

Optimized Airport Security Infrastructure System (OASIS)

Elizabeth Castaneda, Jamie Gonzalez, Shannon Harris, Joon Kim

Abstract— It has been suggested that the current security measures being implemented in airports around the country produce “soft targets” in the form of lengthy queues. These soft targets heighten the risk of a terrorist attack within airport premises that could potentially have the same impact as destroying a commercial flight. Using Washington Dulles International Airport as a case study, this study examines the security measures being implemented in the airport and designs a methodology that will result in improved allocation and usage of security resources. Two alternatives are designed that make use of layered, defense-in-depth security measures that aim to deter terrorist attacks by using the concept of unpredictability. Models of these alternatives are built and the best alternative is selected by analyzing simulation outputs and evaluating them based on a value function. At the end of the study, an Optimized Airport Security Infrastructure System (OASIS) that will provide a more efficient and reliable method for screening passengers and their luggage is proposed.

I. INTRODUCTION

SINCE the terrorist attacks on September 11, 2001, it has been mandated by law to appropriately screen air travellers to ensure that certain items and persons prohibited from flying do not board commercial airliners. This screening is done by 43,000 trained and certified Transportation Security Officers (TSO) stationed at over 450 airports across the country. Combined with over 1,000 credentialed security inspectors, these professionals screen over two million passengers daily and deliver both security and customer service at the airport. [1] Although these thorough measures exist, the United States Government Accountability Office (GAO) has published reports documenting shortcomings and discrepancies in the operational and managerial aspects of aviation security within airports.

It has been proposed that these discrepancies have created possible “soft targets” in the form of lengthy queues in the airport where passengers need to be processed for either check-in or security screening. These soft targets heighten the risk of a terrorist attack that could have the same impact as destroying a commercial flight. Moreover, some believe that the security measures provide passengers with a false sense of security by implementing a static defense aimed to protect against clever terrorists who are constantly trying to

find a way to penetrate it.

This paper presents a design of an Optimized Airport Security Infrastructure System (OASIS) which will provide a more efficient and reliable method for screening passengers and their luggage. OASIS will decrease both the occurrence of soft targets within the airport and the possibility of an attack during a flight. Washington Dulles International Airport is used as the case study. The recommendations and conclusions that will be presented are specific to Washington Dulles International Airport, but are also general enough so as not to lose relevance in the context of other airports in the country.

II. SYSTEM DESCRIPTION

A. System Overview

OASIS is designed to provide security measures that will guard against explosive, biological, and chemical threats in a more efficient and reliable manner. The scope of this study is narrowed to cover the security checks that a passenger goes through from the time of arrival at the airport, to the time of boarding the airplane. Furthermore, only outgoing domestic and international flights are considered. It is assumed that passengers from incoming flights have been adequately screened prior to their departure from the originating airport, and do not pose any security threats upon arrival at the destination airport.

B. External Systems

OASIS interacts with five major external systems, as illustrated in Fig. 1. These systems are the Passengers, an Emergency Support System, Maintenance System, Equipment Suppliers, and the Transportation Security Administration (TSA). Passengers are all individuals who go to the airport for the purposes of travelling or using other services found in the airport. They will be subject to the security measures being implemented there. The Emergency Support System refers to the external systems that provide assistance in case of fires, terrorist attacks, and other similar emergencies. This includes the Fire and Police Departments. The Maintenance System provides maintenance support to the various components of OASIS in case of a system or subsystem malfunction or failure. Equipment Suppliers refer to organizations and companies that provide the airport with the equipment needed to implement the security measures. The TSA is responsible for ensuring that the security measures being implemented in the airport comply with the regulations mandated by law.

Manuscript received April 9, 2006. This work was supported in part by the George Mason University (GMU) Center for Air Transportation Systems Research. Dr. George Donohue and Dr. Andy Loerch of GMU are the faculty advisors.

Authors are undergraduate students of GMU's Systems Engineering and Operations Research Department in Fairfax, VA 22030. (e-mail: cgonzale@gmu.edu).

