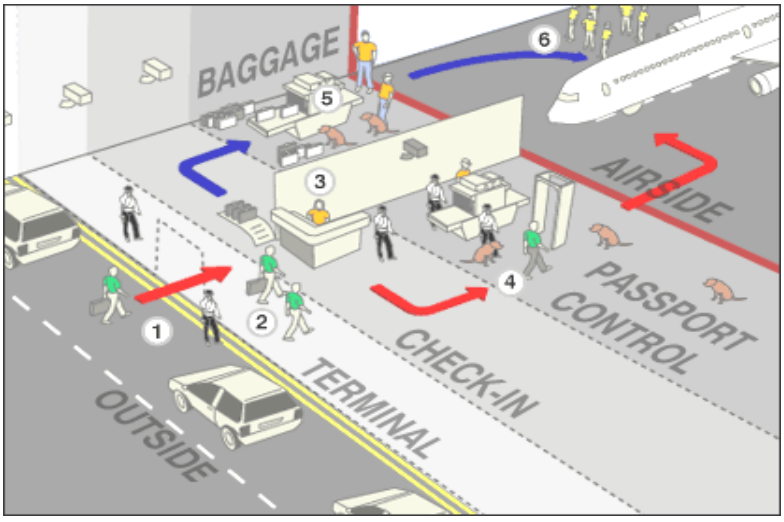
After the site visit, the ICAO's audit team analyzes and assesses the airport's current condition against the Annex 17 standards. The USAP report summarizes all defects and qualitatively evaluates the components of an airport's security system by assigning them to one of the categories shown in Table 2.6.

Table 2.6: USAP's Report Evaluation Sets (ICAO, 2002d)

Metric	Explanation
Set1	Meets the Annex 17 standard. Recommendations may be made to further enhance measures or to address any problems linked to the quality of implementation.
Set2	Does not meet the Annex 17 standard. A category 2 item represents a minor need for improvement for compliance to be achieved. In this case, improvement is necessary to ensure proper implementation of this Annex 17 standard and action should be taken by the contracting state.
Set3	Does not meet the Annex 17 standard. A category 3 item represents a serious need for improvement for compliance to be achieved. In this case, improvement is essential to correct the deficiencies and to comply with Annex 17. The Contracting State should give high priority to corrective action.
Not confirmed	
Not Applicable	

2.5.3 Security measures at airports

Airports have been targeted by terrorists worldwide during the last four decades (Zuzak, 1990), and similarly, the aviation industry as a whole has become a fertile environment for different types and levels of threats (Lazarick, 2001). To mitigate the security risk at airports, a number of security measures have been developed and implemented both nationally and internationally, for example, airports in the United Kingdom were the first authorities to implement strengthened security measures in the early 1990s (Drury, 1998). After the bomb threat in July 2006, in which an apparent plot to detonate bombs onboard aircraft at Heathrow Airport in London was discovered, security measures were heightened in UK airports. The new measures are graphically represented in Figure 2.8 (BBC, 2006).



1. Road access to airports is restricted. No parking zones outside airport terminals, traffic monitored by CCTV and police.
2. Armed police and CCTV monitor terminal building.
3. All passengers asked about contents of bags and whether they packed them personally. All sharp objects must be placed into checked-in baggage.
4. Passports required for most check-ins, passengers' passports inspected. Names of all passengers flying to the US must be submitted to US officials for cross-referencing against a database of "high-risk" terror suspects. All passengers must pass through a metal detector and all hand baggage is scanned with an X-ray machine. Sniffer dogs and chemical hand swabs are currently used to detect explosives. Explosives detector machines are currently being developed and may well be introduced in the future.
5. Checked baggage passes through large-scale x-ray machines. All bags are kept completely separate from passenger areas in the terminal.
6. Airside' is only access to aircraft area from the terminal is via controlled boarding points only. Ground staffs are submitted to background checks. Security pass system limits access to aircraft to only vital personnel and CCTV monitors the aircraft area.

Figure 2.8: Heightened Security Measures in UK Airports [sic] (BBC, 2006)

In the US, the Federal Civil Aviation Administration (FAA) also implemented major security measures in the 1990s. FAA measures, which were highlighted by Rao and Keith (1999), include passenger profiling, positive passenger bag match, trace explosive-detection devices, and procedures such as baggage hand searches. In addition, on September 14, 2001, the FAA tightened security and implemented new security measures in US airports nationwide. Examples of procedures at passenger terminal areas are illustrated in Figure 2.9 (The Washington Post, 2001). Recently in January 2008, the US Government published a National Aviation Security Policy, Strategy, and Mode-Specific Plans. The plan "addresses threats to aviation using a risk-based methodology to complement the overarching National Infrastructure Protection Plan (NIPP) and seeks to deter and prevent terrorist attacks against aviation, mitigate damage and expedite recovery and minimize the impact of an attack to the aviation system." (Dillon, 2009)

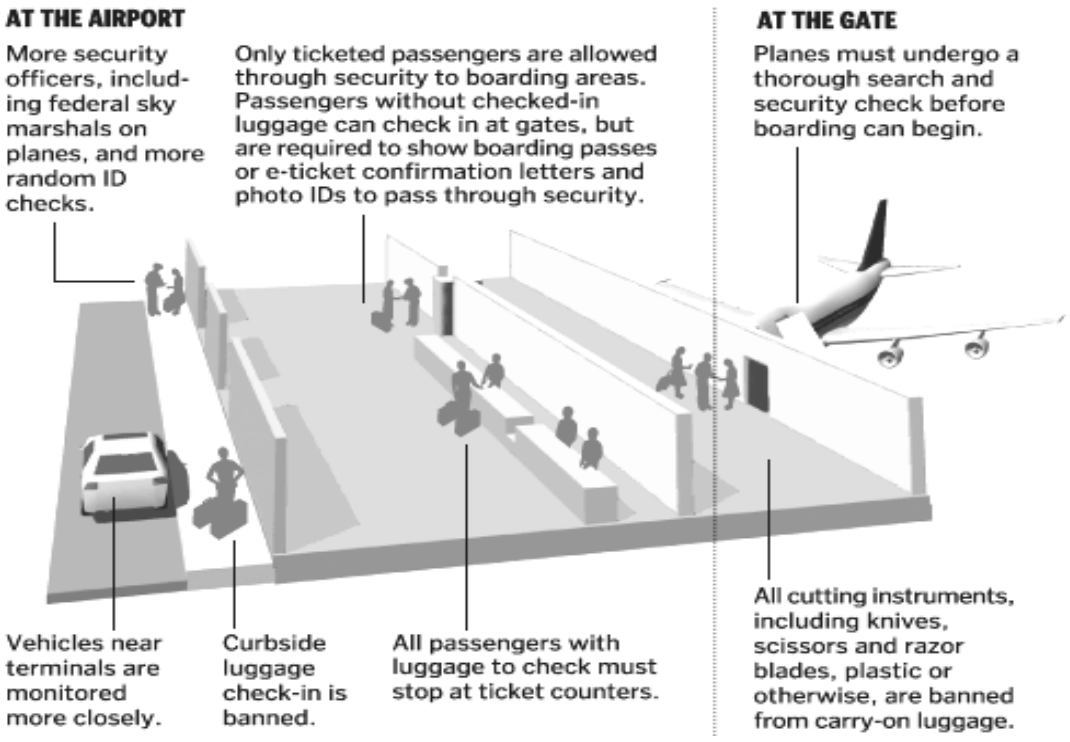


Figure 2.9: Security measures in US Airports Post 9/11 (The Washington Post, 2001)

Moreover, in Canada, the Canadian Air Transport Security Authority (CATSA, 2006) enforced more security measures, as illustrated in Figure 2.10. Likewise, in Japan, as illustrated in Figure 2.11, the security measures were also tightened up to include routine patrols, reinforced perimeters with sensors, access control at different gates, airport staff screening, passenger and cabin crew screening, hold baggage screening, and x-ray cargo screening. In addition, security guards were deployed at access gates, aircraft, and cargo terminal (Manabe, 2006).

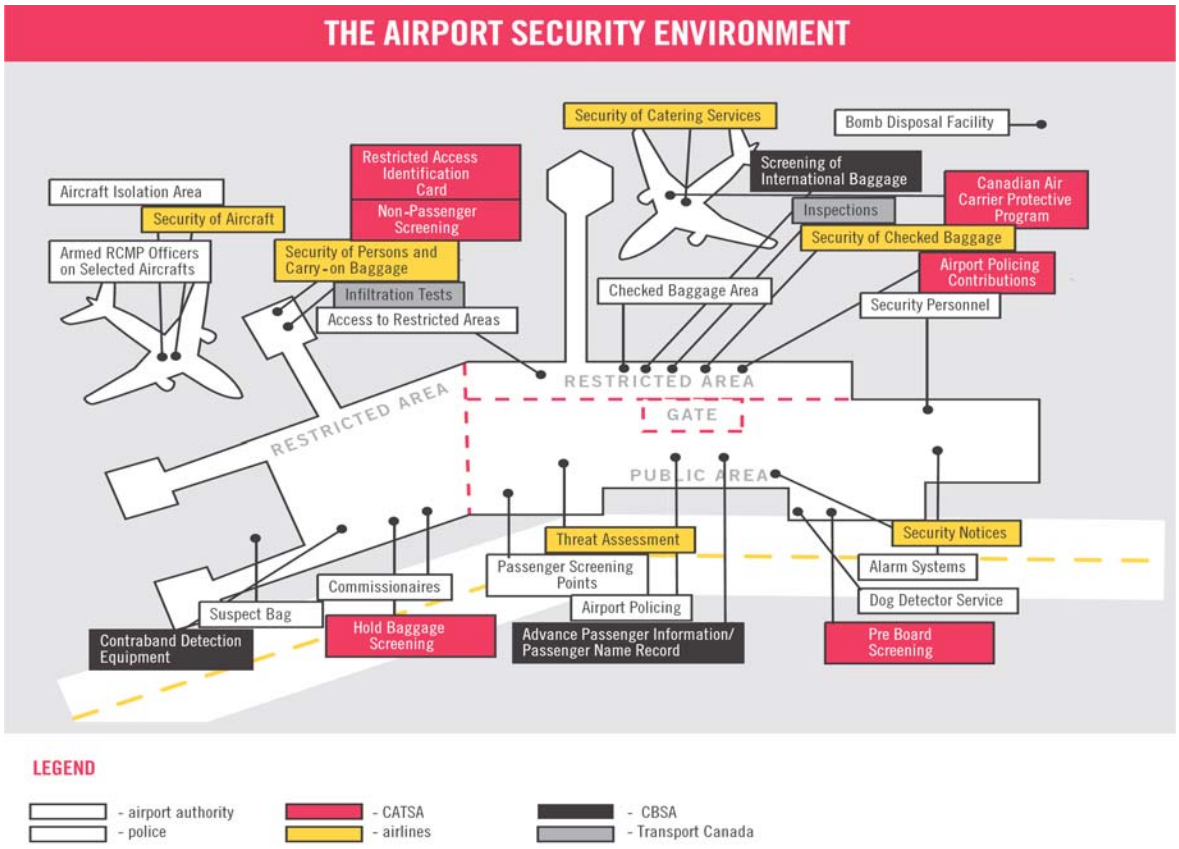


Figure 2.10: The Airport Terminal Security Environment (CATSA, 2006)

2.5.4 Security Technologies at Airports

Modern airports are changing their conventional role from being just premises for airplane operations and are becoming multidisciplinary business parks. Some scholars are claiming that airports are potential models of concurrent enterprises (Kesseler, 2003). As a result, cutting-edge

technologies in communication, IT systems, data, control, management, etc; have become an urgent necessity for running, maintaining, repairing, controlling, and securing modern airports at both the single-airport and multiple-airport levels.

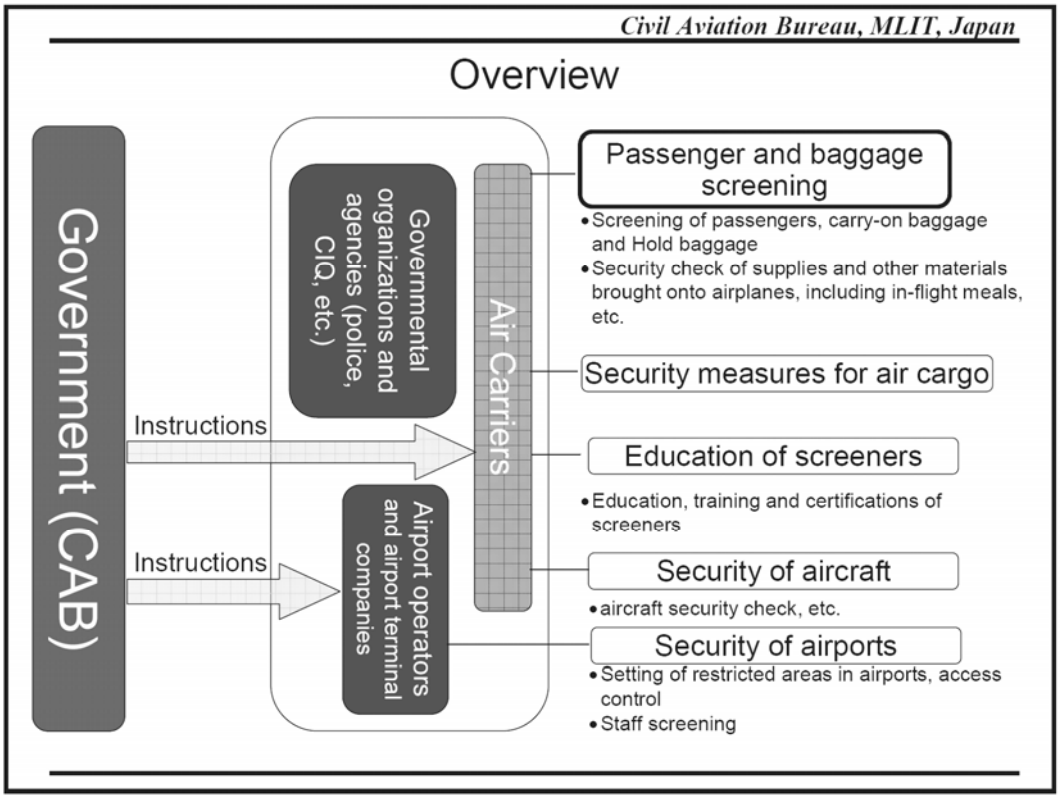


Figure 2.11: Overview of Aviation Security Measures at Airports in Japan (Manabe, 2006)

The utilization of explosives and nonmetallic weapons has initiated growing levels of security threats at airports. These new challenges have encouraged the investigation of new passenger screening technologies, including chemical-trace-detection techniques and imaging methods (NAS, 1996). Furthermore, the AT explosive-detection systems, x-ray applications, non-ionizing radiation, biometrics, and radio frequency identification (RFID) are technologies currently used at some airports and that will have wide deployment in the near future. The most commonly used and promising security-related technologies are summarized in the following sections.

X-Ray Applications

Automated x-ray technology has been used at airports to scan passengers' checked baggage in order to detect any hidden metal weapons, and consequently prevent potential high-jacking. After the blowing up of Pan Am flight 107 over Lockerbee, researchers developed three new explosive-detection systems (EDS) based on dual energy x-ray technology, and a fourth one based on radio frequency (RF) magnetic resonance technology, with special attention on advanced technology explosive-detection systems (ATs) (Rao and Keith, 1999). X-ray scanners have been used for a long time in airport security systems, but the side-effects of x-rays motivated researchers to explore other safer technologies (Profile, 2005).

AT Explosive Detection Systems

Some airports in the United States of America use the following examples of AT explosive-detection systems (Rao and Keith, 1999):

1. Vivid VIS-M rapid detection systems with a scatter detection enhancement feature.
2. EG and G Z-Scan 7 dual energy dual view system.
3. HI-Scan 10065 multi-energy explosive-detection device.
4. Qscan-500 quadrupole resonance analysis-based explosives-detection device.

Non-ionizing Radiation

Recent developments have produced a new scanning technology based on what is called "terahertz radiation," which operates with much lower energy and is therefore considered safer than x-rays (Profile, 2005). Recent advancements in pulsed laser and semiconductor technology have overcome the ''terahertz gap'' and have made commercially viable to use terahertz Technology in practical applications such as pharmaceutical drug discovery, medical imaging, and airport security (Profile, 2005).

Biometric

Is an authentication tool used to verify and identify a person identity through evaluating and matching his or her unique "physical and behavioral traits." Biometric technology is based on recognition of "common physical biometrics, including fingerprints; hand or palm geometry; and retina, iris, or facial characteristics. Behavioral characteristics include signature, voice (which also has a physical component), keystroke pattern, and gait." (Liu and Silverman, 2001). Biometrics applications are becoming the most secure and reliable techniques, because it is hard for these identifiers to be borrowed, stolen, or forgotten, and forging one is practically impossible (Liu and Silverman, 2001). On the other hand, biometric techniques lack standardization among different vendors. In addition, there are variations in accuracies and other technical concerns about physical and behavioral biometrics, as depicted in Table 2.7.

Table 2.7: Comparison of Biometrics (Liu and Silverman, 2001)

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

* The large number of factors involved makes a simple cost comparison impractical.

Radio Frequency Identification (RFID)

Cerino and Walsh (2000) referred to RFID as identification technology that automatically matches the item being read with its tag. Due to its potential advantages and wide range of frequencies it can employ, international co-operative research initiatives between aviation

industry partners such as airport authorities, suppliers, and/or air transport companies have been carried out. The testing will investigate the expected performance levels of different RFID frequencies that have promising functionality for aviation facilities with respect to the operational and security facets of passengers' baggage tracking, sorting, and reconciliation (Cerino and Walsh, 2000). Breakthrough technologies can enhance security measures at airports and improve overall performance levels by reducing screening and other security check times, increasing check productivity, and mitigating threat levels and vulnerability to actions of unlawful interference against civil aviation security.

2.5.5 Security Training Programs

According to several experts, human operators' abilities to recognize a threat in passengers' luggage are the most critical component in any airport aviation security system (Schwaninger, 2003). Consequently, successful training of security staff is a cornerstone of any security programs. The following are current broadly used training programs (Koller et al., 2007):

1. X-Ray Tutor (XRT), a computer-based (Schwaninger, 2003).
2. Threat image projection (TIP) program known as 3i-TIP System.
3. TIP Multiple Views Library (TIP MVL).
4. X-Ray Object Recognition Test (X-Ray ORT).
5. X-Ray Prohibited Items Test (X-Ray PIT).
6. X-Ray Competency Assessment Test (X-Ray CAT).
7. Theoretical Test on Computer (TEC).

The Security Industry Association (SIA) has reported that airport security is positively correlated with the lack of proper security training (SIA, 2008). For example, in a bomb-detection test

carried out by Transportation Security Administration (TSA) agents at Newark Liberty International Airport in the USA, in 20 tests out of 22, the operator failed to detect the bombs hidden in the luggage. The test revealed that most scanner machine operators do not pursue standard operating procedures in conducting their duties as directed and that they lack adequate training to fulfill their responsibilities (Marsico, 2006). This deficiency is being increasingly recognized and several authorities as well as airports are planning to increase investment in the important element of aviation security: effective and efficient training of screeners. A number of computer based training programs are dedicated to this objective. X-Ray Tutor (XRT) is one of the most widely used.

The X-Ray Tutor is being used to investigate potentials of x-ray image tutoring technology for aviation security screeners (Schwaninger, 2004). It is employed at 400 US airports, 19 German airports, and several airports in other European countries and Asia. The Canadian Air Transport Security Authority (CATSA) is also performing extensive testing of X-Ray Tutor at several Canadian airports in collaboration with the University of Zurich (UZ, 2006). X-Ray Tutor is designed to enhance aviation security screeners' ability to identify forbidden items within a passenger's baggage as they appear in images produced by x-ray-based screening devices (Koller et al., 2007). Schwaninger et al. (2005) claimed that screeners need the ability to deal with two main categories of factors influencing x-ray effectiveness: image-based and knowledge-based. Hardmeier et al. (2006) argued that image-based factors such as "bag complexity, superimposition by other objects, and rotation of objects" are based on visual-cognitive abilities and that knowledge-based factor are also relevant to the training screeners.

2.6 Risk-Based Security Research

In recent research government agencies and scholars have investigated a number of areas related to airport security risk and vulnerability. Governmental efforts have included, for example, the Australian Office of Transport Security (AOTS), who issued an Aviation Risk Context Statement (ARCS) in January 2005 (AOTS, 2005). In the USA, the TSA Office of Threat Assessment and Risk Management is working with economists to analyze the costs verses the benefits of precautionary measures (Jacobson et al., 2003). The TSA is also currently developing a Vulnerability Assessment Management System (TVAMS) to collect critical threat and vulnerability assessment data (Yalcinkaya, 2005). This research domain is helpful in addressing the levels of threats, vulnerability, consequences, of the security systems in airports.

2.6.1 Risk-Based Methodologies

After Sept. 11 incidents, the aviation security approaches focused on risk-based methodologies (Elias, 2008). To this extent, researchers developed a number of qualitative and quantitative methodologies to assess threats, vulnerabilities, and consequences in different disciplines. According to Stickles et al. (2003), airports confront two distinct sources of threat, the first is external threats and the second is internal threats. Within the civil aviation context, as shown in Figure 2.12, Elia B. (2008) has defined the relationship between the most important threat sources, tactics that can be used by adversaries, and the potential targets.

Weichselgartner (2001) argued that adopting a conceptual approach in vulnerability reduction, in any domain, will have positive impacts on diminishing the consequences. This research compiles different definitions of vulnerability.

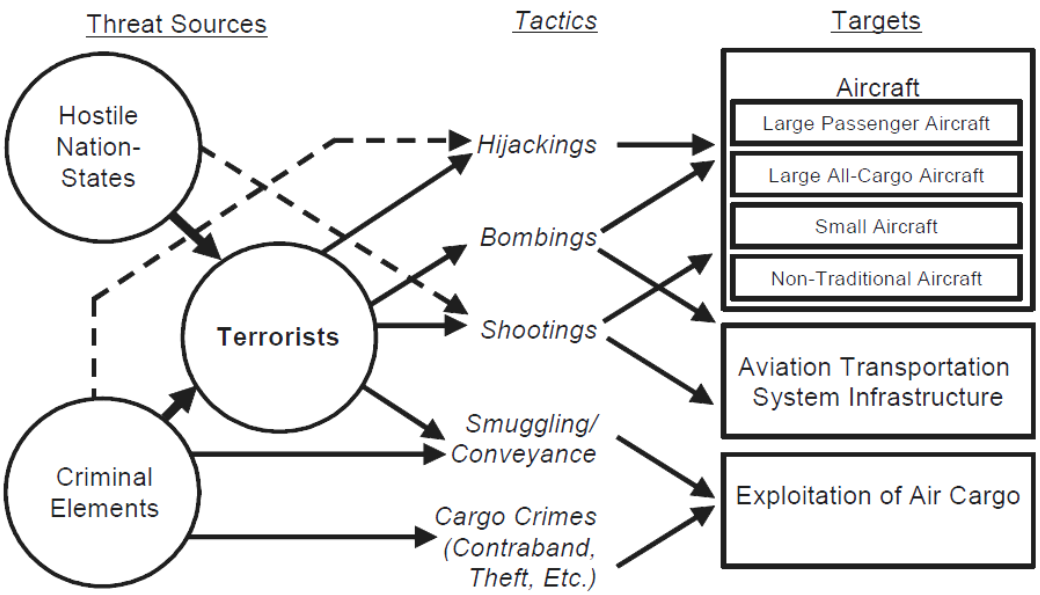


Figure 2.12: Aviation Security Threat Sources, Tactics, and Targets (Elias, 2008)

In the airport domain, Veatch et al. (1999) studied vulnerability using a scenario-based methodology and applied it to two major US airports. One of the useful aspects of this research is the practical formulation of consequence as a function of three parameters: Casualties (F), Downtime (U), and Exposure (E), as shown in Equation 2.1.

$$C = 0.5F + 0.2U + 0.3E \qquad 2.1$$

Where: F… indicates the level of casualties resulting from an adversary act,
U… represents the amount of time airport operations are delayed, and
E… represents exposure to public

This representation is useful in Veatch et al. (1999) research and can be extended to include other consequences related to property loss. The consequence scale used in Veatch et al. is shown in Table 2.8. Another important result of this research is the development of a relative attractiveness scale for aircraft assets as depicted in Table 2.9. This concept can be extended further more to include other airport facilities and assets.

Table 2.8: Consequence Scale (Veatch et al., 1999)

Level	Casualties	Facility Downtime	Exposure	Scale
Very High	> 25 Fatalities	> 24 Hours	Public Outcry/Dismay	5
High	11 – 25 Fatalities	> 16 – 24 Hours	Congressional Mandates	4
Moderate	1 -10 Fatalities/ Multiple injured	>8 -16 Hours	Potential Litigation	3
Low	1 Person Injured	8 Hours or Less	Major Investigation	2
Very Low	No Injuries	No Downtime	Minor Investigation	1

Table 2.9: Relative Attractiveness Scale (Veatch et al., 1999)

Attractiveness Rating	Value	Typical Examples
Extremely Attractive	5	Out of service aircraft
Very Attractive	4	Aircraft with passengers and an identified threat or an air carrier with an identified threat
Attractive	3	Aircraft with passengers or an operational terminal
Less Attractive	2	Passenger aircraft without passengers or support services essential for operations
Unattractive	1	An in-service cargo aircraft or retail operations

In more recent research, Dillon et al. (2009) developed an Anti-terrorism Risk-Based Decision Aid (ARDA) for assessing the investments of protecting U.S. Navy assets. The research analyzes thousands of possible attack scenarios considering 15 attack types, (Figure 2.13), 160 types of U.S. Navy facilities and 22 possible countermeasures to mitigate risk taking into account interesting ease factor of attack modes as shown in Figure 2.14.

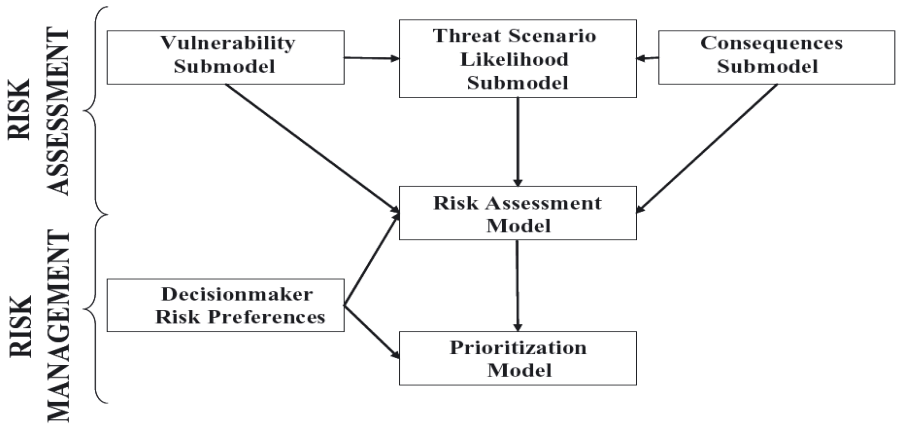


Figure 2.13: Risk Scoring and Prioritization Model (Dillon et al., 2009)

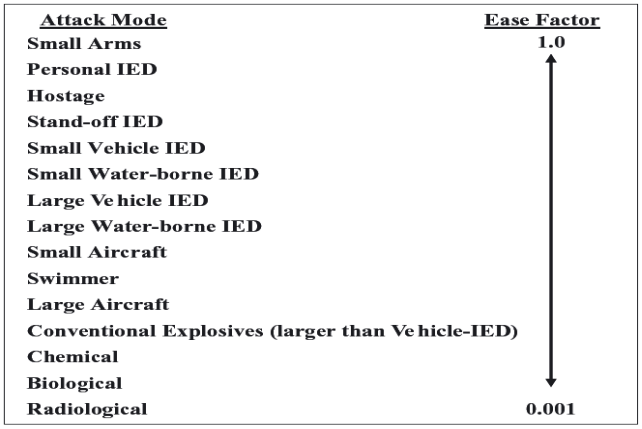


Figure 2.14: Possible Attack Modes, (Dillon et al., 2009)

In another effort, Hunt and Kellerman (2007) presented expert system software, Aviation Security Risk Assessment Program (CASRAP), to evaluate airport security threats, vulnerabilities, and consequences. Their research quantifies the security risk in terms of dollars of asset loss caused by potential threat. They divide the airport into two major areas; physical and virtual, as shown in Figure 2.15.

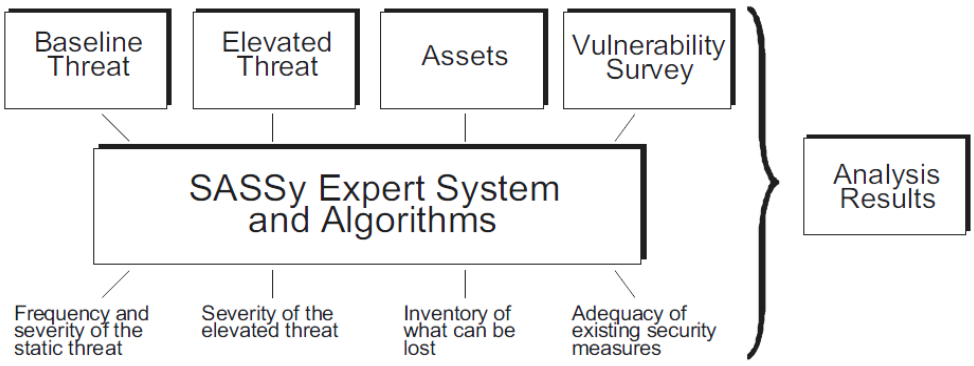


Figure 2.15: CASRAP, (Hunt and Kellerman, 2007)

Accordingly based on frequency, severity of threats, and chances of successful attacks, the tool produces a baseline risk expressed in dollars. A summary of other security risk assessment research is presented in Table 2.10.

Table 2.10: Examples of Research on Aviation and Airport Security

Title	Author	Objective	Output/Product	Comments
Airport Vulnerability Assessment - An Analytical Approach	Lazarick R., (1998)	Addresses both the process used to conduct "The Airport Vulnerability Assessment Project" in the US, as well as an unclassified look at the results which have been achieved for the initial airport assessments.	Findings resulted from the initial airport assessments. Countermeasures are commonly recommended for security improvements. A summary of learned lessons. Project status and anticipated schedule for the next year.	
Risk Assessment of Aviation Security and Evaluation of Aviation Security Policies	Yalcinkaya, R. (2005)	Addresses possible threats from terrorists and criminals against the aviation industry and offer possible solutions to deal with terrorist and criminal attacks, to determine whether existing security measures and safeguards are adequate or need improvement.	A list of recommended remedies was presented, which can be evaluated as responses to the vulnerabilities of aviation security.	Unavoidable limitations are: implementing these policies, precautions, and efforts can not thoroughly answer performance questions; agencies do not explain every detail of policies, because the concept of security issues is highly restricted and confidential; and there are limited empirical studies.
A Unified Framework for Risk and Vulnerability Analysis Covering both Safety and Security	Aven, T. (2006)	Develop a unified framework for risk analysis and management tasks.	A framework for risk analysis, covering both safety and security has been defined and quantified. The framework is based on two dimensions: possible consequences and associated uncertainties.	The developed framework is a useful approach for assessing risk and vulnerability in any system if the probabilities and uncertainties of this system can be defined.
A Systems Framework for Safety and Security: The Holistic Paradigm	Hessami, A. G. (2004)	Develops a holistic paradigm for a systems framework for safety and security.	A systemic and holistic framework of seven principles with a scalable architecture was developed, to suit the safety and security assurance at any level of perspective and scale.	
Risk Assessment of Aviation Security and Evaluation of Aviation Security Policies	Yalcinkaya, R. (2005)	Addresses aviation security risks and vulnerability problems, and offers possible solutions for eliminating them.	By using mitigation, means of transfer, and acceptance forms of risk management, possible strategies were presented to reduce the impact of risks in aviation security.	The thesis is oriented towards policies and strategies related to the mitigation of risk and vulnerability in aviation security.

2.6.2 Simulation and Modeling Studies

Using simulation techniques helped researchers to develop some decision support tools. In an attempt to develop a 2-D spatially aware software for the Transportation Security administration (TSA) called Security Checkpoint Optimizer (SCO), Wilson et al. (2006) used the discrete event simulation technique. The advantage of the SCO is its graphical interface model that enables security personnel to simulate their own passenger screening process. Once the security checkpoint(s) layout (Figure 2.16) and process parameters are defined, "SCO simulates passenger movement using both path-based and pathless movement algorithms to mimic a semi-autonomous passenger traversal of a 2-D space. The software is designed to allow analysts to perform multiple "what-if" analyses to balance benefits and tradeoffs."

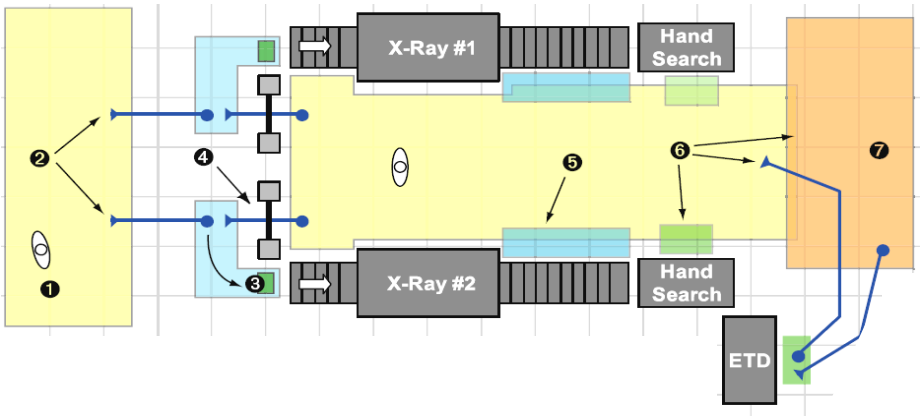


Figure 2.16: Two-Lane Security Checkpoint (Wilson et al., 2006)

One of the interesting features of this research is the application of security effectiveness in terms of the probability (p_d), to detect a threat based on the chance of not detecting it by a set of equipments at a given checkpoint (which, in fact, is the reliability of those equipments to detect specific types of threats through the related security check points), as shown in Equation 2.2.

$$P_d = 1 - \prod_{i=1}^{n} (1 - p_{d(i)}) \qquad 2.2$$

Where, $p_{d(i)}$ the effectiveness of equipment (i), i.e., the probability of the equipment to detect a threat.

While this representation is useful, this study did not differentiate the types of threats. Also, it did not consider multiple checkpoints in the analysis, or separate the analysis for passenger versus their cabin baggage and checked-in luggage. These considerations are important and are addressed in the present research and included in evaluating the overall terminal security risks.

Other simulation research, Rountree and Demetsky (2006), studied air cargo systems, and four security scenarios of cargo flow to test the overall effectiveness, cargo throughput, and evaluated the system costs, and the average time taken to process cargo through the facility. This research has the potential to be used as a guide by aviation decision makers to upgrade security measures in air cargo facilities.

In another research effort, Berkowitz and Bragdon (2006) used a 4-D simulation framework (Figure 2.17) to virtually investigate potential methods to deal with safety and security concerns in US seaports. The team tested the possible advantages of 4-D and evaluated in a virtual real-time format (air-land-seaport access) the likely vulnerabilities that might be generated by port stakeholders. The developed 4-D technique assisted with the generation of both surface and underwater scenarios in the context of seaports. These scenarios will help evaluate different events and personnel training situations. Although this technique was developed for port safety and security, its principles and logic have potential applications to the analysis of the performance of airport security systems.

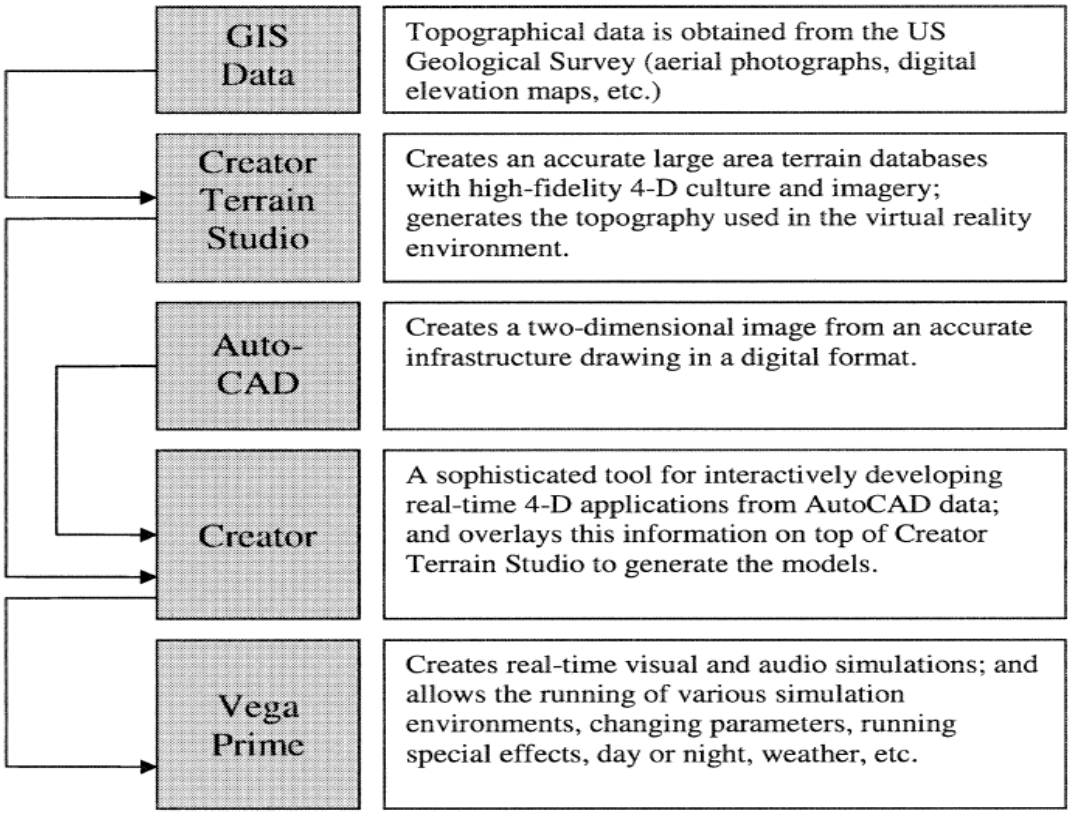


Figure 2.17: Simulation Flow Work [sic] (Berkowitz et al., 2006)

Some researchers have used modeling approaches to evaluate and assess airport security. Wilson, D. L. (2005) carried out an experimental study to provide a better understanding of new technologies and their impact on security systems in an airport's operational environment. The study modeled the passenger and carry-on baggage screening process to provide comprehensive guidelines on how simulation modeling can help to evaluate, assess, and fine-tune equipment selection and other operational factors in passenger and baggage security check-points.

