Decision Support Tool for Strategic Fiscal Analysis

AggiE-Challenge Project Semester 2
Preventing Nuclear Terror
Spring 2013

ISEN Team Members: Cameron Richardson, Jenny Flam, Samridhi Bhandari
NUEN Team Members: Michael Krutak, Sarah Camba, Shane Seabolt

Project Overview

The AggiE-Challenge is a program designed to actively engage undergraduate students with multidisciplinary team projects which are related to engineering challenges that society is currently facing. Specifically, the “Decision Support Tool for Strategic Fiscal Analysis” project is a part of a larger group of 14 projects known as the Grand Challenges for Engineering which are presented by the National Academy of Engineering (NAE).

The NAE Grand Challenge category that houses the “Decision Support Tool for Strategic Fiscal Analysis” (DSTSFA) project is called “Preventing Nuclear Terror” and the goal of this challenge is to address key issues regarding nuclear terrorism and nuclear security within the United States. The DSTSFA project focuses on providing a cost efficient analysis of protecting nuclear storage facilities while maintaining a desired level of strength within the facility. The tool will minimize the risk associated with housing nuclear material within a storage facility and will simultaneously increase the strength associated with that facility and the facility’s security. While the optimal strength of the facility is determined, the tool will calculate the minimum amount of financial resources needed so as to provide this optimal strength.

The final outcome of this AggiE-Challenge project will be a fully functional Decision Support Tool (DST) that will provide a complete financial analysis for short, mid, and long-range financial decision-making. The tool will provide decision makers with the optimal financial solution to safely securing nuclear material in any given nuclear facility. The tool will be implemented on multiple platforms (Microsoft Excel using VBA and Java Applet) and will allow for users to address specific details and design criterion pertaining to the nuclear facility undergoing revision.

Tool Description

The tool’s design will be in the form of decision making software. The user interface will remain simple so that the user will be able to easily enter specifications regarding the facility’s security strength and budgetary constraints.

The tool will first prompt the user for various items of information ranging from the size of the facility to the number of guards that are operating within each section of the facility. These items of information are called risk
factor variables and are the key pieces of data that the tool will manipulate to improve the facility. Next, the program will categorize the risk factor variables into groups called risk factors groups which will allow the tool to organize and calculate the strengths associated with different aspects of the facility. After categorizing the input variables, the DST will use this information and a set of strength algorithms to calculate the current strength of the facility. Next, the tool will use this calculated strength to set constraints for a method of optimization known as linear programming. The linear programming method will use these constraints and manipulate the risk factor variables so that they improve the overall strength and minimize the cost of the facility while still meeting the constraints that have been placed upon the system. Finally, the tool will display the optimal value for each risk factor variable in an easy to read and easy to navigate fashion.

The new strength of the facility and the new cost of operating the facility will be displayed to the user with an option that allows the user to change variables and see how each change affects the overall strength and cost of the nuclear storage facility. All data and calculations done by the DST will be stored so as to make retrieval of information at a later date quick and easy. Users will be able to re-visit the facility’s optimization in order to upgrade the security system or to re-analyze the cost analysis of the system.

The full list of risk factor groups and their corresponding subgroups, the strength algorithms, the interdependence model, and a description of the linear programming method can be found under “Model” below.

Methods/Research

The focus of this semester was on the security of existing storage sites. In order to get an idea of the types of systems and infrastructure that needed to be considered, literature and subject matter experts were consulted. Since the actual specifications for nuclear weapons sites are classified, a general approach was undertaken. Research focused on security for industrial sites and the types of systems that could be implemented. This was accomplished through review of handbooks and material written on security, risk assessment, and minimum standards.

Literary Review:

Architectural security codes and guidelines: best practices for today's construction challenges: For existing buildings there are minimum standards that must be met for environmental, energy, IT, safety vs. affordability and demographics. This book references those guidelines that must be met for a existing building and how to improve upon existing systems.

Perimeter Security: The safety of workers and materials can only be ensured by outfitting all points of entry with the appropriate alarm and surveillance equipment. This comprehensive hands-on resource focuses on designing, installing, and maintaining perimeter security for buildings.

Vulnerability Assessment of Physical Protection Systems: An important part of security is the assessment of the site’s current vulnerability. This important step-by-step details for performing the VA, data collection and analysis, important notes on how to use the VA to suggest design improvements and generate multiple design options. The goal being to organize and use the information at their sites and allow them to mix the physical protection system with other risk management measures to reduce risk to an acceptable level at an affordable cost and with the least operational impact.

Design and evaluation of physical protection systems: References to security expectations and changes since 9/11. The threat chapter includes references to new threat capabilities in Weapons of Mass Destruction, and a new figure
on hate crime groups in the US. This second edition also includes some references to the author's recent book on Vulnerability Assessment, to link the two volumes at a high level.