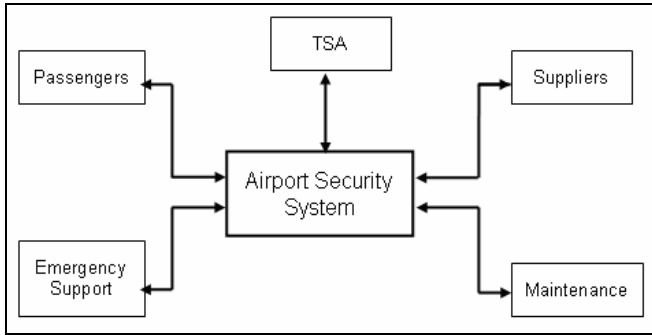


Fig. 1. External Systems Diagram

C. Functional Architecture

OASIS performs four main functions. These include Airline Personnel Functions, Security Personnel Functions, Check-in functions, and Screening. Fig. 2 shows each of these functions and their most important inputs, outputs, controls, and mechanisms. Check-in functions are done through the Passenger Information database that contains details about individuals and their flight (e.g. flight number, destination, etc). Check-in is facilitated by Airline Personnel. Screen Passengers and Baggage refer to the security checks being implemented in the airport. This is done using the security equipment available in the airport. The screening of passengers and their baggage is facilitated by Security Personnel.

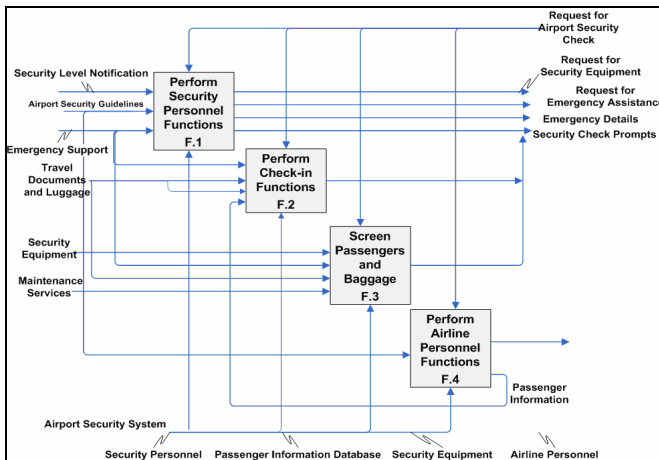


Fig. 2. Functional Architecture

D. Generic Physical Architecture

The generic physical architecture of OASIS is shown in Fig. 3. It defines the hierarchy of the physical components of the system, and its top-level components are those that perform the top-level functions shown in Fig. 2. They are the Security Personnel, Security Equipment, the Passenger Information Database, and the Airline Personnel.

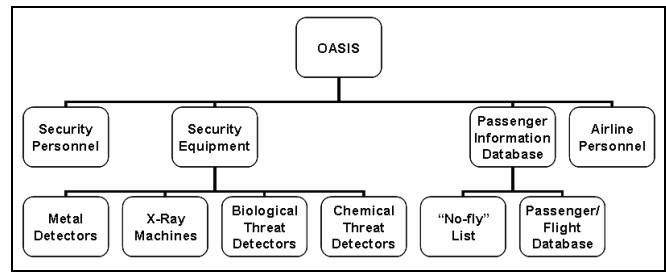


Fig. 3. Generic Physical Architecture

III. SYSTEM DESIGN

OASIS aims to minimize the occurrence of soft targets in the airport while increasing the reliability and efficiency of the security screening. Two alternative Airport Security Infrastructure System designs are proposed. Based on modeling and simulation results and the degree to which they satisfy the stakeholders' value hierarchy, the best design alternative is recommended.

There are two types of errors in threat detection that may occur: false alarms and false clears. False alarms refer to preventing a non-threatening passenger from going through the system. These can cause unnecessary delays for passengers and may result in missed flights. False clears refer to letting a threat go through the system. These may have more significant effects such as considerable passenger injury or destruction in the airport.

