FIXED-SITE PHYSICAL PROTECTION SYSTEM MODELING*

Leon D. Chapman
Sandia Laboratories, Albuquerque, New Mexico

ABSTRACT

An evaluation of a fixed-site safeguard security system must consider the interrelationships of barriers, alarms, on-site and off-site guards, and their effectiveness against a forcible adversary attack whose intention is to create an act of sabotage or theft. A computer model has been developed at Sandia Laboratories for the evaluation of alternative fixed-site security systems. Tradeoffs involving on-site and off-site response forces and response times, perimeter alarm systems, barrier configurations, and varying levels of threat can be analyzed. The computer model provides a framework for performing inexpensive experiments on fixed-site security systems for testing alternative decisions and for determining the relative cost effectiveness associated with these decision policies.

INTRODUCTION

In considering the various fixed-site safeguard measures, one is rapidly overwhelmed by a multitude of interactions and tradeoffs that must be taken into account. The deployment and characteristics of barriers, alarms, and guard forces (both on-site and off-site responses), must certainly affect any adversary that would try to attempt an act of sabotage or theft. However, it is not intuitively obvious just how these fixed-site safeguard measures can accommodate the number of attackers, the type of weapons employed, the resources used for barrier penetration, the mobility, or the type of attack (sabotage or theft) (1).

For example, would the addition of a 2-foot concrete barrier provide more cost-effective adversary delay for the arrival of an off-site response force than would two extra on-site guards? What are the roles of alarms in providing early assessment or warnings to the on-site security force? Which barriers should be alarmed? In general, alarms placed toward outer barriers are less reliable, but does this imply that only inner barriers should be alarmed? The answer is somewhat elusive since early adversary detection by the security force certainly provides more freedom in selecting the tactics to repel the aggressor. It is not a difficult task to provide cost and reliability functions for various types of barriers, alarms, and guard forces; the real question is system integration--what is the proper mixture of barriers, alarms, and guards at a fixed-site to satisfy a desired level of security? How can a fixed-site security design be evaluated? With these types of questions in mind, it becomes clear that a technique to investigate the various security tradeoffs is required.

MODEL DESCRIPTION

A computer model has been developed at Sandia Laboratories for evaluating alternative fixed-site security systems (2). The simulation model written in the GASP IV simulation language (3) (all FORTRAN based) processes both discrete and continuous events and would normally be referred to as a combined simulation model. Discrete events would include beginning and ending of barrier breaks, alarm trips, on-site and off-site guard force alerts and arrivals, beginning and ending of the battle(s), barrier(s) installed based upon alarms (activated delays), sabotage completion, theft completion, and delaying battle tactics. Continuous events would primarily include those events during a battle between the adversary and the defenders of the fixed-site.

The model requires as input the characteristics of the fixed-site to be evaluated. As shown in Figure 1, this would include information on the number of barriers, the type of each barrier, which barriers are alarmed, and the thickness of barriers if the barrier is concrete or wood. In addition to barrier information, the size and response time of the on-site response forces, the perimeter of the site, the size and response time of the off-site response forces, and the dedication and sophistication of the guard forces are required input data.

BARRIERS	ON-SITE RESPONSE FORCES	RESPONSE FORCES
·Type	·Number of Guards/ Force	·Number of Guards
Fence	·Response Time	·Response Time
Chainlink Fence	·Dedication/ Training	·Dedication/ Training
Metal Door	Low	Low
Vault	Medium	Medium
Concrete Walls/ Bldg.	High	High
Wood Walls/Bldg.		
Vehicle		
Activated Delay		
Zero Delay		
·Thickness		
Concrete Walls/ Bldg.		
Wood Walls/Bldg.		
·Distance Between Barriers		
·Alarms		
Location		
Probability		