*Security risk assessment and management: a professional practice guide for protecting buildings and infrastructures:* This guidebook sets forth a systematic, proven set of best practices for security risk assessment and management of buildings and their supporting infrastructures. The methods set forth by the authors stem from their research at Sandia National Laboratories and their practical experience working with both government and private facilities. The book provides the reader with the analytical tools needed to determine whether to accept a calculated estimate of risk or to reduce the estimated risk to a level that meets your particular security needs.

**Meetings with Subject Matter Experts:**

Another part of our research was reaching out to subject matter experts. Our time with them gave us an inside look into the real world issues associated with nuclear security at storage sites. Their insight also provided an idea of how security is currently evaluated and where our model could fit into their work.

*Mr. Richard Mac Namee, lecturer at the Bush School of Government and Public Service.* His background is in security threat assessment and analysis at government and private high-risk sites. We consulted with him on what types of security and systems that needed to be included in our model, as well as discussed the challenges associated with evaluating site in a system as opposed to a site by site basis as is the current standard. He proposed that our model could be used for private industry sites as well as government. The risks and challenges associated with them are not very different.

*Mr. Phillip Gibbs, Savannah River National Laboratory.* His background is specializing on insider threat and working to minimizing the probability that a security threat will come from the current employees in a site. This is now a larger threat that an outsider attack and something that our model will encompass in the future.

**Assumptions**

Due to the vast amount of information and differences in information that nuclear security entails, our team has had to narrow the scope of the project in order to make the end goal much more feasible. In order to do this, we have made different assumptions regarding different aspects of our project that pertain to nuclear security on some level. At later stages in the project, we will attempt to remove these assumptions in order to create a tool with greater utility for a wider range of circumstances. The assumptions that we have made for this semester are as follows:

**Circular Zone Model:** Because there are numerous nuclear storage facilities that all have different sizes and shapes, we discovered a need to have one uniform model for evaluating facility strength. Because of this, we developed a model that assumes that all the facilities, regardless of size and shape, can be evaluated in the same way by assuming that they are circular in shape. The size of the circle is in turn affected by the size of the facility; however, the shape of the model will always be the same. By allowing all of the facilities to conform to this model, we are creating a method of strength evaluation that will be consistent for each facility, regardless of varying sizes or differences in risk factor variables. Because the Circular Zone Model is being used to calculate a conceptual strength, there are no actual changes being made to the facilities but every facility can be evaluated on the same standard of strength.

**3 Zone Model:** The 3 Zone Model works in conjunction with the Circular Zone Model. The 3 Zone model assumes that in any given facility there are only three different types of zones. Each zone represents some area that makes up
part of the facility. Because we have developed our tool to be as uniform as possible in relation to the calculation of strength, each zone has the same risk factor variables regardless of whether they are present in the zone or not.

The first zone is the least critical and is the most exterior portion of the facility. Zone 1 is made up of the area from the external facility perimeter to any building that is housed within the facility. Zone 1 is normally uncovered, meaning that it is exposed to the sky; however, it can also be made up of any access points that allow access from outside of the perimeter into the zone. Zone 1 does not house any nuclear material and is primarily made up of roads, guard towers, and guard patrols.

Zone 2 is the summation of any building within the facility that does not house nuclear material. The area of every building of this type is added together and, using the Circular Zone Model, is redistributed in the form of a circle so as to evaluate its strength. Zone 2 consists of every building that does not house nuclear assets and is primarily made up of hallways, offices, and laboratories that do not deal with nuclear material. The majority of the facilities staff operates in Zone 2.

Zone 3 is the summation of any building within the nuclear storage facility that does house nuclear material. Zone 3 is typically the innermost portion of any building and is guarded by high levels of security clearance. Although nuclear materials may be spread out in different locations throughout the facility, Zone 3 in the Circular Zone Model is the total area of any interior location that houses nuclear assets. As in Zone 2, Zone 3 is added together and re-distributed as a circle so as to evaluate its strength.

All three zones serve a specific purpose within the facility and we have found that there is no need to have more than three different zones. A schematic displaying the Circular Zone Model, the 3 Zone Model, and all risk factor groups that make up the facility can be found in Figure 1.1 Below as well as in Figure 1.1 of Appendix B.
These are the assumptions that have been made this semester only. A full list of assumptions that have been made for this project can be found in Appendix A – Assumptions.
Model

The overall model of our Decision Support Tool operates in three steps. The first step is to organize all of the risk factor variables in the facility. Because the circular Zone Model and 3 Zone Model were developed in a way that allow for each zone to have the same risk factor variables, the organization of variables becomes easier. If a zone does not have a specific variable, then the risk factor is recorded as a null and the strength algorithms operate without using the variable. The full list of Risk Factor Variables can be found below under the section titled “Risk Factors.”