A. Design Alternatives

Alternatives to the current airport security design aim to minimize the occurrence of false alarms and false clears, and maximize throughput. Two design alternatives are being tested to fit these specifications. Both alternatives involve assigning passengers into groups to access security. The first involves assignment of groups based on the results of a linear program, and the second, a planned assignment into groups based upon an initial screening. These alternatives both focus on dynamic, defense-in-depth strategy instead of static defense. They also have the feature of unpredictability that will deter terrorists from attempting to attack the system. The types of threats that the system will check for are false documents, threats on passengers, and threats in carry-on luggage.

Design Alternative 1: Grouped Random Access Method (OASIS-GRAM). OASIS-Grouped Random Access Method (GRAM) is based on a method proposed by Vellara Babu, Rajan Batta, and Li Lin in their paper "Passenger grouping under constant threat probability in an airport security system" [2]. It consists of a multi-layered system of security with M_1 mandatory check stations, and M_2 "special" check stations. Passengers are divided into groups that will go through a combination of the mandatory and special checkpoints. The maximum number of groups to be used will be between 1 and $2^{|M_2|}$. The number of distinct assignment of the groups will be calculated by the

combination of $2^{|M_2|}$ and n , where n is the number of groups. This method makes use of a Linear Program (LP) to calculate the percentage of passengers that will be assigned to a particular group. The objective function aims to minimize false alarm rates. There are two main constraints that ensure the following: 1. that the false clear probability is within Federal Aviation Administration specifications (2), 2. that passengers are screened within the given available time (3). A main assumption of this method is that all passengers pose the same threat to the system. Passenger attributes such as race, gender, and age are not taken into consideration. The linear program formulation is shown below:

$$(P) \text{ Min } (1 - \alpha) \sum_{i=1}^n x_i \left(1 - \prod_{j=1}^K q_j \right), \quad (1)$$

s.t.

$$\alpha \sum_{i=1}^n x_i \sum_{k=1}^K \beta_k \prod_{j=1}^K (1 - p_{jT_k}) \leq \delta, \quad (2)$$

$$N_j \sum_{i=1}^n x_i (1 + z_i (p_j \alpha + (1 - q_j)(1 - \alpha))) \frac{t_j}{S_j} \leq T_j, \quad (3)$$

$$\forall j, \quad (4)$$

$$\sum_{i=1}^n x_i = 1, \quad (4)$$

$$0 \leq x_i \leq 1 \quad \forall i. \quad (5)$$

The variables used are defined in Table I.

TABLE I
VARIABLES USED IN LINEAR PROGRAM

VARIABLE	DESCRIPTION
α	threat probability
j	check station
k	number of known possible threats that can be carried by the passengers/items
T_k	a particular type of threat k
β_k	probability that the type of threat is T_k , given that there is a threat item
p	probability of detecting a threat at a check station
p_{jT_k}	probability of detecting a threat T_k at station j , given threat item T_k
q	probability of clearing given that there is no threat
q_j	probability of clearing a non-threat item at station j
x_i	fraction of the population that form group i
y_{ij}	1 if group G_i passengers report to check station j , 0 otherwise
N_t	expected number of passengers arriving during a particular time interval
t_j	Time available to check the fraction of passengers of N_t that is reporting to station j
t_j	Time taken to check one passenger at station j
S_j	number of servers at station j
z_j	≥ 0 ; a multiplier for the station j

A diagram of a sample GRAM security process is shown

in Fig. 4.

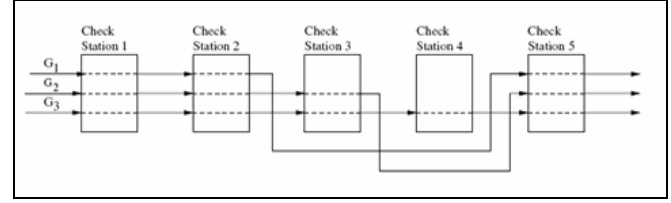


Fig. 4. Sample Grouped Random Access Method [2]

Design Alternative 2: Systematic Assignment Method (OASIS-SAM). This method of passenger screening is similar to the first alternative in that it will have a specified number of mandatory and “special” checkpoints, will check for the same types of threats, and that grouping will be affected by the National Threat Level. It differs in that no equation or LP will be used to determine the number of people who visit special check stations. This process will be dictated by the results of an initial mandatory checkpoint. If a passenger is shown to have a suspicious item on his person or baggage, that passenger will be directed to a specific special checkpoint for further screening. If a passenger is seen to have no suspicious items, then the passenger will be sent to a checkpoint to be checked based on the results of a random variable draw. A diagram of a sample SAM security process is shown in Fig. 5. T1, T2, and T3 represent the groups into which the passengers are assigned after the initial check.