Figure 1 - Fixed-Site Characteristics

The model is capable of randomizing the adversary attributes for various attacks against the fixed-site design. These characteristics would include the number of attackers, their weapon type (side arms or automatic weapons), the resources for barrier penetration such as tools without high explosives (HE) or tools with HE as depicted in Figure 2. In addition, four types of adversary attacks are considered--sabotage/internal, sabotage/external, theft/internal, and theft/external. Internal attacks imply that the attackers have an insider working at the fixed-site that may degrade the alarm systems and communication systems. Attacks with internal assistance would then result in a less effective alarm system, a delayed on-site response arrival, and a delayed off-site response arrival. An external attack implies the attackers do not have any inside assistance. The mode of transportation (vehicles, no vehicles, or air vehicles), an important attacker characteristic, and the dedication of the attackers are both random variables in the generation of adversary attributes. In the absence of a defined threat, it is better to evaluate the fixed-site design with several variations in the attacker characteristics. This ultimately will provide or help define the breakover point of the site design to a specific level of threat. Thus, it seems very appropriate to permit the computer to generate a large number of varying attacker characteristics to emulate a spectrum of threats. If a specific threat definition is known in advance, it can certainly be used as input and the site can be evaluated against this threat definition.

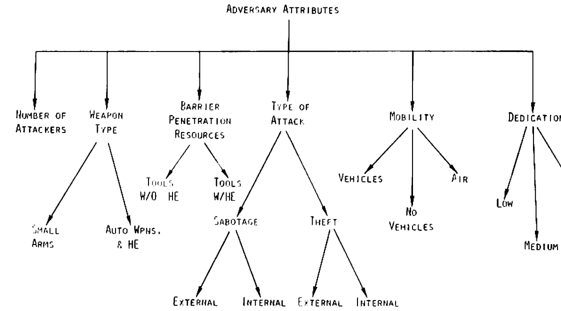

Figure 2. Adversary Attributes

---

*This work was supported in part by the Nuclear Regulatory Commission's Special Safeguard Study conducted at Sandia Laboratories during March - October 1975.

Given these inputs, the computer model can then be utilized to simulate a large number of adversary attacks (as characterized in Figure 2) against the site design to evaluate the effectiveness of the design. Figure 3 depicts the general operational procedure of the combined computer simulation model. After the site characteristics have been selected, adversary attributes are generated and an attack is simulated against the fixed-site. Barrier breaks, delays of barriers, crossing times between barriers, and advancements are simulated by a random sample from defined probability distributions (4). Alarms at a given barrier may trigger communications to the on-site guard force, which is scheduled to arrive and assess the situation. Off-site guards are called if a serious alarm condition exists, and a battle takes place between the on-site guards and the adversary. During the battle phase, the adversary advancement is assumed to be interrupted. If the adversary wins, then his advancement continues until interrupted by the arrival of the off-site guard force or the completion of the theft or sabotage. Then, another attack is generated against the site. After a large number of attacks have been simulated, statistics can be accumulated to determine the relative effectiveness of this particular site design against various levels of threat.

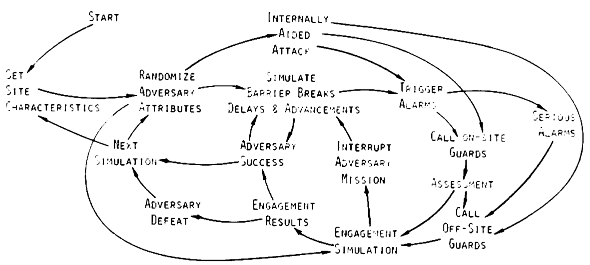

Figure 3. Fixed-Site Combined Simulation Model

A small force engagement model has been included to provide reasonable battle results (5). Figure 4 is a causal-loop diagram that illustrates the essential characteristics of the engagement model. Consider an attack against the fixed-site by the adversary. As the adversary penetrates barriers, an alarm will probably be sounded. Since all barriers will not be alarmed, there will be a delay from the initial starting of the attack sequence until the first alarm is sounded. Another delay accounts for the arrival time of the on-site guard force (defenders). The battle is then started. If one assumes the defenders can take up defended positions, given adequate time from the alarm, then the defenders will ambush the attackers.