After all of the risk factor variables have been recorded, the DST calculates the strength of the facility as it currently exists. This is done via the use of the strength algorithms which are found below. The strength algorithms provide an individual strength for each risk factor variable for each zone. Once the strength has been calculated individually for each risk factor, they are then combined via a system of weights and averages to find the overall strength of each zone. This step is then repeated to combine the strength of the three zones into one total facility strength. The strength algorithms for each risk factor are discussed in more detail below in the section titled “Strength Algorithms.”

Finally, the DST uses this existing facility strength in conjunction with linear programming to improve the overall strength of the facility while minimizing the cost of operating the facility. Linear programming is a mathematical method that uses linear algebra to manipulate a system of equations to solve for an objective function. In our project, the system of equations is made up of risk factor interdependencies where the variables for each equation are the risk factor variables. The objective function in our situation is to maximize the strength associated with each variable by using the strength algorithms. This step is explained in more detail below under the section titled “Interdependency Model.”

Risk Factors

As stated earlier, the variables that are being manipulated by our tool are called risk factor variables. We have tried to limit our number of variables that our tool uses so as to simplify the mathematical calculations done by our tool. Because of this we have selected risk factors groups that we believe play the most important role in evaluating the strength of a nuclear storage facility. The risk factor groups and their corresponding risk factor variables are as follows:

1. Nuclear Assets
   a. Type of Nuclear Material
   b. Amount of Nuclear Material
2. Personnel
   a. Security Personnel
      i. Number of Patrolling Guards
      ii. Radius of Patrol by Patrolling Guards
      iii. Number of Response Guards
      iv. Response Time of Response Guards
3. Security Systems
   a. Detection Systems
   b. Delay Systems
4. Adversaries
   a. External Adversaries
   b. Internal Adversaries
5. Support Structures
   a. Size of the Facility
Each of these risk factor variables plays a role in the overall strength of the nuclear facility. The strength algorithms for each risk factor variable can be found below in the section titled “Strength Algorithms.”

**Strength Algorithms**

As was mentioned above, the strength algorithms that we have developed are the method by which we are evaluating the strength of the facility. The Spring 2013 semester has primarily been focused around the development of these algorithms. Each algorithm was developed via the combination of a parent logistics equation as well as geometric relationships within the first zone. That being said, we have only been able to develop the strength algorithms for Zone 1 at this time. Because we developed the Circular Zone Model and the Three Zone Model to be uniform across all three zones, the strength algorithms for each risk factor within each different zone should be relatively similar and should not require much more time to develop. The first part of the fall semester of 2013 will be used to complete the development of the strength algorithms for each zone.

As stated earlier, the strength algorithms are a combination of a parent function and geometric relationships. The parent function that was used was a logistics equation because it most closely resembles the behavior that we would like the strengths of each risk factor to exhibit. A graph displaying this behavior can be found in Figure 1.3 in Appendix B. The geometric relationships that were used in combination with this parent function all stem from the Circular Zone Model which can be seen in Figure 1.1 in Appendix B.

Each risk factors strength algorithm for Zone 1 can be found below.

**Nuclear Assets**

Because we have only developed the strength algorithms for Zone 1 at this time, and because Zone 1 does not house any nuclear assets, we do not currently have a strength algorithms associated with nuclear assets. This strength algorithm will be developed within the first couple of weeks of the Fall 2013 semester.

**Security Systems**

**Detection Systems**

For our zone 1 model, we used only motion detectors as our detection device. This assumption was made to simplify the model for now and identify a method to calculate the strength rating. We are calculating strength rating of the detection systems based on their overall coverage with respect to the perimeter around the facility. Firstly, we looked up total facility areas for some of the DOE sites in US such as Sandia National Labs, Los Alamos National Labs, Pantex Plant, and Y-12 Storage site. We then, calculated the average facility area and then based our calculations for the strength rating on our circular zone model with area corresponding to the average facility area. The motion detector used for this method was linear displacement motion sensor, for which we obtained the coverage length, coverage area and field of view from navy manuals. An arc-tan function was used to get a value for strength since we needed to bind the strength to a highest unattainable rating of 100. Also, the function needed to show the properties of significant change in strength at lower values of x (ratio of coverage length of detector to total perimeter multiplied by a factor of k) and insignificant change in strength at higher values of x.

Thus, the obtained equation for strength rating is as follows:
Strength Rating = \frac{\tan^{-1}\{4 \times x\}}{0.5 \times \pi} \times 100

Where \( x = \frac{\text{coverage length of detector} \times \text{number of detectors}}{\text{sum of circumferences}} \)

Since we have assumed our model facility to be at 80% strength, we used a factor of 4 in this function since it roughly corresponds to 80% on the arc tan function graph.