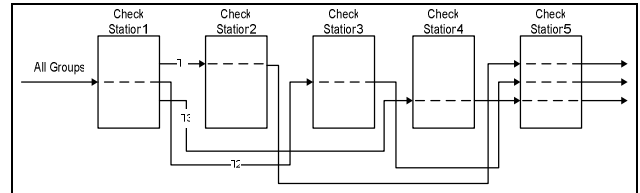


Fig. 5. Sample Systematic Assignment Method

B. Value Hierarchy

To help select the best design alternative, a value hierarchy with stakeholder determined weights will be used. The proposed value hierarchy, as shown in Fig. 6, has three top level items, namely reliability, throughput, and safety. These are then broken down further into various other criteria that are important in evaluating the design alternatives. Each of the alternatives is evaluated on each of the metrics in the value hierarchy and their overall scores are computed using the stakeholder given weights and the following utility functions:

$$U(x) = .25U_{\text{Reliability}}(x) + .5U_{\text{Throughput}}(x) + .25U_{\text{Security}}(x)$$

where

$$U_{\text{Reliability}}(x) = .4U_{\text{FA}}(x) + .4U_{\text{PD}}(x) + .2U_{\text{Availability}}(x) \quad (6)$$

$$U_{\text{Throughput}}(x) = .5U_{\text{BlockTime}}(x) + .5U_{\text{ServiceRate}}(x)$$

$$U_{\text{Security}}(x) = .5U_{\text{FC}}(x) + .5U_{\text{RiskMetric}}(x)$$

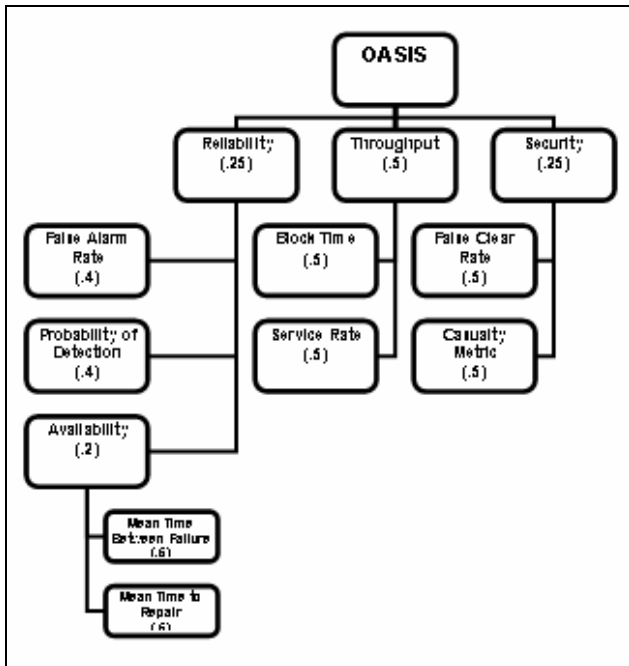


Fig. 6. Value Hierarchy

C. Figures of Merit

The best design alternative is selected using a utility function that considers the metrics shown in the value hierarchy.

System Reliability, Probability of Detection, False Alarm Rates, and Availability are key aspects that must be considered in selecting design alternatives. The alternatives should be able to easily adapt to the acceptable levels of Probability of Detection and False Alarm Rates as determined by the National Threat Level.

For throughput, it is particularly important to consider the total passenger block time (i.e. the amount of time/number of hours a passenger is required to arrive before the scheduled flight) so as not to lose the convenience and time-efficiency of travelling by plane. A high service rate also ensures that queues do not build up and create soft targets.