The operational research approach also was used by Martonosi, S. E. (2005) to develop mathematical models to address prominent problems in aviation security related to Computer Aided Pre-screening Systems (CAPPS) and Secure Flight systems. The research presented a

review of some security risk assessment policies, synthesis of literature, discussion, use of approximate dynamic programming methods for allocating security checkpoints and cost-wise choices. Based on practical operational data and hypothetical modeling assumptions, the research states that quantitative methods were found to be helpful tools for shedding light on some of the intricacies of aviation security issues.

Jacobson, et al. (2003) adopted a case-study approach to model passengers and their baggage operational procedures though the baggage screening security systems at airport terminals. In an attempt to answer how and where to assign the required screening devises, and measure how effective are they, the research investigates how discrete optimization techniques can help decision makers to optimally deploy the measures of a baggage security screening system. The research quantifies the effectiveness of baggage screening security device systems based on identifying three performance measures. Those measures are: (1) Uncovered Flight Segments (UFS), which quantifies number of uncovered flights, (2) Uncovered Passenger Segments (UPS), which quantifies number of passengers on uncovered flights, and (3) Uncovered Baggage Segments (UBS) which quantifies number of unscreened selected bags. The optimization model included some deployment constraints on a set of fights, such as, the number of un-cleared passengers, the number of flights, and the size of the aircraft.

Hessami, A. G. (2004) applied an empirical investigation approach, by investigating number of airlines accidents, to propose a new paradigm for holistic systems assurance, and developed a systems framework for safety and security. The new framework is based on two fundamental facets: safety performance and the security vulnerabilities. The research, within the context of organization and learning, categorized and describes seven systemic assurance principles (Figure

2.1); which are: Proactivity, Prevention, Protection, Preparedness, Recovery, Organization and Learning, and Continual Enhancement; and argued that these principles are the foundation for any systemic and holistic approach to safety and security assurance.

2.6.3 Security Management Systems

Various researchers have introduced security management systems to various applications. Based on a survey and scenario approach, Tzannatos E. S. (2003) developed a Decision Support System (DSS) for the Promotion of Security in Shipping. As depicted in Figure 2.18, the author structured the research to develop a DSS that relays of a DSS-resident database of all relevant threats in terms of type and intensity, and any means or vulnerabilities, by which threats can be realized.

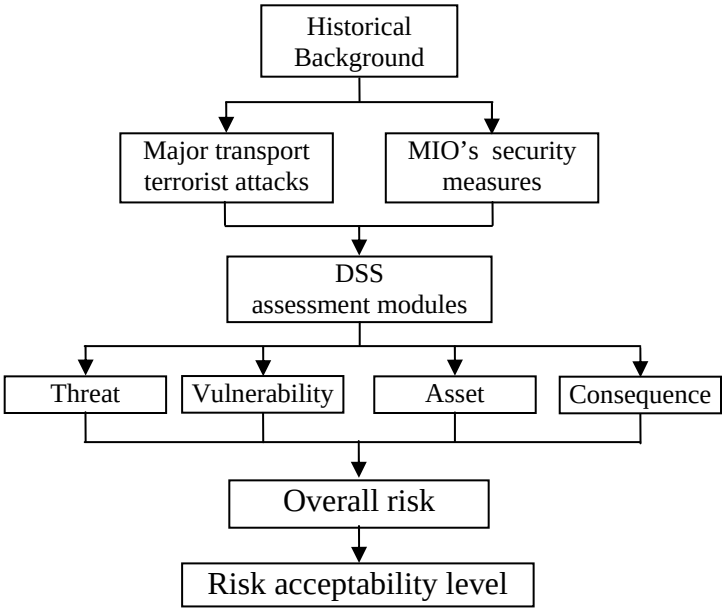


Figure 2.18: DSS structure (Tzannatos, 2003)

To assess the risks, the research adopted three risk factors as the basis for DSS investigations and assessment methodology (Figure 2.19). The factors are: probability of a specific threat to occur,

likelihood that an attempt will be successful (exploited vulnerabilities), and severity of its consequences (impact significance of the asset loss). The research generally has three major phases: (1) Risk assessment phase, which threats, vulnerabilities, and consequences are assessed; (2) Setting acceptable levels of risk phase, which defines the threshold of accepted risk level; and (3) Security control and planning phase, in which countermeasures and cost-effective mitigation measures are addressed and compared.

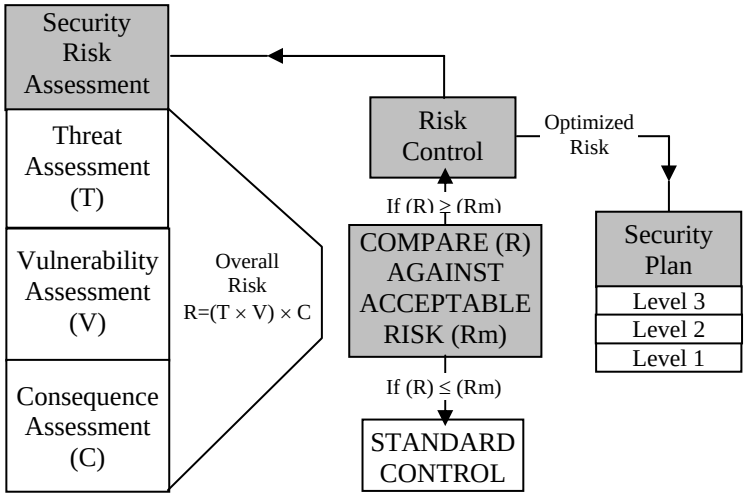


Figure 2.19: DSS Methodology (Tzannatos, 2003)

Among research features, was the use of five quantitative risk factors assessment levels based on a subjective expert judgment that assigns scores 1- 5 for each risk factor (threats, vulnerabilities, and consequences), and a scale of 1 – 125 to quantify overall risk. The DSS executes a detailed comparison among the constituent factors of risk to detect the conditionally acceptable scenarios and produces a security risk matrix, which informs the user about the scenarios allocated to the various risk levels and their corresponding vulnerabilities, thus, being prime candidates of security optimization. The DSS initiates a risk re-assessment to arrive to the risk optimized matrix within the framework of a cost-benefit analysis.

Using discussion and case-study approach, Corazzola and Poli (2003) developed an improved Decision-Making approach through Effective Asset Management. The research furnishes engineering and public works planners with tools for making condition assessment-based decisions and utilizing features of GIS systems. The author reviewed and synthesized literature, and overviewed real-life examples of municipalities. The research results include guidelines for designing a customized condition assessment strategy that will meet the needs of a given organization, and addresses that the developed strategy has potential uses and application in other infrastructure areas.

Vose D. (2008) in his book "Risk Analysis: A Quantitative Guide", presented a comprehensive background on risk analysis in the first part of the book. While, in the second part he devoted it to risk analysis distributions, modeling and simulation, and forecasting processes. The book highlights the process of risk analysis modeling and global optimization methods. As depicted in Figure 2.20, the book describes a road map to develop a risk assessment metric that can be utilized in different domains.

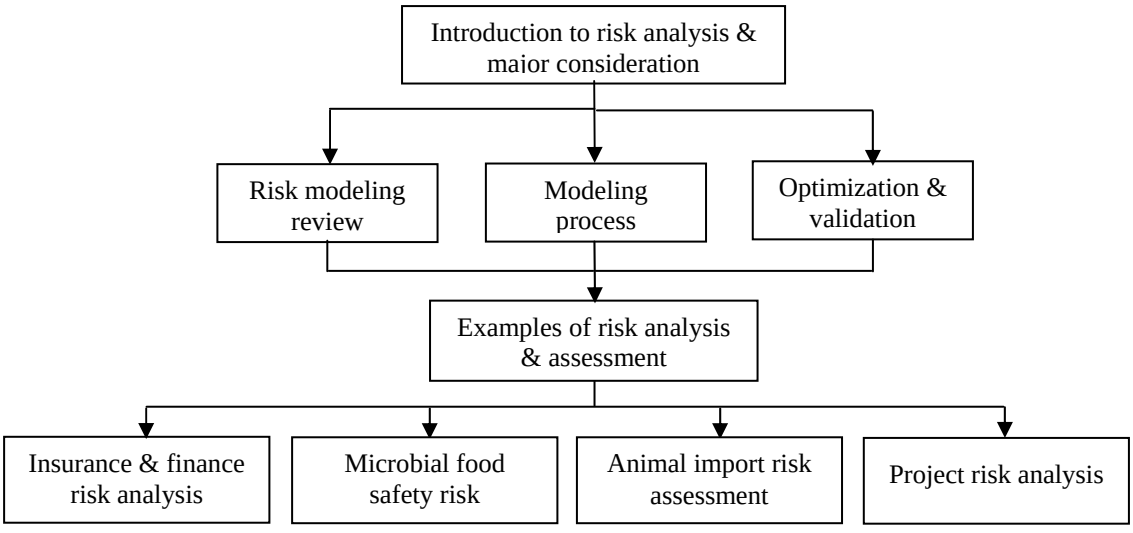


Figure 2.20: Vose (2008) Book General Structure

Some advantages of the book are: useful Spreadsheet examples along with related programming code, introduces the use of Monte-Carol simulation in risk applications, and discusses the most common risk modeling errors. Other example of security management systems, risk assessment software, and benchmarking research are depicted in Tables 2.11 and 2.12.

2.7 Summary

Aviation security is an essential requirement to airports. Airports are becoming more demanding of society's vital dynamic assets in the transportation infrastructure and will benefit from emerging infrastructure management systems; therefore, any asset management system for an airport should include aviation security as one of its objectives. Since the 1960s, aviation safety and security has caught the attention of governments and international agencies, but airports have continued to be targeted by different adversaries worldwide. Following the 9/11 attacks, in response to these incidents, ICAO published Annex 17 and started USAP, both of which aim to promote safeguard civil aviation operations against acts of unlawful interference. Consequently, the attention of airport authorities has been refocused to airport risk-based security management systems and assessment methodologies, especially, since 2005 when the US aviation infrastructure and the security of America's critical infrastructure were graded at D+ and I, respectively. Recently, researchers have begun to develop qualitative and quantitative risk-based methodologies to assess the three risk dimensions: threats, vulnerabilities, and consequences. Although, a number of quantitative risk-based research studies have been carried out in the area of airport security systems; however, research gaps can be listed as follows:

1- No research has been found on asset management for airport security systems as defined by ICAO's Annex 17, particularly for international airports terminals.

Table 2.11: Example of Security Management Systems and Risk Assessment Software

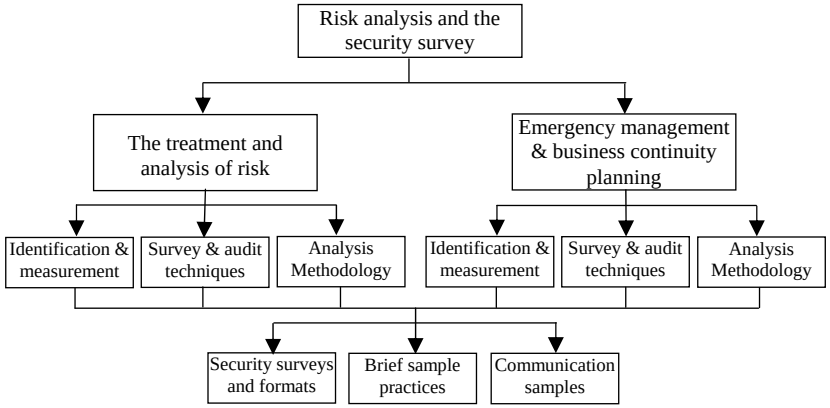
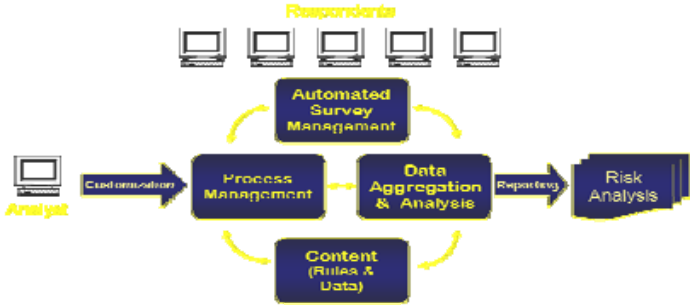
Title	Research Structure/ Methodology	Unique Features	Comments/ Criticism
Risk Analysis and the Security Survey (Broder J. F., (2008)		- Specifically oriented to security environment. - Provides pertinent formats for security checklists & surveys. -Provides an inclusive reference for risk analysis methodologies and cost/benefit analysis. - The book introduces systematically the concept of comprehensive emergency management (mitigation, preparedness, response, and recovery).	- Useful and practical security checklists and surveys. - Provide professional risk analysis examples. - Illustrates Technical specifications of some security aspects.
RiskWarch	The process examines five variable functions: 1. Specific Assets to be protected (value) 2. Potential Threats to the various assets 3. Vulnerabilities that would allow the threats to materialize 4. Kinds of Losses that the threats could cause 5. Safeguards that would reduce the loss or eliminate the threats 	- Multiple application software. - Links risk assessment results with financial data or without, and with Return on Investment Data or w/o. - Widely used and tested by various clients. - Quantifies risk and provides ROI metric based on the safeguards selected. - Automatically generates a complete management-ready case summary report. - Threats are categorized as: natural disasters, criminal activity, terrorism, theft, and systems failures. - Contains more than 160 controls, with default values for implementation, and life cycles.	- Claims that it reduces needed for Risk Analysis by 70%. - Customizable software. - Has a Web-Based surveys tool. - Runs mitigation strategies. - Produce assessment data supported with graphics, charts, and quantitative measures. - Software purchase and training are needed.

Table 2.12: Example of Security Benchmarking Research

	Title	Author	Type	Objective	Methodology/ Work Program	Output/Product	Comments
Benchmarking	Benchmarking Security and Border Control	SH&E International Air Transport Consultancy (2005)	Consultancy study	Identifies the impact government services and measures, and national and international legislation in the field of security and border control have on the costs and the quality of the passenger-handling process.	Meetings with relevant stakeholders; visits to airports; and directed survey.	A Findings Report was presented.	There were difficulties in collecting some vital information due to the confidential nature of the information.
	Best practice benchmarking: a route to competitiveness?	Francis, G., Hinton, M., Holloway, J. and Humphreys, I. (1999)	Case-study approach (empirical investigations)	Examines the use of best practice benchmarking as an approach to performance improvement in the airline industry.	Benchmarking study based on case-study approach.	A range of benchmarking issues were highlighted, and factors that are likely to increase the adoption of benchmarking as a route to competitiveness were also identified.	The idea of benchmarking is becoming widely used as an empirical approach to evaluating the current status of any item, system, organization, etc., with respect to its counterparts and competitors.
	Balancing User Priorities for Sustainability versus Security	Oberle, R., Pohlman, T., and Roper, K. (2007)	Systematic analysis research	Develops a rating system that balances user priorities for sustainability versus security for better building design.	Review of comparative literature as basis for developing the new model	A decision matrix model.	The user can add new items and change the weighing scheme. Future development indicates the possible utilization of utility curves and the multi-attributable utility theory.
	Benchmarking in civil aviation: some empirical evidence	Fry, J., Humphreys, I. and Francis, G. (2005)	Case-study approach (empirical investigations)	Explores the use of best practice benchmarking in civil aviation.	Questionnaire surveys of the top 200 airlines and the top 200 airports; and interviews with airline and airport managers.	The surveys revealed a very high utilization of benchmarking through a series of comparison study findings.	

2- Most research has focused on a scenario approaches, and didn't deal with security issue at airport in terms of combinations of defined systems, such as passenger and cabin baggage screening system, access control system, etc.

3- Most studies did not consider threat sources in terms of passengers, cabin baggage, and checked-in luggage, and accordingly, assess vulnerabilities and consequences based on probabilities not to detect the potential threats (i.e., equipment's effectiveness to detect the concerned threats).

4- Performance measures have been concerned mostly with the overall service quality at airports, not the broader aspects dimensions of security systems.

5- Most research security effectiveness was inputs based on relative probability of detecting certain threats based on security subject matter experts.

6- Although previous research attempted to measure security risk quantitatively and some upgrade countermeasures that can be compared with respect to cost and gained benefit based on pair-comparison or prioritization approaches, they do not include detailed airport oriented quantitative assessments of threats, vulnerabilities, and consequence.

7- Most of previous airport security assessment methodologies lack risk-based security decision support systems and non-traditional techniques-based optimization model for Passenger and Cabin Baggage Screening System, to provide guidelines for optimum upgrade strategy.

The gaps mentioned above and the crucial need for a security risk-based framework create a need for a decision support system that will help airport officials easily assess the status of their airports' security systems quantitatively, satisfy standards and system's constraints, and efficiently allocate financial resources in order to improve security levels.

CHAPTER 3
SECURUTY RISK METRIC

3.1 Introduction

For many years, risk assessment studies in civil aviation were directed at safety and aircraft accidents. However, after the events of September 11, 2001, the focus of most security-related risk assessment has shifted to threats, vulnerabilities, and their consequences. Based on the literature review in chapter 2, this chapter presents the development of a metric for quantitatively assessing the security risk at an airport. The metric can be used to evaluate the security risk both at the level of all security systems and also at the level of the whole airport level. The metric involves a methodological assessment for quantifying the three dimensions of risk: threats, vulnerability, and consequences. The metric assesses and considers the overall security risk at international airport terminals based on threats arise from passengers, cabin baggage, and checked-in luggage. Later chapters present the use of the developed metric for developing a risk-based optimization model that can optimize upgrades to airport security systems.

3.2 Dimensions of Airport Security

The ICAO definition of civil aviation security and the definitions of risk found in the literature were used as the basis of a comprehensive approach for deriving a definition of airport security risk assessment and for determining its dimensions: threats, vulnerabilities, and their consequences (Figure 3.1).

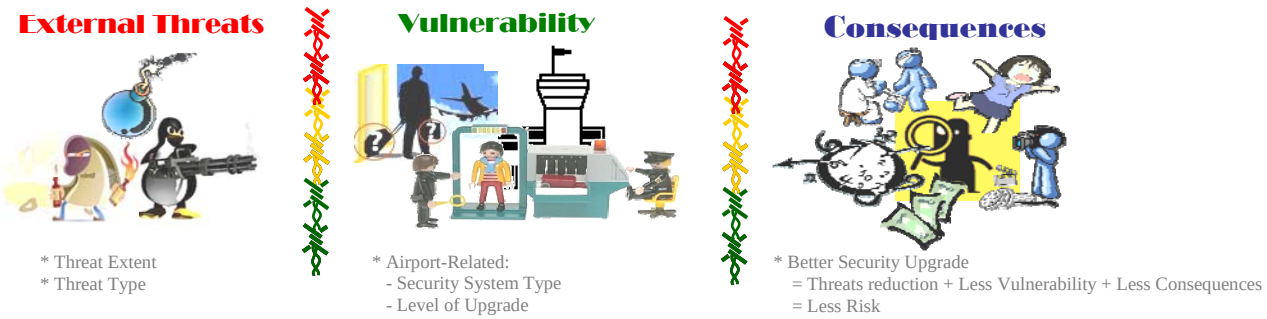


Figure 3.1: Dimensions of Security Risk (Google Images, 2009)

According to civil aviation security definition of the ICAO, this research defines airport risk assessment as the in-place security measures (including human, physical, and non-physical resources) for detecting, deterring, mitigating airport threats, and for diminishing vulnerabilities in order to safeguard airports against acts of unlawful interference (ICAO, 2002). This research deals with the assessment of the security risk to the passenger and cabin baggage screening system, as one of the seven airport security systems (ICAO, 2002b) at the airport terminal level, as defined by ICAO Annex 17. Brief highlights of the three dimensions of security risk dealt with in this research follow:

3.2.1 Threats

According to Elias (2008) and Stickles et al. (2003), sources of security threats can originate either internally (e.g., theft, smuggling, vandalism) or externally (e.g., criminals, extremists, terrorists). Since the proposed framework focuses on airport security, it deals with only terrorist-related external threats because most other threats can be handled by the local airport police force, and are not the direct responsibility of airport security. In general, however, a threat can be defined as "any indication, circumstance, or event with the potential to cause loss or damage to an asset." Another definition of a threat is "the intention and capability of an adversary to undertake actions that would be detrimental to valued assets." (API/NPRA, 2004)

As defined in Tzannatos (2003) and API/NPRA (2004), a threat can have five levels, ranging from "none" to "very high." "None" means that no action on the part of the adversary is expected at all; therefore, an attack will not occur. In contrast, a "very high" level means continuous or intensive attacks are likely, and the adversary has the intention and the capabilities of launching an attack that would have destructive consequences. Table 3.1 provides a detailed description of

each of the six threat levels, along with a related threat score. A threat level is defined in this research as the level of the likelihood that a potential threat will occur. Therefore, the levels selected by security experts reflect their assessment of the level of likelihood that threats will occur. Threats levels are assessed with respect passengers, cabin baggage, and checked-in luggage, and the associated risks are quantified accordingly.

Table 3.1: Threat Rating Criteria (based on API/NPRA, 2004; Tzannatos, 2003)

Level	Threat description	Score
Very High	Identifies a credible threat to airport assets, so that continuous or intensive attacks are likely to occur, and that the adversary demonstrates the capability and intention of launching an attack targeting the airport or one of its assets on a frequently occurring basis, and specialized security advice should be sought	5
High	Identifies a credible threat to airport assets based on knowledge of the adversary's capability and intention of attacking airport assets that involve high levels of expertise, resources, and support and based on related incidents having taken place at similar airports or in similar situations	4
Medium	Identifies a possible threat to airport assets based on the adversary's desire, limited expertise, resources, or opportunity to compromise similar assets.	3
Low	Identifies random low-level subversion threats to airport assets, with few known adversaries who would pose a threat to airport assets, involving low levels of expertise and resources	2
Very Low	Identifies an attack is unlikely to occur or that there is credible evidence of capability or intent, with no history of actual or planned threats against airport assets	1
None	No threats	0

Threats are not identical in all airports but different at hub airports, international airports, and domestic airports. In addition to local sources of threats, the occurrence of a threat is also influenced by other regions in the world that experience high levels of risk because the airport concerned is the final destination of travellers from such regions. Therefore, passengers, their cabin baggage, and their checked-in luggage that are carried by airliners originating from high-risk regions should also be considered as possible sources of threat.

3.2.2 Vulnerability

Vulnerability is one of the key dimensions of risk, and can generally be defined as "any weakness that can be exploited by an adversary to gain unauthorized access and subsequent

destruction or theft of an asset." (API/NPRA, 2004) Within the context of an airport, vulnerability represents the inability of a security system to apply effective mitigation measures, i.e., inability to detect, deter, delay, and respond to threats. Vulnerability can be the result of any weakness or deficiency in the system's management practices (policies and rules); equipment and devices; and operational security practices (design, specifications, and procedures).

As with threats, vulnerability has also six extended levels that are based on Tzannatos (2003) and API/NPRA (2004), ranging from "None" to "very high." A vulnerability level of "none" means no chance of an adversary affecting airport assets, even by the most intensive attacks. On the other hand, "very high" vulnerability means that no effective or reliable means of mitigation are in place, and the adversary can easily plot a destructive attack against the airport. Table 3.2 shows the expanded description of the six levels of vulnerability and their associated scores.

Table 3.2: Vulnerability Rating Criteria (API/NPRA, 2004; Tzannatos, 2003)

Level	Vulnerability description	Score
Very High	Identifies that there are no effective protective measures currently in place to deter, detect, delay, and respond to the threat, so an adversary can successfully attack the airport assets at any time	5
High	Identifies that there are some protective measures to deter, detect, delay, or respond to the threat, but not a complete or effective application of these security strategies, so it would be relatively easy for the adversary to successfully attack the airport asset, and a limited opportunity and little specialized knowledge would be needed	4
Medium	Identifies that there is no complete and effective application of these security strategies, so an attacker with moderate levels of resource and skill could be expected to exploit the identified vulnerabilities of the airport asset, and the existing countermeasures could likely be compromised	3
Low	Identifies residual vulnerabilities so that at least one weakness exists that an adversary having high level of resource and skill would be capable of exploiting with some effort in order to evade or defeat the countermeasure	2
Very Low	Indicates that no residual vulnerabilities to the threat exist and that the chances that the most intensive adversary would be able to exploit the airport asset are very low	1
None	No vulnerabilities	0

3.2.3 Consequences

Consequences are an important dimension of risk; they are the result of successful attacks and exploited vulnerabilities. Consequences have been defined as "the amount of detrimental impact,

losses, fatalities or damages experienced by an airport asset given that a successful attack has occurred" (AICE/CCPS, 2002; Tzannatos, 2003).

Veatch et al. (1999) quantified the consequences of a successful threat in terms of three aspects: number of fatalities, downtime in number of hours; and level of exposure to the public. Other researchers (e.g., Hunt and Kellerman, 2001; RiskWatch, 2008; etc.) also include the cost of damage to the physical asset (as a percentage of the total replacement cost) as part of the consequences. This research considers four aspects of consequences. Table 3.3 shows the levels of consequence and the associated fatalities, downtime, public exposure, damage level, and scores.

Table 3.3: Revised Consequence Rating Criteria (based on Veatch et al., 1999)

Level	Casualties (F)	Downtime (U)	Exposure (E)	Total Damage (%)	Score
Very High	> 50 Fatalities	> 48 Hours	Public Outcry/Dismay	75% -100%	5
High	25 - 50 Fatalities	24 - 48 Hours	Congressional Mandates	50% - 75%	4
Medium	11 - 25 Fatalities	16 - 24 Hours	Potential Litigation	25% - 50%	3
Low	1-10 Fatalities	8 - 16 Hours	Major Investigation	10% - 25%	2
Very Low	1-5 person injured	< 8 Hours	Minor Investigation	1% - 10%	1
None	No Injuries	0 Hours	No Exposure	No Damage	0

3.3 Airport Security Systems

To design a security metric, useful security documentations were obtained from ICAO Headquarters in Montreal to be used for research purposes. The provisions in the ICAO's *Annex 17* (ICAO, 2002b) for security systems and the *Security Audit Reference Manual* (ICAO, 2002c) were both used for the design of the metric. The seven airport security systems as defined by the ICAO are as follows:

1. Organization and Administration
2. Access Control

3. Passenger and Cabin Baggage Screening

4. Hold Baggage Security

5. In-Flight Security

6. Cargo and Catering

7. Responses to Unlawful Interference and Contingency Arrangements

Due to the wide scope of these security systems, the proposed metric focuses only on the passenger and cabin baggage screening system (PCBSS); however, the metric has been designed to be flexible so that other systems can be included in future research.

3.4 Airport Security Metric

As shown in Figure 3.2, the new security metric can be used to provide a risk index for each airport security system, through a detailed risk assessment of each system, and for an airport as a whole. Since the metric focuses on the PCBSS, the security risk index produced by the metric quantifies only the security risk of the PCBSS.

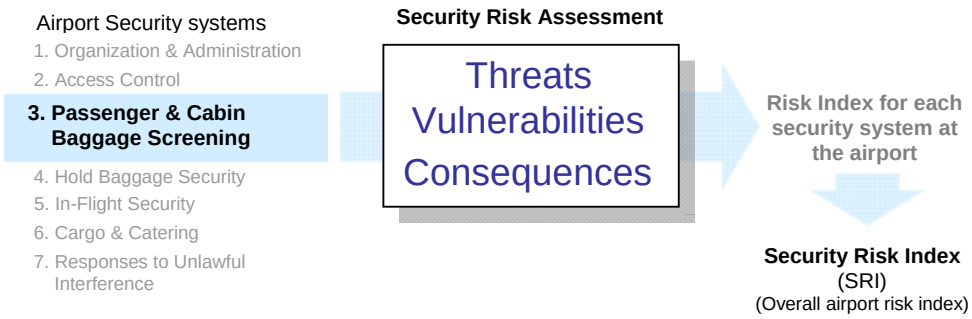


Figure 3.2: Risk-Based Security Metric

The typical PCBSS in a typical airport terminal consists of a set of security checkpoints (SCPs) that can be equipped with a variety of countermeasures options (devices, equipment, and measures), which determine the overall effectiveness of the system. Each SCP is independent of

the others, and each SCP operates based on a specific probability that type of security breach is going to happen. For the airport terminal to be vulnerable, the threat must pass through the entire set of independent SCPs. Thus, the overall effectiveness of the PCBSS depends on the thoroughness and reliability of the component of the system (countermeasures at the various SCPs) in detecting and deterring any threat. Therefore, the more sophisticated the security measures at a specific SCP, the less vulnerable the system.

It is possible to represent the vulnerability of a system, based on the independence of the SCPs, using mathematical representation. According to the special multiplication rule for independent events (Walpole and Myers, 1993), when two events A and B are independent, then the probability of both of them happening (that is, the vulnerability) is the product of their independent probabilities of occurring (vulnerabilities) (Equation 3.1), as follows:

$$P(A \cap B) = P(A) * P(B) \qquad \textbf{3.1}$$

For multiple events $E_1, E_2, E_3, \ldots, E_n$, the overall probability of all of them occurring can be calculated using Equation 3.2, as follows:

$$P(E_1, E_2, \ldots, E_n) = \prod_{i=1}^{n} P(E_i) \qquad \textbf{3.2}$$

For example, assume two SCPs A and B are 99% and 98% effective respectively, in detecting a specific threat. The chances of both pieces of equipment not detecting a threat are, thus, also the chance of the airport being vulnerable (i.e., both SCPs not detecting the threat equals $P(A \cap B)$), as follows:

$$P(A \cap B) = P(A) * P(B) = (1 - 0.99) \times (1 - 0.98) = 0.0002$$

Therefore, based on the same principle of independence used by Wilson and Roe (2006), who developed a Security Checkpoint Optimizer, and considering the approach of Jacobson et al. (2003) to quantifying the effectiveness of baggage screening security device systems based on

identifying three performance measures (including passengers, baggage, and flights), Equations 3.1 and 3.2, it is possible to carry out a full risk assessment of the PCBSS by evaluating the three security dimensions: threats, vulnerabilities, and consequences. Since threats and consequences are uncontrollable whereas vulnerabilities are controllable, the metric assesses the vulnerabilities of PCBSS and the risks of each type of security threat at the level of the SCP component with respect to passengers, carry-on baggage, and checked-in luggage. Therefore, the risk assessment can be addressed as follows.

3.4.1 Threat Assessment

Based on the literature investigation (e.g., Figure 2.12) and discussion with airport officials, the types of threats that apply to the passengers and cabin baggage screening system can be divided into three main categories: explosives, sharp blades, and biological attacks. Each category is further subdivided into a number of levels called threat types. The threat categories and their types are defined in Table 3.4. These threats are assessed according to the threat levels shown in Table 3.1 and scored on a scale from 0 to 5.

Table 3.4: Threat Categories and Their Types

1.0 Explosives	2.0 Sharp blades	3.0 Biological Attacks
1.1 Weapons 1.2 Bombs 1.3 Explosive Liquids	2.1 Knives 2.2 Swords 2.3 Razors and Cutters	3.1 Choking 3.2 Nerve 3.3 Blood 3.4 Blister

3.4.2 Vulnerability Assessment

The passenger and cabin baggage screening system in any airport terminal is typically split into two subsystems: departure and arrival. Each of these subsystems has its own security checkpoints (SCP), known as screening stations, as listed in Table 3.5. According to the size and function of the airport, the sequence, the number, and type of departure and arrival security checkpoints may differ from one terminal to another.

Table 3.5: Security Checkpoints in an Airport Terminal

Subsystem	Checkpoint 1	Checkpoint 2	Checkpoint 3	Checkpoint 4	Checkpoint 5
Departure	Curbside/Precheck-in	Airline check-in	Checked luggage	Central gate	Boarding
Arrival	Deplaning Gate	Passport control	In-bond baggage	Transferred baggage	Hold baggage

3.4.3 Consequence Assessment

In any threat category, each type of threat has a potential consequence that is likely to occur. In this research, the assessment principle used by Veatch et al. (1999) has been extended, as follows. The consequences are represented in terms of the number of fatalities, the number of hours of downtime, the amount of public exposure, and the dollar value of the physical damage (percentage of the total replacement cost). Table 3.6 illustrates the four types of potential consequences and their assigned impact weight (w). It should be noted that the category of physical damage to the asset has been given a weight of 20 % based on an input from an airport security expert at the Greater Toronto Airport Authority (GTAA), while the remaining 80% was redistributed among casualties, downtime, and exposure based on the percentages used by Veatch et al. (1999).

Table 3.6: Aspects and Weights of Consequences

Casualties	Downtime	Exposure	Asset Physical Damage
Number of fatalities	Hours of downtime	Public exposure	Dollar value of physical damage as percentage of the total loss
40%	15%	24%	20%

3.4.4 Security Risk Index

One of the paramount objectives of this research is to develop a security risk index (SRI), which would function as a quantitative indicator of the security risk at an airport. When the SRI is used at multiple levels, it can also be regarded as a useful tool for comparing different SRIs for subsystems, systems, and single or multiple airports. Based on the approaches of Tzannatos

(2003), Guthrie et al. (2005), and Sylvie (2005), the overall SRI is determined as the product of the overall threat (T_s), vulnerability (V_s), and consequence (C_s) of a system, according to Equation 3.3.

$$SRI_s = Threat\ (T_s) \times Vulnerability\ (V_s) \times Consequence\ (C_s) \qquad \textbf{3.3}$$

With respect to the PCBSS, the developed security risk metric extends the risk evaluation of Wilson and Roe's (2006) approach for one security checkpoint so that multiple checkpoints can be considered and so that the risks associated with passengers (P), cabin baggage (B), and check-in luggage (L) can be separated. To facilitate the analysis, a database of various mitigation measures was created that includes information about the reliability and the cost of each mitigation measure for detecting each type of threat. Some the information applies to passengers only, and some applies to cabin baggage, checked-in luggage, or a combination. The database entries for reliability and cost information) are based on input from airport security experts.

Threat Analysis

Figure 3.3 illustrates the types of threats that are common to a passenger and cabin baggage screening system. For example, each type of threat is assessed based on user input with respect to the likelihood of that threat occurring. Accordingly, the threat level for each category J is defined as the average of all the types of threat in that category. Therefore, the overall system threat (T_s) can be calculated as follows:

$$T_s = \sum_{j=1}^{J} \left[\frac{\sum_{i=1}^{nj} t_{ji}}{nj} \right] \times J^{-1} \qquad \textbf{3.4}$$

Where T_s is the overall system threat level (0-5)
J is the number of threat categories
n_j is the is number of threat types in threat category j
t_{ji} is the assessment of threat type i in threat category j.

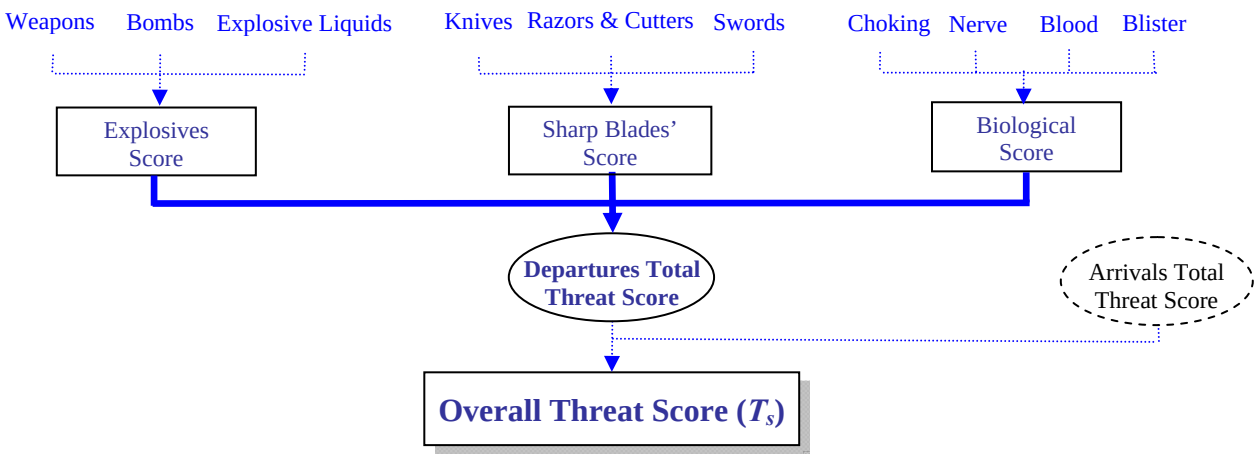


Figure 3.3: Scoring Scheme for calculating the threat to PCBSS

Vulnerability

The basic concept introduced in this research is to assess the vulnerability of each threat type separately based on extending the Wilson and Roe (2006) approach (Equation 2.2 in Chapter 2). Figure 3.4 shows the extension of the approach for each component separately: passengers (P), cabin baggage (B), and checked-in luggage (L). Therefore, the first step was to build a database of a variety of security measures (devices/equipment/measures) and along with their reliability in detecting various types of threats. The analysis can then consider the probability of the threat not being detected through multiple checkpoints. Because checkpoints (SCP*js*) within a subsystem, i.e., departures or arrivals at a specific terminal, have different equipment (measures) that considers either passengers, luggage, or baggage, consider the measures that screen passengers in this subsystem can be considered as $p_1, p_2, \ldots, P$, those that screen cabin baggage as $b_1, b_2, \ldots, B$, and those that screen luggage as $l_1, l_2, \ldots, L$. Therefore, the vulnerability of measures for passengers, for example, is the probability of not detecting a specific type of threat t while the passengers (p) are passing through all security checkpoints SCP_1, SCP_2 and SCP_j in the subsystem under consideration. Therefore, the total vulnerability with respect to passengers (V_{tp})

in any subsystem can be calculated as follows:

$$V_{tp} = 5 \times \left[\prod_{i=1}^{P} (1 - R_{tpi}) \right] \quad \textbf{3.5}$$

Where V_{tp} is the vulnerability of the passengers measures to threat type t in a subsystem j
R_{tpi} is the reliability of the passenger measure i for detecting threat type t
P is the number of passengers measures for detecting threat type t
t is the threat type t

Similarly, the vulnerability of security checkpoints ($SCP_1, \ldots, SCP_j$) with respect to cabin baggage is as follows:

$$V_{tb} = 5 \times \left[\prod_{i=1}^{B} (1 - R_{tbi}) \right] \quad \textbf{3.6}$$

Where V_{tb} is the vulnerability of the cabin baggage measures to threat type t in a subsystem j,
R_{tbi} is the reliability of the passenger measure i for detecting threat type t,
B is the number of cabin baggage measures for detecting threat type t,
t is the threat type t

Likewise, the vulnerability of security check point ($SCP_1, \ldots, SCP_j$) with respect to checked-in luggage is as follows:

$$V_{tl} = 5 \times \left[\prod_{i=1}^{L} (1 - R_{tli}) \right] \quad 3.7$$

Where V_{tl} is the vulnerability of the checked-in luggage measures to threat type t in a subsystem j
R_{tli} is the reliability of the passenger measure i for detecting threat type t
L is the number of cabin checked-in luggage measures for detecting threat type t
t is the threat type t

Consequently, the overall vulnerability V_t of any subsystem (either departures or arrivals) to threat type t is as follows:

$$V_t = \frac{V_{tp} + V_{tb} + V_{tl}}{3} \quad 3.8$$

Based on Equations 3.5 to 3.8, the vulnerability of the overall system to threat type t (SV_t) can be expressed by considering all the total average of all k subsystems, as follows:

$$SV_t = \frac{\sum_{k=1}^{K} V_{t_k}}{K} \quad \textbf{3.9}$$

Accordingly, when all threat types are considered, the overall vulnerability of the system (V_s) can be expressed as follows:

$$V_s = \frac{\sum_{t=1}^{T} SV_t}{T} \qquad \textbf{3.10}$$

where T is the total number of threats in all threat categories

The overall vulnerability of the PCBSS to a single threat type and to multiple threats is illustrated in Figure 3.4.

