SAND99-1851C

VULNERABILITY ANALYSIS CONSIDERATIONS FOR THE TRANSPORTATION OF SPECIAL NUCLEAR MATERIAL

James W. Purvis, Sandia National Laboratories
P.O. Box 5800 MS-0759 Albuquerque, NM 87185 USA 505-844-3975 jwpurvi@sandia.gov

Larry "Nick" G. Nicholson, Sandia National Laboratories
P.O. Box 5800 MS-0759 Albuquerque, NM 87185 USA 505-844-5235 lgnicho@sandia.gov

Abstract

The vulnerability analysis methodology developed for fixed nuclear material sites has proven to be extremely effective in assessing associated transportation issues. The basic methods and techniques used are directly applicable to conducting a transportation vulnerability analysis. The purpose of this paper is to illustrate that the same physical protection elements (detection, delay, and response) are present, although the response force plays a dominant role in preventing the theft or sabotage of material. Transportation systems are continuously exposed to the general public whereas the fixed site location by its very nature restricts general public access.

INTRODUCTION

The purpose of this paper is to present an overview of vulnerability analysis (VA) considerations for Material Transportation Systems (MTS). Generally, we are concerned with nuclear material, but the principles apply to any target being transported. While there are some similarities between a fixed site and a transportation system, transportation systems have a different function than fixed sites: the movement of target material as well as protection from theft or sabotage.

Physical protection during transportation is more complex than that at a fixed-site. The same physical protection system (PPS) elements (detection, delay, response) are present, but the response force now plays the dominant role in preventing the theft or sabotage of the target material. Transportation systems may be continuously exposed to the general public, whereas a fixed site location by its very nature restricts general public access.

Fixed sites usually have restricted access, a detection/assessment/delay perimeter, and simple operating conditions such as dayshift, nightshift, weekends and holidays. In contrast, the MTS has no defined technological perimeter, both the target and the PPS are mobile, and the system is affected by many variables such as terrain, weather, construction, traffic, accidents, and response force times. In spite of all this, the vulnerability analysis may be somewhat simpler for a transportation system.

VULNERABILITY ANALYSIS METHODOLOGY

The sections that follow discuss the vulnerability analysis methodology, adversary actions and scenario development, the determination of protection system effectiveness, and the implementation of upgrades. The vulnerability analysis methodology generally follows the process presented at each International Training Course for the Physical Protection of Nuclear Materials [1]. For transportation systems, the steps in this methodology are: target identification, threat definition, PPS characterization, scenario development, engagement analysis, and system effectiveness evaluation.

Target Identification

This is the logical first step: if there is no target, then there is no need for further analysis. This step should answer the basic questions: what is the target material being transported/protected, and how

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

valuable is the material to an adversary? When identifying the target the analyst should document several specific characteristics. The type of target material being transported should be identified and described thoroughly. The description should be specific enough that the target can then be categorized using either the DOE Graded Safeguards Table [2] or the IAEA guidelines [3]. The analyst should also determine if the target is a theft target or a sabotage target, the quantity that would be an adversary goal, the adversary task time and any special equipment needed to access the material.

If the target is identified as a radiological sabotage target, determining the level of radiological release becomes critical due to the location of the MTS at the time of the release. The position of the MTS could be virtually anywhere along the route, which may include large metropolitan areas, small urban towns or the rural countryside.

Threat Definition

This step answers the questions: What are we protecting against? Who wants the material and why? In identifying adversary personnel involved in an MTS vulnerability analysis the analyst should develop a design basis threat (DBT) statement. The analyst should begin by referring to the threat definition information initially determined for the fixed site locations where the material is stored or accessed when not in transport. The primary threat objectives are theft and sabotage, and the threat categories include insiders, outsiders, and insider-outsider collusion. The analyst should acquire the standard threat characterization information, such as adversary tactics, numbers, capabilities, training, and motivating factors, as well as the descriptions of each category.