For the Security aspect, False Clear Rates should be considered, as these determine the level of risk that passengers are exposed to. False Clear rates should also be easily adjusted based on the National Threat Level in that a higher threat level should have a lower False Clear Rate. The casualty metric will be obtained from the casualty model that will be explained in Section IV of this report. It will show the risk that a passenger in a certain position in the queue is exposed to, assuming an explosive is detonated at the center of mass of the queue.

IV. SYSTEM MODELS AND SIMULATION

A. Discrete Event Simulations

A discrete event simulation model will be built for the current airport security system and each of the two proposed

alternatives using Rockwell Software's Arena. A graduate study done at George Mason University [3] provides collected data of passenger inflows for the airport on November 23, 2005, Thanksgiving Day. A 24-hour simulation will be carried out for each of the three models. These simulations will keep track of the system's performance: how accurately it can detect threats and how quickly it can process passengers.

B. Casualty Model

A casualty model, as shown in Fig. 7, is developed to determine how susceptible each of the generated queues is to becoming a soft target. A model of the queues can be developed, and an average queue length can be determined through the discrete-event simulations. The results of the simulation will be used to model the two dimensional queues found at the airport.

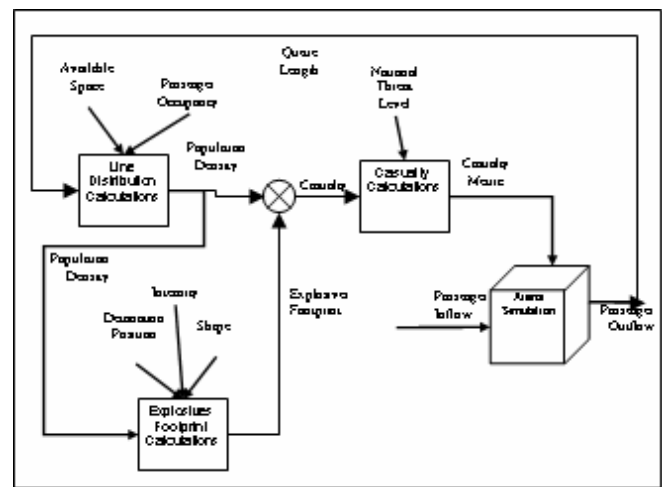


Fig. 7. Casualty Model

The length of the queues in the zigzag, "Disneyland queue" pattern gives a two dimensional distribution model of the population density of the particular lines. Such a distribution is shown in Fig. 8.

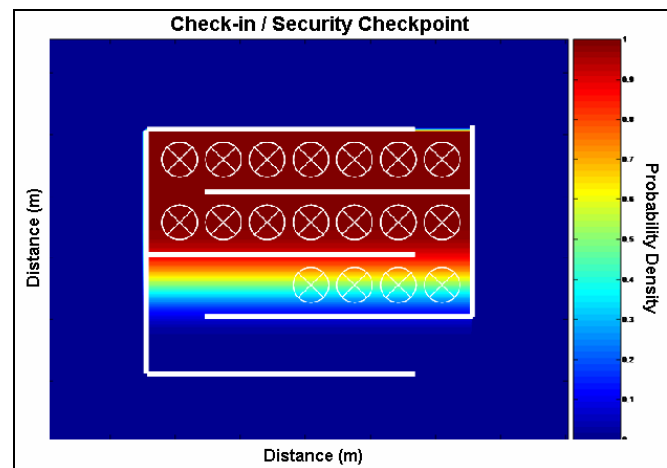


Fig. 8. Mathematical model of the population density of a 20ft x 20ft zigzag line at Dulles Airport

The lethal radius of an explosive device allows an estimation of the expected number of deaths when compared to a population density. Fig. 9 shows the initial lethal radius of an explosive device.