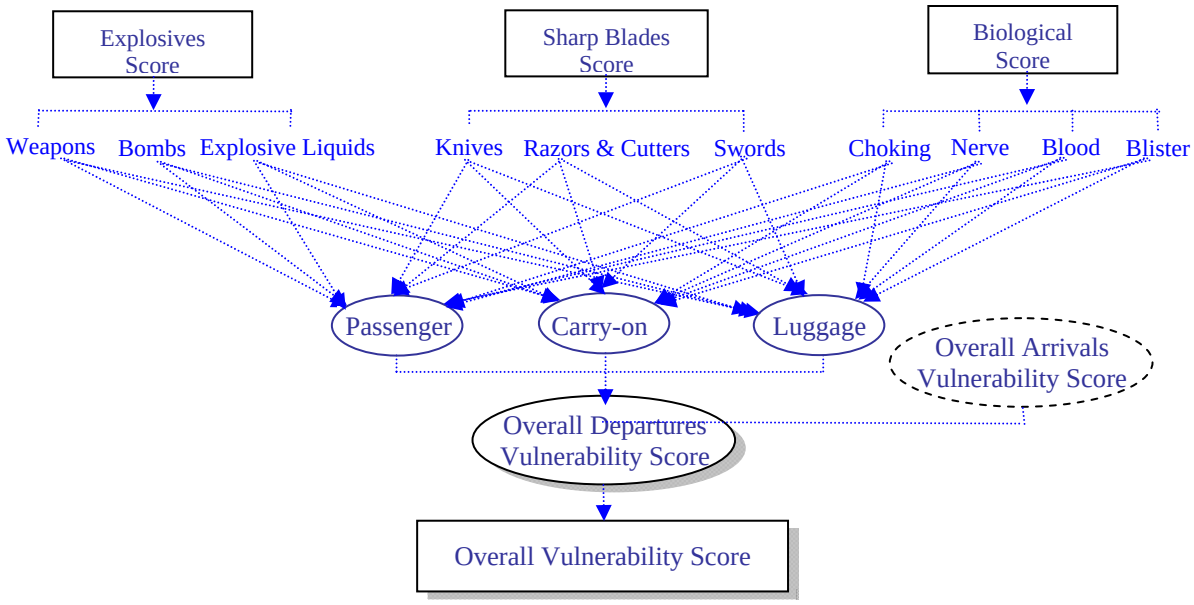


Figure 3.4: PCBSS Vulnerability Scoring Scheme

Consequence Analysis

Depending on its specific characteristics, each threat type *t* has a specific level of consequence for each of the four types of consequence (casualties, downtime, exposure, total loss). For example, a high "knives" threat is expected to have significantly fewer casualties than even a very low "bombs" threat. Therefore, the assessment of consequences must be appropriate for each type of threat. The overall system consequence C_s can then be averaged in hierarchical

order at the system level, as follows:

$$C_s = \frac{\sum_{t=1}^{T} \sum_{i=1}^{Cc} w_i \times C_{ti}}{T \times Cc} \qquad \textbf{3.11}$$

where C_{ti} is user input of the consequence of threat t in consequence category i
W_i is the weight (importance) of the consequence category i
Cc_i is number of the consequence categories
T is number of threat types in all threat categories

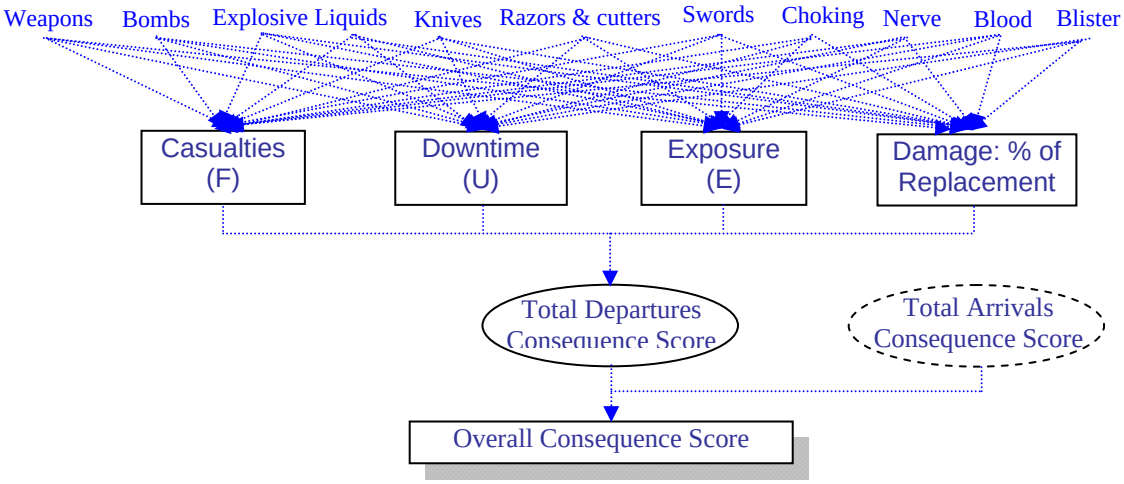


Figure 3.5: PCBSS Consequence Scoring Scheme

Security Risk Index

Based on Equation 3.3, security risk indexes (SRIs) are calculated separately at the level of a single threat type *t* for passengers, cabin baggage, and check-in luggage, and then the overall security risk index for all *t* are averaged for the subsystem and system levels. For example, the security risk index of the threat type *t* with respect to passengers at all checkpoints SCP_1, SCP_2, and SCP_j is the total SRI_{jtp} in a subsystem, which can be calculated using as follows:

$$SRI_{jtp} = [\prod_{j=1}^{J} V_{jtp}] \times T_s \times C_s \qquad \textbf{3.12}$$

where SRI_{jtp} is the SRI of all threat types *t* with respect to passengers at all SCPs (J) in a subsystem
T_s is the overall system-level threat
C_s is the overall system-level consequence

Similarly, the SRI of the security checkpoints ($SCP_1, \ldots, SCP_j$) with respect to cabin baggage can expressed simply, as follows:

$$SRI_{jtb} = [\prod_{j=1}^{J} V_{jtb}] \times T_s \times C_s \quad \textbf{3.13}$$

where SRI_{jtb} is the SRI of all threat types t with respect to cabin baggage at all SCPs (J) in a subsystem
T_s is the overall system-level threat
C_s is the overall system-level consequence

Likewise, the SRI of security checkpoint ($SCP_1, \ldots, SCP_j$) with respect to checked-in luggage is expressed as follows:

$$SRI_{jtl} = [\prod_{j=1}^{J} V_{jtl}] \times T_s \times C_s \quad \textbf{3.14}$$

Where SRI_{jtl} is the SRI of all threat types t with respect to luggage at all SCPs (J) in a subsystem
T_s is the overall system-level threat
C_s is the overall system-level consequence

Consequently, the overall SRI of the k^{th} subsystem (either departures or arrivals) of the PCBSS at an airport terminal towards t^{th} threat type is as follows:

$$SRI_{tk} = \frac{SRI_{tp} \times SRI_{tb} \times SRI_{tl}}{3} \quad \textbf{3.15}$$

Based on Equations 3.12 to 3.15, the SRI for the overall system with respect to t^{th} threat type can be expressed as follows:

$$SRI_t = \frac{\sum_{k=1}^{K} SRI_{tk}}{K} \quad \textbf{3.16}$$

where SRI_{tk} is the overall SRI of a subsystem k with respect to threat type t

Accordingly, the SRI for the overall system with respect to all T threat types can be expressed as follows:

$$SRI_s = \frac{\sum_{t=1}^{T} SRI_t}{T} \quad \textbf{3.17}$$

where SRI_s is overall SRI of the s^{th} security system for all threat categories
SRI_t is the overall SRI of s^{th} system for threat type t

Once the overall SRIs are calculated for each of the airport's security systems, and based on the hierarchical summation of the SRI for an i^{th} airport proposed by Berbash et al. (2008), an SRI calculation map (Figure 3.6) can be developed, and the overall SRI for the airport can be computed, as follows:

$$SRI = \frac{\sum_{s=1}^{S} SRI_s}{S} \quad \textbf{3.18}$$

where SRI is the security risk index of the airport
SRI_s is the security risk index of S security system

Among the advantages of the SRI is the fact that it can be used to identify overall improvements in security risk mitigation, which is defined in this research as the Security Upgrade Benefit (B_{su}). The B_{su} can be determined by computing the difference between the initial SRI before the system is upgraded and SRI after the system is upgraded, as shown in Equation 3.19. The B_{su} can be useful as a measure for comparing upgrade decisions.

$$B_{su} = SRI_{upgrade} - SRI_{baseline} \quad \textbf{3.19}$$

3.4.5 Using the Security Metric

Based on the rating criteria for threat, vulnerability, and consequence assessment, as were illustrated in Tables 3.1 through 3.3 respectively, the metric assigns a score from 0-5 that corresponds to each level of assessed threat, vulnerability, and consequence. Different overall of security risk index (S*RI*) scores for an airport represent unique scenarios for combinations of threat, vulnerability, and consequences. As a result, the respective lower and upper limits of a security risk index for an airport are 0, which means no security risk exists, or 1×1×1=1, which is the lowest level, and 5×5×5=125, which is the highest level. Table 3.7 shows the basis on which the overall security risks index categories and their associated levels should be interpreted nd the categories into which security risk assessment scenarios will fall.

Table 3.7: SRI Categories and their Levels

Score	Category
0 - 5	Acceptable
6 - 25	Very Low
26 - 50	Low
51 - 75	Medium
76 - 100	High
101 - 125	Very High

Furthermore, according to the extended Veatch et al. (1999), Tzannatos (2003) and API/NPRA (2004) approaches, one of the essential milestones in security management is to establish an adequate SRI score, which is in fact, the acceptable risk level, after all possible mitigation measures have been applied based on different risk scenarios. The acceptable risk level for this research is defined to be within the “Acceptable” category, as illustrated in Table 3.7, which quantitatively means that the SRI score ranges from 0 to 5. It should be noted that airports are subject to diverse threat categories and types; therefore, the acceptable security risk index range (0-5) differs from one airport to another because the assessment of risk can be subject to the absolute evaluation of security officials in each individual airport.

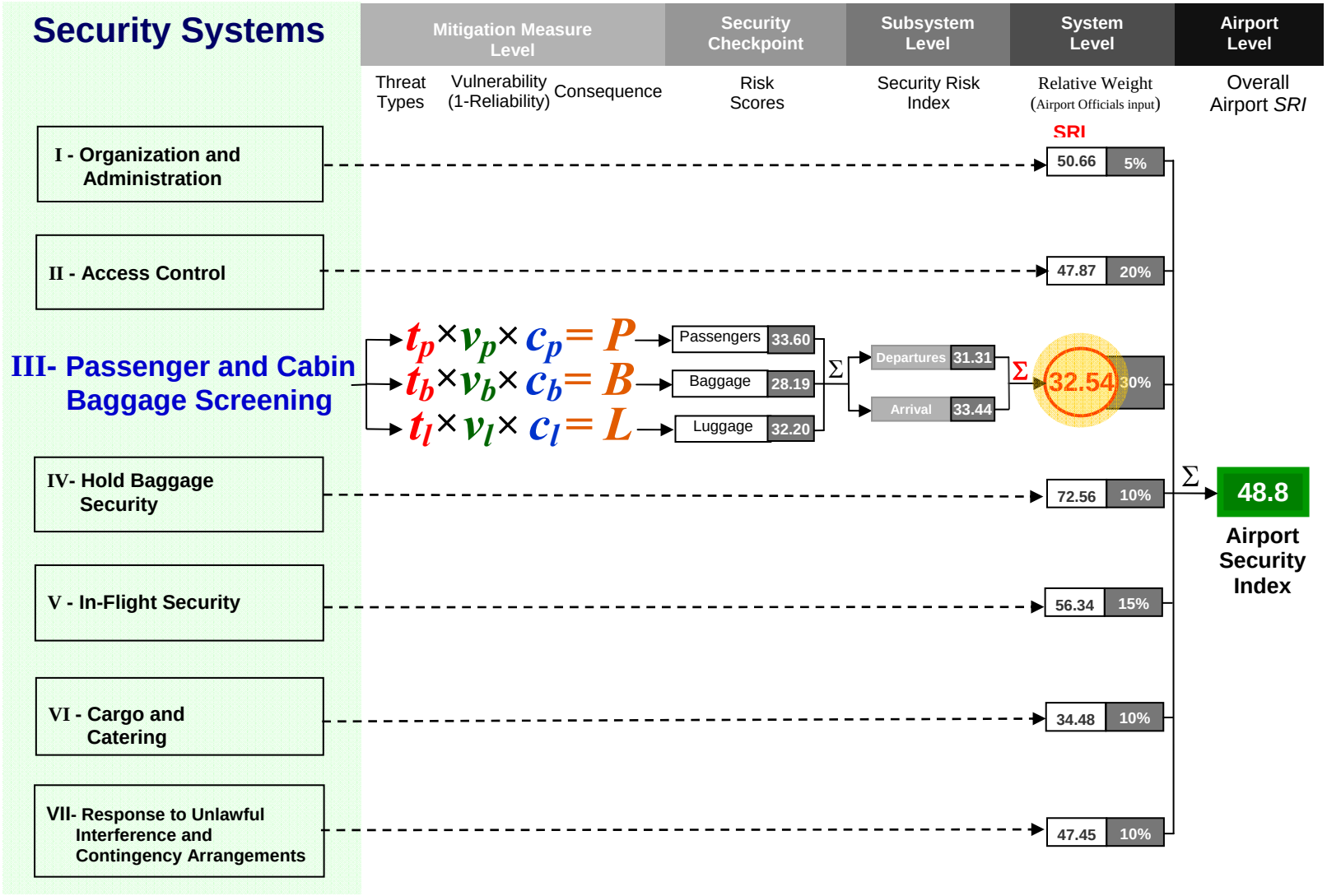


Figure 3.6: SRI Calculation Map for the Subsystem, System, and Airport Levels

The SRI score represents possible outcomes of the assessment of threat, vulnerability, and consequence. In terms of threat status, vulnerability status, and consequences, the assessment can be interpreted as the number of fatalities, the hours of downtime, the amount of public exposure, and the dollar value of physical damage (percentage of the total replacement cost). For example, if the overall SRI score for an airport is 67, according to Table 3.7, the score falls within the "Medium" category (51-75). Table 3.8 interprets the score of 67 based on the threat, vulnerability, and consequence rating criteria listed in Tables 3.1 through 3.3 respectively, and on the extended approaches of Veatch et al. (1999), Tzannatos (2003) and API/NPRA (2004).

Table 3.8: Example of SRI Interpretation

Score	Threat	Vulnerability	Consequence			
			Casualties No.	Downtime	Exposure	Loss %
67	Attacks are likely to be limited by attacker expertise, resources, or opportunity	Attacker with moderate levels of resource and skill could be expected to exploit the vulnerabilities identified	1 – 10 Fatalities / multiple injuries	> 8 – 16 hours of asset closing/ interruption	Potential litigation	Total damage valued at 25% - 50% of asset replacement

3.5 Summary

Among the vital features of the newly developed security risk metric presented here is the SRI for the passenger and cabin baggage system, which is one of the most important security systems at airport terminals. The SRI with respect to passengers, cabin baggage, and checked-in luggage is calculated by assessing the three dimensions of security risk: threats, vulnerabilities, and consequences. As a quantitative measure, the SRI helps airport security officials acquire deep risk-based insight into the security status of their airports, to evaluate the level of security improvement needed, and to obtain a solid reference for prioritizing the potential upgrades. In addition, once a security risk metric have been developed for all airport security systems, the SRI will enable airport authorities to make comparisons between components of security subsystems,

subsystems, and complete systems at both the single and multiple terminal levels. The developed security metric can be extended to multiple systems at a single airport and also to multiple airports. As presented in the next chapter, the SRI has also been further utilized in order to develop an automated airport security upgrade decision support system. This system enables security officials to obtain a better understanding of the different levels of upgrades for each security system along with their implications in terms of cost savings, improvements in the effectiveness of their security systems, and the overall enhancement of airport performance.

CHAPTER 4
DECISION SUPORT SYSTEM FOR AIRPORT SECURITY UPGRADES

4.1 Introduction

Many policy and decision makers advocate using a risk methodology for security assessment (Dillon et al., 2009). In this chapter, a risk-based approach is presented as the basis for the development of a decision support framework for upgrading the security measures for airport passenger and cabin baggage screening system (PCBSS). The framework uses the security risk metric described in Chapter 3 in order to assess the security deficiencies in existing systems at international passenger terminals. Based on a detailed database that inventories the probability of security measure(s), device(s), and equipment, detecting each threat type, the framework optimizes the most cost-effective upgrade strategy.

4.2 Proposed Framework

The main components of the proposed framework for upgrading the security systems in airports as shown in Figure 4.1, are as follows:

1. Analysis models that include a new security assessment model based on the security metric described in Chapter 3 and an upgrade options model for defining the cost and performance of security countermeasures

2. A decision support module, which is basically a cost-optimization model for prioritizing upgrade actions, and considering practical constraints and performance requirements

In the next sections, each of these components is discussed in more detail relative to a PCBSS.

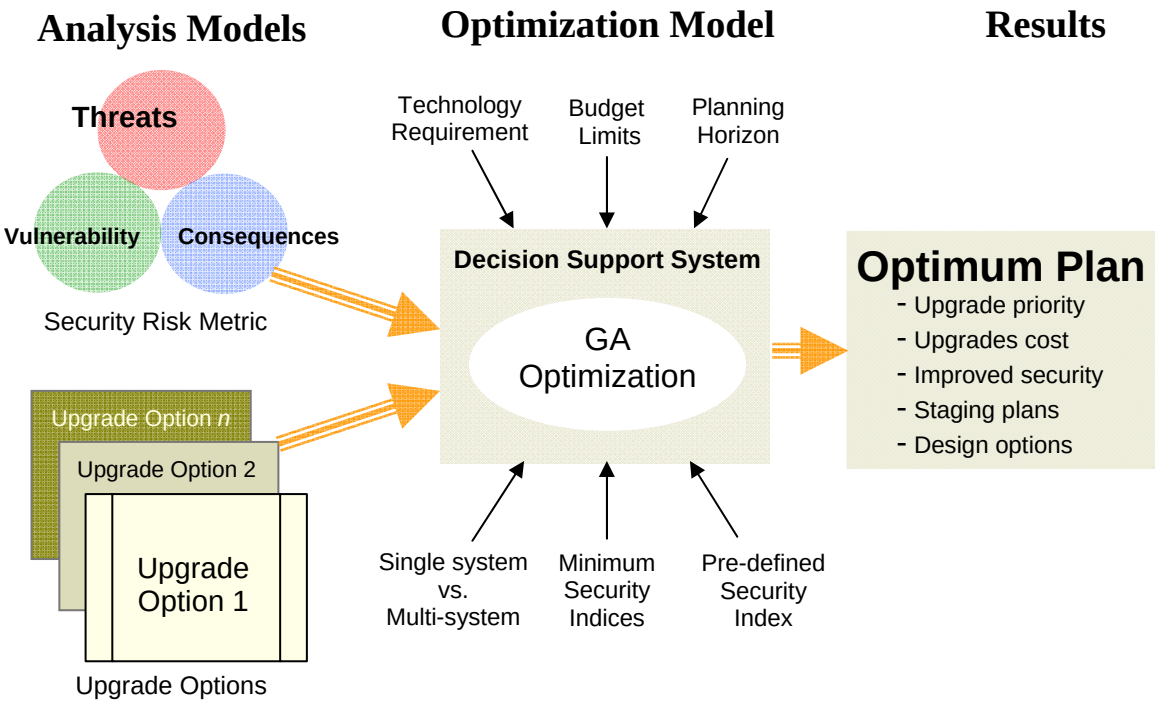


Figure 4.1: The Conceptual Decision Support System Framework

4.3 Analysis Models

4.3.1 Implementing the Security Risk Metric

The security risk metric is an assessment tool for facilitating data collection with respect to the three security risk dimensions of the PCBSS: threats, vulnerabilities, and consequences. The assessment tool applies the criteria listed in Tables 3.1 through 3.3, and Equations 3.3 through 3.13. The assessment of the threats, vulnerabilities, and consequences was implemented using MS Excel spreadsheets. The spreadsheet models a hypothetical example of an airport terminal, with security checkpoints in the departures and arrivals subsystems (directions) in any airport configuration. The spreadsheets implemented and the analysis metric calculations are described briefly in the following sections.

Threat Assessment Spreadsheet

The user can select each airport terminal separately and can enter data with respect to the three main threat categories along with their types (Figure 4.2). This process is followed for all terminals in the departures and arrivals subsystems. The user has the ability to complete the assessment using the drop-down menus to choose one of six levels in order to define the level of each threat type for both departures and arrivals directions. Then, in real time, the metric spreadsheet calculates the threat scores using a central tendency measure (arithmetic mean) to produce indices for each threat type (PCBSS subsystem component), category (PCBSS subsystem: departures or arrivals), and terminal (PCBSS system). The metric also automatically provides a brief description of the overall threat assessment for the terminal under investigation, based on criteria listed in Table 3.1, as shown in Figure 4.2.

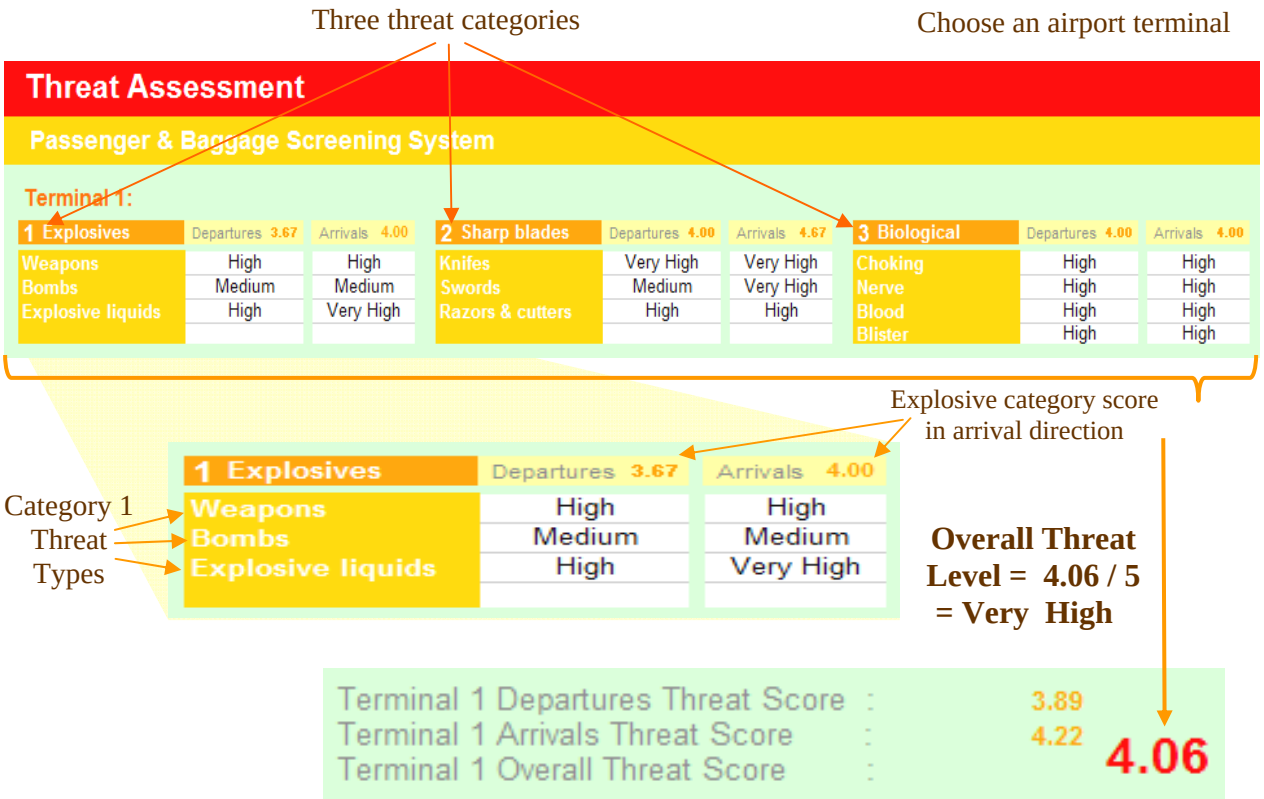


Figure 4.2: Threat Assessment Spreadsheet for Terminal 1

For the example shown in Figure 4.2, the overall threat risk score is 4.06 out of 5. According to the criteria used, the level is classified as very high, which means that "a credible threat exists against the airport assets, so that continuous or intensive attacks are likely to occur and that the adversary demonstrates the capability and intent to launch an attack targeting the airport or one of its assets on a frequently occurring basis, and specialized security advice should be sought." If the score was less than 4, then the threat risk is the high level, which means a relatively lower level of threat.

Vulnerability Assessment Spreadsheet

The vulnerability PCBSS can be assessed based on the reliability of the existing measures in detecting potential threats. To facilitate the assessment, the PCBSS is divided into subsystems (Departures and Arrivals), which are further split into a number of security checkpoints (SCPs). Each SCP incorporates a number of mitigation measures (devices, equipment, and measures) that designed to detect, deter, mitigate, or defend against adversary attacks. Therefore, based on from security experts inputs with respect to the reliability of detecting detect threat types (the effectiveness of the measure in detecting threat types), who rated them on a scale from 0 (N/A) to 1 (very high), a comprehensive measures database was built in order to store probabilities, technical information, and cost data associated with each measure. A sample of the database is shown in Figure 4.3.

The database includes the probabilities of detection associated with most accredited measures in terms of equipment, devices, and measures that scan passengers, cabin baggage, and checked-in luggage. The database inventories the measures of mitigation according to the type of the

measure, technology used, and usage; the reliability of the measure for detecting different threats types; and the associated cost of a single measure or combinations of measures.

Database of Detection Probabilities & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Avg.	Probability that Security Device(s) will Detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Singular Cost
	Ray Scanner Devices & Measures												
1	N/A	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0
2	Metal Detector Gate (PMD2/PTZ) + Operator	42%	85%	50%	0%	95%	95%	95%	0%	0%	0%	0%	44,000
3	Metal Detection Gate+ 1 Guard	44%	86%	60%	0%	97%	97%	97%	0%	0%	0%	0%	84,000
4	Metal Detection Gate + Hand-held Metal Detelctors	45%	87%	70%	0%	97%	97%	97%	0%	0%	0%	0%	44,240
5	Metal Detection Gate + 1 Guard + Hand-held Explosive Trace Detectors	57%	90%	95%	95%	97%	97%	97%	0%	0%	0%	0%	67,000
6	Metal Detection Gate + 1 Guard + DeskTop Explosive Trace Detectors	57%	90%	95%	95%	95%	97%	97%	0%	0%	0%	0%	85,500
7	Metal Detection Gate + 1 Guard + Hand-held Metal Detectors + 1 Physical Search Guard + Sniffing Dog	69%	90%	95%	95%	95%	97%	97%	30%	30%	30%	30%	84,240
8	Metal Detection Gate+ 1 Guard + Hand-held Explosive Trace Detectors + 1 Physical Search Guard + Sniffing Dogs	69%	90%	95%	95%	97%	97%	97%	30%	30%	30%	30%	107,000
9	Metal Detection Gate + 1 Guard + Desktop Explosive Trace Detectors + 1 Physical Search Guard + Sniffing Dogs	69%	90%	95%	95%	95%	97%	97%	30%	30%	30%	30%	125,500
10	Metal Detection Gate + 1 Guard + Desktop Explosive Trace Detectors + 1 Physical Search Guard + Sniffing dogs + Biological Agent Detector	93%	90%	95%	95%	95%	97%	97%	95%	90%	90%	90%	148,500

Figure 4.3: Sample from the Database of the Reliability and Cost Information of the Security Measures

To enable a vulnerability assessment of the i^{th} measure at the j^{th} SCP in the k^{th} subsystem in the s^{th} system, the metric presents data in a hierarchical order that allows the user to assess their vulnerabilities and consequent vulnerability scores both separately and simultaneously.

Accordingly, as shown in Figure 4.4 once the user identifies all i measures at each of j SCPs, the vulnerability spreadsheet retrieves their corresponding levels of detection reliability from the database and calculates the vulnerability scores for each i^{th} measure with respect to passengers, cabin baggage, and checked-in luggage. Based on Equations 3.6 to 3.11, the spread sheet, calculates the vulnerability of all t^{h} threat types towards all SCPs for all k^{th} subsystems at the

PCBSS levels. As the user enters the in-place measures, the metric displays simultaneously the corresponding current vulnerability scores for individual or all passenger, cabin baggage, and checked-in luggage measures; departure, arrival, and PCBSS levels; and the corresponding SRI for these levels. For the example shown in Figure 4.4, the vulnerability score of the PCBSS is 3.63, which means that the system's level of vulnerability is between 3 and 4, or, according to Table 3.2, at the high level.

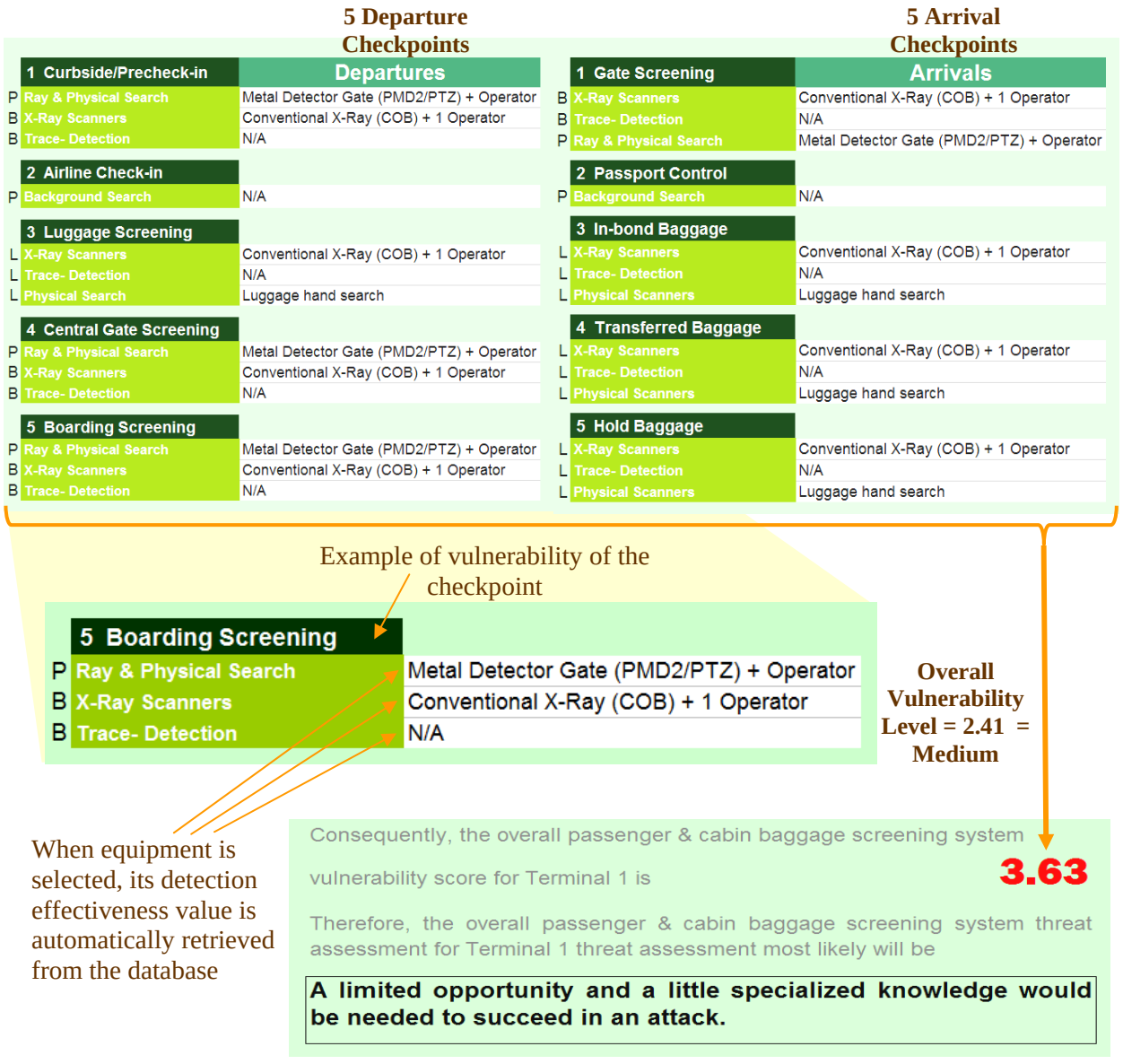


Figure 4.4: Vulnerability Assessment Spreadsheet

The interpretation of this score is that “a credible threat exists against the airport assets based on knowledge of the adversary's capability and intent to attack the airport assets, which involve high levels of expertise, resources, and support and based on related incidents having taken place at similar airports or in similar situations.” The metric thus provides a comprehensive assessment of vulnerability at a terminal’s departures, arrivals, and PCBSS levels. As well, once all other airport systems have been assessed, the metric automatically calculates the overall SRI for the airport and predicts the most applicable vulnerability status.

Consequence Assessment Spreadsheet

As shown in Figure 4.5, each threat type under each threat category has consequence associated with cases in which an adversary succeeds in exploiting the current vulnerabilities. Therefore, a database was developed in order to define the consequences of each level of each threat type in terms of the four main categories of consequences: casualties, downtime, exposure, and damage value. Once the user determines the level of each type of threat, the Excel functions automatically retrieve from the database the corresponding detailed consequences: how many casualties would be expected, for how long the terminal will be shut down, what the level of public exposure might be, and what percentage of damage to the terminal building is expected. The metric then calculates simultaneously encountered consequence scores for every category at the departures, arrivals, and terminal levels. For the example shown Figure 4.4, the SRI for the PCBSS is 2.58, which means that the system’s level of consequence is below 3, or according to Table 3.3, at the medium level. The interpretation of this score is that “fatalities range from 11 - 25 people; the terminal downtime would be between 16 and 24 hours, potential litigation is to be implemented, and damage would be a maximum of 25-50% of the total terminal replacement cost.”

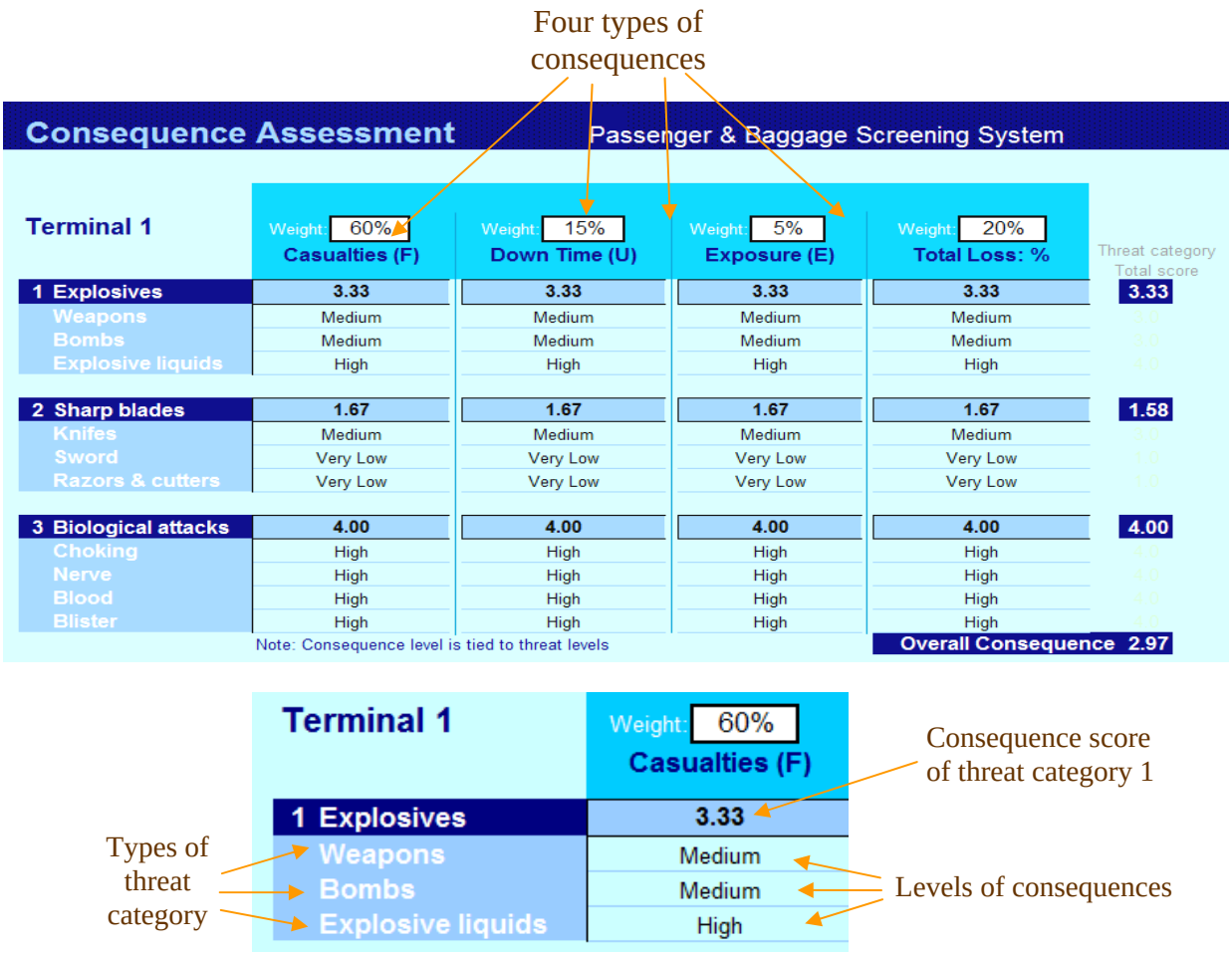


Figure 4.5: Consequence Assessment Spreadsheet

Once all data are input, the metric calculates the SRI based on Equation 3.9. Since the acceptable SRI is defined, according to Table 3.7, the SRI score ranges from 0 to 5. In other words, any SRI score above 5 will require the application of the countermeasures necessary to mitigate the risk and maintain it at an acceptable level, that is, less than or equal to 5. This stage is very important since implementing security upgrades, is in fact, a trade-off between benefit/cost and the mitigated level of risk. Hence, a defined threshold should always be set up initially before any security risk assessment is begun, and before mitigation alternatives and their associated benefit/cost ratios are determined and loaded into the background of the framework.