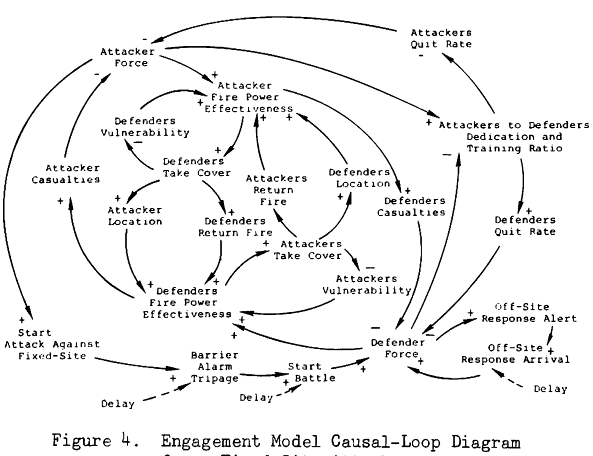

Figure 4. Engagement Model Causal-Loop Diagram for a Fixed-Site Attack

The ambush begins with the defenders having a significant firepower effectiveness which causes attacker casualties and ultimately reduces the attack force. The attackers immediately start taking cover which reduces their vulnerability, thus reducing the defenders firepower effectiveness. As the attackers take cover, they start returning fire which increases their firepower effectiveness as they begin locating the defenders. This, in turn, causes the defenders to start taking casualties. At the beginning of the battle, the call for assistance of the off-site response force is instituted. Presumably, the off-site response force arrival time is 30-60 minutes. The dedication and sophistication of each force plays an important role in the quit rate of the respective forces. For example, if the defenders are outnumbered 5:1, then the quit rate would certainly be higher than if the forces were of equal strength. This engagement model, which is essentially a non-linear Lanchester (6, 7) battle model with time-varying coefficients, is utilized for all engagements. If the attackers ambush the defending force, then the battle roles as described above are essentially reversed.

In the model, a hypothetical fixed-site concentric shell configuration of barriers is assumed. There are many paths by which the attacking force could choose to attack any given fixed-site. The assumption here is to always use the shortest identifiable path leading to the vital area; therefore, one simply defines the concentric shell barriers to correspond with this shortest path. Additional paths can be studied by changing the concentric shell configuration. If there were more than one vital area at a fixed-site location, then each vital area would be considered independently; and appropriate barrier locations could then be configured for each vital area.

EVENT SEQUENCE OF FIXED-SITE COMPUTER MODEL

Figure 5 from run number 5 represents an event sequence of one attack on the fixed-site. The threat attributes consist of 10 attackers, with automatic weapons, special equipment with HE for barrier penetration, no vehicles, low dedication, a mission of theft, and with no assistance from site personnel. The attack begins at barrier break 1, which is a four strand barbed wire fence with a mean delay of approximately 0.1 minutes.** The end of barrier break occurs at 0.13 minutes, and the alarm is checked for the detection of a penetration. Barrier 1 did not have an alarm. The attackers require 1.0 minutes to cross the area between barrier 1 and 2. The beginning of barrier break 2 starts at 1.13 minutes. Barrier 2 is a double chain link fence. The end of barrier break 2 occurs at 3.11 minutes, at which time a check for another alarm is made. There is no alarm on barrier 2. Time for crossing to the next barrier is calculated, and the attackers arrive at barrier 3 at 3.71 minutes. Successful crossing of the vehicle barrier occurs at 7.02 minutes, and a check for an alarm is made. This barrier is not alarmed. The beginning of barrier break 4 commences at 7.64 minutes. Barrier 4 is a 2-foot concrete building and requires the use of HE for penetration. The HE explosion which occurs at time 10.14 is either detected from the sound of the explosion by the on-site personnel, or the HE alarm device on barrier 4 provides the detection. The alert of the on-site response force is sounded along with the off-site response alert since the alarm came from the final barrier. This would represent a serious alarm or critical situation. The barrier installed, based upon alarms, was completed at time 15.14 minutes. The attackers continue to work and finish the barrier 4 penetration at 15.91 minutes, and another check for alarm is made. The serious alarm was previously sounded so nothing occurs. The attackers start barrier break 5 at 16.28 minutes. The 5 man on-site SWAT force arrives at 19.95, and the battle is initiated using delay tactics to provide additional delay time until reinforcements can arrive. The 5 man additional on-site force arrived at 25.96 minutes and is placed into the battle. A continuous battle takes place until the arrival of the 10 man off-site response force at 40.14 minutes. The defenders quickly overwhelm the attackers at