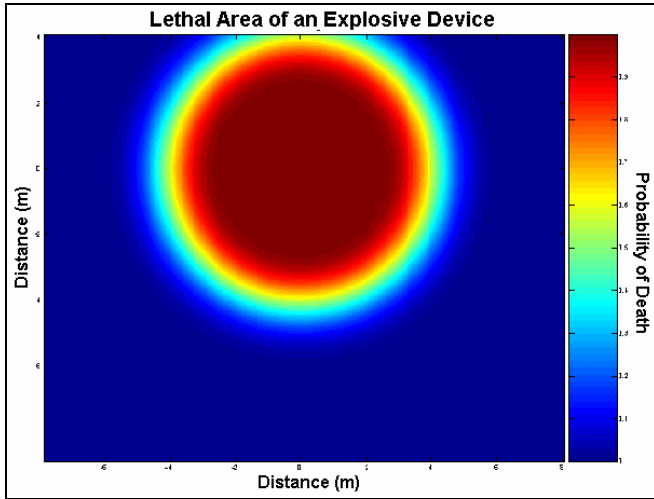


Fig. 9. Casualty radius of an explosive device

Using the U.S. Army Field Manual [4], a formula was derived on the relationship between lethal radius and amount of explosives for multiple types of bombs and materials. Table II outlines the relative effectiveness of various explosive compounds normalized with Trinitrotoluene (TNT) as reviewed by the U.S. Army. This data is without antipersonnel shrapnel used. Fig. 10 plots various lethal blast radii of explosive materials used in bombs. Actual data has not been found for this measure and a generic formula was derived:

$$\text{lethal radius} = k \times \text{relative effectiveness} \times \sqrt[3]{\text{weight}} \quad (7)$$

where, k is a arbitrary constant used for scaling. Once again, antipersonnel shrapnel was not used when modeling the blast radius.

TABLE II
RELATIVE EFFECTIVENESS OF EXPLOSIVE MATERIALS
NORMALIZED WITH TNT

Explosive Compound	Relative Effectiveness
Ammonium nitrate	0.42
Black powder	0.55
TNT	1.00
C-4	1.34
Nitroglycerine	1.50
RDX	1.60
PETN	1.66

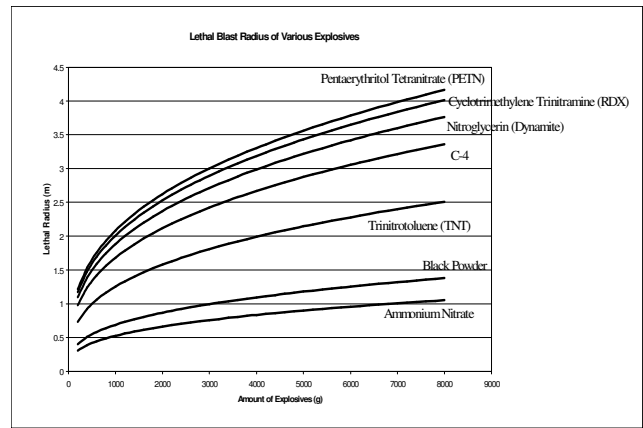


Fig. 10. Lethal blast radii of various explosive compounds

Through a simple multiplication, Fig. 11 shows the probability of death in a given line if an explosive device is detonated at the queue's center of mass. This model is a representation of the intersection of the probability density model (i.e. Fig. 8) and the lethal blast radius model (i.e. Fig. 9).

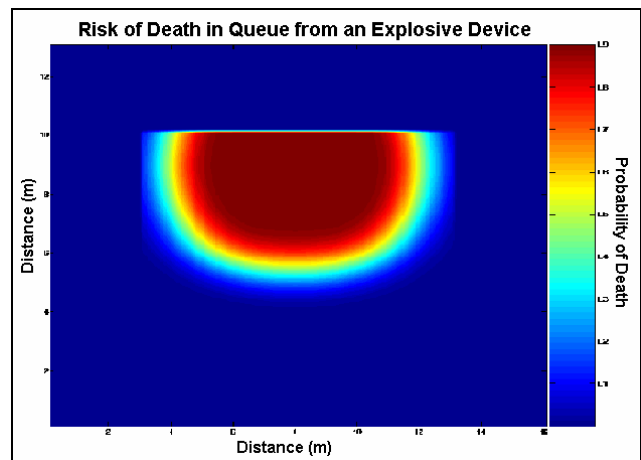


Fig. 11. Model of the probability of death when an explosive device is detonated

C. Simulation Assumptions

The following is a list of the most critical simulation assumptions that have been made for the purpose of this project:

- All passengers pose the same potential threat to the system regardless of individual attributes such as race, sex, and religion.
- Passengers enter and go through the system individually. There are no families or groups of people that travel together.
- All passengers arrive at the airport between 2 hours and 30 minutes before their scheduled flight. This duration is divided into six 15-minute intervals and during each one, a sixth of the passengers for that flight arrive uniformly.
- All passengers occupy an area of 60.96 cm x 60.96 cm (2 ft x 2ft) in a check-in or security queue.