Delay Systems

A delay system can be defined as any security system that delays a target adversary. For our delay system we decided that we would choose a set of checkpoint stations, such as a metal detector, in combination with some number of personnel to make up a delay system within an access point. The delay system strength algorithm is the most complicated in that it involves selecting checkpoint stations from a table and providing the number of personnel that would be operating the delay system. The algorithm uses Boolean logic to check if the delay system meets certain government requirements, and displays the strength of the delay system.

Each station that is selected has a suggested number of personnel to operate the station. If the delay system does not meet the total required number of personnel as suggested then they attain a strength rating that is proportional to the number of personnel that they actually have in relation to the suggested number of personnel. Each station that is selected is considered to have a strength of 30, 20, or 15 out of 100. If the station checks a personnel’s identification without requiring a personnel to be present then it merits a strength of 30. If the station suggests personnel but can operate without personnel present then it merits a strength rating of 20. If the station must have a personnel present to operate then it merits a strength rating of 10.

After the user has selected all of the checkpoint stations that make up the delay system then it sums all of the respective strength ratings and multiplies it by the factor of actual personnel to suggested personnel to attain the total strength of the delay system up to 100.

Personnel

Response Guards

The strength of response guards was measured on the basis how their numbers varied on the arc tan scale. We assumed that the response forces were stationed on the guard towers for zone 1 and they had uninterrupted communication line with the central alarm station. We calculated the average number of response guards by finding total number of personnel in a nuclear facility then subtracting the patrolling guards, observational guards, security guards at an access points. This gave us an estimate of number of response guards present in an 80% strength facility. The algorithm for the strength rating is as follows:

\[
\text{Strength Rating} = \left( \frac{200}{\pi} \right) \left( \text{ATAN(Number of Response Guards \times TAN(2 \pi) \times \frac{1}{2}} \right)
\]

Response Time
Firstly, we calculated the fastest response time possible in an average facility using Fitts law and then calculated response time for an 80% strength rating. After analyzing the change in strength with respect to change in response time, we identified that arc-cosine function mapped the change better than arc-tan function. Thus, the algorithm for strength rating is as follows:

\[
\text{Strength Rating} = \left( \frac{200}{\pi} \right) \text{ACOS}(\text{Number of Response Guards} \times \cos\left(\frac{2}{5}\pi\right)) \]

**Application of Human Factors in the Project**

This semester, use of human factors and ergonomics principles has been significant both in formulating equation for fastest response time and for designing the graphical user interface for the tool. Firstly, we used the equations from movement time and reaction time to find the fastest response time for the response personnel in the facility. The assumptions made for this calculation were:

a. The response personnel were housed in the guard towers.

b. The guard towers were optimally place throughout the facility.

From these assumptions, we were able to calculate the smallest distance between a guard tower and a detection point. The equations used are as follows:

\[
\text{Response Time} = \text{Reaction Time} + \text{Movement Time}
\]

The response time obtained was considered to be the best possible response time and then we adjusted the value to our facility model and a strength rating of 80.

Similarly, human factors guidelines on effective display and controls were used while designing the graphical user interface for the tool. The tool was made user-friendly with effective display techniques such as displaying information which requires minimum cognitive resources to process. We will certainly use more of these principles next semester as the tool builds upon more complexity.

**Patrol Guards**

The assumption was made that the patrolling guards would patrol around an assigned guard tower at a specific radius. Each individual guard tower would be used as a base for communications and launching of the response team. The number of patrol guards that was made equal to a successful strength rating of 80 was set to 2. Should the number of patrol guards patrolling around a guard tower be greater than or less than 2, the strength rating was output using the formula:

Number of Patrolling Guards:

\[
\text{strength rating} = \frac{200}{\pi} \left( \tan^{-1}\left( P \times \tan\left( \frac{73.333 \times \pi}{200} \right) \right) \right)
\]

Where P: = Number of patrolling guards

**Patrol Radius**

A distance then needed to be determined for a strength rating of 80. With the idea that too great a distance from the guard towers would hinder response time and that too little a distance would hinder area covered by the patrolling guards, 1/3 the distance recommended distance between guard towers was chosen as an appropriate patrol
radius. At 1/3 the distance between two towers the patrolling guard is neither too close nor too far from the guard tower. 1/3 the distance between two guard towers would be approximately 620 feet.

\[
\text{strength rating} = (-900) \left( \frac{R}{620} - \frac{1}{3} \right)^2 + 100
\]

Where \( R \) = Patrolling radius in feet

Support Structures

Access Points

A program input is the number of access points a facility contains. An access point is therein defined as a point of entrance or possible point of intrusion from which a documentation and paperwork station, three exterior threat checkpoints, a security office, and a minimum of one supervising personnel. Using Comanche Peak Nuclear Power Plant as a model for access point security personnel needs, a strength rating of 80 necessitates four paperwork station personnel, three exterior checkpoint personnel, one security office personnel, and one supervising personnel. The overall strength rating then given to the facility for access point strength was the summation of individual strengths of the four divisions of the access point weighted evenly by multiplication by 0.25. It should be noted here that a strength rating of 80 is the margin between an adequate facility security and an inadequate facility security.