Based on Berbash et al. (2008), the aggregated SRI and its hierarchical summation for an i^{th} airport can also be used for further analysis and to develop a framework for decision support strategies related to cost-effective security upgrades for other security systems at the airport level. This concept is explained through a hypothetical summary of the threats, vulnerabilities, and consequences for the PCBSS at two airport terminals as shown in Table 4.1. As well, once all other airport systems have been assessed and their scores determined, the metric automatically calculates a total SRI for the airport, as shown in Figure 3.6.

Table 4.1: SRI Summary for Terminals 1 and 2

	Terminal 1	Terminal 2
Threat	4.06	4.65
Vulnerability	2.41	2.57
Consequence	3.33	3.78
Terminal's Security Risk Index (SRI)	**32.54**	**45.23**
Overall Security Risk Index (SRI)	**38.89**	

4.3.2 Security Upgrade Model

The framework's second model (Figure 4.1) is a security upgrade options model. To offer a wide range of flexible options, the developed upgrade options model uses all mitigation measures stored in the database and their associated reliability and cost data. For the purposed of this research, the cost includes only the capital investment plus total operating expenses for one year. However, the model is designed to be easily extended to consider multiple years, in two-year or three-year slices. In the developed model, the costs are expressed in terms of unit cost of the device or measure, based on the nature of the system or the systems component(s) or on the percentage of complete substitution of the system required or the replacement of some of its main functional components. Using the database inventory of measures, the GA-based

optimization model generates and tests different sets and combinations of sets of mitigation alternatives, in order to arrive to the most cost-effective upgrade scenario. In extreme cases, more or fewer mitigation alternatives can be considered. Table 4.2 illustrates the calculation of an example of output from the upgrade options model. The security benefit is defined as the mitigation enhancement achieved by each mitigation alternative or combination of alternatives, which ranges in value from 0 to 1.00 (i.e., 0 % to 100 %).

Table 4.2: of Enhancement Values for Determining the Effect of Upgrade Decisions

Existing Device/Measure	Effectiveness	Device/Measure	Effectiveness	Improvement
Metal Detector Gate	42 %	Dielectric Portal+1 Guard + Desktop Explosive Trace Detectors	56.1 %	56.1 % – 42 % = 0.14

Based on Table 4.2, it is possible to establish a Security Upgrade Benefit (B_{su}), the general form is represented as follows:

$$B_{su} = SRI_{\,after\ upgrade} - SRI_{\,before\ upgrade} \qquad \textbf{4.1}$$

where B_{su} is the security upgrade benefit for the PCBSS

Structure of the Security Upgrade Model

When studying security upgrade options, decision makers are often faced with many challenges and constraints that must be considered in the decision-making process:

1. Technology-level requirements and the compatibility of upgrades with existing systems
2. Preferences of airport officials for a desired SRI level
3. Preset priorities (security level) of some systems, subsystems, or subsystem components
4. Allowable yearly expenditures

The developed security upgrade model is structured to help a decision maker search for the most cost-effective upgrade strategy (upgrade type, level of upgrade, priority of upgrade, etc.) among the feasible upgrading scenarios (combinations of mitigation alternatives). The model incorporates the output from the Security Risk Metric (presented in Chapter 3) as well as the upgrade options.

An additional consideration is the fact that in practice, vulnerability is the most controllable risk dimension. Thus, once a terminal's baseline SRI is determined, the security upgrade model, which is based on the specific security needs and constraints set by the security officials, enables decision makers to execute detailed "what-if" analysis scenarios, and to justify scenarios that have an SRI less than or equal to the acceptable level and that satisfy all needs and constraints.

The advantage of the framework is that its security upgrade model uses the SRIs produced by the security metric; thus, different subsystem components, subsystems, systems, and airport terminals can be compared and prioritized according to specific criteria. Therefore, when adjusting any vulnerability level, meaning changing the type of one or more screening devices, piece of equipment, or measures, as a result, mitigation alternatives are then revised and a corresponding cost-effective upgrade plan is calculated accordingly.

For practicality and simplicity, the framework was modeled in a MS Excel spreadsheet using hypothetical data (though the model was partially validated through the used of data supplied by the management of an international airport, as presented in the next chapter).

Figure 4.6 shows a screen shot of the model's MS Excel spreadsheet for the PCBSS. SCPs in both directions (departures and arrivals) are on the far left in column C; column D lists all the security checkpoints in both subsystems; column G indicates the type of existing

countermeasures, whose index numbers are shown in column I; columns H and M indicate the suggested upgrade mitigation measure and their index numbers; the reliability of existing measures is shown in column J; the indexes for the upgrade options (decision variables) are shown in column L; and columns O and Q show upgraded reliability and cost calculations, respectively.

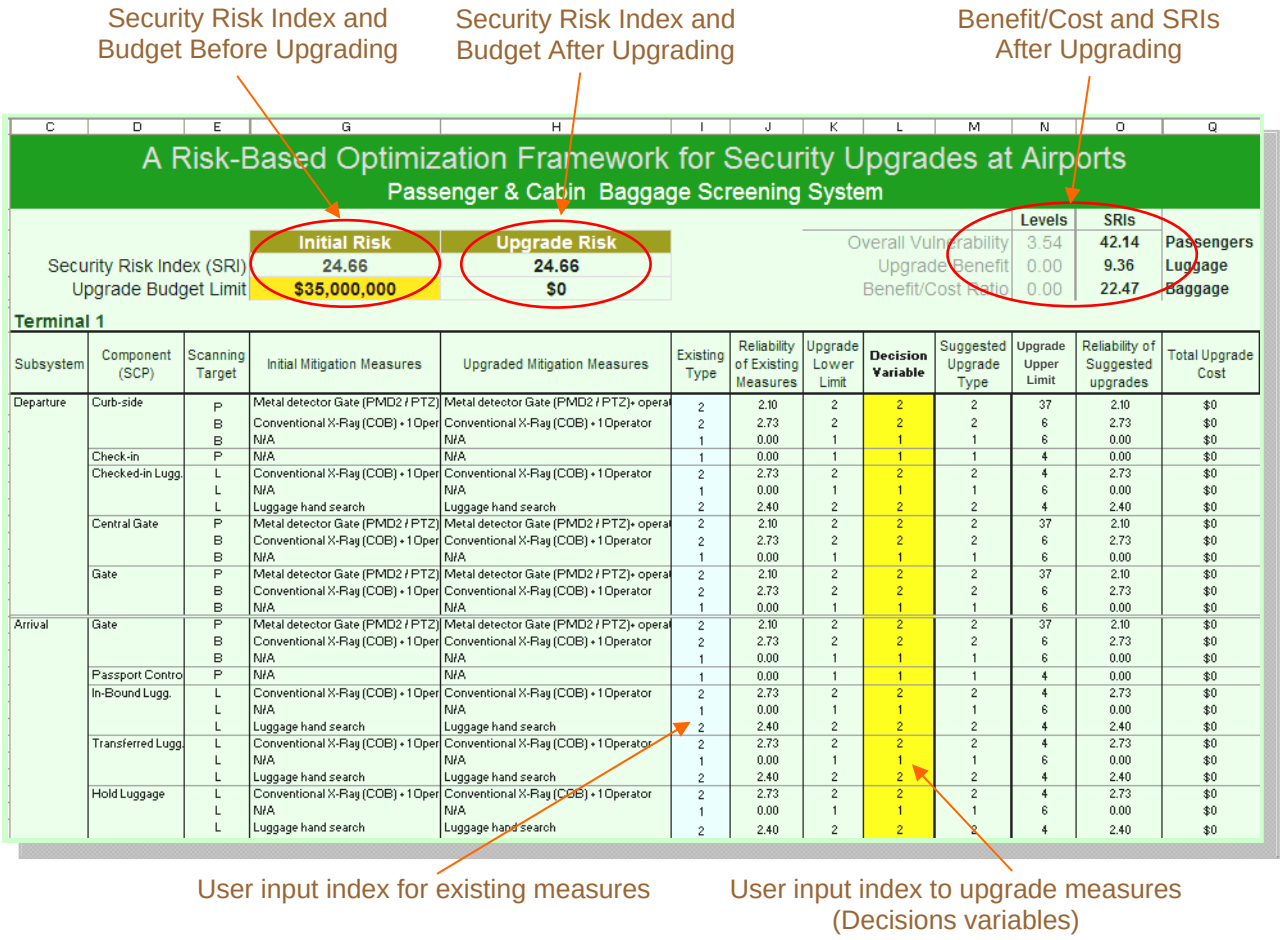


Figure 4.6: Model Formulation (Terminal 1 PCBSS)

The top part of the spreadsheet also shows the overall upgrade vulnerability score; overall security risk indices (before and after); detailed security risk indices for passengers, cabin baggage, and checked-in luggage; the budget limit; total upgrade costs; the upgrade benefit; and the total benefit-cost ratio.

4.4 Decision Optimization

To examine the functionality of the framework, the module was initially run using hypothetical data at the PCBSS level, including screening checkpoints in both directions (departure and arrival), as well as the cost of each upgrade decision option, as shown in the example presented in Figure 4.3. To validate the developed framework theoretically, the decision support module was tested with three different methods of solving the upgrade problem in order to search for the optimum cost-effective upgrading strategy. The three methods were a simple ranking method, such as manual priority ranking; a mathematical optimization technique, such as the linear technique; and a non-traditional optimization technique, such as genetic algorithms (GAs). The optimum strategy identifies two main types of output: the specific type of upgrade decision and the associated cost of the upgrades.

4.4.1 Priority-Based Ranking Method

The priority-based ranking method uses the new security risk metric database (i.e., the reliability indexes), to calculate an upgrade decision priority index, indicated in column P in Figure 4.7, for each security measure at all SCPs and subsystem levels. The priority index for a security measure PIi is determined by calculating the difference between 5 and its initial reliability index (Ri), as follows:

$$PI_i = \left(5 - initial\ R_i \right) \qquad \textbf{4.2}$$

The assumed criterion is that the i^{th} measure at the j^{th} SCP that has the highest priority index should be upgraded first, followed by the others in descending order, and so on. Therefore, the first step is the calculation of the priority index for every i^{th} measure at the j^{th} SCP for both the departure and arrival subsystems and the second step is to sort all PIs and rank them in descending order, as shown in column P in Figure 4.7 the priority index.

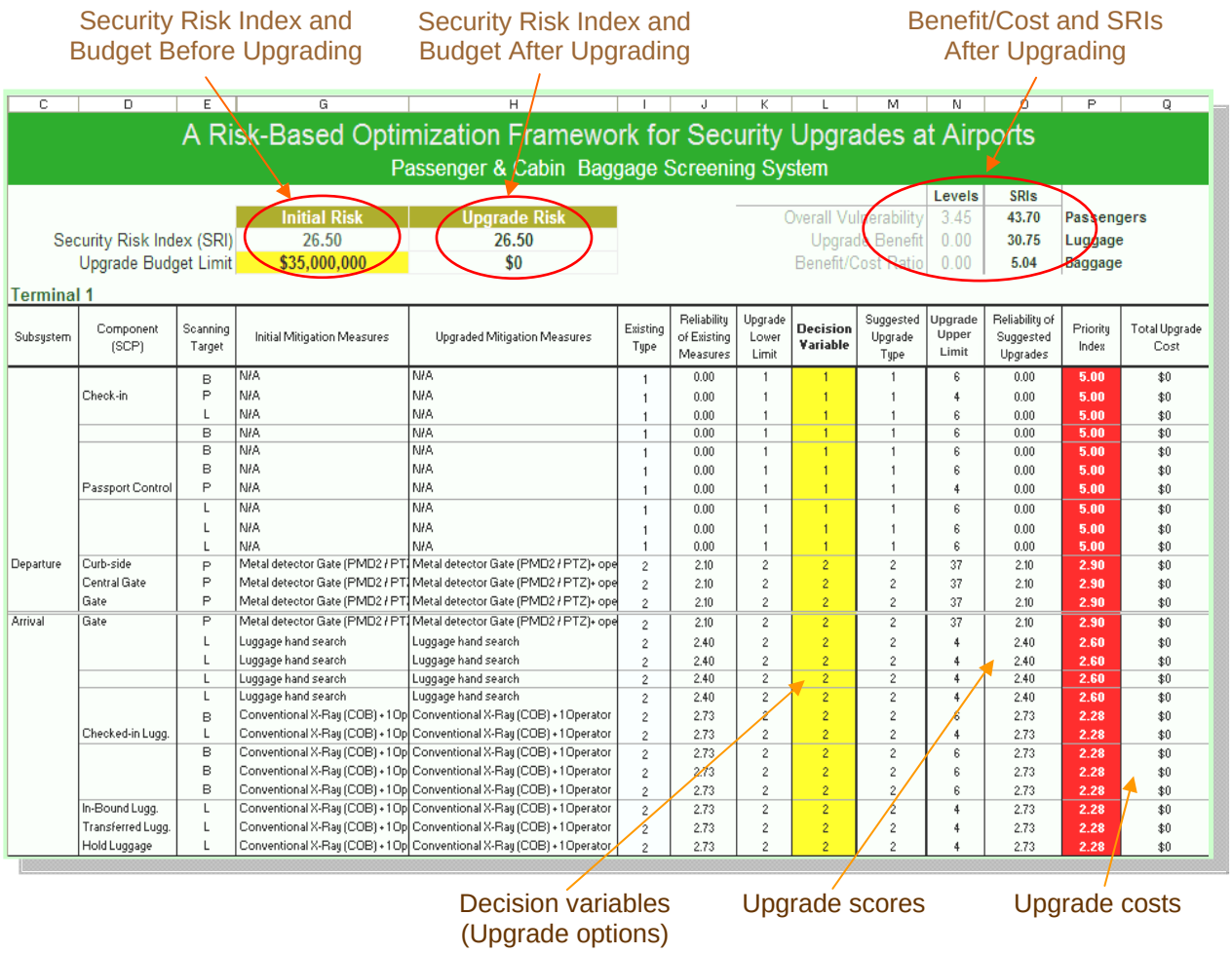
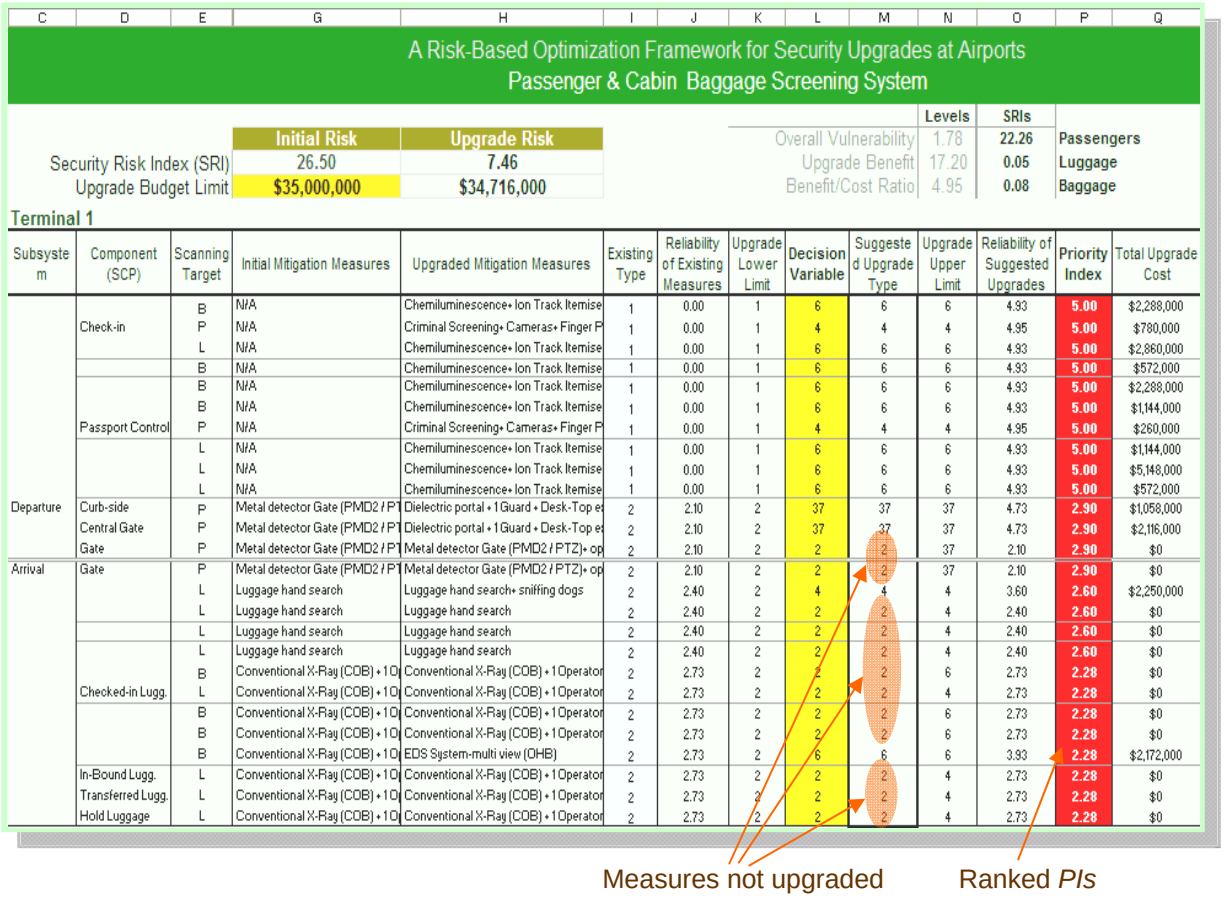


Figure 4.7: Security Checkpoints Ordered According to Priority

The lowest priority index shown in Figure 4.7, is 2.28. Since the upgrade plan is for one year only, the subsystem components that have a PI=5 will be upgraded with the mitigation measures that have the highest score, and then those with a PI< 5 will be upgraded as long as the allowable upgrade budget limitations are met. When budget constraints are about to exceeded the limitations, and some eligible measures remain to be upgraded, those measures will be upgraded. As can be seen in the example shown in Figure 4.8, the total allowable upgrade budget is $35,000,000 and the initial SRI = 26.50. The results of applying the priority index (*PI*) approach are as follows: the SRI achieved was 7.46, which reflects a significant improvement in the

security level; however, the approach did not succeed in upgrading all measures. Due to budget limitations, this manual solution left six measures not upgraded.



A Risk-Based Optimization Framework for Security Upgrades at Airports
Passenger & Cabin Baggage Screening System

	Initial Risk	Upgrade Risk
Security Risk Index (SRI)	26.50	7.46
Upgrade Budget Limit	$35,000,000	$34,716,000

	Levels	SRIs	
Overall Vulnerability	1.78	22.26	Passengers
Upgrade Benefit	17.20	0.05	Luggage
Benefit/Cost Ratio	4.95	0.08	Baggage

Terminal 1

Subsystem	Component (SCP)	Scanning Target	Initial Mitigation Measures	Upgraded Mitigation Measures	Existing Type	Reliability of Existing Measures	Upgrade Lower Limit	Decision Variable	Suggested Upgrade Type	Upgrade Upper Limit	Reliability of Suggested Upgrades	Priority Index	Total Upgrade Cost
		B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$2,288,000
	Check-in	P	N/A	Criminal Screening+ Cameras+ Finger P	1	0.00	1	4	4	4	4.95	5.00	$780,000
		L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$2,860,000
		B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$572,000
		B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$2,288,000
		B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$1,144,000
	Passport Control	P	N/A	Criminal Screening+ Cameras+ Finger P	1	0.00	1	4	4	4	4.95	5.00	$260,000
		L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$1,144,000
		L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$5,148,000
		L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$572,000
Departure	Curb-side	P	Metal detector Gate (PMD2 / PT	Dielectric portal + 1 Guard + Desk-Top e	2	2.10	2	37	37	37	4.73	2.90	$1,058,000
	Central Gate	P	Metal detector Gate (PMD2 / PT	Dielectric portal + 1 Guard + Desk-Top e	2	2.10	2	37	37	37	4.73	2.90	$2,116,000
	Gate	P	Metal detector Gate (PMD2 / PT	Metal detector Gate (PMD2 / PTZ)+ op	2	2.10	2	2	2	37	2.10	2.90	$0
Arrival	Gate	P	Metal detector Gate (PMD2 / PT	Metal detector Gate (PMD2 / PTZ)+ op	2	2.10	2	2	2	37	2.10	2.90	$0
		L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$2,250,000
		L	Luggage hand search	Luggage hand search	2	2.40	2	2	2	4	2.40	2.60	$0
		L	Luggage hand search	Luggage hand search	2	2.40	2	2	2	4	2.40	2.60	$0
		L	Luggage hand search	Luggage hand search	2	2.40	2	2	2	4	2.40	2.60	$0
		B	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	6	2.73	2.28	$0
	Checked-in Lugg.	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	4	2.73	2.28	$0
		B	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	6	2.73	2.28	$0
		B	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	6	2.73	2.28	$0
		B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	3.93	2.28	$2,172,000
	In-Bound Lugg.	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	4	2.73	2.28	$0
	Transferred Lugg.	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	4	2.73	2.28	$0
	Hold Luggage	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operator	2	2.73	2	2	2	4	2.73	2.28	$0

Measures not upgraded

Ranked *PIs*

Figure 4.8: MS Excel Spread-Sheet of Priority index-based Solution

To examine the optimality of any upgrade decision, the benefit-cost ratio (B/C) for the priority-index-based solution is calculated, as follows:

$$B_s / C_s = \frac{B_{su}}{C_{PCB(s)}} \times 10^7 \qquad \textbf{4.4}$$

where $B_{su(s)}$ is the benefit/cost ratio for PCBSS upgrades
$C_{PCB(st)}$ is the cost of upgrading the PCBSS

Due to the budget constraints, the benefit-cost ratio (B/C) for the priority-index-based solution was found to be 4.95. Therefore, it is clear that this method does not provide an optimum

solution because 12 measures are left not upgraded, the SRI score achieved is higher 5, and the B/C ratio is low.

4.4.2 Mathematical Optimization

Since the priority-index-based solution does not arrive at an optimum upgrade plan and does not take into consideration all constraints, the model was run using the Solver software, an MS Excel add-in tool based on mathematical linear optimization techniques, in order to search for the optimum plan. The first step was to formulate the optimization objective function. In this case, the optimization objective function is set to maximize the PCBSS's benefit/cost ratio ($B_{su(s)}$) over the planning horizon (one year), as expressed in Equation 4.4. The second step is to determine the optimization variables and to set the constraints. Decision variables were classified into a one-year level that deals with the 26 SCPs. Therefore, the objective function can be expressed mathematically as follows:

$$Max \sum_{t=1}^{T} B_{st} / C_{st} = \frac{B_{su(st)}}{C_{PCB(st)}} \times 10^{7} \quad \forall t \qquad \textbf{4.4}$$

where $B_{su(s)}$ is the benefit/cost ratio for PCBSS upgrades at one year (t)
T is number of planning horizon years, and
$C_{PCB(st)}$ is the cost of upgrading the PCBSS at year (t)

It should be noted that the benefits are not quantified in dollars. However, the B/C ratio is not just a unitless value, rather the B/C used in this research, is in fact, a value that represents the amount of risk reduction per dollar, which is a maximized return on investment. This objective function is also compared later with other objective function, such as the minimization of the

overall SRI. Generally, the optimization objective function is subject to the following constraints:

1. The total annual upgrade costs (C_t) in a given year should be less than or equal to the maximum budget limit in that year (B_t) and can be expressed as follows:

$$\sum_{t=1}^{T} C_t \quad \leq \quad B_t \quad \forall_t \qquad \textbf{4.5}$$

The overall security risk index achieved for passengers (SRI_P) should be greater than or equal to the minimum acceptable level and also less than or equal to the maximum level, which can be expressed as follows:

$$\textbf{\textit{acceptable level}} \; \forall_p \geq SRI_P \geq \textbf{\textit{min level}} \; \forall_p \qquad \textbf{4.6}$$

The overall security risk index achieved for cabin baggage (SRI_B) should be greater than or equal to the minimum acceptable level and also less than or equal to the maximum level, which can be expressed as follows:

$$\textbf{\textit{acceptable level}} \; \forall_b \geq SRI_B \geq \textbf{\textit{min level}} \quad \forall_b \qquad \textbf{4.7}$$

The overall security risk index achieved for checked-in luggage (SRI_L) should be greater than or equal to the minimum acceptable level and also less than or equal to the maximum level, which can be expressed as follows:

$$\textbf{\textit{acceptable level}} \; \forall_l \geq SRI_L \geq \textbf{\textit{min level}} \quad \forall_l \qquad \textbf{4.8}$$

The security risk index achieved for any security subsystem (SRI_k) should be greater than or equal to the minimum acceptable level, and it should be less than or equal to the maximum level, which can be expressed as follows:

$$acceptable\ level\ \forall_k \geq SRI_k \geq min\ level\ \forall_k \quad \textbf{4.9}$$

The security risk index achieved for any security system (SKI_s) should be greater than or equal to the minimum acceptable level, and it should be less than or equal to the maximum level, which can be expressed as follows:

$$acceptable\ level\ \forall_s \geq SRI_s \geq min\ level\ \forall_s \quad \textbf{4.10}$$

The overall airport security index achieved (SRI_a) should be greater than or equal to the minimum acceptable level, and it should be less than or equal to the maximum level, which can be expressed as follows:

$$acceptable\ level \geq SRI_a \geq min\ level \quad \textbf{4.11}$$

The third step was to determine the expected solution space. According to Nunoo and Mrawira (2004), the solution space is expected to be huge. The number of potential solutions can be denoted as $R^{N \times T}$, where R is the number of suggested upgrade alternatives for each mitigation measure at each screening checkpoint, N is the total number of similar security checkpoints, and T is the number of years in the objective planning span. In this context, at a typical PCBSS level, the assigned values for R vary from one screening checkpoint (subsystem) to another and from one screening target measure (subsystem component) to another. For example, according to the reliability database (Figure 4.3), there are 37 (R=37) upgrade options (alternative mitigation

measures) for ray and physical search screening measures in each subsystem (departure and arrival directions), there are 4 SCPs that use ray and physical search screening measures (N=4), and the planning horizon is set to be one year (T=1). According to Nunoo and Mrawira (2004), the number of potential mitigation combinations is then $R^{N \times T}$, where R is the number of upgrade options for each mitigation measure, N is the total number of SCPs in the concerned subsystem, and T is the number of years in the objective planning span. Therefore, for example, the number of possible combinations of solutions specifically for ray and physical search in a subsystem equals $37^{4 \times 1}$. Once the planning horizon is increased to more than one year (N>1), the solution space increases exponentially for this single subsystem component. Likewise, the total solution space for the whole system will be extremely large since it will include the accumulative summation of all combinations of single subsystem components.

The next step was to feed the optimization model with the objective function and to set the associated constraints. Solver was then run, but due to the large number of feasible solutions, Solver could not deal with this optimization problem. Solver showed a failure message, as illustrated in Figure 4.9.

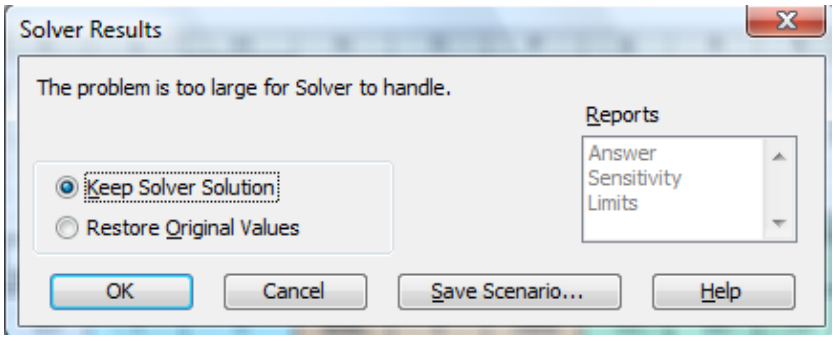


Figure 4.9: Solver Failure Message to deal with the Optimization Problem

4.4.3 The Non-Traditional Optimization Technique

Since Solver failed, a non-traditional algorithm-based optimization technique was used. Based on the Flintsch and Chen (2004) comprehensive review of various soft computing techniques, the genetic algorithms (GAs) technique was selected. The developed optimization model uses the GAs mechanism to investigate feasible upgrading scenarios (combinations of mitigation alternatives) in order to optimize the upgrade strategy (upgrade type, level of upgrade, priority of upgrade, etc.). The optimization model Figure 4.10 incorporates the output from the Security Risk Metric described in Chapter 3 as well as from the upgrade options model.

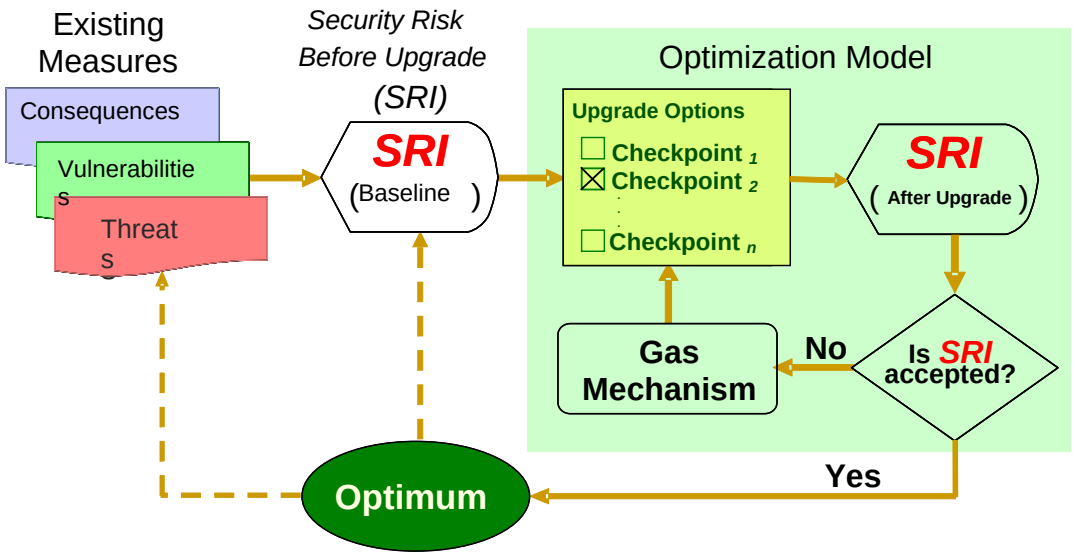


Figure 4.10: The Conceptual Optimization Model

The model utilizes the ability of GAs to deal with large solution spaces, to arrive at a solution that is close to the optimum solution, and not to become stuck at local minima (Goldberg, 1989). As Holland (1975) explained, the process of implementing the GAs technique can be summarized in the steps illustrated in Figure 4.11. The approach is based on a chromosome designed as a string of $N \times T$, where N is the total number of unique combinations of mitigation

measures per subsystem in the PCBSS at the single-airport terminal level (26 in this case, distributed in 5 SCPs in departures and 5 SCPs in arrivals), and *T* is the number of years in the planning horizon (one in this case). The values of the string bits are correlated with optimization variables to make up the chromosome structure (Holland, 1975). Each chromosome element (gene) holds a value from 1 to 4, 5, 6, or 37, depending on the type of SCP measure, and corresponds to one of the upgrade options (one means do nothing). The general chromosome structure is shown in Figure 4.12.

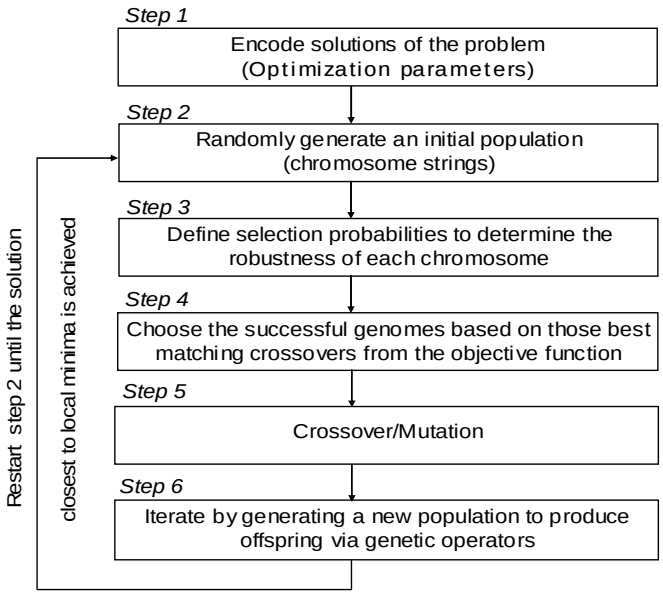


Figure 4.11: Steps in the GAs process (based on Holland, 1975; Matthew, 2008)

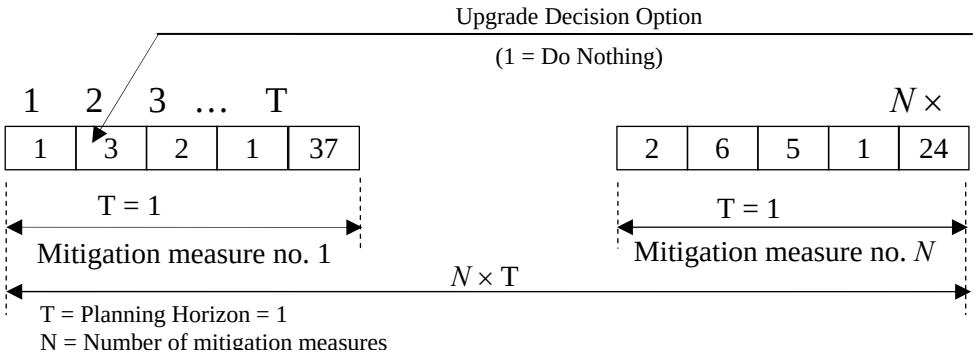


Figure 4.12: The GA Chromosome Structure

Moreover, the optimization model, which is based on input from security officials, executes detailed "what-if" analysis scenarios in order to justify scenarios that have an SRI less than or equal to the acceptable level and that satisfy the other needs and constraints. To this end, the optimization model initiates an SRI re-assessment process through the GAs mechanism (Figure 4.13) for determining the near optimum upgrade scenario and suggesting the best cost-effective measures that will produce the lowest possible SRI and the best benefit/cost ratio. Individual scenarios that present significant vulnerability along with critical threats or consequences are thus detected and eliminated.

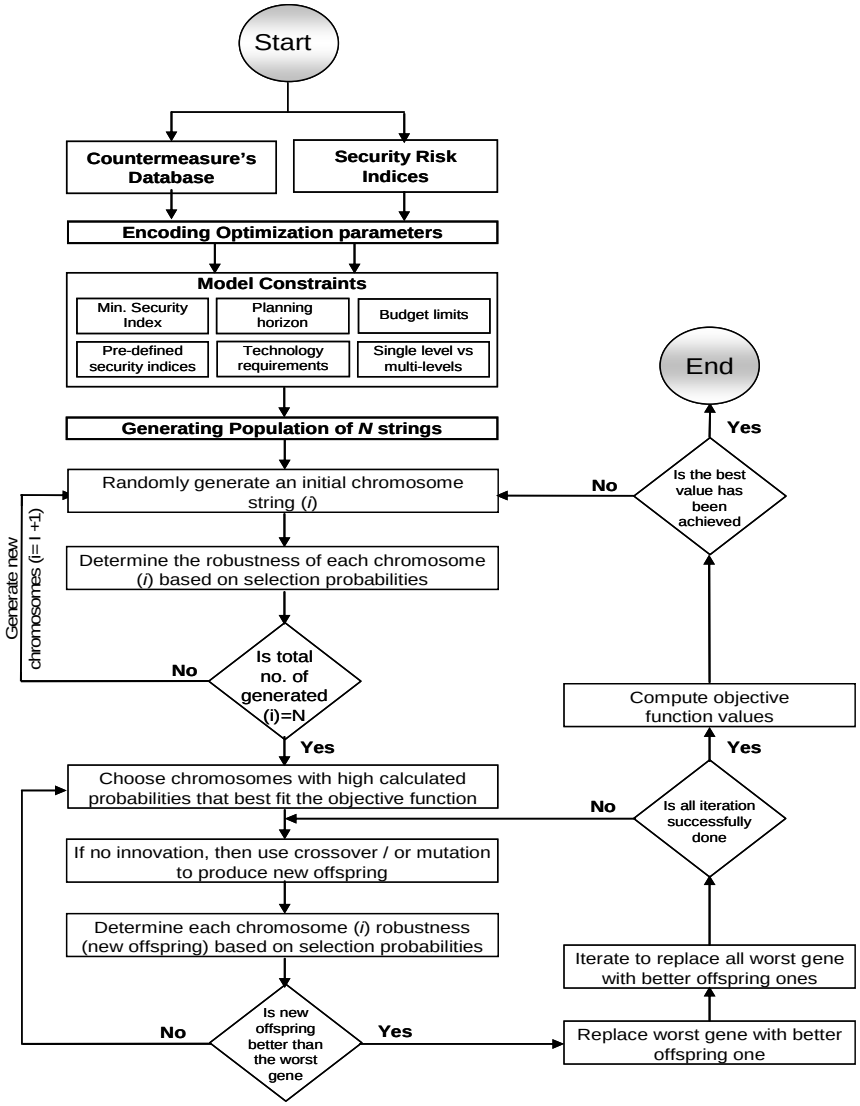


Figure 4.13: GA Mechanism of the Optimization Model

As shown in Figure 4.6, airport officials center specific data and can thus manually force the system to meet a specific security index (cell H7), targeted security scores (column 0), the total planning horizon budget (cell G8), and the allowable budget (cell H8). The Gas, based on the type and the cost of the measures retrieved from the database (Figure 4.3), run different random upgrade scenarios. Once the global optimum scenario is found, the system displays the suggested upgrade decision options in column M, and their associated upgrade expenditures in column Q. In addition, airport officials can pre-define some of the upgrade decisions (column M) and can tweak them manually to suit their airport's special needs or other policy issues. To ensure that an upgrade decision is considered up to a specific limit, an upper limit is introduced (column N) that forces the model to consider the specified limits at the same time. Once the user enters all the desired input data, he can then proceed by running Evolver-GA-based software. When Evolver runs, an Evolver Settings window pops up (Figure 4.14), and the user must perform the following tasks:

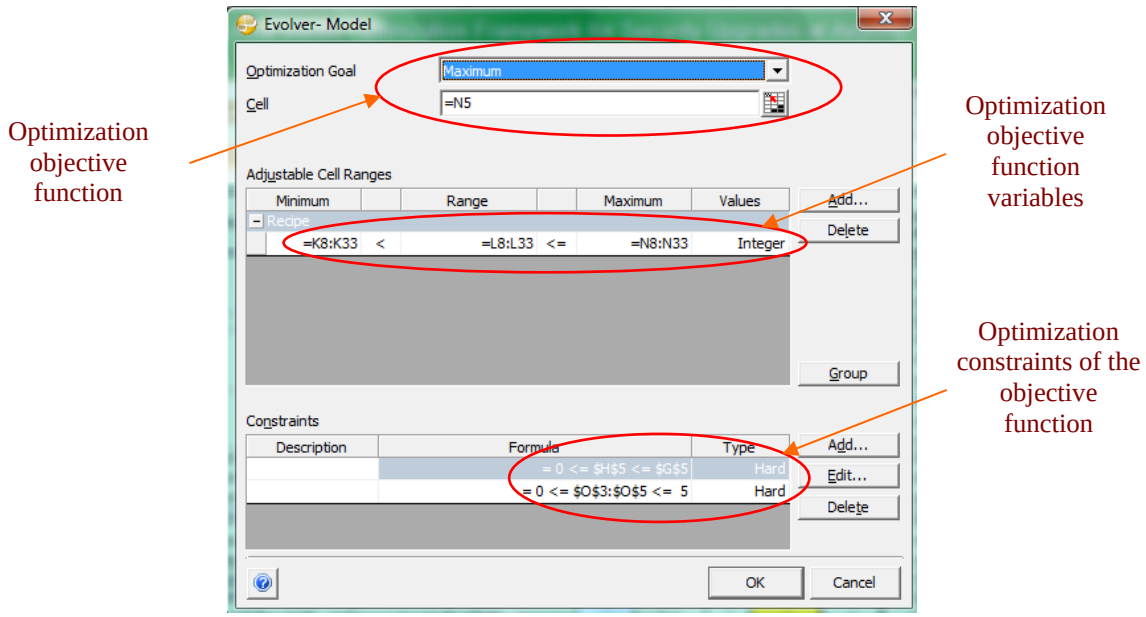


Figure 4.14: Evolver Settings

1. Define the objective function cell, and choose from three optimization options: minimize, maximize, or find value closest to a specific target value. In this case, it would be *B/C* cell (Equation 4.4), and the optimization option, which is maximization.
2. Set adjusting cells (optimization objective function variables), which in this case, would be the upgrade decision cells in column *N*.
3. Select optimization constraint cells as defined in Equations 4.5 through 4.10.