** All the parameters for barriers, guard arrivals, crossing times between barriers, etc., are normally distributed with a mean, variance, lower bound, and upper bound in the model.

that point, and the end of the battle takes place at 41.16 minutes after the beginning of the attack on the site. This ends the event sequence of one attack on the fixed-site.

```
        RUN NUMBER    5
TIME= Ø.ØØ  EVENT= 1  BEGIN BARRIER BREAK 1
TIME=  .13  EVENT= 2    END OF BARRIER BREAK 1
TIME=  .13  EVENT= 3    ALARM CHECK FOR BARRIER  1
TIME= 1.13  EVENT= 1  BEGIN BARRIER BREAK 2
TIME= 3.11  EVENT= 2    END OF BARRIER BREAK 2
TIME= 3.11  EVENT= 3    ALARM CHECK FOR BARRIER  2
TIME= 3.71  EVENT= 1  BEGIN BARRIER BREAK 3
TIME= 7.Ø2  EVENT= 2    END OF BARRIER BREAK 3
TIME= 7.Ø2  EVENT= 3    ALARM CHECK FOR BARRIER  3
TIME= 7.64  EVENT= 1  BEGIN BARRIER BREAK 4
TIME=1Ø.14  EVENT= 3    H.E. ALARM
TIME=1Ø.14  EVENT=12    ON-SITE RESPONSE ALERT
TIME=1Ø.14  EVENT= 9    OFF-SITE RESPONSE ALERT
TIME=15.14  EVENT= 8    ;;;;BARRIER INSTALLED BASED UPON ALARMS;;;;
TIME=15.91  EVENT= 2    END OF BARRIER BREAK 4
TIME=15.91  EVENT= 3    ALARM CHECK FOR BARRIER  4
TIME=16.28  EVENT= 1  BEGIN BARRIER BREAK 5
TIME=19.95  EVENT= 4  START BATTLE,  5 MAN ON-SITE FORCE ARRIVAL
TIME=21.95  EVENT=13          STOP BATTLE---DELAY TACTICS
TIME=23.95  EVENT=13       START BATTLE---DELAY TACTICS
TIME=25.95  EVENT=13          STOP BATTLE---DELAY TACTICS
TIME=25.96  EVENT= 4  START BATTLE,  5 MAN ADDITIONAL ON-SITE FORCE ARRIVAL
TIME=4Ø.14  EVENT=1Ø  ARRIVAL OF OFF-SITE RESPONSE FORCE, 1Ø MEN
TIME=4Ø.14  EVENT= 4  START BATTLE, 1Ø MAN OFF-SITE FORCE ARRIVAL
TIME=41.16  EVENT= 5       END OF BATTLE
      OFFENDERS=19  ATTACKERS =      Ø     TIME FOR BATTLE =     1.Ø2
TIME=41.16  EVENT=11       RESTART SIMULATION

      ATTACKER ATRIBUTE 1 =1Ø.ØØ Number of Attackers
      ATTACKER ATRIBUTE 2 = 2.ØØ Automatic Weapons
      ATTACKER ATRIBUTE 3 = 3.ØØ Special Equipment, with H.E.
      ATTACKER ATRIBUTE 4 = 2.ØØ No Vehicles
      ATTACKER ATRIBUTE 5 = 1.ØØ Low Dedication
      ATTACKER ATRIBUTE 6 = 4.ØØ Theft, With No Inside Assistance
```

Figure 5 - Run 5 Event Sequence

A graphical representation of the battle and arrival of the on-site and off-site response forces is shown in Figure 6. The total defender population and the attacker population is shown as a function of time. The arrival of the 5 man on-site guards occurs at time equal to 19.95. The 5 man additional on-site force arrives at 25.96 minutes. The two forces continue to fight while taking casualties until the arrival of the 10 man off-site force at 40.14. The battle ends very shortly then and this concludes one attack sequence.