- All security personnel have been adequately trained and are capable of doing their tasks.
- In order to decrease simulation size and length, only a quarter of the airport will be simulated. This means that the collected passenger arrival data, as well as the airport resources (i.e. the number of security checkpoints and check-in counters), will be decreased by a factor of 4.

D. Preliminary Results

Currently, simulation models have been built and airport data is being collected so that reliable simulation results can be obtained. The casualty model was run to approximate the number of casualties based upon varied queue shapes and lengths. A blast radius of 8 ft is assumed and the explosive is detonated at the queue's center of mass. Fig. 12 shows a graph of these results.

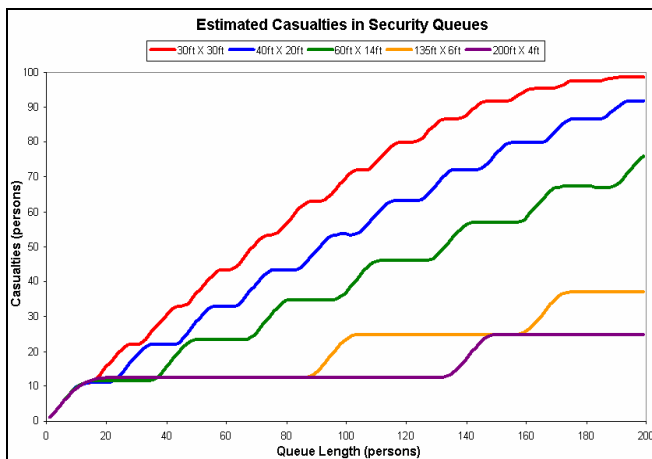


Fig. 12. Estimated Casualties in Security Queues given the queue dimensions and

Based upon this graph, one preliminary recommendation would be to build a queue in a rectangular shape as opposed to one with a square shape.

E. Analysis Plan

The main purpose of this study is to alleviate the problem of soft targets by increasing throughput, without sacrificing screening reliability. Analysis of the alternatives discussed above will determine which alternative best meets this criteria. To perform this analysis, the queue length from the arena model will be placed in the casualty model.

The casualty model will be used to determine whether the queues generated in the simulation of the alternatives present soft targets. Based upon the risk of death generated in the casualty model, changes may be made in the Arena model or queue shape, as shown in the preliminary casualty estimation in Fig. 12, to improve the alternative. Data from the simulation, such as false alarm and false clear rates, and passenger block times will be placed into the utility functions and the alternative with the highest score is recommended for implementation.

V. CONCLUSION

We foresee that the alternatives presented will provide an enhancement to the airport security system currently being used. Both alternatives focus on increasing throughput, especially for the first line of defense, by proposing the use of screening equipment with higher processing times such as the millimeter wave backscatter. Moreover, these alternatives involve grouping the passengers intelligently so that not everyone will have to go through every layer of security. This strategy will not only decrease the problem of soft targets but also deter a potential threat from attacking the system due to its unpredictability.

REFERENCES

- [1] "Who We Are." *Transportation Security Administration, US Department of Homeland Security*. 8 September 2006. <http://www.tsa.gov/who_we_are/index.shtm>.
- [2] Babu, Vellara L., Rajan Batta, and Li Lin. "Passenger Grouping Under Constant Threat Probability in an Airport Security System." *Science Direct - European Journal of Operational Research* 168 (2004): 633-644. 8 Nov. 2006.
- [3] Szurgyi, Stephen. *Modeling and Simulation of Dulles International Airport's Transportation Security Administration Departure Screening Area*. George Mason University. Fairfax, 2005.
- [4] Army Research Office. *Elements of Armament Engineering (Part One)*. Washington, D.C.: U.S. Army Materiel Command, 1964.