The next step is to determine the population size, generation of the random number seed (randomly or fixed), and the stop criteria. This can be performed using the options, as shown in Figure 4.15. Other available options include general options, such as pause on error and graph progress, and options for updating the display, such as every calculation, with only the best result, and never.

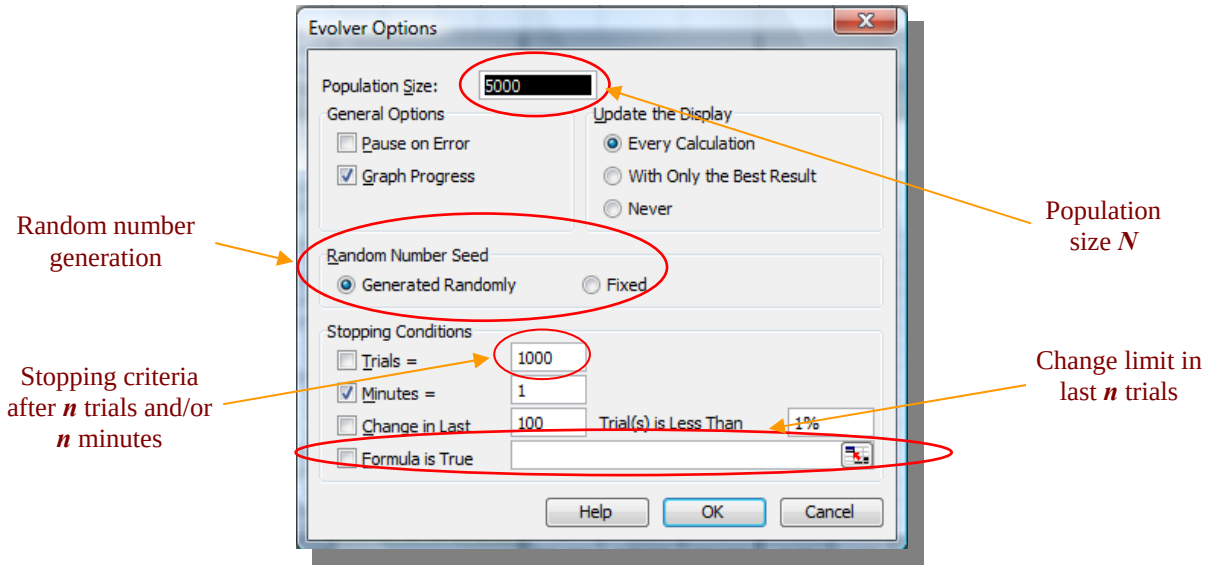


Figure 4.15: Options for Evolver Settings

The stopping criteria include the following options: stop at a specific number of trials, after a specified number of minutes after the beginning of the run, when the change after a specified

number of trials is less than a specified percentage, or when a pre-defined formula becomes true. Once Evolver's settings are properly entered as desired, the GA evolutionary process runs until it arrives at the best solution near the global optima, which will be equivalent to the optimum upgrade strategy that satisfies all constraints as well as the Evolver settings. As illustrated in Figure 4.16, the GA-based model for maximizing the B/C ratio was able to achieve better results than the priority index-based model. It should also be noted that the passenger risks score decreased from 22.26 in the priority index-based solution to 2.85 in the Gas B/C-based solution.

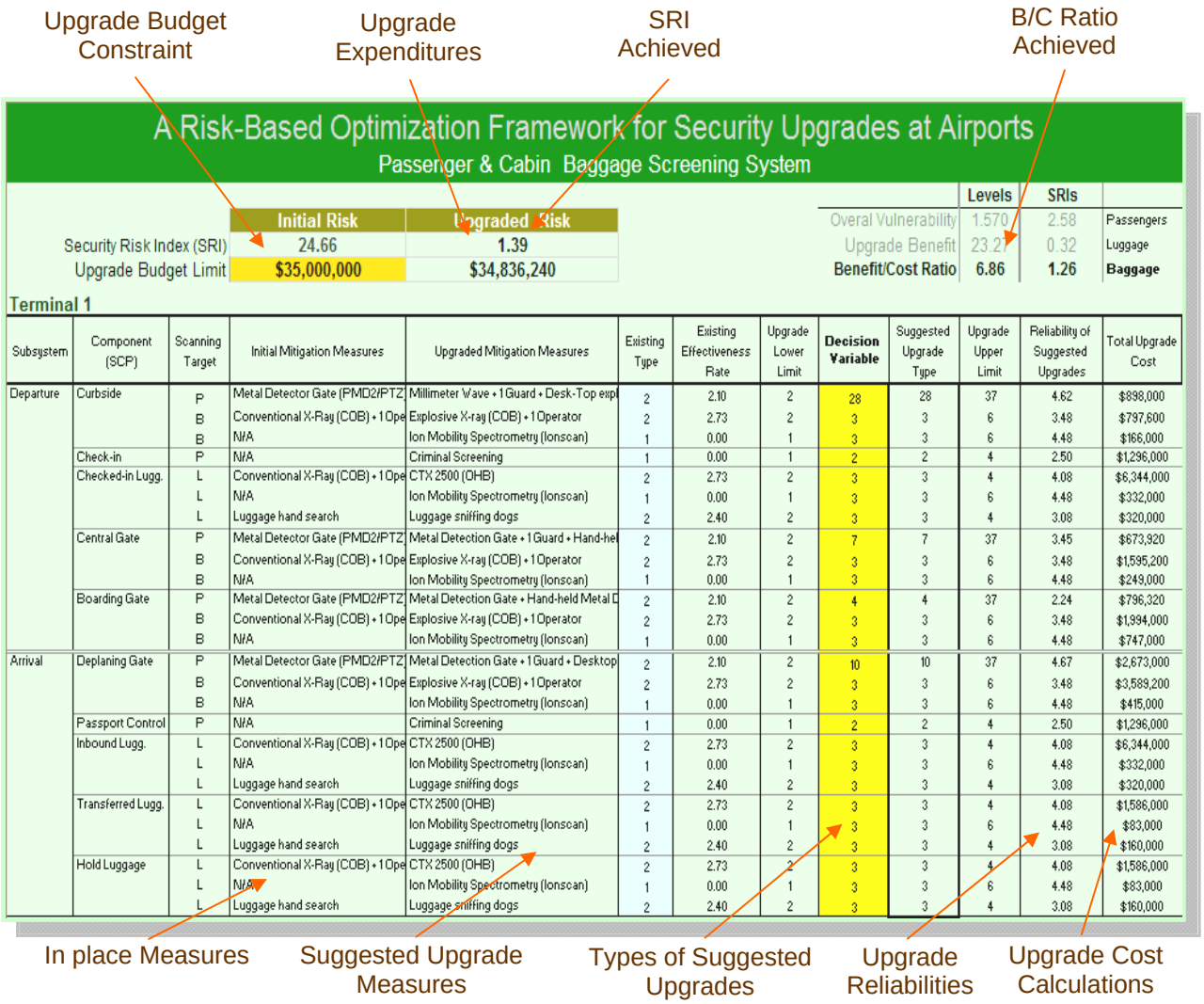


Figure 4.16: Optimization Solution for maximum B/C ratio with Risk reduced to 1.39

As the GAs model is run for the second time based on minimizing the overall SRI, a summary is produced that compare the results of all experiments, as shown in Table 4.3. The summary proves that the results of the Gas-based solution for minimizing the SRI are very encouraging and that the use of a GA approach is a promising technique for determining the near optimum upgrade strategy.

Table 4.3: Comparative Results

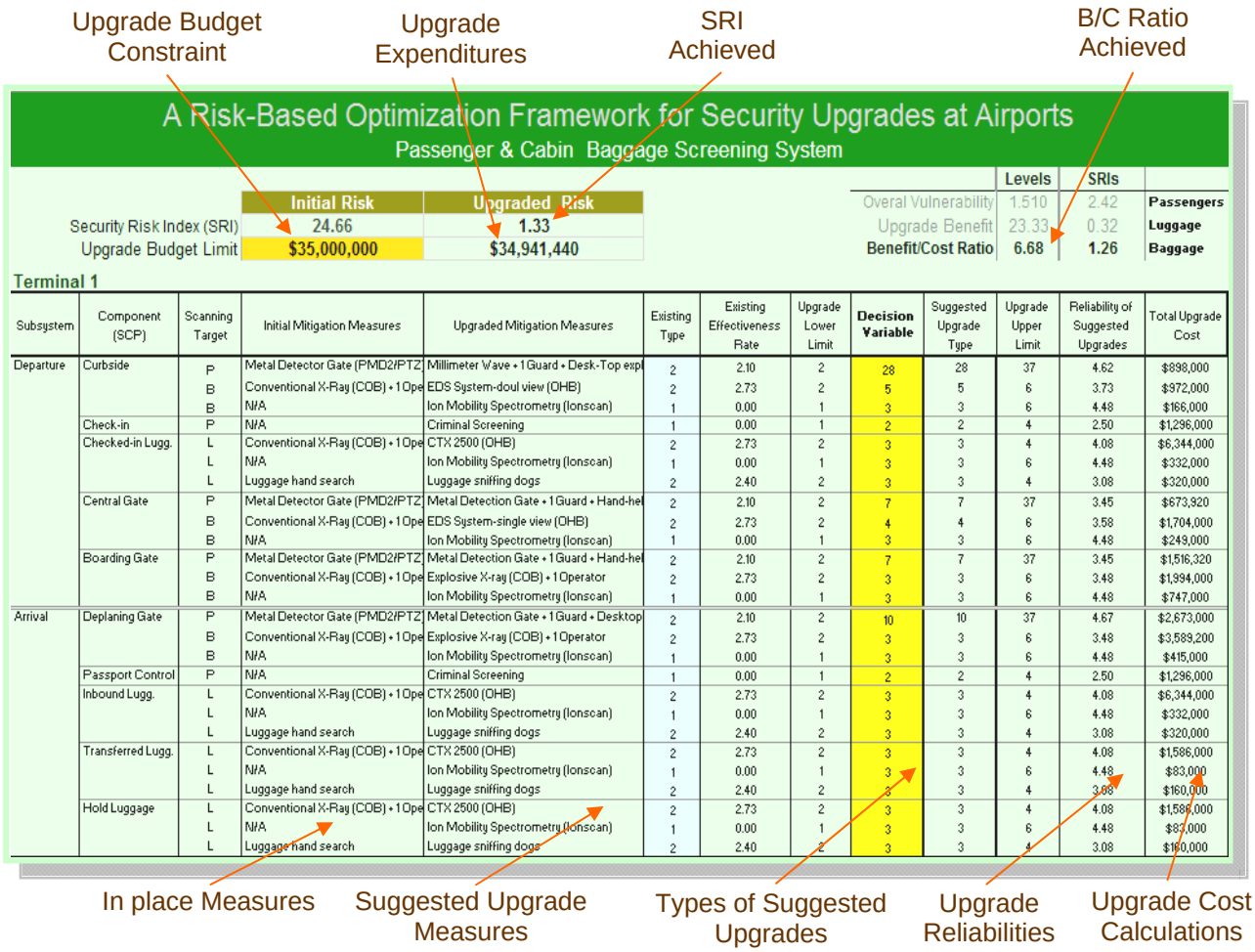
Solution	Achieved Risks			Achieved SRI	Benefit Cost / Ratio	Total Budget Expenditures
	Passengers	Cabin Baggage	Checked-in Luggage			
Priority Index	22.26	0.05	0.08	7.46	4.95	$34,716,000
Optimization (max. B/C)	2.58	0.32	1.25	1.39	6.86	$33,938,240
Optimization (min. SRI)	**2.42**	**0.32**	**1.26**	**1.33**	**6.68**	**$34,940,440**

As shown in Figure 4.17, the minimum SRI-based GA solution would slightly improve the maximizing B/C ratio results. Table 4.3 shows the summary of the three experiments and also shows that the System's SRI would be decreased from 17.73 to 1.26. In terms of the total actual upgrade expenditures and the maximum utilization of the original total planning horizon budget, the minimum SRI-based GA-based solution achieved high level of utilization at 99.77%. With respect to the upgrades risks and the B/C ratio, the GA-based solution realized the lowest level of risks 1.33 and the highest B/C ratio (6.86).

4.5 Discussion of Results

The results shown in Table 4.3 suggest that decisions related to PCBSS upgrades can be optimized using the developed security metric and optimization model. The following observations can be made:

1. Determining upgrade decisions based on simple ranking does not lead to the best solutions.



Subsystem	Component (SCP)	Scanning Target	Initial Mitigation Measures	Upgraded Mitigation Measures	Existing Type	Existing Effectiveness Rate	Upgrade Lower Limit	Decision Variable	Suggested Upgrade Type	Upgrade Upper Limit	Reliability of Suggested Upgrades	Total Upgrade Cost
Departure	Curbside	P	Metal Detector Gate (PMD2/PTZ	Millimeter Wave + 1 Guard + Desk-Top exp	2	2.10	2	28	28	37	4.62	$898,000
		B	Conventional X-Ray (COB) + 1 Ope	EDS System-doul view (OHB)	2	2.73	2	5	5	6	3.73	$972,000
		B	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$166,000
	Check-in	P	N/A	Criminal Screening	1	0.00	1	2	2	4	2.50	$1,296,000
	Checked-in Lugg.	L	Conventional X-Ray (COB) + 1 Ope	CTX 2500 (OHB)	2	2.73	2	3	3	4	4.08	$6,344,000
		L	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$332,000
		L	Luggage hand search	Luggage sniffing dogs	2	2.40	2	3	3	4	3.08	$320,000
	Central Gate	P	Metal Detector Gate (PMD2/PTZ	Metal Detection Gate + 1 Guard + Hand-he	2	2.10	2	7	7	37	3.45	$673,920
		B	Conventional X-Ray (COB) + 1 Ope	EDS System-single view (OHB)	2	2.73	2	4	4	6	3.58	$1,704,000
		B	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$249,000
	Boarding Gate	P	Metal Detector Gate (PMD2/PTZ	Metal Detection Gate + 1 Guard + Hand-he	2	2.10	2	7	7	37	3.45	$1,516,320
		B	Conventional X-Ray (COB) + 1 Ope	Explosive X-ray (COB) + 1 Operator	2	2.73	2	3	3	6	3.48	$1,994,000
		B	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$747,000
Arrival	Deplaning Gate	P	Metal Detector Gate (PMD2/PTZ	Metal Detection Gate + 1 Guard + Desktop	2	2.10	2	10	10	37	4.67	$2,673,000
		B	Conventional X-Ray (COB) + 1 Ope	Explosive X-ray (COB) + 1 Operator	2	2.73	2	3	3	6	3.48	$3,589,200
		B	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$415,000
	Passport Control	P	N/A	Criminal Screening	1	0.00	1	2	2	4	2.50	$1,296,000
	Inbound Lugg.	L	Conventional X-Ray (COB) + 1 Ope	CTX 2500 (OHB)	2	2.73	2	3	3	4	4.08	$6,344,000
		L	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$332,000
		L	Luggage hand search	Luggage sniffing dogs	2	2.40	2	3	3	4	3.08	$320,000
	Transferred Lugg.	L	Conventional X-Ray (COB) + 1 Ope	CTX 2500 (OHB)	2	2.73	2	3	3	4	4.08	$1,586,000
		L	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$83,000
		L	Luggage hand search	Luggage sniffing dogs	2	2.40	2	3	3	4	3.08	$160,000
	Hold Luggage	L	Conventional X-Ray (COB) + 1 Ope	CTX 2500 (OHB)	2	2.73	2	3	3	4	4.08	$1,586,000
		L	N/A	Ion Mobility Spectrometry (Ionscan)	1	0.00	1	3	3	6	4.48	$83,000
		L	Luggage hand search	Luggage sniffing dogs	2	2.40	2	3	3	4	3.08	$160,000

Figure 4.17: Optimization Solution for minimizing SRI with Risk reduced to 1.33

2. Of the three methods tested, GA decisions are capable of producing the best upgrade solution, in this case, a minimum SRI of 1.89. The GA decisions also achieved a better B/C ratio and vulnerability levels.
3. The performance of the GAs and their ability to allocate upgrade funds efficiently are promising, especially when the objective function is geared toward minimizing the overall SRI. The solution also achieved the maximum reduction in the risks associated with passengers, baggage, and luggage.

4.6 Summary and Conclusion

To respond to the need for airport security officials to have a decision support tool to help them upgrade their airports' security systems cost-effectively, a risk-based optimization framework has been developed successfully. The framework highlights some of the main upgrade constraints with respect to budget and the level and type of mitigation measures, and illustrates methods of integrating them with other factors. The application of an optimization approach based on the utilization of artificial intelligence techniques (e.g., GAs) will help airport authorities in their crucial mission to investigate multiple "what-if" scenarios and to make decisions that optimize and prioritize the costs of upgrades to their PCBSS. Initially, setting the optimization model based on maximizing the benefit/cost ratio as the target objective function, which already incorporates the upgraded SRI, produced promising results. However, switching the objective function to minimize the overall SRI produced results that are more encouraging. Therefore, the latter approach was adopted during the validation process. Chapter 5 presents a real-life case study at an international airport in order to validate the model. An approach based on expert opinion was also implemented through consultations and research meetings with subject experts from the Greater Toronto Airport Authority and the Libyan Civil Aviation Authority as part of the process of validating the optimization framework.

CHAPTER 5

Validation of the Airport Security Upgrade Framework

5.1 Introduction

This chapter presents two approaches to validating the proposed framework components. The first was to acquire experts at the Greater Toronto Airport Authority (GTAA) their overall evaluation and expectations. The second was to conduct a case study at one of the Libyan Civil Aviation Authority's (LYCAA) international airports. The security risk metric and the optimization model were used in modeling and presenting the case study at the passenger and cabin baggage screening system (PCBSS) level. Furthermore, the actual decision made by the LYCAA and those suggested by the developed framework were compared with respect to expected benefits, the SRI, total upgrade expenditures, and the benefit-cost ratio. A sensitivity analysis was conducted and the confidence interval was also investigated.

5.2 GTAA Feedback

Over the course of a year, research meetings, interviews, and conference calls were held with GTAA airport security personnel at the advisory and managerial levels. The research meetings, interviews, and conference calls were very useful in the development of the new metric and the prototype of the development framework, particularly with respect to the following points:

1. Verifying the definition and categorization of the types and levels of threats, and their potential consequences that actually confront airport security,
2. Consistent list format providing a positive evaluation of the suggested vulnerability assessment approach based on checkpoint configuration and the reliability of screening measures, and

3. Confirming the metric's quantitative assessment of threats, vulnerabilities, and consequences at different levels; the output of the optimization model; and the use of genetic algorithms in arriving at an optimum upgrade plan.

During the research meetings, interviews, and a live demonstration of the prototype system GTAA personnel stated that they were interested in the developed framework. They indicated that the framework is beneficial and that the optimization feature is innovative and non-existent in other systems they are aware of. They also suggested that it will be more powerful when extended to include other security systems, and will help decision makers in their efforts to optimize all aspects of upgrades to airport security. GTAA personnel commented positively about the practicality of the security metric and the optimization model. In addition, they valued the ability of the framework to maximize the return on investment in security upgrades. After the demonstration, GTAA security officials indicated their willingness to provide real data for testing the framework and extending it to meet GTAA needs. However, due to confidentiality issue and the sensitive nature of security data, the GTAA was not able to provide the data required.

5.3 Libyan Case Study

The developed framework was used with data collected from the Libyan Civil Aviation Authority (LYCAA). Currently, the LYCAA does not have a risk metric or an optimization model for security system upgrades. The LYCAA is a state agency that owns and operates three international and ten domestic airports. The LYCAA officials were helpful and cooperative in providing the security data from an international airport necessary for validating the developed optimization framework, which for confidentiality reasons has been kept undeclared. Related data and information were also collected through interviews and meetings, field visits, and some

LYCAA documentation. The interviews included meetings with the Chairman of LYCAA, some of the passenger and cabin baggage screening engineers, airport security officials, and a number of other LYCAA officials. The data collected include: in place screening measures; configuration of current security checkpoints, the reliability of existing measures, available upgrade options and their cost, and the budget available for upgrades.

5.3.1 Security Assessment of Existing Measures

The security risk status of the designated international airport was assessed in terms of the current threat levels, vulnerabilities, and expected consequences. Figures 5.1 to 5.4 show the current status of the airport security assessment.

Threat Assessment

According to the threat assessment shown in Figure 5.1, the threat was assessed at a very high level (score = 4.44/5), which, according to the description in Table 3.1, means "Identifies that a credible threat exists against the airport assets, so that continuous or intensive attacks are likely to occur, and that the adversary demonstrates the capability and intent to launch an attack targeting the airport or one of its assets on a frequently occurring basis, and that specialized security advice should be sought."

Threat Assessment

Passenger & Baggage Screening System

Terminal 1:

1 Explosives	Departures 4.33	Arrivals 4.33	2 Sharp blades	Departures 4.00	Arrivals 4.00	3 Biological	Departures 5.00	Arrivals 5.00
Weapons	Very High	Very High	Knifes	High	High	Choking	Very High	Very High
Bombs	High	High	Swords	Medium	Medium	Nerve	Very High	Very High
Explosive liquids	High	High	Razors & cutters	Very High	Very High	Blood	Very High	Very High
						Blister	Very High	Very High

Terminal 1 Departure Threat Score : 4.44
Terminal 1 Arrival Threat Score : 4.44
Terminal 1 Overall Threat Score : 4.44

Therefore, the airport overall threat assessment is most likely to be
Continuous or intensive attacks are likely, and specialized security advice should be sought.

Figure 5.1: LYCAA Airport's Threats Assessment

Vulnerability Assessment

To evaluate the vulnerability assessment, the existing security screening measures at the LYCAA airport terminal were entered into the prototype, as shown in Figure 5.2. Accordingly, the vulnerability assessment towards threats (Figure 5.3) is assessed as high level (score= 3.54/5), which based on the description in Table 3.2, means "*there are some protective measures to deter, detect, delay, or respond to the asset, but not a complete or effective application of these security strategies and so it would be relatively easy for the adversary to successfully attack the airport asset, and a limited opportunity and a little specialized knowledge would be needed*". Figure 5.3 shows the detailed vulnerability calculated towards each threat type and the aggregated vulnerabilities for passengers, cabin baggage, and checked-in luggage, calculated for both the departure and the arrival subsystems.

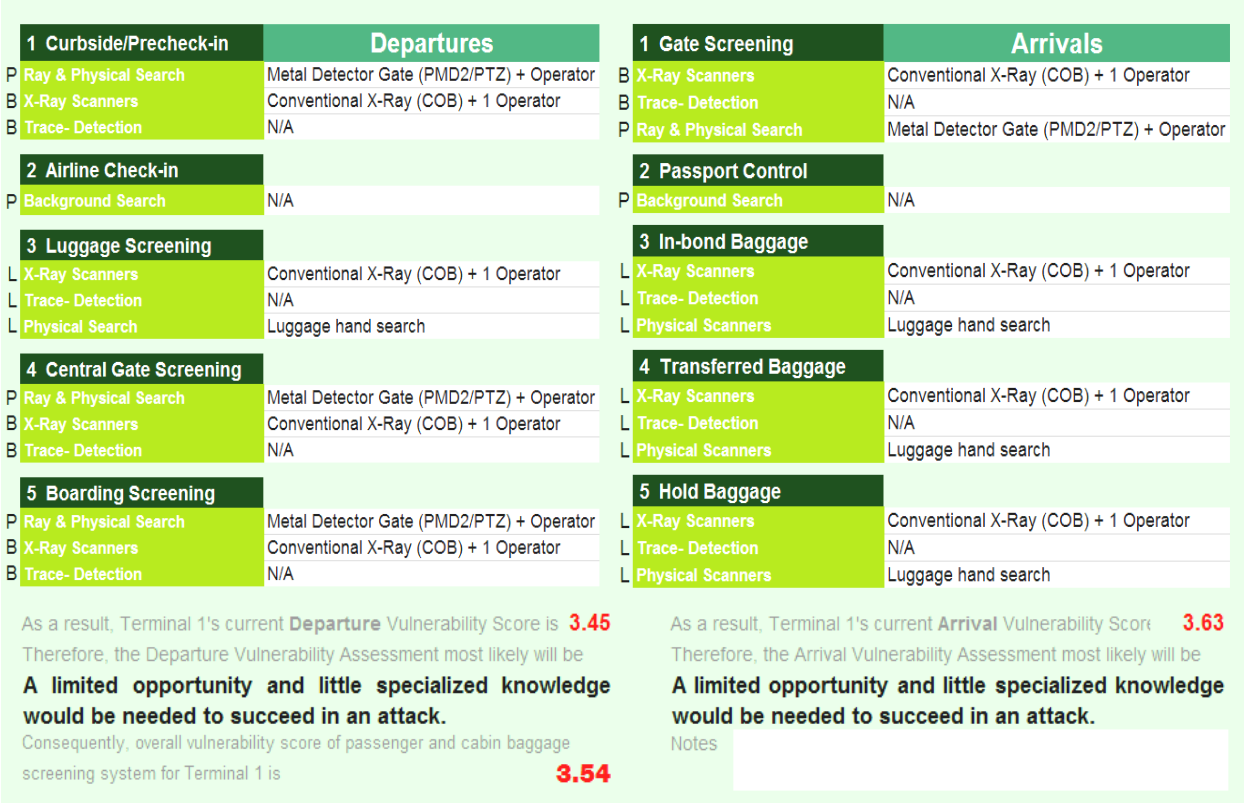


Figure 5.2: Existing Security Screening Measures

Vulnerability to Threat Types

	Explosives			Blades			Biological				
	1	2	3	4	5	6	7	8	9	10	
P	0.75	2.50	5.00	0.25	0.25	0.25	5.00	5.00	5.00	5.00	
B	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
P	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
P	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
B	2.5	2.5	3.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	
P	0.8	2.5	5.0	0.3	0.3	0.3	5.0	5.0	5.0	5.0	
B	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
P	0.8	2.5	5.0	0.3	0.3	0.3	5.0	5.0	5.0	5.0	
B	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
Passengers:	1.8	3.1	5.0	1.4	1.4	1.4	5.0	5.0	5.0	5.0	3.43
Luggage:	3.2	3.2	3.7	2.8	2.8	2.8	3.7	3.7	3.7	3.7	3.29
Baggage:	3.5	3.5	3.8	2.9	2.9	2.9	4.3	4.3	4.3	4.3	3.64
	2.8	3.3	4.1	2.4	2.4	2.4	4.3	4.3	4.3	4.3	3.45

Vulnerability to Threat Types

	Explosives			Blades			Biological				
	1	2	3	4	5	6	7	8	9	10	
P	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
B	0.8	2.5	5.0	0.3	0.3	0.3	5.0	5.0	5.0	5.0	
P	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
P	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
B	2.5	2.5	3.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	
P	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
B	2.5	2.5	3.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	
P	2.0	2.0	2.5	0.8	0.8	0.8	3.5	3.5	3.5	3.5	
B	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	
B	2.5	2.5	3.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	
Passengers:	2.9	3.8	5.0	2.6	2.6	2.6	5.0	5.0	5.0	5.0	3.95
Luggage:	3.2	3.2	3.7	2.8	2.8	2.8	3.7	3.7	3.7	3.7	3.29
Baggage:	3.5	3.5	3.8	2.9	2.9	2.9	4.3	4.3	4.3	4.3	3.64
	3.2	3.5	4.1	2.8	2.8	2.8	4.3	4.3	4.3	4.3	3.63

Figure 5.3: Vulnerability of Existing Measures

Consequence Assessment

The assessment of the consequences was determined to be High (score = 3.67/5) as shown in Figure 5.4. Based on the description in Table 3.3, this means "25 - 50 Fatalities, 24 - 48 Hours town time, Congressional Mandates, and 50% - 75% total loss."

Consequence Assessment

Passenger & Baggage Screening System

Terminal 1

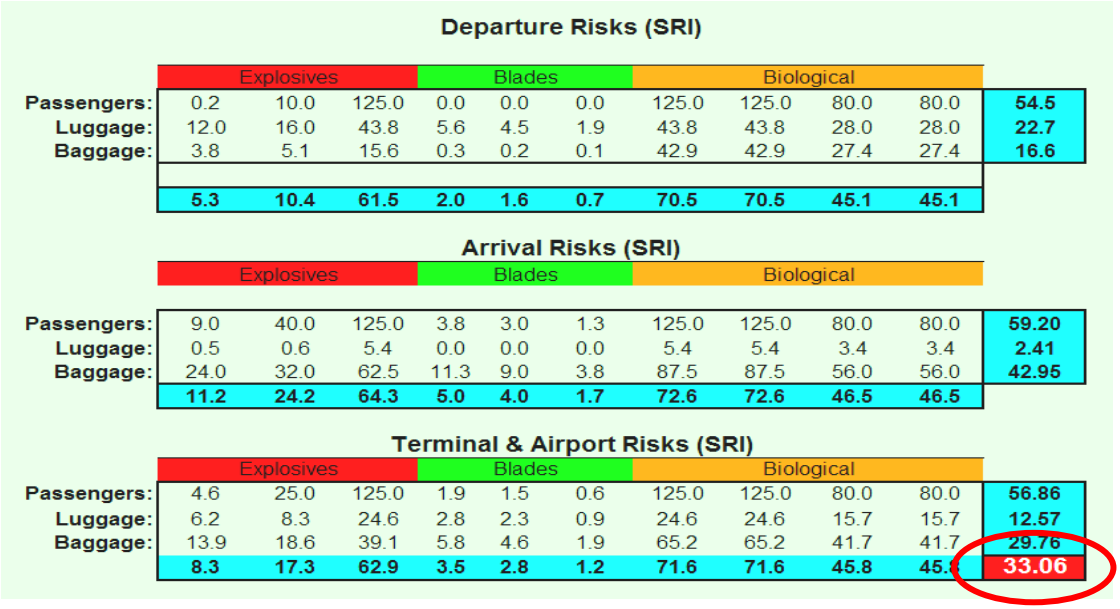
	Casualties (F)		Down Time (U)		Exposure (E)		Total Loss: %	
1 Explosives 4.33	Departures 4.33	Arrivals 4.33	Departures 4.33	Arrivals 4.33	Departures 4.33	Arrivals 4.33	Departures 4.33	Arrivals 4.33
Weapons	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High
Bombs	High	High	High	High	High	High	High	High
Explosive liquids	High	High	High	High	High	High	High	High
2 Sharp blades 1.67	Departures 1.67	Arrivals 1.67	Departures 1.67	Arrivals 1.67	Departures 1.67	Arrivals 1.67	Departures 1.67	Arrivals 1.67
Knives	Medium	Low	Medium	Low	Medium	Low	Medium	Low
Sword	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
Razors & cutters	very low	Low	very low	Low	very low	Low	very low	Low
3 Biological atta 3.67	Departures 5.00	Arrivals 5.00	Departures 5.00	Arrivals 5.00	Departures 5.00	Arrivals 5.00	Departures 5.00	Arrivals 5.00
Choking	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High
Nerve	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High
Blood	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High
Blister	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High

Therefore, the consequence scores for the Terminal 1 PCBSS are as follows:

Departure **3.67** Arrival **3.67** PCB System's Overall SRI **3.67**

Figure 5.4: Consequence Assessment for the LCAA Airport

Upon evaluating the threats, the vulnerability, and the consequences, the security risk indexes for passengers, cabin baggage, and luggage were calculated for each terminal subsystem (departure and arrival) and for the overall terminal, as shown in Figure 5.5. Based on the calculations in Figure 5.5, the overall Security Risk Index was 33.06; therefore, the PCBSS need to be upgraded in order to achieve an acceptable SRI (0 – 5).



Departure Risks (SRI)

	Explosives			Blades			Biological				
Passengers:	0.2	10.0	125.0	0.0	0.0	0.0	125.0	125.0	80.0	80.0	**54.5**
Luggage:	12.0	16.0	43.8	5.6	4.5	1.9	43.8	43.8	28.0	28.0	**22.7**
Baggage:	3.8	5.1	15.6	0.3	0.2	0.1	42.9	42.9	27.4	27.4	**16.6**
	5.3	**10.4**	**61.5**	**2.0**	**1.6**	**0.7**	**70.5**	**70.5**	**45.1**	**45.1**	

Arrival Risks (SRI)

	Explosives			Blades			Biological				
Passengers:	9.0	40.0	125.0	3.8	3.0	1.3	125.0	125.0	80.0	80.0	**59.20**
Luggage:	0.5	0.6	5.4	0.0	0.0	0.0	5.4	5.4	3.4	3.4	**2.41**
Baggage:	24.0	32.0	62.5	11.3	9.0	3.8	87.5	87.5	56.0	56.0	**42.95**
	11.2	**24.2**	**64.3**	**5.0**	**4.0**	**1.7**	**72.6**	**72.6**	**46.5**	**46.5**	

Terminal & Airport Risks (SRI)

	Explosives			Blades			Biological				
Passengers:	4.6	25.0	125.0	1.9	1.5	0.6	125.0	125.0	80.0	80.0	**56.86**
Luggage:	6.2	8.3	24.6	2.8	2.3	0.9	24.6	24.6	15.7	15.7	**12.57**
Baggage:	13.9	18.6	39.1	5.8	4.6	1.9	65.2	65.2	41.7	41.7	**29.76**
	8.3	**17.3**	**62.9**	**3.5**	**2.8**	**1.2**	**71.6**	**71.6**	**45.8**	**45.**	**33.06**

Figure 5.5: Security Risk Indexes for Existing Measures

5.3.2 Upgrade Options and Cost Data

The budget and cost data were based on the information collected during interviews and meetings with LYCAA and security professionals at the designated International Airport. Most of the cost data were based on unit prices for the screening equipment, obtained from LYCAA upgrade contracts. Other cost data were obtained from current offers submitted to the LYCAA for consideration. For simplicity, some combinations of two or more mitigation measures were used to facilitate smooth upgrade decision choices. The cost data gathered (for single and combinations of measures) were grouped into five main categories: ray and passenger physical

search, two types of X-ray scanners, background checks, trace detection, and physical screening. Under each category, a number of principal mitigation measures were identified as shown in Table 5.1.

Table 5.1: Cost Estimate for Upgrade Options

Category	Measure / Device	Qyt.
Ray and passenger physical search	Security guard (Operator)	20-36
	Metal detector gate (PMD2 / PTZ)	20-36
	Entry scan gat	20-36
	Millimeter wave gate	20-36
	Dielectric portal gate	20-36
	Handheld metal detectors	16-26
	Handheld explosive trace detectors	20-36
	Desktop explosive trace detectors	20-36
	Physical search guard	8-16
	Sniffing dog	2-8
	Biological agent detector	2-8
X-ray scanners	Conventional X-Ray (COB)	20-36
	Explosive X-ray (COB)	20-36
	EDS System-single view (OHB)	20-36
	EDS System doul view (OHB)	20-36
	EDS System multi-view (OHB)	20-36
Rotating X-ray scanners	CTX 2500 (OHB)	2-8
	CTX 5500 DS (OHB)	2-8
	CTX 9000 (OHB)	2-8
Background check	Criminal Check	1-2
	Biometric cameras and Fingerprints	20-36
Trace detection	Chemiluminescence	8-16
	Ion mobility spectrometry (Ionscan)	8-16
	Ion track itemizer	8-16
Physical scanners	Luggage hand search	8-16
	Luggage-sniffing dogs	2-8

The total allowable upgrade budget was determined to be $40,000,000. This budget was intended to cover all suggested upgrading measures (equipment and guards) for a one-year plan. For confidentiality reasons, unit prices have been omitted, actual quantities have been provided a range, and the total costs have been adjusted by an agreed-upon factor with respect to one of the designated items.