Several collected computer statistics from 300 attacks have been gathered. The computer time required for one attack sequence on the CDC 6600 machine averages about 1 second; the 300 attacks required about 250 seconds of central processor time and 70K of memory. This small amount of computer time and memory requirements illustrate a very efficient method of performing experiments (simulated attacks on the fixed-site design) prior to or after a site design has been completed. The computer model provides an excellent tool for measuring the cost effectiveness of fixed-site security upgrades.

CONCLUSIONS REGARDING FIXED-SITE INTEGRATION

With the assistance of the computer model, many decisions concerned with site security can and have been evaluated from a safeguard cost effectiveness standpoint. The model provides a framework for performing inexpensive experiments on fixed-site security systems and for determining the relative cost effectiveness incurred with each alternative decision. Although the model is operational, work is being continued for the improvement of input data for alarm detection systems, barrier delays, etc. What has evolved with the development of this fixed-site computer model is a structured approach that is analytically based and that provides an evaluation of proposed fixed-site security changes. The validity of the model should improve as better data are found and different site configurations are studied.

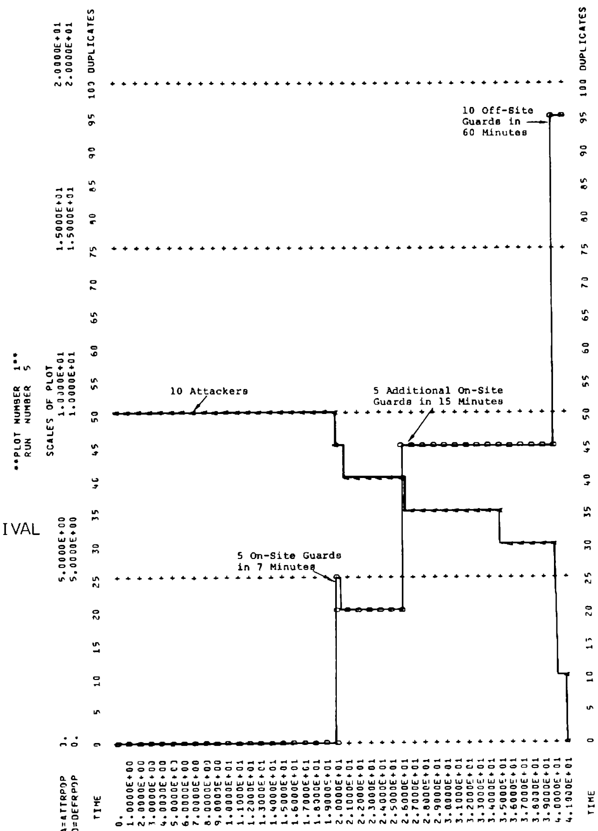

Figure 6. Plot of Run 5 Event Sequence

REFERENCES

1. Todd, J. L., and W. C. Nickell, Physical Security System Effectiveness Evaluation - A Status Report, SAND75-0391, Sandia Laboratories, Albuquerque, New Mexico, July 1975.

2. Chapman, L. D., A Model for Evaluating Alternative Fixed-Site Security Systems, SAND75-0512, Sandia Laboratories, Albuquerque, New Mexico, December 1975.

3. Pritsker, A. A. B., The GASP IV Simulation Language, John Wiley and Sons, 1974.

4. Army Field Manual, FM 5-25, Explosives and Demolitions, May 1967.

5. Bennett, H. A., Dynamic Model of a Terrorist Attack, SAND75-0514, Sandia Laboratories, Albuquerque, New Mexico, to be published.

6. Lanchester, F. W., Aircraft in Warfare: The Dawn of the Fourth Arm, Constable, London, 1916.

7. Morse, P. M., and G. E. Kimball, Methods of Operations Research, John Wiley and Sons, 1951.