<table>
<thead>
<tr>
<th>Station Type</th>
<th>Number of Personnel</th>
<th>individual strength</th>
<th>weighted strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation and Paperwork Station</td>
<td>4</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>Security Office</td>
<td>2</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>Supervising Personnel</td>
<td>1</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td>Exterior Threat Checkpoint</td>
<td>3</td>
<td>80</td>
<td>20</td>
</tr>
<tr>
<td><strong>Total Access Point Strength:</strong></td>
<td><strong>80</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The equation programmed to accept the input of number of personnel and output the strength for that specific division of the access point was derived from an exponential function with a horizontal asymptote at 100 (max strength rating), which sees the largest change in the strength rating near the strength rating value of 80 which relates to the recommended number of personnel mentioned previously. All four divisions of the access point use the same strength rating equation shown below.

\[
\text{strength rating} = \frac{100}{1 + 5 \times e^{-\left(\frac{Y}{7}\right)\left(2 \ln(2) + \ln(5)\right)X}}
\]

Y: Recommended number of personnel
X: Number of personnel in the facility

Guard Towers

Each nuclear facility whether a research lab or weapon storage facility needs guard towers in order to fully secure the site. The number of guard towers found to be needed in a facility roughly
paralleling the average of four different DOE and DOD facilities such as Comanche Peak, Pantex, Limerick and Los Alamos. The number assumed to effectively secure the site was found to be nine with the knowledge that Limerick currently has seven guard towers and risk analyst have been quoted saying that is not enough. This assumption was further solidified by using a simple comparison between response time and

The equation for strength rating of the number of guard towers in the

\[
\text{strength rating} = \frac{200}{\pi \cos^{-1}\left(\frac{2\pi}{\gamma}\right)}
\]

\(\delta\): Number of guard towers
\(\gamma\): Recommended number of guard towers

The guard towers were then given two other strength ratings based on the data inputs of greatest and least distance between two adjacent guard towers along with the greatest and least distance between a guard tower and the exterior facility wall. The prospected distance that the guard tower should be from the wall and to the nearest other guard tower was determined to be 3700 feet and 1750 feet respectively. 3700 was calculated by finding the difference between radii of the average size for Zones 1 and 2, then dividing that number by 2. 1750 was the chord length between two guard towers should the perimeter of the circle equidistant to Zone 1 and Zone 2 contains nine guard towers. The equations used to relate the greatest and least distance between towers (Angular) and from the towers to the exterior wall (Radial) are as follows:

**Angular Guard Tower Location**

\[
\text{strength rating} = 100 \times e^{-0.001(G_A - S_A)}/\sqrt{\delta}
\]

\(\delta\): number of guard towers
\(G_A\): greatest distance between two adjacent guard towers
\(S_A\): smallest distance between two adjacent guard towers

**Radial Guard Tower Location**

\[
\text{strength rating} = \frac{200 \cos^{-1}\left(\frac{2(G_R - S_R)}{9R}\right)}{\pi}
\]

\(\delta\): number of guard towers
\(R\): radius located halfway between the perimeter of Zone 1 and 2; i.e. where the guard towers should be positioned
\(G_R\): greatest distance between two adjacent guard towers
\(S_R\): smallest distance between two adjacent guard towers

The different components of the total guard tower strength were then given an equal weight of 1/3, which is depicted below in the table for Guard Tower Strength Information. The current table illustrated is based on a system with an equal number of guard towers to the recommended number of 9, as well as having no variation in the location, either radially or angularly, of the guard towers.
### Guard Tower Strength Information

<table>
<thead>
<tr>
<th>Angular Guard Tower Location Information</th>
<th>Radial Guard Tower Location Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater Distance Between 2 Adjacent Guard Towers</td>
<td>Greatest Distance of Guard Tower From Exterior Wall</td>
</tr>
<tr>
<td>1750</td>
<td>3700</td>
</tr>
<tr>
<td>Smallest Distance Between 2 Adjacent Guard Towers</td>
<td>Smallest Distance of Guard Tower From Exterior Wall</td>
</tr>
<tr>
<td>1750</td>
<td>3700</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strength of Guard Towers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Strength</td>
</tr>
<tr>
<td># of Guard Towers</td>
</tr>
<tr>
<td>Angular Location of Guard Towers</td>
</tr>
<tr>
<td>Radial Location of Guard Towers</td>
</tr>
</tbody>
</table>