5.3.3 Comparison of Decision Approaches

According to LYCAA's international airport security professionals, the PCBSS is re-assessed and upgraded every two to three years. Currently, to comply with the latest ICAO security audit, the PCBSS should be immediately upgraded to the minimum acceptable risk level (0-5). The current LYCAA upgrading process is similar to the simple ranking approach presented in Chapter 4, with a small difference: the security checkpoints are sorted manually according to their subjective importance and reliability, not according to their risk index. Decisions are then made to allocate upgrades to the top-ranked items. Thus, using the developed framework, it is possible to simulate the decisions made by the LYCAA officials and to compare them with the decisions determined by the optimization framework. The main objective of the developed optimization framework is to reduce the overall security risk index to within an acceptable level (0 – 5). The comparison of the LYCAA simple ranking approach and the proposed optimization model was based on the following results:

- Vulnerability scores (passengers, cabin baggage, and checked-in luggage)
- The overall SRI
- The security upgrade benefit
- The benefit-cost ratio

Case 1 - LYCAA Decisions Using Simple Ranking for Maximum Upgrades

According to the practice of LYCAA official, the security checkpoints were prioritized according to their importance, as illustrated in Table 5.2 and this priority ranking approach governs the upgrade decisions. Figure 5.5 shows an MS Excel spreadsheet that models the in-place and upgrade mitigation measures at LYCAA's international airport. Part A shows the existing mitigation types or combination of types. Part B shows the suggested upgrade options. Part C presents LYCAA's priority ranking of all SCPs. Part D show the associated upgrade cost.

The SCP that has the top priority is upgraded first to the maximum level, and then the next one that has the second priority will be upgraded to the second to the highest level, and so on.

Table 5.2: Simple Ranking Index for Checkpoints

Subsystem	Security Checkpoint	Priority (1 = Highest – 10 = Lowest)
Departure	Curb-side / Pre-Check-in	1
	Airline check-in screening	2
	Out bound luggage screening	3
	Passenger central gate screening	5
	Gate screening	8
Arrival	Gate screening	4
	Passport control	6
	Inbound luggage screening	7
	Transit luggage screening	9
	Transferred luggage screening	10

As can be seen in Figure 5.6, following the LYCAA strategy for spending the available budget resulted in an inability to upgrade a number of security checkpoints. As expected, the new overall SRI (**6.15**), is still higher than the acceptable limit (0-5), and the overall passenger vulnerability is extremely high (17.11) compared to 1.23 and 0.11 for cabin baggage and checked-in luggage, respectively. Therefore, it is clear that the simple ranking strategy does not fully meet the upgrade objectives, and the following observations can be made about the LYCAA approach:

1- LYCAA's decision using simple ranking for maximizing upgrades is not efficacious.

2- Close attention should be paid to the mitigation measures at security checkpoints that require large expenditures, in order to determine whether or not to upgrade them to their highest level or to the acceptable level of reliability.

3- Upgrading some security checkpoints to their highest level does not guarantee the achievement of either the lowest SRI or the best B/C ratio.

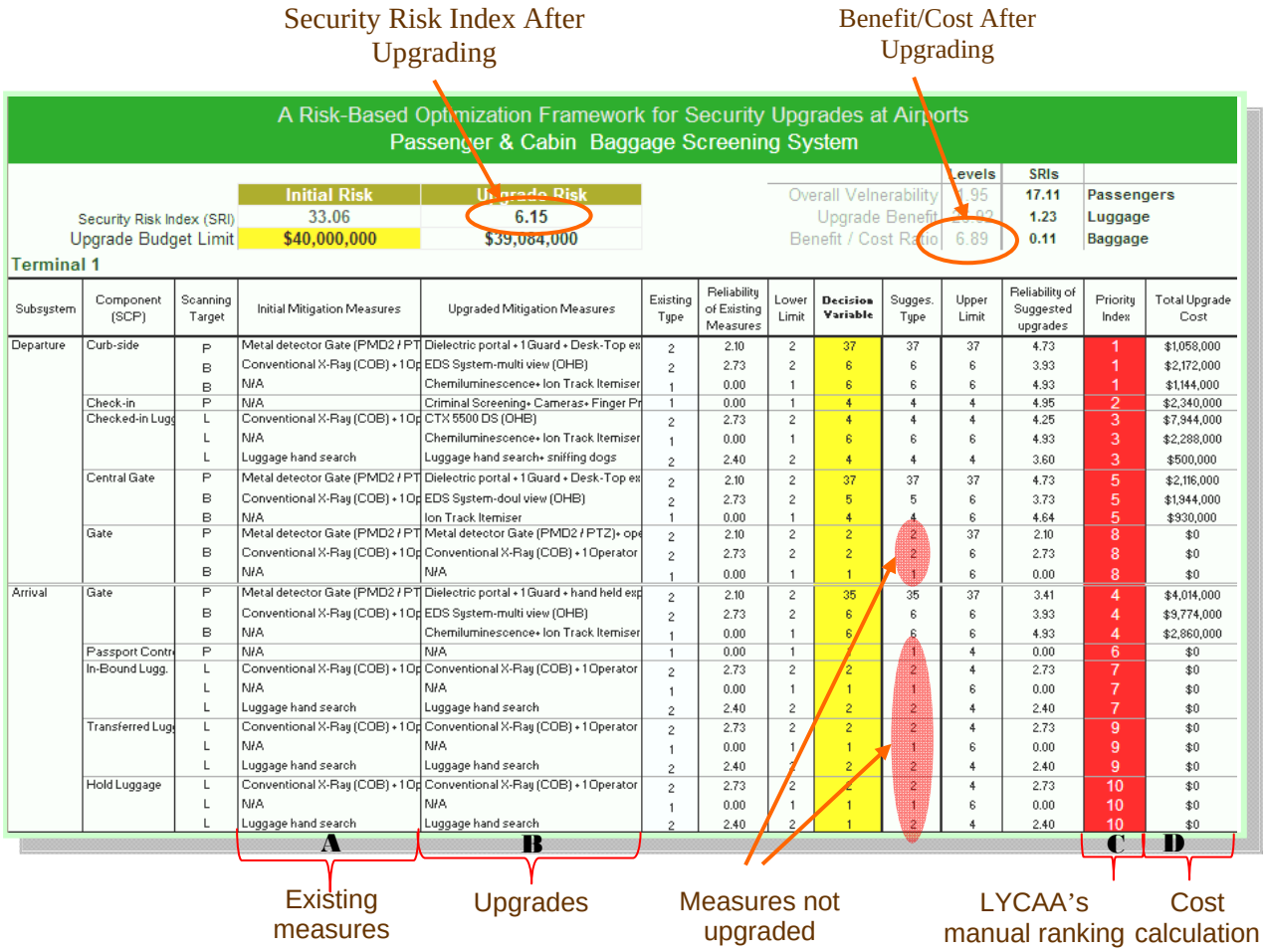
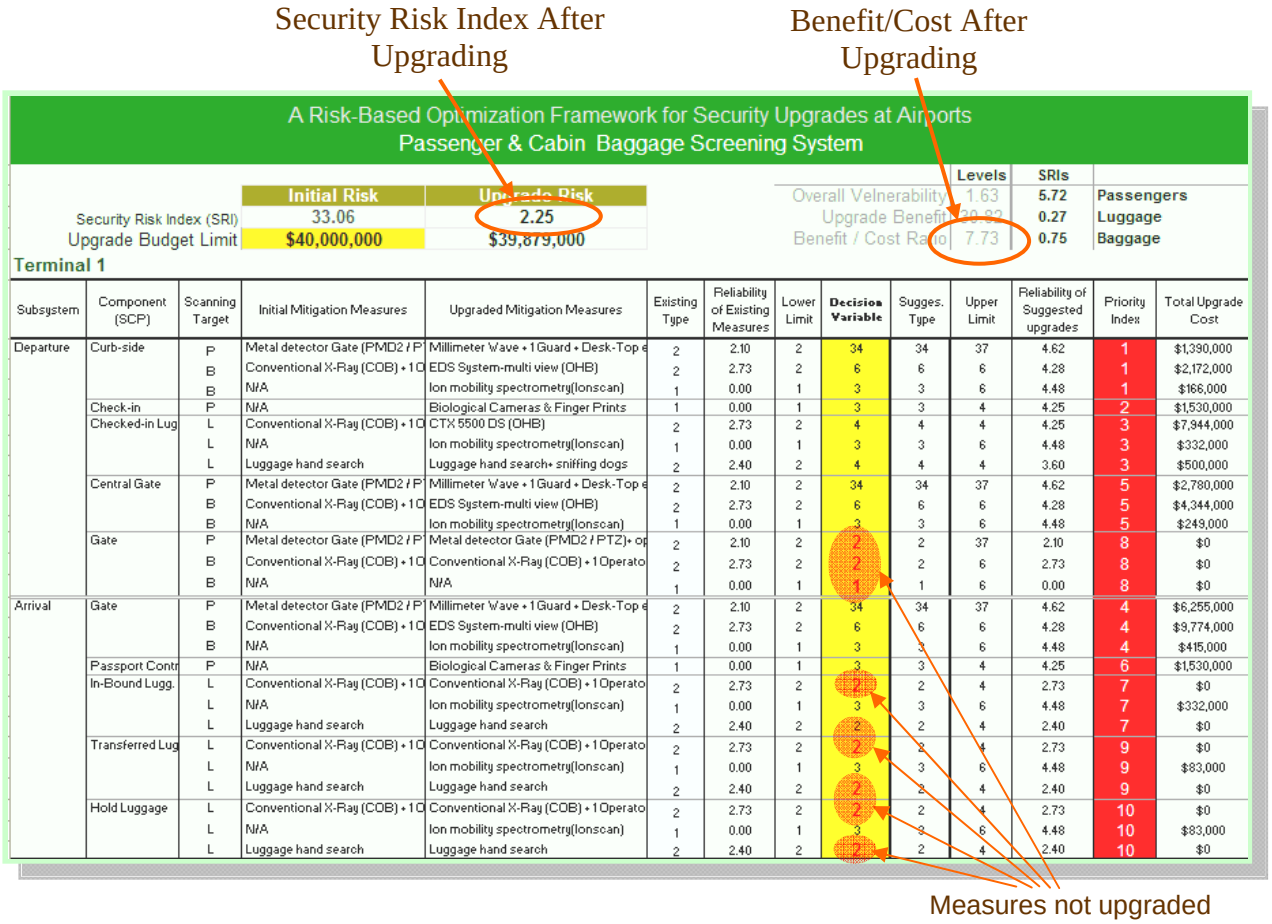


Figure 5.6: Case 1 - Simple Ranking Decisions for Maximizing Upgrades

Case 2- LYCAA Decisions Using Simple Ranking Under Reliability Constraints

Another manual approach is used in which each security measure is upgraded not to the maximum (as in case 1) but to an acceptable level of equipment reliability, in order to save costs. The acceptable reliability level is assumed to be 4.25. With this approach, the same LYCAA priority ranking is kept, but each security measure is upgraded only to the acceptable reliability

level. Figure 5.7 presents the results of the modified LYCAA strategy. Although some measures have been left without upgrades, this approach achieved better results than the approach in case 1. The overall SRI has been substantially reduced, to 2.25, compared with the SRI produce with the original LYCAA strategy (6.15). In addition, the passenger risk has also been substantially improved.



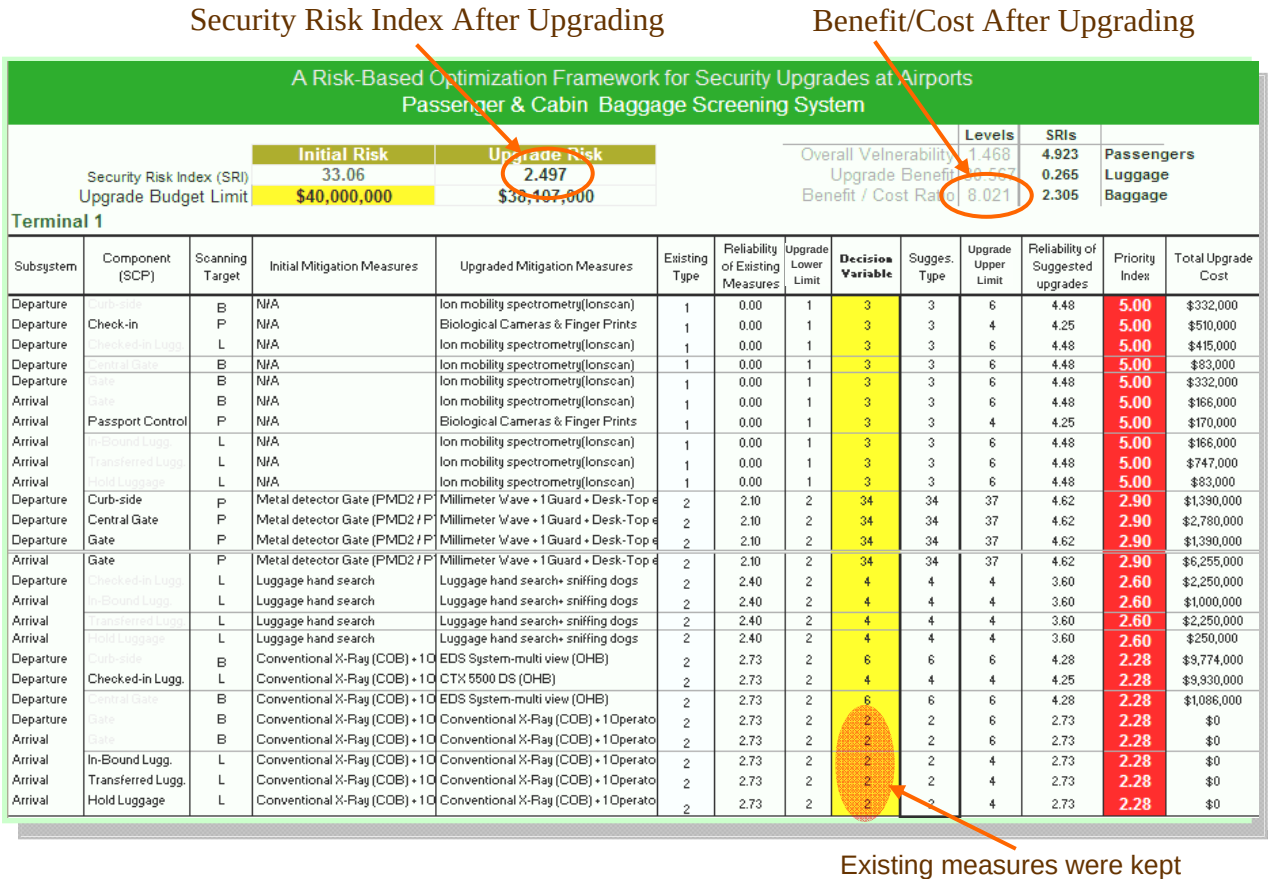
Subsystem	Component (SCP)	Scanning Target	Initial Mitigation Measures	Upgraded Mitigation Measures	Existing Type	Reliability of Existing Measures	Lower Limit	Decision Variable	Sugges. Type	Upper Limit	Reliability of Suggested upgrades	Priority Index	Total Upgrade Cost
Departure	Curb-side	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	1	$1,390,000
		B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	1	$2,172,000
		B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	1	$166,000
	Check-in	P	N/A	Biological Cameras & Finger Prints	1	0.00	1	3	3	4	4.25	2	$1,530,000
	Checked-in Lug	L	Conventional X-Ray (COB) + 1 O	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	3	$7,944,000
		L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	3	$332,000
		L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	3	$500,000
	Central Gate	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	5	$2,780,000
		B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	5	$4,344,000
		B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5	$249,000
	Gate	P	Metal detector Gate (PMD2 / P	Metal detector Gate (PMD2 / PTZ)+ op	2	2.10	2	2	2	37	2.10	8	$0
		B	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	6	2.73	8	$0
		B	N/A	N/A	1	0.00	1	1	1	6	0.00	8	$0
Arrival	Gate	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	4	$6,255,000
		B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	4	$9,774,000
		B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	4	$415,000
	Passport Contr	P	N/A	Biological Cameras & Finger Prints	1	0.00	1	3	3	4	4.25	6	$1,530,000
	In-Bound Lugg.	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	7	$0
		L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	7	$332,000
		L	Luggage hand search	Luggage hand search	2	2.40	2	2	2	4	2.40	7	$0
	Transferred Lug	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	9	$0
		L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	9	$83,000
		L	Luggage hand search	Luggage hand search	2	2.40	2	2	2	4	2.40	9	$0
	Hold Luggage	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	10	$0
		L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	10	$83,000
		L	Luggage hand search	Luggage hand search	2	2.40	2	2	2	4	2.40	10	$0

Figure 5.7: Case 2 - Simple Ranking Decisions under a Reliability Constraint of 4.25

Case 3 - Simple Ranking Based on the Risk Index

This approach is based on the risk index for each security measure rather than on a subjective priority as in cases 1and 2. The priority indexes for different measures were calculated accordingly to Equation 4.9, sorted in descending order, and the top-ranked one was upgraded to

an acceptable reliability level (4.25), until the budget is entirely utilized. Figure 5.8 presents the results of this approach. The risk indexes of all security measures are highlighted. The overall SRI is 2.497, which is slightly higher than in case 2. However, this approach improved the benefit-cost ratio to 8.021, which is slightly better than in case 1 or 2, and the upgrade cost is almost 1.77 million less than in case 2. It is possible, therefore, to conclude that this solution produces slightly better results than those in case 2.



Subsystem	Component (SCP)	Scanning Target	Initial Mitigation Measures	Upgraded Mitigation Measures	Existing Type	Reliability of Existing Measures	Upgrade Lower Limit	Decision Variable	Sugges. Type	Upgrade Upper Limit	Reliability of Suggested upgrades	Priority Index	Total Upgrade Cost
Departure	Curb-side	B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$332,000
Departure	Check-in	P	N/A	Biological Cameras & Finger Prints	1	0.00	1	3	3	4	4.25	5.00	$510,000
Departure	Checked-in Lugg.	L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$415,000
Departure	Central Gate	B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$83,000
Departure	Gate	B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$332,000
Arrival	Gate	B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$166,000
Arrival	Passport Control	P	N/A	Biological Cameras & Finger Prints	1	0.00	1	3	3	4	4.25	5.00	$170,000
Arrival	In-Bound Lugg.	L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$166,000
Arrival	Transferred Lugg.	L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$747,000
Arrival	Hold Luggage	L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	5.00	$83,000
Departure	Curb-side	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	2.90	$1,390,000
Departure	Central Gate	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	2.90	$2,780,000
Departure	Gate	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	2.90	$1,390,000
Arrival	Gate	P	Metal detector Gate (PMD2 / P	Millimeter Wave + 1 Guard + Desk-Top e	2	2.10	2	34	34	37	4.62	2.90	$6,255,000
Departure	Checked-in Lugg.	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$2,250,000
Arrival	In-Bound Lugg.	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$1,000,000
Arrival	Transferred Lugg.	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$2,250,000
Arrival	Hold Luggage	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$250,000
Departure	Curb-side	B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	2.28	$9,774,000
Departure	Checked-in Lugg.	L	Conventional X-Ray (COB) + 1 O	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	2.28	$9,930,000
Departure	Central Gate	B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	2.28	$1,086,000
Departure	Gate	B	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	6	2.73	2.28	$0
Arrival	Gate	B	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	6	2.73	2.28	$0
Arrival	In-Bound Lugg.	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	2.28	$0
Arrival	Transferred Lugg.	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	2.28	$0
Arrival	Hold Luggage	L	Conventional X-Ray (COB) + 1 O	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	2.28	$0

Figure 5.8: Case 3 - Simple Ranking Decisions Based on the Risk Index

Case 4 – GA-Based Optimization Decisions

Another approach is to upgrade the existing measures using the optimization feature of the used framework with two objective functions: maximize the benefit-cost ratio and minimize the

security risk index (case 4, as illustrated in Figure 5.9). The goal is to compare decisions produced by used the framework with previous decisions for the same reliability constraint (**4.25**). It should be noted that both objective functions arrive at exactly the same upgrade results. Thus, it is clearly shown that the overall B/C and SRI have improved more than in the previous three cases. The GA optimization solutions have achieved an overall B/C ratio of **8.053** and have reduced the overall risk to **1.428**. A summary of the upgrade decisions in the various cases is shown in Table 5.3 and in Figures 5.6 to 5.12. The overall security risk index has decreased, from a high of 6.15 using LYCAA's simple ranking decisions to 1.248 produced with optimization approach.

Subsystem	Component (SCP)	Scanning Target	Initial Mitigation Measures	Upgraded Mitigation Measures	Existing Type	Reliability of Existing Measures	Upgrade Lower Limit	Decision Variable	Sugges. Type	Upgrade Upper Limit	Reliability of Suggested upgrades	Total Upgrade Cost
Departure	Curb-side	P	Metal detector Gate (PMD2 / P	Metal Detection Gate+ 1 Guard + Desk-	2	2.10	2	35	35	37	4.67	$442,000
		B	Conventional X-Ray (COB) + 1C	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	$2,172,000
		B	N/A	Ion Track Itemiser	1	0.00	1	4	4	6	4.64	$620,000
	Check-in	P	N/A	Biological Cameras & Finger Prints	1	0.00	1	3	3	4	4.25	$1,530,000
	Checked-in Lug	L	Conventional X-Ray (COB) + 1C	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	$7,944,000
		L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	$332,000
		L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	$500,000
	Central Gate	P	Metal detector Gate (PMD2 / P	Metal Detection Gate+ 1 Guard + Desk-	2	2.10	2	35	35	37	4.67	$884,000
		B	Conventional X-Ray (COB) + 1C	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	$4,344,000
		B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	$249,000
	Gate	P	Metal detector Gate (PMD2 / P	Metal Detection Gate+ 1 Guard + Desk-	2	2.10	2	35	35	37	4.67	$1,989,000
		B	Conventional X-Ray (COB) + 1C	EDS System-doul view (OHB)	2	2.73	2	5	5	6	3.93	$2,430,000
		B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	$747,000
Arrival	Gate	P	Metal detector Gate (PMD2 / P	Metal Detection Gate+ 1 Guard + Desk-	2	2.10	2	35	35	37	4.67	$1,989,000
		B	Conventional X-Ray (COB) + 1C	EDS System-doul view (OHB)	2	2.73	2	5	5	6	3.93	$4,374,000
		B	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	$415,000
	Passport Contr	P	N/A	Biological Cameras & Finger Prints	1	0.00	1	3	3	4	4.25	$1,530,000
	In-Bound Lugg.	L	Conventional X-Ray (COB) + 1C	Conventional X-Ray (COB) + 1 Operato	2	2.73	2	2	2	4	2.73	$0
		L	N/A	Ion Track Itemiser	1	0.00	1	4	4	6	4.64	$1,240,000
		L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	$500,000
	Transferred Lug	L	Conventional X-Ray (COB) + 1C	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	$1,986,000
		L	N/A	Chemiluminescence+ Ionscan	1	0.00	1	5	5	6	4.75	$508,000
		L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	$250,000
	Hold Luggage	L	Conventional X-Ray (COB) + 1C	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	$1,986,000
		L	N/A	Ion mobility spectrometry(Ionscan)	1	0.00	1	3	3	6	4.48	$83,000
		L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	$250,000

Figure 5.9: Case 4 - GA-Based Optimization Decisions

As a result, compared to the other approaches, the optimization model using the GA technique was able to achieve the best results, considering the same budget limit, and to utilize the available budget to the maximum. The security systems in the designated LYCAA airport can therefore be upgraded to the acceptable reliability level (**4.25)** with a total upgrade expenditure of $39,294,000.

Table 5.3: Comparison of the Decision Approaches

Decision Approach (Case)	Expenditure ($)	SRI	B/C	Detailed Risks		
				Passenger	Baggage	Luggage
Case 1- Simple ranking for maximum upgrades	39,084,000	6.15	6.89	17.11	0.11	1.23
Case 2- Simple ranking under reliability constraints	39,879,000	2.25	7.73	5.720	0.750	0.270
Case 3- Simple ranking based on risk index	38,107,000	2.497	8.021	4.923	2.306	0.265
Case 4- GA-based optimization	39,294,000	1.428	8.051	2.885	1.134	0.264

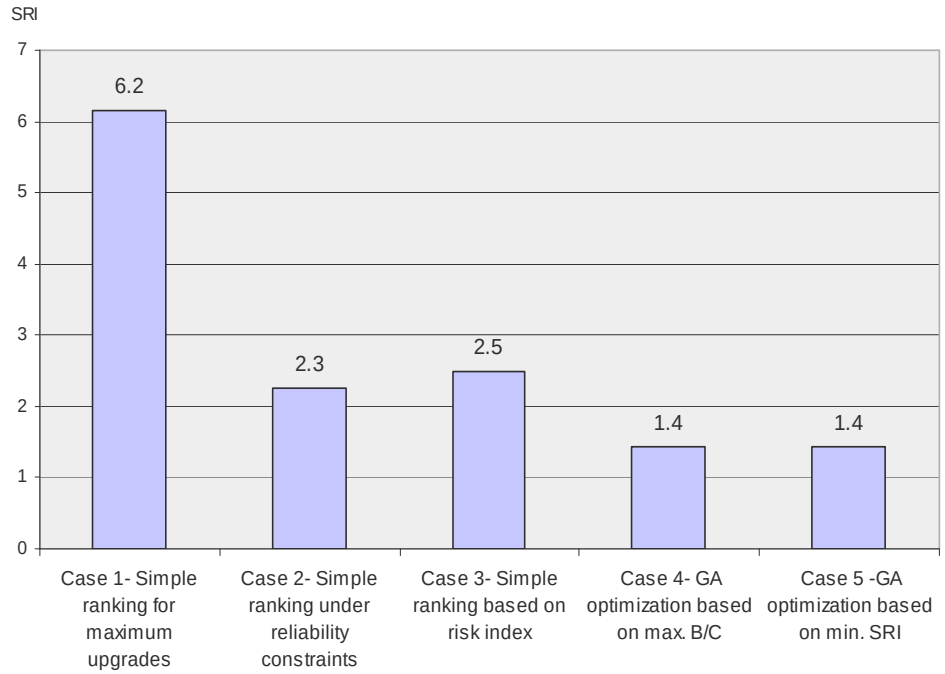


Figure 5.10: Comparison of the SRI Values

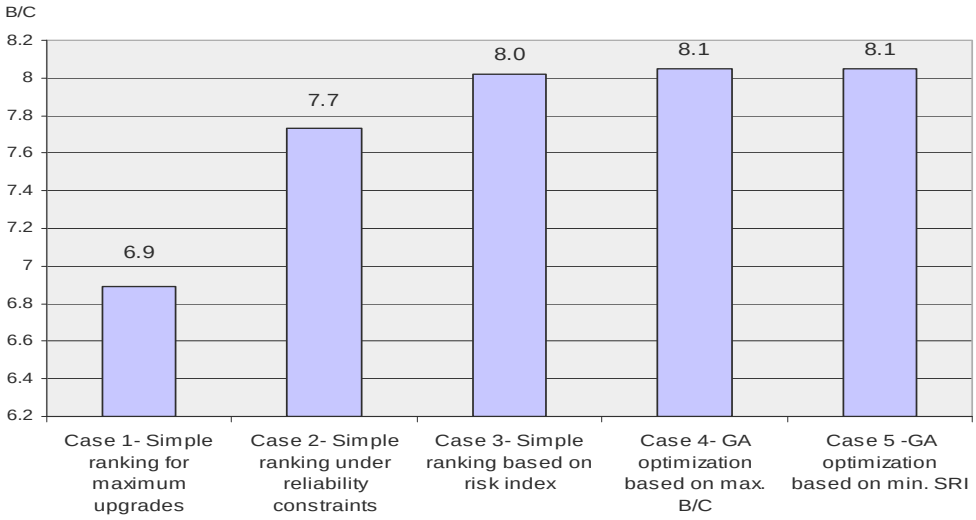


Figure 5.11: Comparison of the B/C Ratios

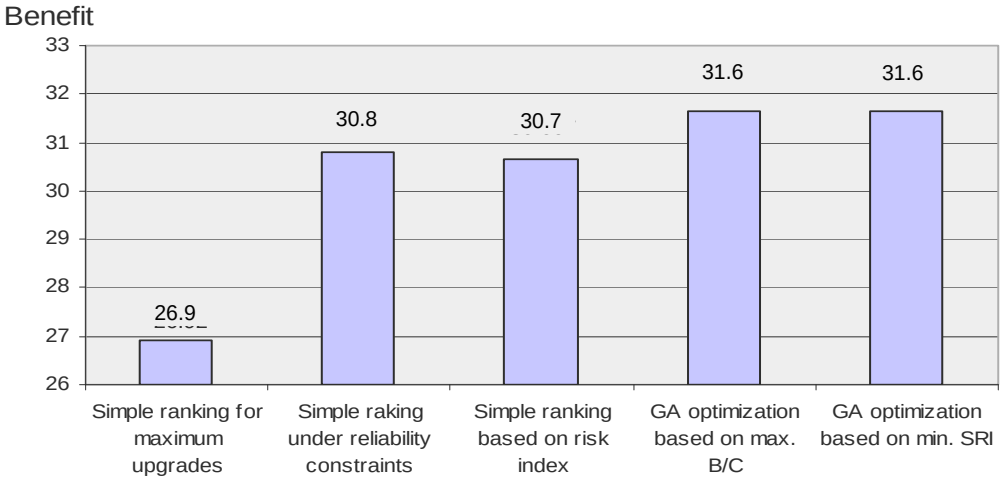


Figure 5.12: Comparison of the Upgrade Benefits

5.3.4 Additional Experiments

Once the performance of the optimization model was validated, the following additional experiments were carried out to provide security decision makers with meaningful analysis for them to use as part of the decision support:

1- The effect of different upgrade budgets ($10M - $40M) on the security risk index (SRI) was examined.

2- The upgrade budget level that achieves the minimum SRI was determined.

3- A detailed sensitivity analysis was conducted with respect to the upgrade decisions and the level of confidence in the decision made.

Effect of various upgrade budgets

For the testing of the effect of upgrade budgets, the optimization was run under different budget limits ranging from $10M to $35M. All previous constraints remained the same. The objective function in the first run was thus set to minimize the overall security risk index, and in the second run, it was set to maximize the B/C ratio. The results of all runs are shown in Tables 5.4 and 5.5, and in Figures 5.13 to 5.15.

Table 5.4 The Effect of Different Upgrade Budgets on Minimizing the SRI

Experiment	Budget Limit	Upgrade Budget ($10M)	Min. SRI	Achieved B/C	Detailed Risks		
					Passenger	Baggage	Luggage
1	$10	9.914	2.389	30.941	4.107	2.314	0.747
2	$20	19.758	2.011	15.717	2.981	2.306	0.747
3	$30	28.427	1.589	11.072	2.885	1.135	0.747
4	$35	34.834	1.586	9.037	2.887	1.134	0.747

Table 5.5: The Effect of Different Upgrade Budgets Maximizing the B/C Ratio

Experiment	Budget Limit	Upgrade Budget ($10M)	Max. B/C	Achieved SRI	Detailed Risks		
					Passenger	Baggage	Luggage
1	$10	9.691	20.802	13.606	37.756	2.314	0.747
2	$20	19.542	11.376	10.846	29.716	2.307	0.515
3	$30	29.790	10.566	1.589	2.885	1.134	0.747
4	$35	34.967	8.891	1.967	2.877	2.304	0.747

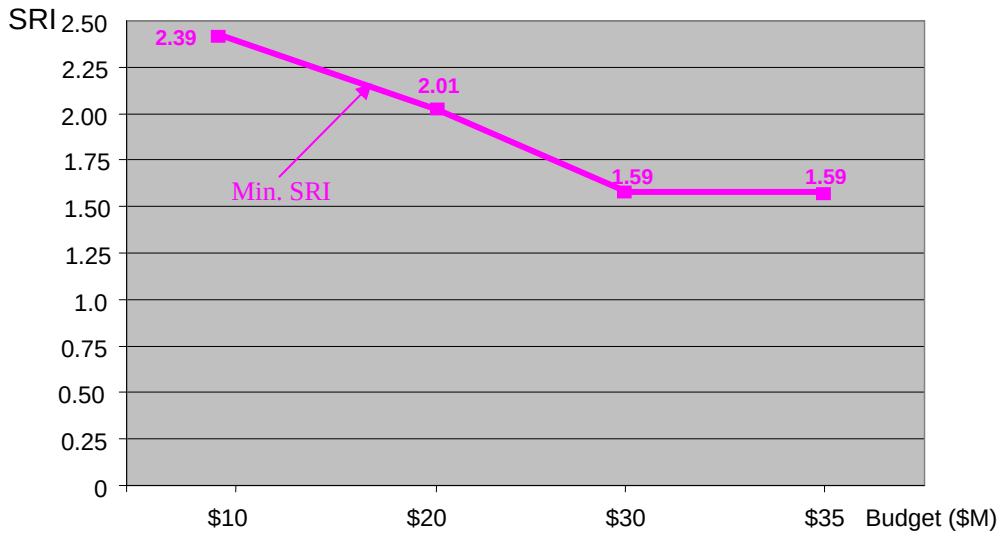


Figure 5.13: Effect of Different Budget Limits on Minimizing the SRI

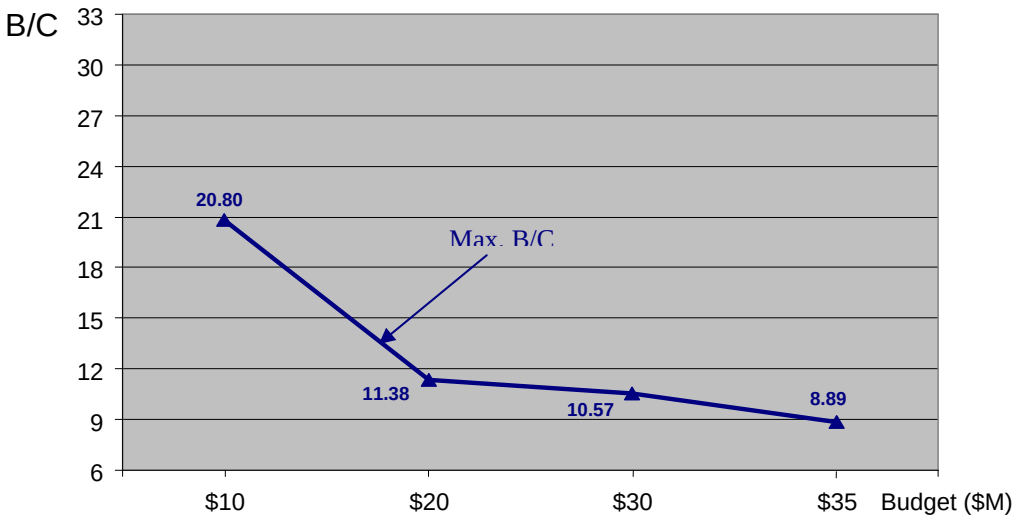
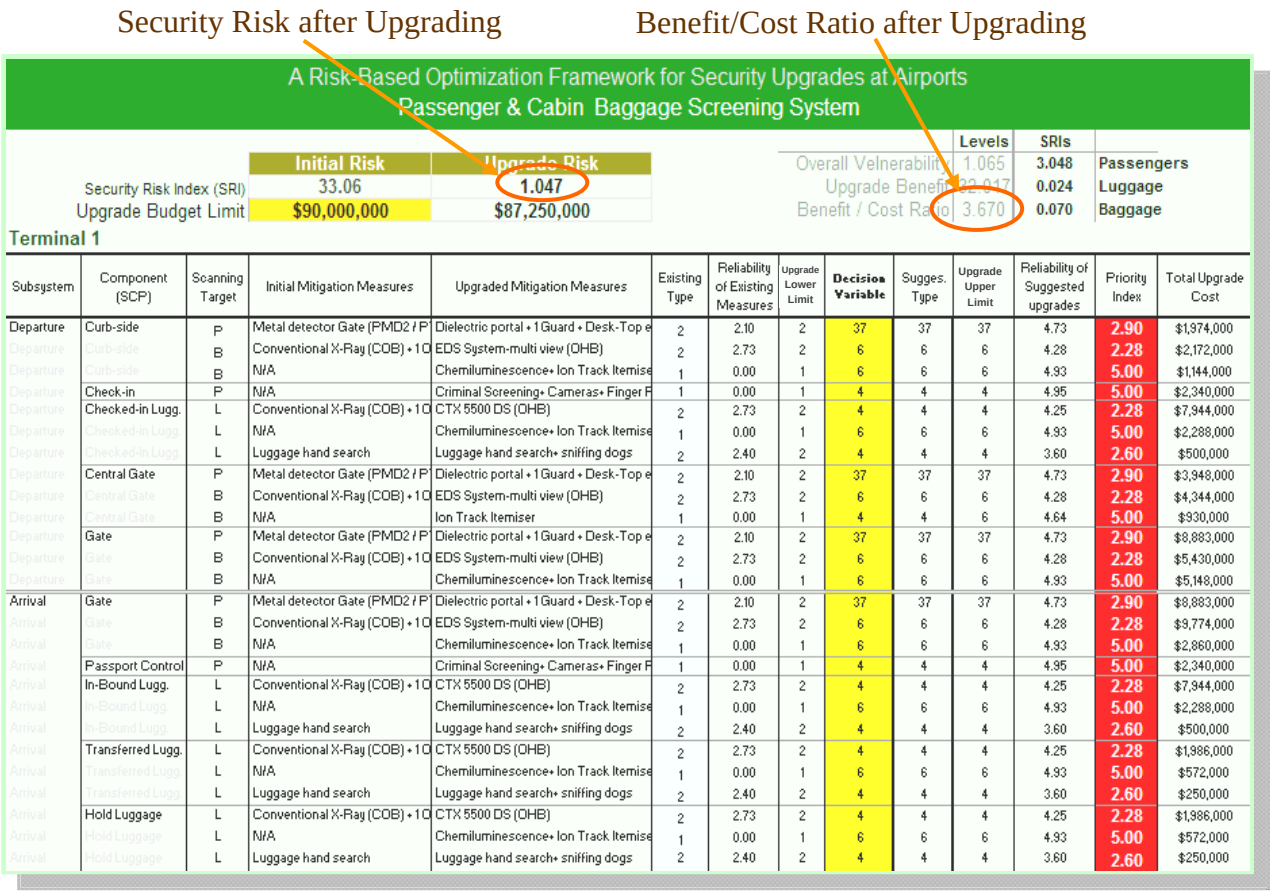


Figure 5.14: Effect of Different Budget Limits on Maximizing the B/C Ratio

As shown in Figures 5.13 and 5.14, the effect of different upgrade budgets is to produce different results in terms of minimum SRI and maximum B/C for each budget limit. It can also be noted that optimizing the upgrades based on minimizing the overall SRI produces better results. Furthermore, both objective functions arrive at the same minimum SRI (1.59) for $30 million budget limit and a very close maximum B/C ration (10.97 and 11.07) at that budget limit. The conclusion is that the cost of the optimum upgrade strategy in this case is $28,427,000.

Upgrade Budget That Achieves the Minimum SRI

As shown in Equation 3.13, for this test, the objective function was set to minimize the overall SRI with no constraints on budget and considering the same reliability constraint used in the previous test. It was assumed that the model is capable of achieving the lowest SRI score. As shown in Figure 5.15, the budget associated with the minimum SRI achieved is $87,250,000, and the minimum SRI achieved is 1.047.