Total Guard Tower Strength 93.33324

### Interdependency Model

After the existing strength of the facility has been calculated using the strength algorithms, the tool then proceeds to the final step in optimizing the nuclear storage facility. The first part of this step involves creating a system of equations. This system of equations is made up of equations representing interdependencies within the nuclear facility. Each risk factor has some dependency relationship with the other risk factors. Because of this we can represent these dependencies in an interdependency model. With this model we can begin to see how each change in the facility effects not only one risk factor, but all of the risk factors and the nuclear facility as a whole, both in risk/strength as well as financial implications. The interdependency model can be found below in Figure 1.2, as well as under Figure 1.2 in Appendix B.

Figure 1.2: Interdependency Model
As can be seen from Figure 1.2 each risk factor has some form of dependence with another risk factor. This being said we can recognize that as one risk factor changes, other risk factors that depend on the parameters of that risk factor will have to change accordingly. We recognize that because of this need to change, certain risk factors are dependent on others. Each arrow in the model above represents an equation. The arrow points from the dependent risk factor to the independent risk factor. Each of these equations changes with some constant that is unique to the equation which in turn constrains the system of equations so that the solution remains feasible with respect to the overall objective function. These constants are set by the existing facility strength that was solved for in the previous step. After the system of equations has been created, the tool will manipulate the linear program and will solve for the optimal values for each risk factor variable so as to minimize the cost associated with operating the facility. After these values have been calculated, the strength algorithms are then used again to re-calculate the strength of the facility.

This model was developed during the Fall 2012 semester of the project and is in need of adjusting; however, we believe that the structure of the model is accurate. We will be spending the remainder of our time focusing on developing the program to be able to solve this system of equations, but in the meantime we have found that this model solves the problems that we currently have.

**Project Timeline**

**Semester 1**

We met our AggiE-Challenge team, were briefed on what the full scope of the project entailed, and began work on the DSTSFA Project. As a team we researched political and technical documents pertaining to nuclear security, spoke with professors and graduate students about the project and followed their guidance as far as how to proceed, and began to reach out to other knowledgeable members of the Texas A&M network that could potentially aid in our understanding of nuclear security. During research we began to formulate a set of risk factors that we believed to have a major influence on the strength and financial aspects of the nuclear facility. During one interview with Dr. Charlton and Dr. Boyle, of Texas A&M University’s Nuclear Engineering Department, we learned of a way to represent and measure the risk associated with nuclear facilities. Using this representation and our set of key risk factors we were then able to procure a model off of which we will base our DST.

**Semester 2**

During the Spring 2013 semester, our team has made giant strides towards completion of the project. We have developed not only a method to evaluate nuclear storage facilities without actually having data relating to the facilities, but we have also decided on how the DST will operate. We have completely mapped out the process for evaluation of strength as well as how we will optimize the risk factor variables. We have successfully developed strength algorithms that can evaluate the strength of each zone in a nuclear facility in a way that will allow for minor changes that will allow for variation between the zones. We have developed a proof of concept that shows that our calculations are relatively correct and that will aid us in making our algorithms more accurate in the future. We have done research that has lead us in the appropriate direction in solving our nuclear terror problem and we are becoming ever closer to completion of our project. Finally, we have begun to develop a user interface for our tool which will be both functional and easy to use.

**Semester 3**

In the last semester of our project, we will have a lot of work to complete. We must first finish developing our strength algorithms for each zone. Next we will need to ensure that our linear program will work for optimizing the strength and financial aspect associated with the nuclear facility. After we have completed both of these tasks we
will be able to completely program the decision support tool. We will continue to work on the user interface of the tool as we proceed, and hopefully, the way in which we have already developed the program will aid us in the continuing development of the tool. Our end goal will be a completely functional Decision Support Tool that will be able to increase the security of a nuclear storage facility and decrease the cost associated with operating the facility by making simple changes to the numerous risk factor variables.
Appendix A – Assumptions

3 Zone Model: The 3 Zone Model works in conjunction with the Circular Zone Model. The 3 Zone model assumes that in any given facility there are only three different types of zones. Each zone represents some area that makes up part of the facility. Because we have developed our tool to be as uniform as possible in relation to the calculation of strength, each zone has the same risk factor variables regardless of whether they are present in the zone or not. The first zone is the least critical and is the most exterior portion of the facility. Zone 1 is made up of the area from the external facility perimeter to any building that is housed within the facility. Zone 1 is normally uncovered, meaning that it is exposed to the sky; however, it can also be made up of any access points that allow access from outside of the perimeter into the zone. Zone 1 does not house any nuclear material and is primarily made up of roads, guard towers, and guard patrols.

Zone 2 is the summation of any building within the facility that does not house nuclear material. The area of every building of this type is added together and, using the Circular Zone Model, is redistributed in the form of a circle so as to evaluate its strength. Zone 2 consists of every building that does not house nuclear assets and is primarily made up of hallways, offices, and laboratories that do not deal with nuclear material. The majority of the facilities staff operates in Zone 2.

Zone 3 is the summation of any building within the nuclear storage facility that does house nuclear material. Zone 3 is typically the innermost portion of any building and is guarded by high levels of security clearance. Although nuclear materials may be spread out in different locations throughout the facility, Zone 3 in the Circular Zone Model is the total area of any interior location that houses nuclear assets. As in Zone 2, Zone 3 is added together and redistributed as a circle so as to evaluate its strength.

Access Points: This tool will only focus on visible access points. These include: doors, and checkpoints. The hidden access points which we will not consider include: air ducts, tunnels, crawl spaces, skylights, sewers, attics, chimneys, and exhaust fans. The reason for this is that the design of this device would be based on an inaccurate estimate if these were included.

Circular Zone Model: Because there are numerous nuclear storage facilities that all have different sizes and shapes, we discovered a need to have one uniform model for evaluating facility strength. Because of this, we developed a model that assumes that all the facilities, regardless of size and shape, can be evaluated in the same way by assuming that they are circular in shape. The size of the circle is in turn affected by the size of the facility; however, the shape of the model will always be the same. By allowing all of the facilities to conform to this model, we are creating a method of strength evaluation that will be consistent for each facility, regardless of varying sizes or differences in risk factor variables. Because the Circular Zone Model is being used to calculate a conceptual strength, there are no actual changes being made to the facilities but every facility can be evaluated on the same standard of strength.

Cyber Terrorism: Our team has the assumed cyber terrorism is covered by someone else. This will eliminate the need for virtual security and all of the related costs.

Equation Assumptions:
- \( P(\text{Threat}) = 1 \) because: We are looking at identical nuclear facilities in terms of the attractiveness of the nuclear assets they contain. Therefore, the likelihood of an adversary attack would be the same for each facility.

- \( P(\text{Consequence}) = 1 \) because: We are assuming that if we fail to secure any 1 nuclear asset within the nuclear facility then the consequences are inevitable.

Fixed Locations: We narrowed the scope of the tool to only be used for nuclear facilities that are fixed in their location. This was useful in that it eliminated numerous risks such as transportation of nuclear material, or mobile facilities such as nuclear submarines. By only focusing on fixed location facilities we will be more able to create a universal tool that can be used for similar sites.
Informational Systems: We will assume that all informational systems are sufficient and do not affect the cost of a nuclear facility. The purpose of this is to …

Item Accountable Nuclear Assets: In order to simplify the data representing the nuclear assets within a given nuclear facility, we have decided to incorporate facilities that house item-accountable nuclear assets as opposed to mass-accountable nuclear assets. This means that we will only consider facilities that house nuclear weapons and nuclear weapon components. We have chosen to do this because it allows us to have a more definite representation of the exact amount of nuclear assets being housed by the facility. With mass accountable nuclear assets, there is the possibility of having fractions of weight that would be hard to measure and account for. Therefore the ability to count the number of assets as a whole integer will be very beneficial in the mathematical representation of the nuclear assets.

Non-Profit Facilities: Our team has recognized that for-profit nuclear facilities have an additional goal of generating revenue, which is incorporated in their financial analysis. In order to simplify our tool, we have decided to ignore this additional goal, which will decrease the total number of needs that our tool has. Therefore, we will only be focusing on facilities that operate under the government (DoE facilities as well as government contractors) that are not for profit facilities.

Optimizing Existing Facilities: Before one can create a new facility, one must first know the optimal way of creating said facility. This requires us to have preexisting data to base our design decisions off of which can only come from optimizing current facilities. Thus, we would already need to optimize the current facilities before we could even begin to create new ones. Therefore, we decided not to concern ourselves with the creation of a new facility, but rather to focus on optimizing existing facilities only, which in turn substantially decreased the amount of work necessary.

Personnel: In order to eliminate confusion from all of the varying costs associated with personnel, our team has decided to assume that the personnel are adequate for the facility described and the associated costs are invariant with the total facility costs. This will help concentrate our focus on the nuclear assets relationship with costs associated within each facility.