Subsystem	Component (SCP)	Scanning Target	Initial Mitigation Measures	Upgraded Mitigation Measures	Existing Type	Reliability of Existing Measures	Upgrade Lower Limit	Decision Variable	Sugges. Type	Upgrade Upper Limit	Reliability of Suggested upgrades	Priority Index	Total Upgrade Cost
Departure	Curb-side	P	Metal detector Gate (PMD2 / P	Dielectric portal + 1 Guard + Desk-Top e	2	2.10	2	37	37	37	4.73	2.90	$1,974,000
Departure	Curb-side	B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	2.28	$2,172,000
Departure	Curb-side	B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$1,144,000
Departure	Check-in	P	N/A	Criminal Screening+ Cameras+ Finger P	1	0.00	1	4	4	4	4.95	5.00	$2,340,000
Departure	Checked-in Lugg.	L	Conventional X-Ray (COB) + 1 O	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	2.28	$7,944,000
Departure	Checked-in Lugg.	L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$2,288,000
Departure	Checked-in Lugg.	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$500,000
Departure	Central Gate	P	Metal detector Gate (PMD2 / P	Dielectric portal + 1 Guard + Desk-Top e	2	2.10	2	37	37	37	4.73	2.90	$3,948,000
Departure	Central Gate	B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	2.28	$4,344,000
Departure	Central Gate	B	N/A	Ion Track Itemiser	1	0.00	1	4	4	6	4.64	5.00	$930,000
Departure	Gate	P	Metal detector Gate (PMD2 / P	Dielectric portal + 1 Guard + Desk-Top e	2	2.10	2	37	37	37	4.73	2.90	$8,883,000
Departure	Gate	B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	2.28	$5,430,000
Departure	Gate	B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$5,148,000
Arrival	Gate	P	Metal detector Gate (PMD2 / P	Dielectric portal + 1 Guard + Desk-Top e	2	2.10	2	37	37	37	4.73	2.90	$8,883,000
Arrival	Gate	B	Conventional X-Ray (COB) + 1 O	EDS System-multi view (OHB)	2	2.73	2	6	6	6	4.28	2.28	$9,774,000
Arrival	Gate	B	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$2,860,000
Arrival	Passport Control	P	N/A	Criminal Screening+ Cameras+ Finger P	1	0.00	1	4	4	4	4.95	5.00	$2,340,000
Arrival	In-Bound Lugg.	L	Conventional X-Ray (COB) + 1 O	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	2.28	$7,944,000
Arrival	In-Bound Lugg.	L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$2,288,000
Arrival	In-Bound Lugg.	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$500,000
Arrival	Transferred Lugg.	L	Conventional X-Ray (COB) + 1 O	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	2.28	$1,986,000
Arrival	Transferred Lugg.	L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$572,000
Arrival	Transferred Lugg.	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$250,000
Arrival	Hold Luggage	L	Conventional X-Ray (COB) + 1 O	CTX 5500 DS (OHB)	2	2.73	2	4	4	4	4.25	2.28	$1,986,000
Arrival	Hold Luggage	L	N/A	Chemiluminescence+ Ion Track Itemise	1	0.00	1	6	6	6	4.93	5.00	$572,000
Arrival	Hold Luggage	L	Luggage hand search	Luggage hand search+ sniffing dogs	2	2.40	2	4	4	4	3.60	2.60	$250,000

Figure 5.15: GA Optimization Upgrade Budget That Achieves the Minimum SRI

Detailed Sensitivity Analysis

Another experiment conducted was a detailed sensitivity analysis to test the level of confidence in the results produced by the framework. In this experiment, the sensitivity analysis was based

on running the optimization model under ten different threat levels that varied by ± 20% from the initial threat level. The original constraints and budget limit of $40M remained the same. The objective with this scenario was to minimize the overall SRI. As a result, the ten optimization experiments were run using ten randomly selected threat levels that were about ± 20% of the original threat level (4.44), ranging from 4.46 to 4.22. The resulting SRI levels range from 1.255 to 1.474. The results of the ten runs are shown in Table 5.6. As shown in Table 5.6 and Figures 5.16 to 5.18, as the threat level changes within a ± 20% range, the SRI changes accordingly. It can be noted that even if the overall threat score is the same, different threat combinations produce different upgrade decisions. In the various scenarios, the standard deviation of the threat levels is 0.083, and the mean threat level is 4.3275. As a result, the average of the optimization results is an SRI of 4.431 (STDV = 0.122). The small standard deviation indicates confidence that even with a ± 20% change in the threat levels, the upgrades will achieve a low SRI of 1.431, which is falls within the acceptable risk level (0-5).

Table 5.6: Levels of Threat Sensitivity Versus the SRI

Scenario	Overall Threat Level	SRI	B/C	Overall Vulnerability	Detailed Risks			Upgrade Budget
					Passenger	Baggage	Luggage	
1	4.33	1.47	8.04	1.27	3.00	1.11	0.32	$39,688,000
2	4.26	1.40	7.16	1.30	2.68	1.04	0.47	$39,550,000
3	4.46	1.53	7.97	1.30	2.92	1.13	0.52	$39,754,000
4	4.22	1.64	6.74	1.40	2.51	1.98	0.43	$39,962,000
5	4.42	1.44	8.25	1.26	2.89	1.15	0.27	$39,901,000
6	4.26	1.30	7.28	1.24	2.69	1.05	0.17	$39,783,000
7	4.36	1.42	6.86	1.32	2.59	1.00	0.66	$39,480,000
8	4.31	1.26	6.79	1.25	2.66	0.95	0.15	$39,714,000
9	4.35	1.26	6.75	1.24	2.59	0.93	0.27	$39,616,000
10	4.38	1.41	7.98	1.26	2.89	1.09	0.26	$39,720,000
μ	4.33	1.43	7.39	1.30	2.74	1.18	0.37	
σ	0.08	0.12	0.61	0.05	0.17	0.33	0.1786	

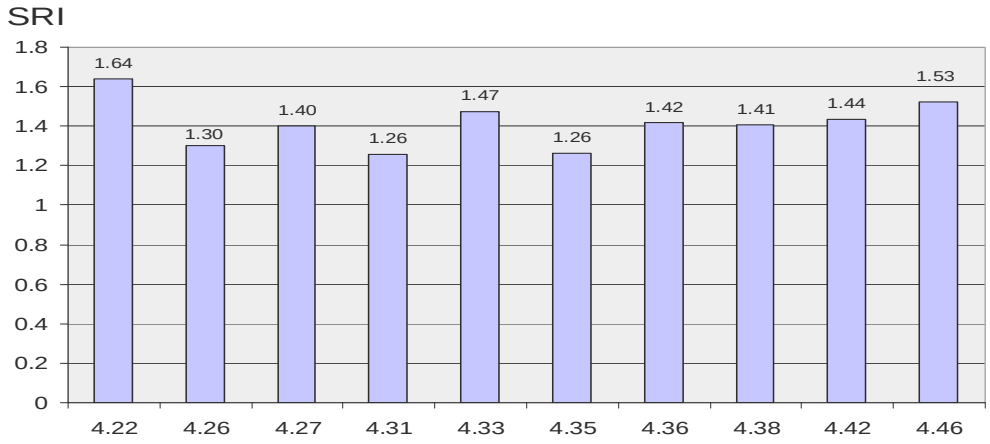


Figure 5.16: Sensitivity Plot of Threat versus the SRI

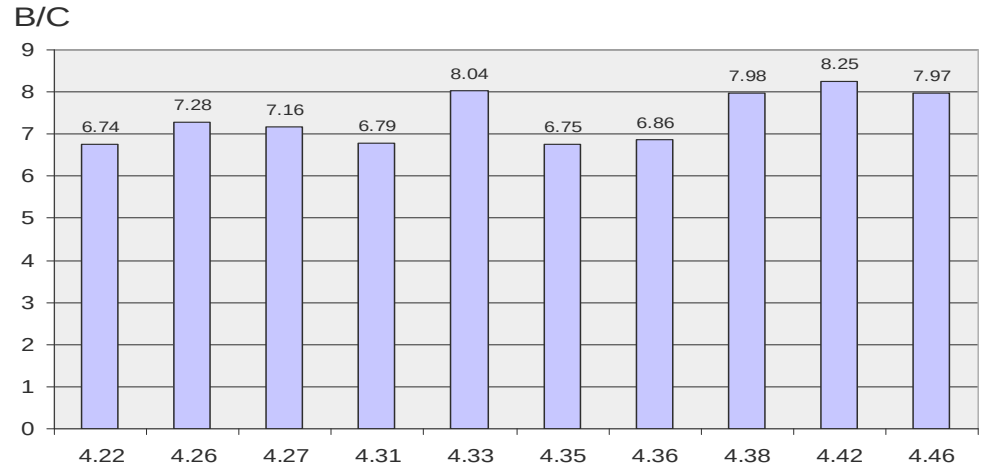


Figure 5.17: Sensitivity Plot of Threat versus the B/C Ratio

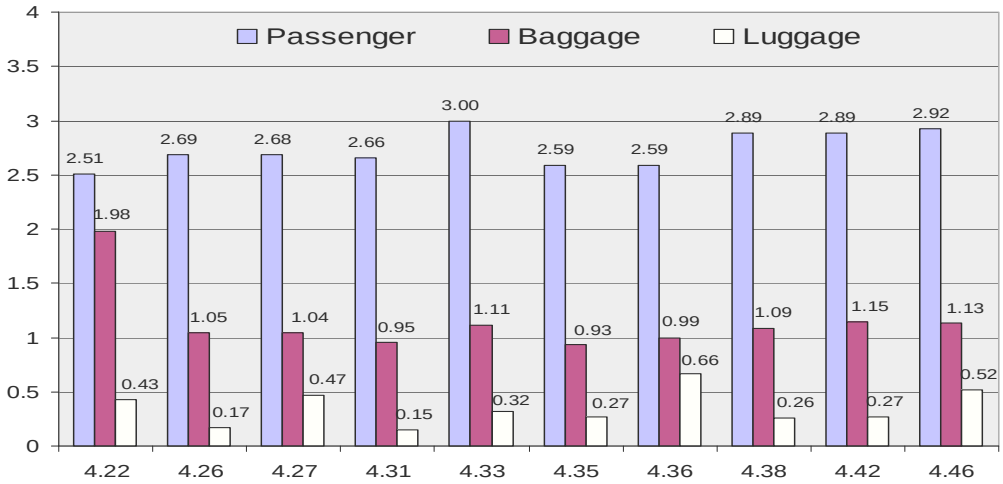


Figure 5.18: Sensitivity Comparison of Detailed Risk Levels

To test the degree of confidence in these results, the confidence principle was used to return a value that can be used to construct a confidence interval for the means of the ten optimization runs. Since the confidence interval is a range of values, is defined as the mean (x) ± confidence. For any population (number of different threat levels) mean μ_0 in this range, the probability of obtaining a sample mean further from μ_0 than x is greater than alpha; for any population mean μ_0 not in this range, the probability of obtaining a sample mean further from μ_0 than x is less than alpha.

Based on Table 5.6, the data mean of all SRIs (1.431), the standard deviation (0.12), and the size (8) were used to construct a two-tailed test at significance level alpha (5%) of the hypothesis that the population mean is μ_0. The hypothesis is then not rejected if μ_0 is in the confidence interval, and it is rejected if μ_0 is not in the confidence interval. The confidence interval does not allow the inference that there is probability 1 – alpha that the next threat level will have an SRI that is within the confidence interval. Therefore, assuming that alpha equals 0.05, the area under the standard normal curve equals (1 - alpha), or 95%; this value is therefore ± 1.96. Thus, the confidence interval can therefore be calculated as follows:

$$Confidence \quad Interval \quad = \chi \pm 1.96 \left(\frac{\sigma}{\sqrt{n}} \right) \qquad \textbf{5.1}$$

Using Equation 5.1, the confidence interval is 0.0291. Accordingly, the confidence interval then equals 1.431 ± 0.0291 or approximately [1.402, 1,460]. To test this hypothesis, SRIs of the fourth (1.641), fifth (1.437), sixth (1.301), and eighth (1.255) threat levels were chosen and their means (μ_0) were computed and checked in order to determine whether they fell within the range of the confidence interval, the mean equals 1.410, which definitely falls within the range of the

confidence interval. Therefore, it can be said with 95% confidence that the mean of all SRIs of any number of threat levels within a ± 20% range of the original threat level and at a fixed budget (i.e., in this case, $40,000,000) ranges from approximately 1.402 to 1,460. Generally, these results show that the mean SRI for any number of threat levels μ_{SRI}, in this interval, the probability of obtaining a sample mean (μ_{SRI}) greater than 1.460 is only 5% likely to happen. Likewise, any mean threat level (μ_{SRI}) less than 1.402 is only 5% likely to happen.

5.4 LYCAA Feedback

Research meetings and interviews were held with security personnel at LYCAA headquarters and LYCAA's international airport, a survey questionnaire was completed, and LYCAA official tested and reviewed the framework by entering their in-place and proposed upgrade screening measures. The following feedback was collected:

1. The security metric was a valuable attribute of the framework that will facilitate security risk assessment at airports and will enable decision makers to evaluate and prioritize upgrade strategies more accurately.
2. The optimization model adds advantageous features that will help security officials allocate their constrained resources more cost-effectively.
3. The overall performance and simplicity of the framework as well as the multiple levels of SRI and security scores make it a practical and reliable user-friendly tool for any risk-based plan for upgrading security infrastructure at airports.
4. The flexibility of the framework enables security officials to consider the effects of changing one or more mitigation measures at the SCP, subsystem, and system levels as well as the resulting SRIs.

5. The optimization model makes it easy for decision makers to run “what if” scenarios, and to investigate the effects of imposing specific constraints or of forcing the framework to comply with specific security requirements or needs.
6. The ability of the framework to produce detailed security scores, SRIs, and comprehensive descriptions and assessments at different levels is a significant feature that LYCAA officials appreciated and valued.
7. The customization capabilities enhance practicality of the framework so that it can be used for optimizing multiple-year upgrade plans.

5.5 Conclusion

A risk-based optimization framework has been successfully developed. The framework considers practical upgrade constraints and uses an optimization approach to help airport authorities make cost-effective decisions that will maximize the return on upgrade investments. The optimization framework was validated through expert opinions from GTAA personnel and a real-life case study at an LYCAA international airport. Feedback from both GTAA and LYCAA officials verified the usefulness and functionality of the developed framework and its prototype.

CHAPTER 6
CONCLUSION

6.1 Summary

As pivotal links in the mass transportation infrastructure, airports have a substantial impact on regional and national economies. After the 9/11 tragedy, airport security has been of paramount importance in Canada and worldwide. To improve aviation security, governments and airport authorities have devoted significant resources to developing strategies and implementing more tightened security measures. Extensive programs have been initiated to help detect, deter, and mitigate security risks. At the research level, a number of studies have examined airport security by assessing prospective threat scenarios, deficiencies in the security systems that contribute to possible exploitation of the vulnerability of airports, and the potential forms of the consequences of breaches of security.

To help airport authorities make cost-effective decisions with respect to airport security upgrades, this research has developed a practical risk-based optimization framework for upgrading PCBSS in airport terminals. The framework features an innovative security metric for quantifying the three main dimensions of security risk at airport terminals: threats, vulnerabilities, and consequences. It then uses the results to produce a security risk index (SRI). The security metric was built to assess the PCBSS at any international airport terminal. The risk dimension associated with threat is categorized as explosives, sharp blades, and biological attack. Under each category a number of threat types are identified: the explosive category includes weapons, bombs, and explosive liquids; sharp blades includes knives, swords, razors, and cutters; and biological attack can be associated with choking, nerve, blood, and blister.

Vulnerabilities are assessed based on how the countermeasure (in place and suggested) is effective in detecting the potential threats at the level of system (terminal), subsystems (departure and arrival), and subsystem components (security checkpoints). The consequences are addressed from four perspectives: casualties, downtime, public exposure, and the amount of loss expressed as a percentage of the total replacement cost of the whole or part of the terminal.

The framework has an additional novel attribute: an optimization model that integrates the SRI, the upgrade options, and a genetic algorithm (GA) mechanism in order to produce cost-effective upgrade decisions. Since realistically, vulnerability is the only risk element that can be improved, a database was built that inventories the reliability (i.e., effectiveness) and cost data of state-of-the-art mitigation measures (equipment, devices, and measures). The database is dynamically linked with the optimization model so that multiple "what-if" scenarios can be investigated whenever any mitigation measure is changed, thereby enabling the decision makers to observe the resulting overall SRI, the benefit that would be derived from the security upgrade, the total cost of the upgrade, and the benefit cost ratio for each scenario.

Hypothetical data were used to test the functionality and performance of the framework, and three different approaches to decision making were examined: a manual decision approach based on simple ranking and risk priority index strategies, mathematical optimization, and an automated approach that uses an evolutionary algorithm. The performances of the three decision approaches were compared, and the results indicate that the GA-based decision strategy is more effective than the other two strategies. The GA-based strategy was therefore used to further validate the framework through a real-life case-study at an international airport. To ensure the optimality of the upgrading decisions, realistic constraints, including budget limits, minimum

and maximum upgrade limits, and specific levels of minimum upgrade types, were introduced into the optimization model.

Two objective functions were experimented with: one for maximizing the benefit/cost ratio and one for minimizing the overall SRI. The goal was to ensure that the framework is capable of producing the most cost-effective upgrade strategy with respect to suggesting the best countermeasures, optimizing the upgrade budget, and satisfying the constraints. Although the objective functions were formulated to optimize upgrade plans for multiple years, to simplify the optimization process the framework was run so that it considered a one-year planning horizon. Security officials are nevertheless able to optimize multiple-year plans by feeding the optimization model with the optimization decisions for the first year as input (starting GA population) for the second year, and so on.

A comparison of the results of the two objective functions reveals that the “minimizing SRI” decision strategy is the most promising approach. Consequently, based on the literature, on information obtained from several research interviews and meetings with security professionals at the GTAA, and on needs with respect to practicality and user friendliness, a risk-based optimization framework prototype was developed and modeled in an MS Excel spreadsheet environment in order to facilitate the framework validation.

The framework was validated through a demonstration to a group of security officials at the GTAA in order to obtain the opinions of security experts and through practical implementation in a real-life case study at a LYCAA international airport. A variety of decision strategies were tested: LYCAA’s priority rank-based and priority index-based approaches, a GA-based

maximizing the B/C ratio, and a GA-based solution for minimizing SRI. The results were compared, and then presented to and validated by security officials at the LYCAA Headquarters and at the designated LYCAA international airport. The framework was found to be dynamic and flexible in its ability to compute and display simultaneous aggregated and overall SRIs, user-friendly with respect to its interface, interactive in permitting users to introduce or eliminate constraints and to select specific measures, and capable of performing multiple "what-if" upgrade scenarios that can satisfy the various technical needs and requirements related to security at an airport terminal.

6.2 Conclusions

The following conclusions can be drawn:

1. It is feasible to quantify airport security risks using the developed threat, vulnerability, and consequence security metrics.
2. Security system upgrades at airports can be optimized using the preceding metrics and the developed optimization model based genetic algorithm.
3. Optimizing upgrade decisions based on minimizing the overall security risk index is the best strategy for determining the most cost-effective upgrade decisions.
4. The testing with the decision approaches, experiments, and sensitivity analysis presented proven the framework's capability of innovatively producing upgrade results that involve minimal expenditure, the lowest risk, and a quantified return on investment.
5. Based on the validation feedback, the framework's flexibility, dynamic interactivity, and simplicity will make it a helpful decision support tool for security officials at airports.

6. An additional advantage of the developed framework is its potential to be extended to include other security systems in airports in order to produce an overall security risk index at the airport level.

6.3 Research Contribution

Based on the literature survey in Chapter 2, the development of the security risk metric and optimization model, and the results and findings determined through research validation, this research has made the following contributions:

1. A comprehensive automated risk-based framework has been developed for the assessment and upgrading of security systems at airport terminals. Focusing on the PCBSS, the framework incorporates an analytical model that assesses the threats, vulnerabilities, and consequences related to the PCBSS, and it incorporates a dynamic optimization model based on GAs mechanism that provides a near optimum upgrade plan.
2. The developed framework (security metrics and GA-based optimization model) is a potentially useful internal tool that allows aviation officials, airport authorities, and security personnel to assess the risk status of their security systems, and to determine the required cost-effective rectifying actions that will to maintain the security risk at a specified level of service.
3. An innovative security metric that quantifies PCBSS security risks in the form of SRIs has been produced. As a product of the developed security metric, the SRIs provide a quantitative means of determining the level of security risk at the levels of the subsystem components, the subsystem, and the system. Likewise, when the security metric is

expanded to include a network of airports, the metric has the potential of being beneficial at the national airport network level.

4. The framework is the first tool of its kind that quantitatively assesses the dimensions of risk at airport terminals and that fully incorporates the results of the assessment (SRIs) into an automated optimization model that was a GA-mechanism-based methodology to search for the solutions.
5. One of the main advantages of this research is that the aggregated and overall security indexes can be employed to facilitate different types of security infrastructure upgrades, decision-making analysis with respect to techniques, and strategies over different planning horizons, and with a variety of constraints and needs.
6. The incorporation of the GA mechanism enables the framework to handle large-scale optimization cases that involve huge solution spaces, which is a typical problem in complex infrastructure management systems.
7. The flexible, interactive, and automatic features of the framework make it a unique decision support tool that offers airport security decision makers the opportunities to customize it and tweak its models in order to meet the specific upgrade constraints of their airport and to satisfy special security requirements and needs at specific levels.

6.4 Future Research

The following summary of recommendation is based on feedback from both GTAA and LYCAA security officials and on discussions about ways to enhance the security metrics and the optimization model and to improve the overall performance of the framework:

1- Introduce priority weights at the security checkpoints (SCPs) and subsystem levels in the case of a single system and at the system level in the case of multiple systems. The

objective is to allocate upgrade funds to the most influential SCP at the subsystem level and to the most influential subsystem at the system level and so on.

2- Expand the optimization model to include two-to three-year planning horizons or to use two-to three-year slices, and modify the associated constraints and needs accordingly.

3- Continue developing the MS Excel spreadsheet prototype so that overall performance can be improved and the framework will be capable of producing customized detailed security reports. Decision makers will then be able to specify individual parameters immediately after the assessment is complete, to tweak or modify them during the subsequent steps in the optimization process.

4- Develop the framework so that it can consider a multi-objective optimization function, and test the approach of incremental effectiveness (e.g., improvements in the SRI versus the B/C).

5- Since the framework has been developed using a risk-based metric, and due to the significance of its security metrics and optimization model, GTAA and LYCAA officials recommended expanding the developed framework and customizing it so that it includes all other security systems at the airport level, with the goal of adoption by the entire airport authority.

6- Continue the ongoing co-operation with GTAA and LYCAA security personnel in order to collect more practical data and integrate them into the framework. It is assumed that more collaboration and involvement of security experts will help with the reviewing, feedback, and authenticating of the design and with the integration and implementation of the developed risk-based framework.

References

Adebiyi, K. A., Charles-Owaba, O.E, & Waheed, M.A. (2007). Safety performance evaluation models: a review. *Journal of Disaster Prevention and Management*, Vol. 16, No. 2, pp. 178-187. Emerald Group Publishing Limited.

Airports Council International North America (ACI-NA) (1999). *The economic impact of US airports: airports make it happen*. Washington: Airports Council International North America.

Airports Council International North America (ACI-NA) (2009). Washington: Airports Council International North America.

American Institute of Chemical Engineers. Center for Chemical Process Safety (AICE/CCPS). Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, Ccps Guidelines Series. New York, NY: Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2003.

American Petroleum Institute and National Petrochemical & Refiners Association (API/NPRA) (2004). Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition. Washington, D.C.: API Publishing Services, pp 5.

Airport Security Report (2003). Systemic Vulnerabilities To Aviation Security Remain, Survey Says. Airport Security Report. Potomac: Sep 10, 2003. Vol. 10, Iss. 18; pp. 1.

American Society of Civil Engineers (ASCE). (2003). 2003 Progress Report: An update to the 2001 report card. Retrieved October 12, 2007, http://www.asce.org/reportcard/pdf/fullreport03.pdf

American Society of Civil Engineers (ASCE). (2005). Civil Engineers Give Nation's Infrastructure a (D+). ASCE Report Card. Retrieved October 12, 2007, http://www.asce.org/files/pdf/reportcard/2005reportcardpdf.pdf

American Society of Civil Engineers (ASCE). (2007), Report Card for America's Infrastructure- Security [I]. Retrieved October 27, 2007. http://www.asce.org/reportcard/2005/page.cfm?id=32#condition

Antonni, D. (2002). Annex 17 standards will be primary focus of forthcoming security system audits. *ICAO Journal*, Vol. 57, No. 5, pp11-13.

Archibald, T. (2007). Expanding U.S. Airspace Capacity: Implementing A Next Generation Air Traffic Control System in The U.S. *Canadian Aviation Industry Review*, InterVISTAS' Canadian Aviation Intelligence Report, InterVISTAS Consulting Inc., May 2007, pp. 16.

Ash, J. (2007). Canadian Aviation Industry Review. *InterVISTAS' Canadian Aviation Intelligence Report*, InterVISTAS Consulting Inc., June 2007, pp. 1.

Associated General Contractors of America (AGCA) (1982). Our fractured Framework: Why America Must Rebuild. Associated General Contractors of America, Washington.

Australian Office of Transport Security (AOTS). (2005). Aviation risk context statement Canberra: Department of Transport and Regional Services.

Aven, T. (2006). A unified framework for risk and vulnerability analysis covering both safety and security. *Journal of Reliability Engineering and System Safety*, Vol. 92, Iss. No. 6, pp 745–754.

Benham, B. (2004). Global airport security. *Travel + Leisure Magazine*, Retrieved April, 2007, http://www.travelandleisure.com/articles/global-airport-security/?page=1

Benoit, L. E. (2006). A study of performance measurement in Canadian air transport security. A study submitted to the Canadian Air Transport Security Authority (CATSA) Act Review Advisory Panel. Ottawa: Benoit & Associates.

Berbash, K. M., Hegazy, T., and Haas, C. (2008). Developing a new metric to assess Security systems in airports. A paper accepted to be published in the proceedings of Annual Conference of the Canadian Society for Civil Engineers, pp. CO-495-1 to 9. Québec City.

Berkowitz, C., and Bragdon, C. (2006). Advanced simulation technology applied to port safety and security. Proceedings of the Ninth International Conference on the Applications of Advanced Technology in Transportation, August 13-16, 2006, pp. 516-521, Chicago.

Berrick, C. (2003). Efforts to measure effectiveness and address challenges. Testimony before the Committee on Commerce, Science and Transportation, U.S. Senate, United States General Accounting Office. Washington.

Bouisset, J.-F. (1994). Security technologies and techniques: airport security systems. *Journal of Testing and Evaluation*, Vol. 22, No. 3, pp. 247-250. Retrieved January 27, 2008, http://journalsip.astm.org/JOURNALS/TESTEVAL/PAGES/209.htm.

British Broadcasting Corporation (BBC) (2006). Graphic: Airport security. BBC, August 10 2006. Retrieved October 11, 2007, http://news.bbc.co.uk/2/hi/4780161.stm

Canadian Air Transport Security Authority (CATSA). (2006). CATSA Position Paper: Our vision for Aviation Security, pp. 5. Ottawa: Ministry of Transport.

Cerino, A. and Walsh, W.P. (2000). Research and application of radio frequency identification (RFID) technology to enhance aviation security. National Aerospace and Electronics Conference. NAECON 2000. Pro*ceedings of the IEEE 2000*, pp. 127-135. Retrieved October 26, 2007, http://ieeexplore.ieee.org/iel5/7186/19355/00894901.pdf?tp= &isnumber=&arnumber=894901

The Construction Engineering Research Laboratory (CERL). (2007). The US Crop of Engineers. Retrieved October 17, 2007, http://www.cecer.army.mil/td/tips/product/details.cfm?ID=62&LAB=1

Corazzola R., and Poli J. (2003). Improved decision-making through effective asset management. Annual Conference of the Transportation Association of Canada, St. John's, Canada

Darklord (2008). Little progress in U.S. airport security. Fly away simulation. Retrieved Mar. 3, 2008,: http:// http://flyawaysimulation.com/article2330.html

De Bruijne, M. and Van Eeten, M. (2007). Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, Vol.15, No. 1, pp. 18-29.

De Jong, K. A., Spears, W. M., and Gordon, D. F. (1993). Using genetic algorithms for concept learning. Naval Research Laboratory, Washington, and Fairfax, VA: George Mason University, USA. Retrieved March 24, 2008, http://coblitz.codeen.org:3125/citeseer.ist.psu.edu/cache/papers/cs/162/http:zSzzSzwww.aic.nrl.navy.milzSzpaperszSz1993zSzAIC-93-50.pdf/dejong93using.pdf

Department for Transport (DfT). (2003). The future of air transport. The Great Minster House, London: UK. Retrieved Apr. 20, 2007, htpp//:dft.gov.uk/aviation/whitepaper.

Department of Homeland Security (DHS). (2003). Aviation security funding shrinks in face of budget deficits. A*irport Security Report*, Vol.10, Iss. 15; pp.1.

Department of Homeland Security (DHS) (2009). "National Infrastructure Protection Plan." Homeland Security Presidential Directive-7, USA.

Dillon R. L., Liebe R. M., and Bestafka T. (2009). "Risk-Based Decision Making for Terrorism Applications." Risk Analysis, Vol. 29, No. 3, pp. 321-335.

Drury, I. (1998). UK airports set the security standard. *Journal of Security Surveyor*, The British Library, pp. 11-13.

Elbehairy, H., Elbeltag, E., Hegazy, T., and Soudki, K. (2006). Comparison of two evolutionary algorithms for optimization of bridge deck repairs. *Journal of Computer-Aided Civil and Infrastructure Engineering*, No. 21, pp. 561-572.

Elbehairy, H. (2007). Bridge management system with integrated life cycle cost optimization. Ph. D. Thesis, University of Waterloo, Waterloo, Canada.

Elias, B. (2008). "National Aviation Security Policy, Strategy, and Mode-Specific Plans: Background and Consideration for Congress." CRS Reports for Congress, Congressional Research Services, Order Code RL34302.

Enoma, A., and Allen, S. (2007). Developing key performance indicators for airport safety and security. *Journal of Facility Management*. Emerald Group Publishing Limited, Vol. 25 No. 7, 2007, pp. 296-315.

Federal Highway Administration (FHWA). (1995). Recording and coding guide for the structure inventory and appraisal of the nation's bridges". FHWA report no. FHWA-PD-96-001, pp.124. U.S. Washington: Department of Transportation.

Federal Highway Administration (FHWA). (1999). Asset management primer. Washington: Office of Asset Management, Department of Transportation.

Flintsch, G., and Chen, C. (2004). Soft computing applications in infrastructure management. *ASCE Journal of Infrastructure Systems*, December, 2004, pp. 157-166.

Francis, G., Humphreys, I., and Fry, J. (2003). An international survey of the nature and prevalence of quality management systems in airports. *Journal of Total Quality Management and Business Excellence*, Volume14, Issue 7, pp. 819 – 829. Retrieved http://www.informaworld.com/smpp/title~content=t713447980~db=all~tab=issueslist~branches=14 - v14

Francis G., Hinton M., Holloway J. and Humphreys I. (1999). Best practice benchmarking: a route to competitiveness?. *Journal of Air Transport Management*, No. 5, 105-112.

Frederickson, H.G., and LaPorte, T.R. (2002). Homeland Security: The state and local crucible – airport security, high reliability, and the problem of rationality. *Public Administration Review*, Volume 62, pp. 33–43.

Fry, J., Humphreys, I., and Francis, G. (2005). Benchmarking in civil aviation: some empirical evidence. *Journal of Benchmarking*, Emerald Group Publishing Limited, Vol. 12 No. 2, 2005, pp. 125-137.

General Accounting Office (GAO). (2000). U.S. infrastructure, funding trends and opportunities to improve investment decisions: Report to Congress GAO/RCE/AIMD-00-35. Washington: U.S. GAO.

Goldberg, D. (1989). Genetic algorithms in search, optimization, and machine learning: New York Addison-Wesley.

Goldberg, D., and Holland, J. (1988). Genetic algorithms and machine learning. *Journal of Machine Learning*, Vol. 3, No. 2-3, pp.95-99.

Goo, S. (2003). Fliers to be rated for risk level: New system will scrutinize each passenger, assign color code. *The Washington Post*, September 9, 2003; pp. A01. Washington, N.Y.

Gooch, D. (2007). Canadian Airport Council newsletter. July 5th, 2007.

Google, 2009. Google Images.http://images.google.ca/images?hl=en&source=hp&q=airport+secutiy&gbv=2&aq=f&aqi=&aql=&oq=.

Grigg, N. (1988). *Infrastructure engineering and management*. New York; Toronto: J. Wiley.

Government of Canada (2002). The Canadian Government Security Policy (GSP). Ottawa: Treasury Board of Canada Secretariat.

Guthrie, Vernon H., David A. Walker, Charles M. Mitchell, and James J. Rooney. Modeling Security Risk, 2005 [cited April 28, 2005]. Available from http://www.inmm.org/topics/contents/pdfs/Risk.pdf.

Hardmeier, D., Hofer, F., and Schwaninger, A. (2006). The role of recurrent CBT for increasing aviation security screeners' visual knowledge and abilities needed in x-ray screening. *Proceedings of the 4th International Aviation Security Technology Symposium*, November 27 – December 1, 2006.

Hegazy, T., Elbeltagi, E., and Elbehairy, H. (2004), Bridge deck management system with integrated life cycle cost optimization. Annual Meeting, 83rd Transportation Research Board, January 11-15. Washington: Transportation Research Board.

Hessami, A.G. (2004). A systems framework for safety and security: The holistic paradigm. *Journal of Systems Engineering*, Vol. 7, No. 2, pp. 99-112.

Holland, J. (1975). Adaptation in natural and artificial systems". Ann Arbor: the University of Michigan Press.

Hudson, W. R., Haas, R. C. G., and Uddin, W. (1997). *Infrastructure management: Integrating design, construction, maintenance, rehabilitation, and renovation*. New York: McGraw-Hill.

Hunt A. R. and Kellerman K. F. (2007). "Development of An Analysis Tool For Performing Civil Aviation Security Risk Assessment". AKela Inc.

Intelligence Report. June 2007. InterVISTAS Consulting Inc., pp. 1

International Civil Aviation Organization (ICAO). (1944). Chicago convention. Montreal.

International Civil Aviation Organization (ICAO). (2001). Resolution number A33-1. ICAO General Assembly Meeting. October 3-5", Montreal.

International Civil Aviation Organization (ICAO). (2002a). Security Audit Reference Manual (SARM). Revised Edition. Montreal.

International Civil Aviation Organization (ICAO). (2002b). Annex 17: The aviation security. (7th ed.). Montreal.

International Civil Aviation Organization (ICAO). (2002c). Security Audit Reference Manual (SARM). (1st ed.), pp 9-12. Montreal.

International Civil Aviation Organization (ICAO). (2002d). Overview of USAP. Montreal: ICAO. Retrieved Feb. 12, 2008, www.icao.int/icao/en/atb/asa/ USAP_Handouts.pdf.

International Civil Aviation Organization (ICAO). (2007). Performance Indicators. *ICAO Journal*, Vol. 62, Iss. no.1, 5-6.

Jacobson, S., Virta, J., Bowman, J., Kobza, J., and Nestor, J. (2003). Modeling aviation baggage screening security systems: a case study. *IIE Transactions*. Issue no. 35, pp. 259–269.

Karim, M. (2003). Asset management in the airport environment. Master's Thesis, University of Waterloo, Canada.

Kesseler, E. (2003). Transforming air transport to a concurrent enterprise Technical, safety and security perspectives. *The Proceedings of the 9th International Conference of Concurrent Enterprising*, June 16-18 2003, Espoo, Finland.

Koller, S., Hardmeier, D., Michel, S. and Schwaninger, A. (2007). Investigating training and transfer effects resulting from recurrent CBT of x-ray image interpretation. Visual Cognition Research Group, University of Zürich, Department of Psychology. Retrieved Oct. 31, 2007, http://www.psychologie.uzh.ch/vicoreg/publications/doc/KolHarMicSch2007.pdf

Kunreuther H. and Heal G. (2002). "Interdependent Security". The Journal of Risk and Uncertainty, Vol. Volume 26, Numbers 2-3, p.p. 231-249.

Lazarick, R. (1998). Airport vulnerability assessment - An analytical approach. *The International Society for Optical Engineering (SPIE)*, Vol. 3575, pp. 302-310

Lazarick, R. (1998). "Airport vulnerability assessment an analytical approach." Proceedings of IEEE 33rd Annual International Carnahan Conference on Security Technology, pp.40 – 46.

Lazarick, R. (1999). "Airport vulnerability assessment a methodology evaluation." Proceedings of IEEE 33rd Annual International Carnahan Conference on Security Technology, pp.120 – 133.

Lazarick, R. (2001). Applications of technology in airport access control. *IEEE 35th International Carnahan Conference on Security Technology*. London, UK. pp. 85-95.

Lester B. Pearson International Airport (LBPIA). (1985). Restoration program procedure manual. Draft No. 4, May 1985, Toronto.

Lewis, J.A. (2005). Aux armes, citoyens: Cyber security and regulation in the United States. *Telecommunications Policy*, Volume 29, Number 11, pp. 821–830.

Lippert, R., and O'Connor, D. (2003). Security assemblages: Airport security, flexible work, and liberal governance. *Journal of Alternatives*, Vol. 28, pp. 331 - 358.

Liu, S., and Silverman, M. (2001). A practical guide to biometric security technology. *IEEE 35th Annual 2001 International Carnahan Conference on Technology Proceedings*. pp. 27 - 32.

Manabe, H. (2006). Aviation security challenges and international cooperation. Tokyo: Aviation Security Office, Civil Aviation Bureau, Ministry of Land, Infrastructure and Transport. Retrieved Sept. 26, 2007, http://www.ifssa.net/symposiums/2006/Aviation-Security-Challenges.pdf

Marsico, R. (2006). Airport screeners fail to see most test bombs. *The Seattle Times*. Retrieved October 28, 2007, http://seattletimes.nwsource.com/html/nationworld/2003327485_screeners28.html

Matthew, W. (2008). Introduction to genetic algorithms. Retrieved March 24, 2008, http://lancet.mit.edu/~mbwall/presentations/IntroToGA.

McLaughlin, M. (2005). Is Canadian air security audit happy? *Canadian Air Transport Security Authority News*, May 2005, pp.3.

MicroPaver Program. Retrieved October 17, 2007, http://www.cecer.army.mil/paver

Mishalani, R., and McCord, M. (2006). Infrastructure condition assessment, deterioration modeling, and maintenance decision making: Methodological advances and practical considerations. *ASCE Journal of Infrastructure Systems*, September 2006, pp. 145-146.

Moorkamp, M. (2005). Genetic algorithms a step by step tutorial. *Dublin Institute for Advanced Studies*. A presentation given in Barcelona on 29th November 2005. Retrieved March 24, 2008, http://www.dias.ie/~mm/ga_tutorial.pdf.