Project Focus: Our team has decided that we will analyze the nuclear security problem by using a “bottom-up” approach. We decided to use this method due to the large amount of (normally restricted) information. We came to the conclusion that if we started with a narrow idea of what we wanted the tool to accomplish, that we could establish a strong basis for the project to begin with and could then build upon that basis as we sifted through all of the information.

Stakeholders: We have defined the stakeholders of the nuclear facilities to be the Department of Defense, the Department of Energy, the Nuclear Weapons Council, and the US Congress. We have selected these specific groups of people to be the stakeholders, because they will ultimately be the ones that are responsible for the nuclear facilities and are the organizations that will be making any major decisions regarding nuclear security. Thus, we will be designing the DST with these groups in mind.
Appendix B - Figures

Figure 1.1: Circular Zone Model, 3 Zone Model, and Risk Factor Groups Incorporation Schematic
Figure 1.2: Interdependency Model

Figure 1.3: Logistic Equation Behavior
Glossary

**Adversary** - An insider or outsider performing malevolent acts in pursuit of interests harmful to the facility; outsiders are specifically international terrorist organizations with a domestic (within U.S.) presence attempting to attain access to nuclear assets.

**Adversary Task** - A specific act the adversary must perform in order to advance along a path; for example, penetrate a barrier, travel a certain distance, etc.

**Adversary Path** - An ordered collection of actions against a target that, if completed, results in successful theft or sabotage.

**Attack** - An attempt to destroy, expose, sabotage, alter, disable, steal or gain unauthorized access to or make unauthorized use of a nuclear asset.

**Consequence of Threat/Failure** – The assumed consequence of the system’s failure to secure any one item in the nuclear facility will result in misuse of the nuclear weapon in order to cause some amount of harm to the stakeholders or general public.

**Delay Systems** – All forms of physical protection functions of a nuclear facility including: passive barriers and active barriers.

**Design Criteria** – Criteria that is intended to increase the strength of the facility based on the existing vulnerabilities.

**Detection Systems** – All forms of physical protection functions of a nuclear facility including: intrusion sensing, alarm communication, alarm assessment, and entry control.

**Insider Threat** – The threat posed by a current employee of a nuclear facility. This threat is characterized by a high risk of sabotaging or damaging the security of the facility and is affected by the employee’s access, authority, and knowledge.

**Non-Security Personnel** – All of the operative, administrative, and research personnel employed by the nuclear facility intended for managing the overall workings of the facility.

**Nuclear Assets** – All the special nuclear materials that are mass accountable, specifically grams.

**Nuclear Security** – Security measures for nuclear facilities to reduce the chance that nuclear assets could be stolen and fall into terrorist hands, through an outsider or insider attack.

**Nuclear Terrorism** – The use of a nuclear asset by a terrorist or terrorist organization to cause massive devastation to the population.

**Path** – Any physical route taken by the adversaries.

**Security Personnel** – The personnel employed by the nuclear facility intended to guard and protect the assets held by the facility. This also includes response forces.

**Special Nuclear Material** – As defined by the Atomic Energy Act of 1954: Special nuclear materials include plutonium, uranium 233, and enriched uranium 235.

**Stakeholders** – Includes all decision makers, specifically: DOD, DOE, Nuclear Weapons Counsel, and the U.S. Congress.
**Strength** – The ability of the system to effectively counteract the potential vulnerabilities.

**Terrorism** – A criminal act that influences the audience beyond the immediate victim.

**Threat** – An act or potential act that would result in loss of assets or compromise the security of the nuclear facility.

**Threat Space Threshold** – The maximum amount of risk for a facility that is acceptable by the stakeholders. Specifically affected by security measures implemented to minimize vulnerabilities.

**Threat Space** – Area that the personnel at the site

**Risk** – Specific to this project, risk is equal to the combination of vulnerabilities within a particular facility. Risk = Threat x Vulnerability x Consequences.

**Risk Factor** – Necessary considerations within the threat assessment process, i.e. specified attributes and characteristics for each identified external threat.

**Vulnerability** – An exploitable capability or an exploitable security weakness or deficiency specifically those inherent in the design (or layout) of the facility and its protection, or those existing because of the failure to meet (or maintain) prescribed security standards when evaluated against requirements for defined threats.

**Zone 1 - Blue (Property Protection Area):** This zone consists of the exterior perimeter of the property. It includes the first checkpoint for visitors and personnel once their vehicle has been cleared.

**Zone 2 - Red (Limited Area):** This zone consists of the entrance to the buildings inside the Property Protection Area. This area is defined by physical boundaries and may contain sensitive material. Unauthorized personnel require an escort.

**Zone 3 - Yellow (Exclusion Area):** This zone consists of the secure area within the building containing the nuclear assets. Entry will result in close proximity to classified material and/or information.
Bibliography