Morcous, G., and Rivard, H. (2003). Computer assistance in managing the maintenance of low-slope roofs. *ASCE Journal of Computer in Civil Engineering*, Vol. 17, Iss. 4, pp. 230-242.

National Academy of Sciences (NAS), Committee on Commercial Aviation Security, Panel on Passenger Screening, Commission on Engineering and Technical Systems, National Research Council. (1996). Airline passenger security screening: New technologies and implementation issues. *National Research Council*. Washington: The National Academies Press.

Nomani, A. Q., Pasztor, A. (1997). Aviation panel urges security spending. *Wall Street Journal*. (Eastern edition). New York: Feb 10, pp. A.3.

Nunoo, C., and Mrawira, D. (2004). Shuffled complex evolution algorithms in infrastructure works programming. *Journal of Computing in Civil Engineering*, ASCE, Vol.18, no. 3, pp. 257–66.

Oberle, R., Pohlman, T., and Roper, K. (2007). Airport vulnerability assessment - An analytical approach. *ASCE Journal of Architectural Engineering*, Vol. 13, No. 4, December 1, 2007, pp. 180–186.

Peterson, R., Bittel, R., Forgie, C., and Lee, W. (2007). Using USCAP's analytical models, the Transportation Security Administration balances the impacts of aviation security policies on passengers and airlines. *Journal of Interfaces*, Vol. 37, No. 1, pp. 52–67.

Pitt, M., Wai, F.K., and Teck, P.C. (2002) Technology selection in airport passenger and baggage systems. *Emerald Group Publishing Limited Journal of Facilities*, Vol. 20, No. 10, pp. 314–326 (13).

Profile, M. (2005). Emerging technology: Bridging the terahertz gap. *STRATEGIC* DIRECTION, Vol. 21 NO., pp. 40-42, Q Emerald Group Publishing Limited.

Rao, E., and Keith, G. (1999). Advanced technology explosives detection device deployment in the FAA's security equipment integrated program. *Proceedings of IEEE 33rd Annual Security Technology Conference*, pp. 168-176. Retrieved Oct. 18, 2007, http//ieeexplore.ieee.org/iel5/6475/17316/00797908.pdf

Rao, E. (2001). Application of an explosive detection device based on quadrupoleresonance (QR) technology in aviation security. *Publication of IEEE 35th International Carnahan Conference on Security Technology*, pp 282-288. Retrieved October 18, 2007, http://ieeexplore.ieee.org/iel5/7622/20784/00962846.pdf?tp=&isnumber=&arnumber= 962846

Redmill, Felix. Risk Analysis - a Subjective Process, 2002 [cited March 6, 2005]. Available from http://www.systemsafety.org/eJSS_Editions/Edition1/techarticle.html.

Reverdy, P. (2002). Audits help achieve full implementation of security measures at the regional level. *ICAO Journal*, Vol. 57, No. 5, pp14-15 & 28-29

Rountree C. D. and Demetsky M. J. (2006). "Framework for Analysis of Security Measures Within On-Airport Cargo Facility". Journal of The Transportation Research Board: Transportation Research Record, No. 1942, pp. 31-38.

Schwaninger, A. (2003). Training of airport security screeners. *AIRPORT*, 05/2003, pp. 11-13. Retrieved Oct. 31, 2007, http://www.psychologie.uzh.ch/vicoreg/publications/doc/ Schwaninger2004a.pdf

Schwaninger, A. (2004). Increasing efficiency in airport security screening. *AVSEC World 2004*, November 3-5, Vancouver, B.C., Canada. Retrieved on Oct. 31, 2007, http://www.psychologie.uzh.ch/vicoreg/publications/doc/Schwaninger2004a.pdf

Schwaninger, A., Hardmeier, D., and Hofer, F. (2005). Aviation security screeners visual abilities and visual knowledge measurement. *IEEE Aerospace and Electronic Systems*, 20(6), 29-35.

Security Industry Association (SIA). (2008). Airport security - What's being done to address this concern. Retrieved March 3, 2008, http:// http://siaonline.org/ research/ airport.cfm

Seo, J. (1994), Lagrangean relaxation and network approach to large-scale optimization for Bridge Management Systems. Ph.D. thesis, Texas A&M University.

SH&E International Air Transport Consultancy. (2005). Benchmarking security and border control, Final Report, March, 2005. Netherlands.

Stickles, R. P., Ozag H., and Mohindra S. (2003). "Security Vulnerability Assessment (SVA) Revieled." An ioMosaic Corporation Whitepaper.

Sylvie J. R.,(2005). "Developing Best Practices for Industrial Project Life Cycle Security and a Methodology for Measuring Implementation". A Ph.D. Thesis submitted to The University of Texas at Austin, (2005).

Tangen, S., (2003). An overview of frequently used performance measures. Journal of Work Study, Emerald Group Publishing Limited, Vol. 52, No. 7, 2003, pp. 347-354.

The European Parliament (EP). (2002). Regulation (EC) No 2320/2002 of the European Parliament and the Council of 16 December 2002. *Official Journal of the European* Communities, L355, pp. 1-21.

The Greater Toronto Airport Authority (GTAA), (2009). A Research meeting at GTAA headquarters, Mississauga ON, Canada.

The RiskWarch Corporation (2008). Risk Assessment Software®.

Transportation Research Board (TRB). (2007). Synthesis 3: General Aviation Safety and Security Practices. Airport Cooperative Research Program (ACRP).Washington. Retrieved October 15, 2007, http://onlinepubs.trb.org/onlinepubs/acrp/acrp_syn_003.pdf.

Transport Canada (TC). (2006). The annual report. Ottawa: Transport Canada.

The United States Green Building Council (USGBC). Retrieved October 17, 2007, http://www.usgbc.org/DisplayPage.aspx?CMSPageID=1497#CertDoc

The Washington Post (2001). Tighter Security Rules. *The Washington Post Newspaper*, September 14, 2001. Retrieved October 12, 2007, http://www.washingtonpost.com/wp-srv/nation/graphics/attack/aviation_7.html

Tzannatos E. S. (2003). "A decision support system for the promotion of security in shipping". Disaster Prevention and Management, Vol. 12, No. 3, pp. 222-229.

University of Zürich (UZ). (2006). Software Tools. Visual Cognition Research Group, University of Zürich, Department of Psychology. Retrieved October 31, 2007, http://www.psychologie.uzh.ch/vicoreg/software/index.htm

Veatch, J.D.; James, J.W.; May, T.T.; Wood, T.M.; Kruse, E.M. (1999). "An airport vulnerability assessment methodology." Proceedings of IEEE 33rd Annual International Carnahan Conference on Security Technology, pp.134 – 151.

Walpole R. and Myers R. (1993). "Probabilities and Statistics for Engineers and Scientists". 5th ed., Maxwell Macmillan Inc., Canada.

Weichselgartner J. (2001). "Disaster mitigation: the concept of vulnerability revised". Disaster Prevention and Management, Vol. 10, No. 2, pp. 85-94.

Wilson, D. L. (2005). Use of modeling and simulation to support Airport Security. *IEEE A&E systems Magazine*, August 2005, pp. 247- 251.

Wilson, D., Roe, E. K., and So, S. A. (2006). Security checkpoint optimizer (SCO): An application for simulating the operations of airport security checkpoints. *Proceedings of the 2006 Winter Simulation Conference*, pp. 529- 535

Yalcinkaya, R. (2005). Risk assessment of aviation security and evaluation of aviation security policies. A Master of Science Thesis, University of North Texas, Texas.

Zadeh, L. A. (2001). Applied soft computing—Foreword. *Journal of Applied Soft Computing*, Volume 1, No. 1, pp. 1-2(2).

Zuzak, C. (1990). Liability for breaches of aviation security obligations: A Canadian perspective. McGill University, Montreal.

Zuzak, C. (2003). Audits promote consistent implementation of aviation security measures worldwide". *ICAO Journal*, Vol. 58, Iss. no.7, 4-6.

Zuzak, C. 2004. ICAO audits reveal need for national security oversight system. *ICAO Journal*, Vol. 59, No. 7, pp. 9-11.

APPENDIX A

GENETIC ALGORITHMS

A.1 Introduction

Genetic Algorithms (GAs) were initiated as a result of a research done by John Holland in the 60s at University of Michigan in the USA, which published later in 1975. GAs fit into stochastic search methods class". Other stochastic search methods include "simulated annealing, threshold acceptance, and some forms of branch and bound". In addition, contrary to other stochastic search methods "genetic algorithms operate on a population of solutions" (Matthew, 2008). GAs are adaptive heuristic search algorithm premised on nature evolvement principles that first laid down by Charles Darwin of survival of the fittest. The basic concept of GAs is designed to simulate evolution processes in natural system, as such, GAs represent an intelligent utilization of a random search within a defined search space called population. The Main advantages of GAs include derivatives are not required, can be parallelized simply, local minima can potentially be escaped (Moorkamp, 2005). Additionally, GAs have been widely studied, experimented and applied in many fields in engineering worlds, and have been shown to be a powerful adjustable search technique for finding optimal parameters in large and complex spaces (De Jong et al., 1993).

A.2 Genetic Algorithms Principle

Genetic algorithms as probabilistic search procedures designed to work on large spaces involving states that can be represented by strings of bits (1 and 0). These methods are inherently parallel,

using a distributed set of samples from the space (a population of strings) to generate a new set of samples. (Goldberg and Holland 1988).

GAs are modeled slackly to actuate a population of individuals that undergo selection in the presence of variation-inducing operators such as mutation and recombination (crossover). A fitness function is used to evaluate individuals, and reproductive success varies with fitness. The summary of genetic algorithms process is illustrated Figure A1 (Goldberg and Holland 1988; Moorkamp, 2005).

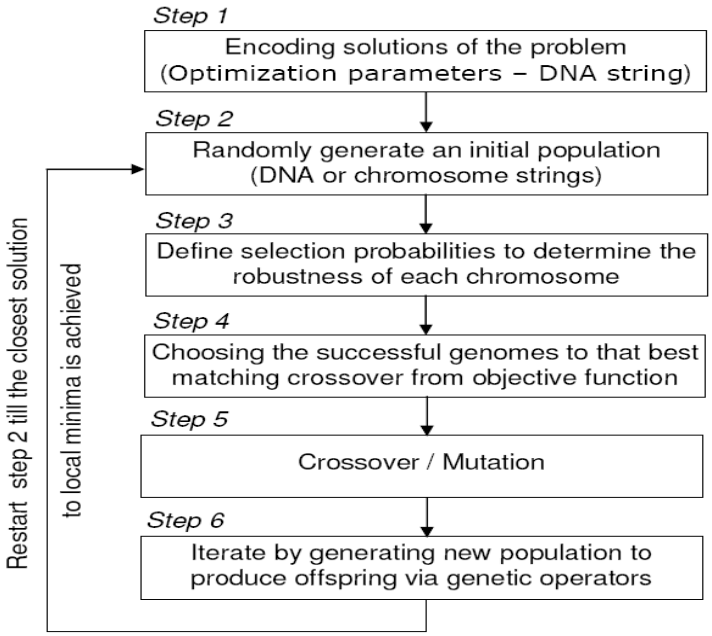


Figure A1: Genetic Algorithms process (Goldberg and Holland 1988; Moorkamp 2005)

A.3 Applying Genetic Algorithms

Modeling of problem internal search space representation is the cornerstone in finding the most optimum solution. Conventionally, GAs used to represent points in the search space by fixed-length strings. Therefore, the first step would be encoding solutions of the problem (optimization parameters), which also known as a genome (chromosome or DNA). Second, defined genomes

population is created by GAs. The algorithm randomly generates a number of DNA strings of the required length of population size N (Moorkamp, 2005). Third, crossover and mutation is applied in between population's chromosomes (parents) to generate new chromosomes (child – offspring) according to a variety of selection criteria. Whereas, these criteria ensure choosing the best genomes to match succeeding crossover, the fitness/ or objective function will determine the robustness of each chromosome.

A.3.1 Iteration

Generating a new population using the successful chromosome is called iteration. For next iteration, only chromosomes that achieved the desired objective function values receive high calculated probabilities, and will be selected to generate new population of a sample size N (Matthew, 2008).

A.3.2 Crossover and Mutation

If there was no innovation, crossover and mutation are the two steps to be used to generate new population space member. Crossover is defined as logically organized change of information. In case of GAs, beyond a preferred point and based on a selected probability two strings exchange their DNA. The exchange output will be new chromosomes (children) that will merge good attribute and similarities with old the strings (parents). Alternatively, mutation is unsystematic in nature in introducing a new string in the population. The idea is to change the value of one of bits in the parameter representation based on a defined probability. Mutation probability is always chosen low to ensure that only about 10% of the population experience mutation (Matthew, 2008).

A.4 Genetic Algorithms Representation

Originally Holland represented chromosomes of genetic algorithms in strings of bits. Other forms of representations are valid too, like "arrays, trees, lists, or any other object Figure A2. But you must define genetic operators (initialization, mutation, crossover, comparison) for any representation". Moreover, it is important that each string "must represent a complete solution to the problem you are trying to optimize" (Matthew, 2008).

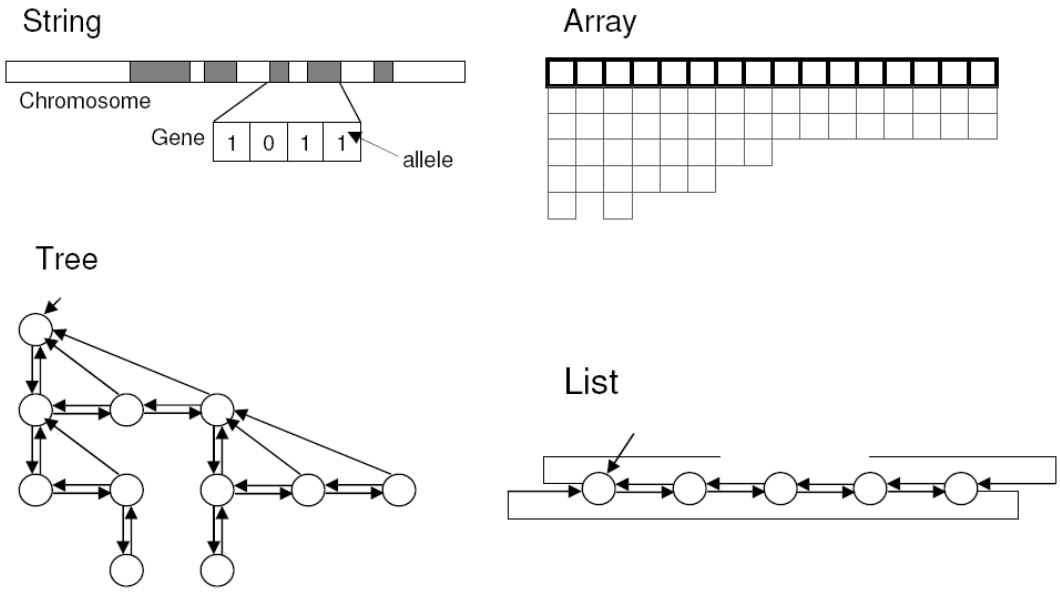


Figure A2: Some examples of GAs representations (Matthew, 2008)

APPENDIX B

MITIGATION MEASURES RELIABILITY AND COST DATABASE

B.1 Passengers' Security Mitigation Measures

Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
1	N/A	0.00%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0
2	Metal detector Gate (PMD2 / PTZ)+ operator	42.00%	85%	50%	0%	95%	95%	95%	0%	0%	0%	0%	44,000
3	Metal Detection Gate+1 guard	43.70%	86%	60%	0%	97%	97%	97%	0%	0%	0%	0%	84,000
4	Metal Detection Gate+ hand held met detelctors	44.80%	87%	70%	0%	97%	97%	97%	0%	0%	0%	0%	44,240
5	Entry Scan + operator	45.00%	95%	70%	0%	95%	95%	95%	0%	0%	0%	0%	70,000
6	Entry Scan+1 guard	45.60%	95%	70%	0%	97%	97%	97%	0%	0%	0%	0%	110,000
7	Entry Scan+ hand held met detelctors	45.60%	95%	70%	0%	97%	97%	97%	0%	0%	0%	0%	70,240
8	Millimeter Wave+ operator	48.20%	97%	50%	50%	95%	95%	95%	0%	0%	0%	0%	120,000
9	Millimeter Wave+1 guard	49.80%	97%	60%	50%	97%	97%	97%	0%	0%	0%	0%	160,000
10	Millimeter Wave+ hand held met detelctors	50.80%	97%	70%	50%	97%	97%	97%	0%	0%	0%	0%	120,240
11	Millimeter Wave+1 Guard + Desk Top explosive trace detectors	53.10%	97%	95%	50%	95%	97%	97%	0%	0%	0%	0%	151,740
12	Millimeter Wave+ 1 Guard + hand held explosive trace detectors	53.30%	97%	95%	50%	97%	97%	97%	0%	0%	0%	0%	183,000
13	Entry Scan+1 Guard + Desk Top explosive trace detectors	54.90%	95%	70%	95%	95%	97%	97%	0%	0%	0%	0%	201,500
14	Entry Scan+ 1 Guard + hand held explosive trace detectors	55.10%	95%	70%	95%	97%	97%	97%	0%	0%	0%	0%	174,740
15	Dielectric porta+ operator	56.10%	99%	98%	70%	98%	98%	98%	0%	0%	0%	0%	160,000
16	Dielectric portal+1 guard	56.10%	99%	98%	70%	98%	98%	98%	0%	0%	0%	0%	200,000
17	Dielectric portal+ hand held met detelctors	56.10%	99%	98%	70%	98%	98%	98%	0%	0%	0%	0%	160,240
18	Dielectric portal+ 1 Guard + hand held explosive trace detectors	56.10%	99%	98%	70%	98%	98%	98%	0%	0%	0%	0%	183,000
19	Dielectric portal+1 Guard + Desk Top explosive trace detectors	56.10%	99%	98%	70%	98%	98%	98%	0%	0%	0%	0%	241,500
20	Metal Detection Gate+1 Guard + Desk Top explosive trace detectors	56.90%	90%	95%	95%	95%	97%	97%	0%	0%	0%	0%	41,500
21	Metal Detection Gate + 1 Guard + hand held explosive trace detectors	57.10%	90.0%	95%	95%	97%	97%	97%	0%	0%	0%	0%	46,000
22	Millimeter Wave+ 1 Guard + hand held metal detectors + 1 Physical search guard + Sniffing dogs	65.10%	97%	95%	50%	95%	97%	97%	30%	30%	30%	30%	201,740
23	Millimeter Wave+ 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs	65.10%	97%	95%	50%	95%	97%	97%	30%	30%	30%	30%	281,500
24	Millimeter Wave + 1 Guard + hand held explosive trace detectors + 1 Physical search guard + Sniffing dogs	65.30%	97%	95%	50%	97%	97%	97%	30%	30%	30%	30%	206,000
25	Entry Scan+ 1 Guard + hand held metal detectors + 1 Physical search guard + Sniffing dogs	66.90%	95%	70%	95%	95%	97%	97%	30%	30%	30%	30%	83,000
26	Entry Scan+ 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs	66.90%	95%	70%	95%	95%	97%	97%	30%	30%	30%	30%	283,000
27	Entry Scan + 1 Guard + hand held explosive trace detectors + 1 Physical search guard + Sniffing dogs	67.10%	95%	70%	95%	97%	97%	97%	30%	30%	30%	30%	69,000
28	Dielectric portal+ 1 Guard + hand held metal detectors + 1 Physical search guard + Sniffing dogs	68.10%	99%	98%	70%	98%	98%	98%	30%	30%	30%	30%	323,000
29	Dielectric portal + 1 Guard + hand held explosive trace detectors + 1 Physical search guard + Sniffing dogs	68.10%	99%	98%	70%	98%	98%	98%	30%	30%	30%	30%	323,000

Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
30	Metal Detection Gate+ 1 Guard + hand held metal detectors + 1 Physical search guard + Sniffing dog	68.90%	90%	95%	95%	95%	97%	97%	30%	30%	30%	30%	64,500
31	Metal Detection Gate+ 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs	68.90%	90%	95%	95%	95%	97%	97%	30%	30%	30%	30%	64,500
32	Metal Detection Gate+ 1 Guard + hand held explosive trace detectors + 1 Physical search guard + Sniffing dogs	69.10%	90%	95%	95%	97%	97%	97%	30%	30%	30%	30%	83,000
33	Dielectric portal+ 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs	74.10%	99%	98%	70%	98%	98%	98%	30%	50%	50%	50%	306,000
34	Millimeter Wave + 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs+ Biological agent detector	92.30%	97%	95%	50%	95%	97%	97%	98%	98%	98%	98%	347,500
35	Metal Detection Gate+ 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs+ Biological agent detector	93.40%	90%	95%	95%	95%	97%	97%	95%	90%	90%	90%	110,500
36	Entry Scan + 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs+ Biological agent detector	93.90%	95%	95%	95%	95%	97%	97%	95%	90%	90%	90%	452,000
37	Dielectric portal + 1 Guard + Desk-Top explosive trace detectors + 1 Physical search guard + Sniffing dogs+ Biological agent detector	94.50%	99%	98%	70%	98%	98%	98%	98%	98%	98%	90%	493,500

B.2 Security Background Mitigation Measures

Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
	Background & Bio measures	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	
1	N/A	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0
2	Criminal Background Screening	50.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	72,000
3	Biological Cameras & Finger Prints	85.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	85,000
4	Criminal Screening+ Cameras+ Finger Prints	99.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	130,000

B.3 X-Ray and Explosives Detection System Measures

Cabin Baggage Security Mitigation Measures

Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
	Ray Scanners Measures												
1	N/A	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0
2	Conventional X-Ray (COB) + 1 Operator	54.50%	60%	60%	50%	85%	85%	85%	30%	30%	30%	30%	93,000
3	Explosive X-ray (COB) + 1 Operator	69.50%	95%	95%	60%	95%	95%	95%	40%	40%	40%	40%	199,400
4	EDS System-single view (OHB)	71.50%	90%	90%	65%	90%	90%	90%	50%	50%	50%	50%	213,000
5	EDS System-doul view (OHB)	78.50%	91%	91%	70%	91%	91%	91%	65%	65%	65%	65%	243,000
6	EDS System-multi view (OHB)	0.855	0.94	0.94	0.85	0.94	0.94	0.94	0.75	0.75	0.75	0.75	543000.00

Checked-in Luggage Security Mitigation Measures

Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
	Ray Scanners Measures												
1	N/A	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	
2	Conventional X-Ray (COB) + 1 Operator	54.50%	60%	60%	50%	85%	85%	85%	30%	30%	30%	30%	93,000
3	CTX 2500 (OHB)	81.50%	95%	95%	80%	95%	95%	95%	65%	65%	65%	65%	793,000
4	CTX 5500 DS (OHB)	85.00%	97%	97%	85%	97%	97%	97%	70%	70%	70%	70%	993,000
5	CTX 9000 (OHB)	90.00%	98%	98%	90%	98%	98%	98%	80%	80%	80%	80%	1,293,000

B.4 Trace Detection Mitigation Measures

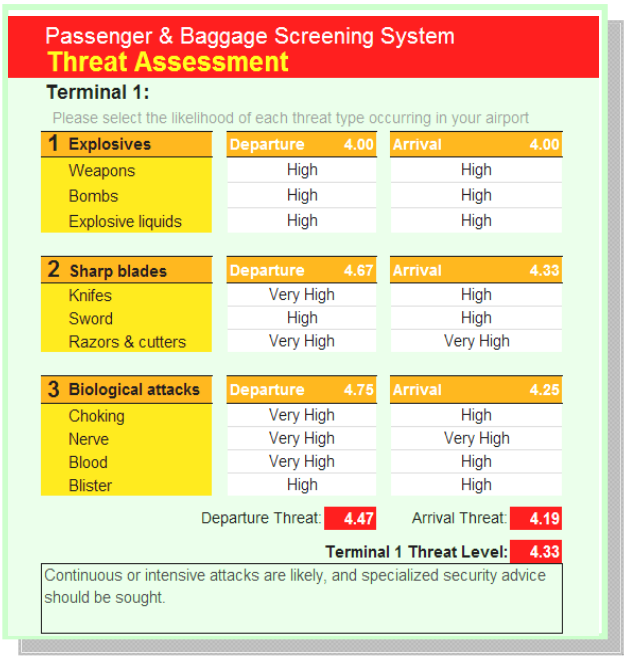
Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
	Trace Detection Measures												
1	N/A	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0
2	Chemiluminescence (EGIS II & III)	84.50%	85%	85%	80%	85%	85%	85%	85%	85%	85%	85%	120,000
3	Ion mobility spectrometry (Ionscan)	89.50%	90%	90%	85%	90%	90%	90%	90%	90%	90%	90%	41,500
4	Ion Track Itemiser	92.70%	93%	93%	90%	93%	93%	93%	93%	93%	93%	93%	155,000
5	Chemiluminescence+ Ionscan	95.00%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	254,000
6	Chemiluminescence+ Ion Track Itemiser + Biological agent detector	98.60%	99%	99%	99%	99%	99%	99%	99%	99%	99%	99%	286,000

B.5 Luggage Physical Search Mitigation Measures

Database of Reliability & Cost of Security Measures (0 to 1)													
Device ID	Countermeasure Type	Detection Effect. Ave.	Reliability of Security Device(s) to detect Threat(s) (0 - 1)										Cost Details
			Explosives			Sharp Blades			Biological Attacks				
			Weapons	Bombs	Explosive liquids	Knives	Swords	Blades & Razors	Choking	Nerve	Blood	Blister	Device + Guards Cost
	Luggae Physical Search Measures	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	
1	N/A	0.00%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0
2	Luggage hand search	48.00%	50%	50%	30%	50%	50%	50%	50%	50%	50%	50%	45,000
3	Luggage sniffing dogs	61.50%	70%	70%	35%	70%	70%	60%	60%	60%	60%	60%	80,000
4	Luggage hand search+ sniffing dogs	72.00%	80%	80%	50%	80%	80%	70%	70%	70%	70%	70%	125,000

APPENDIX C

Sensitivity Analysis Experimental Threat levels



Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

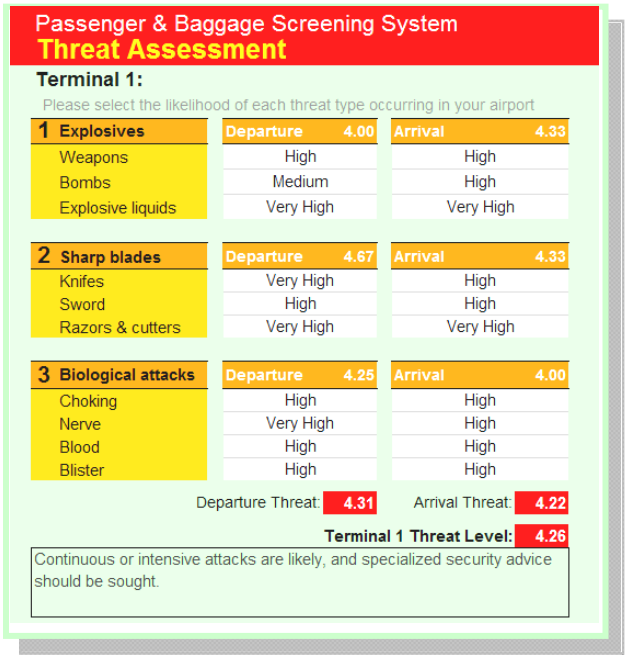
	Departure 4.00	Arrival 4.00
1 Explosives		
Weapons	High	High
Bombs	High	High
Explosive liquids	High	High
2 Sharp blades	**Departure 4.67**	**Arrival 4.33**
Knifes	Very High	High
Sword	High	High
Razors & cutters	Very High	Very High
3 Biological attacks	**Departure 4.75**	**Arrival 4.25**
Choking	Very High	High
Nerve	Very High	Very High
Blood	Very High	High
Blister	High	High

Departure Threat: 4.47 Arrival Threat: 4.19

Terminal 1 Threat Level: 4.33

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 1



Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

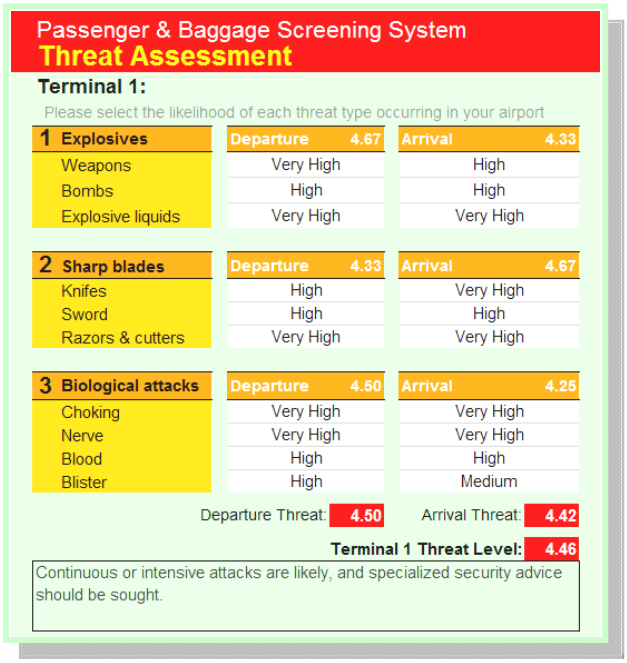
	Departure 4.00	Arrival 4.33
1 Explosives		
Weapons	High	High
Bombs	Medium	High
Explosive liquids	Very High	Very High
2 Sharp blades	**Departure 4.67**	**Arrival 4.33**
Knifes	Very High	High
Sword	High	High
Razors & cutters	Very High	Very High
3 Biological attacks	**Departure 4.25**	**Arrival 4.00**
Choking	High	High
Nerve	Very High	High
Blood	High	High
Blister	High	High

Departure Threat: 4.31 Arrival Threat: 4.22

Terminal 1 Threat Level: 4.26

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 2



Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

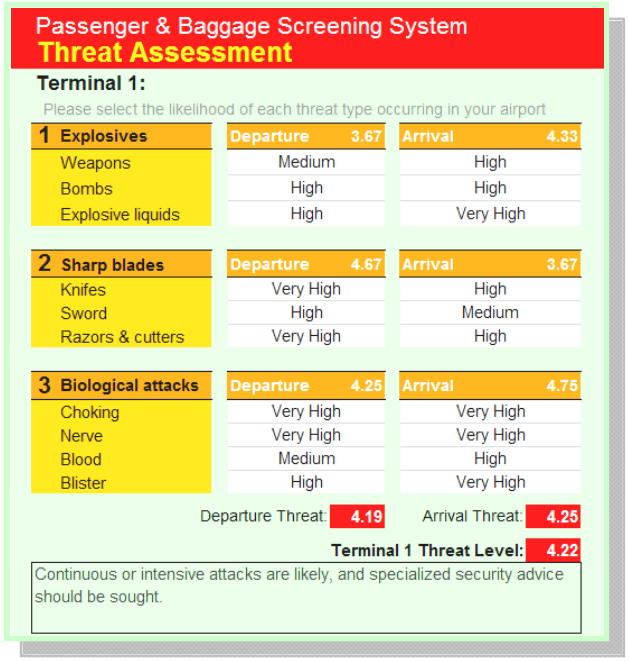
	Departure 4.67	Arrival 4.33
1 Explosives		
Weapons	Very High	High
Bombs	High	High
Explosive liquids	Very High	Very High
2 Sharp blades	**Departure 4.33**	**Arrival 4.67**
Knifes	High	Very High
Sword	High	High
Razors & cutters	Very High	Very High
3 Biological attacks	**Departure 4.50**	**Arrival 4.25**
Choking	Very High	Very High
Nerve	Very High	Very High
Blood	High	High
Blister	High	Medium

Departure Threat: 4.50 Arrival Threat: 4.42

Terminal 1 Threat Level: 4.46

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 3



Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

	Departure 3.67	Arrival 4.33
1 Explosives		
Weapons	Medium	High
Bombs	High	High
Explosive liquids	High	Very High
2 Sharp blades	**Departure 4.67**	**Arrival 3.67**
Knifes	Very High	High
Sword	High	Medium
Razors & cutters	Very High	High
3 Biological attacks	**Departure 4.25**	**Arrival 4.75**
Choking	Very High	Very High
Nerve	Very High	Very High
Blood	Medium	High
Blister	High	Very High

Departure Threat: 4.19 Arrival Threat: 4.25

Terminal 1 Threat Level: 4.22

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 4

Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

	Departure 4.33	Arrival 4.00
1 Explosives		
Weapons	Medium	Medium
Bombs	Very High	High
Explosive liquids	Very High	Very High
2 Sharp blades	**Departure 4.33**	**Arrival 4.33**
Knifes	Very High	High
Sword	Medium	High
Razors & cutters	Very High	Very High
3 Biological attacks	**Departure 4.50**	**Arrival 5.00**
Choking	Very High	Very High
Nerve	Very High	Very High
Blood	Medium	Very High
Blister	Very High	Very High

Departure Threat: 4.39 Arrival Threat: 4.44

Terminal 1 Threat Level: 4.42

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 5

Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

	Departure 4.00	Arrival 3.67
1 Explosives		
Weapons	Medium	Medium
Bombs	High	High
Explosive liquids	Very High	High
2 Sharp blades	**Departure 4.33**	**Arrival 4.67**
Knifes	Very High	Very High
Sword	High	High
Razors & cutters	High	Very High
3 Biological attacks	**Departure 4.25**	**Arrival 4.50**
Choking	High	Very High
Nerve	Very High	Very High
Blood	High	High
Blister	High	High

Departure Threat: 4.19 Arrival Threat: 4.28

Terminal 1 Threat Level: 4.24

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 6

Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

	Departure 4.33	Arrival 4.33
1 Explosives		
Weapons	High	High
Bombs	High	High
Explosive liquids	Very High	Very High
2 Sharp blades	**Departure 4.67**	**Arrival 4.33**
Knifes	Very High	Medium
Sword	High	Very High
Razors & cutters	Very High	Very High
3 Biological attacks	**Departure 4.00**	**Arrival 4.50**
Choking	High	Very High
Nerve	High	Very High
Blood	Very High	High
Blister	Medium	High

Departure Threat: 4.33 Arrival Threat: 4.39

Terminal 1 Threat Level: 4.36

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 7

Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

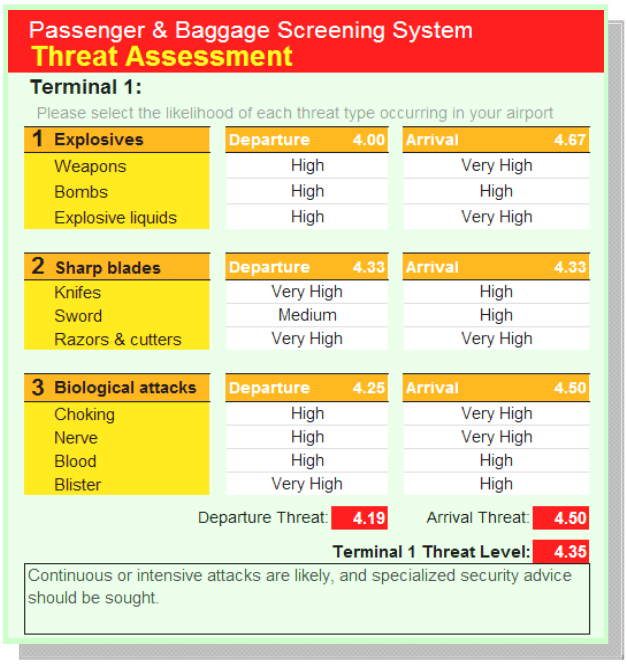
	Departure 4.00	Arrival 4.67
1 Explosives		
Weapons	High	Very High
Bombs	High	High
Explosive liquids	High	Very High
2 Sharp blades	**Departure 4.67**	**Arrival 4.00**
Knifes	Very High	Medium
Sword	High	High
Razors & cutters	Very High	Very High
3 Biological attacks	**Departure 4.25**	**Arrival 4.25**
Choking	High	High
Nerve	High	Very High
Blood	High	High
Blister	Very High	High

Departure Threat: 4.31 Arrival Threat: 4.31

Terminal 1 Threat Level: 4.31

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 8



Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

1 Explosives	Departure 4.00	Arrival 4.67
Weapons	High	Very High
Bombs	High	High
Explosive liquids	High	Very High

2 Sharp blades	Departure 4.33	Arrival 4.33
Knifes	Very High	High
Sword	Medium	High
Razors & cutters	Very High	Very High

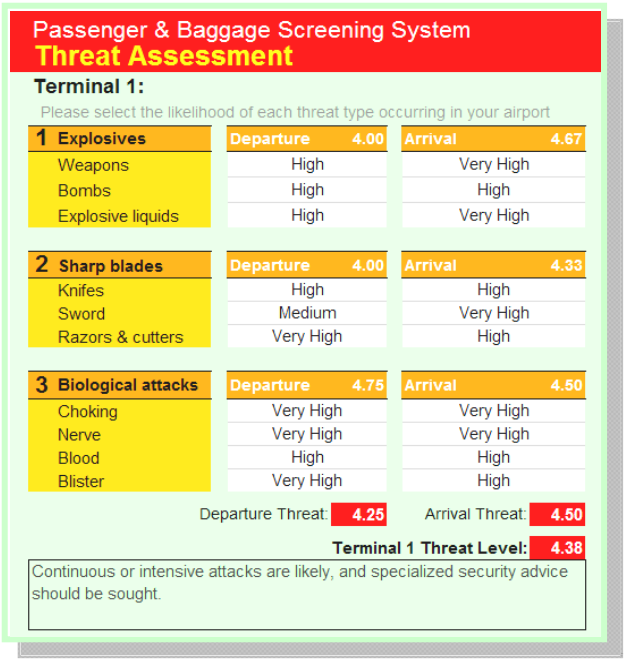
3 Biological attacks	Departure 4.25	Arrival 4.50
Choking	High	Very High
Nerve	High	Very High
Blood	High	High
Blister	Very High	High

Departure Threat: 4.19 Arrival Threat: 4.50

Terminal 1 Threat Level: 4.35

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 9



Passenger & Baggage Screening System
Threat Assessment

Terminal 1:

Please select the likelihood of each threat type occurring in your airport

1 Explosives	Departure 4.00	Arrival 4.67
Weapons	High	Very High
Bombs	High	High
Explosive liquids	High	Very High

2 Sharp blades	Departure 4.00	Arrival 4.33
Knifes	High	High
Sword	Medium	Very High
Razors & cutters	Very High	High

3 Biological attacks	Departure 4.75	Arrival 4.50
Choking	Very High	Very High
Nerve	Very High	Very High
Blood	High	High
Blister	Very High	High

Departure Threat: 4.25 Arrival Threat: 4.50

Terminal 1 Threat Level: 4.38

Continuous or intensive attacks are likely, and specialized security advice should be sought.

Threat levels in Experiment 10