Collecting any historical data involving attacks on moving targets—assassinations, hijacking and attacks on convoys is useful. Information can also be provided by subject matter experts on protection of convoys and shipments of similar materials. This threat statement then indicates, based on similar past incidents and subject matter expert opinions, what type of adversary would conduct a particular type of attack. In addition to the type of adversary, the statement would identify the most common number, capabilities and modus operandi. The number of adversaries may vary depending on their goals and objectives, i.e. sabotage versus theft. Analysis of past incidents and intelligence information is critical in developing credible scenarios. A common order of importance is

1. insider(s) alone
2. outsiders colluding with insider(s)
3. outsiders alone

Excellent descriptions of both insider and outsider threat definitions and attributes from DOE and NRC documents are contained in Reference 1 and will not be repeated here. For the MTS, outsider threat categories include terrorists, criminals, psychotics, disgruntled employees, and violent activists. Insider categories and descriptions are facility and transportation system dependent. In considering the type of insider involved in an MTS, the analyst should identify those individuals with special knowledge of the targeted material, response forces, convoy routes, schedules, and denial systems. This may include material custodians at either the shipping or receiving ends, material handlers, security force personnel and management. The insider typically has the luxury of selecting the best opportunity for success. If the insider is acting in collusion with outsiders, a set timetable may be established and followed.

PPS Characterization

This step in the analysis defines the detection, assessment, and delay and response force characteristics of the MTS. The material transportation system can be considered a moving facility. The MTS may

consist of several material transports and response force carriers such as military escort vehicles and railcars. The area surrounding the MTS automatically changes as the transport moves throughout the designated route. The terrain can change from flat level ground to rolling hills or mountains in a matter of moments. In addition to the terrain variations, the transportation operation exposes the facility to various kinds of public domain including urban and country settings. Each area offers advantages and disadvantages depending on the location of the facility at any given point along the route.

Characterizing an MTS involves: 1) classifying the structure of the transport walls, ceiling and floor, by use of drawings and visual observation, and determining their relationship to the target material, 2) identifying all physical protection system components, as well as the operating systems alarm assessment and communication, 3) evaluating all adversary entry and exit paths to analyze the protection system, 4) reviewing routes in detail to identify: alternate routes, danger zones, scheduled stop locations and choke points, 5) determining the speed and timing of the MTS, as well as the time/distance to stop, and 6) types of transport vehicles used for both target material and response force, i.e., rail, roadway, air, or ship

Response Configuration

The response element is designed to counteract the adversary's actions through engagement and neutralization using one of two strategies: denial or containment. For an MTS, the primary response force also may serve as the detection and assessment elements. Data to be collected must include: who is responding, how many, when, and how well prepared are they. This information is sometimes the hardest to acquire, since the response forces consider keeping it secret as a matter of survivability. The response for a MTS usually has three elements: the primary response force (PRF), secondary response force (SRF), and law enforcement or military elements along the route. With this information in hand, the analyst should then evaluate all possible types of tactics to be used to eliminate the response force. In a fixed-site location the exact location of protective force personnel at any given moment may be difficult to assess. The same freedom does not necessarily exist for a protective force restricted to specific locations such as a security force railcar or motorcade (convoy) configuration.

The PRF is that force immediately available to respond to an encounter with an adversarial force. The PRF usually travels with the MTS, and its primary objective is to survive the initial attack and then to either deny access to the material or contain and neutralize. Important information to collect includes the number of protective force members in the immediate response team, their location in the MTS, availability of hardened fighting positions, types of weapons, tactics, and survivability against various weapons and explosives.

The next item is the availability of a SRF to reinforce the PRF, assist in denying adversaries access to the material, and help prevent the removal or sabotage of the material. The primary differences that could exist between the PRF and SRF include the number of personnel involved, the location in relationship to the MTS, and mobility issues (vehicles/second train/aircraft).

Lastly, identify the types of law enforcement and military response available within a few hours of the incident site. This may be difficult to specify because the MTS could be anywhere along the route when the incident occurs. When reviewing the route selected the analyst should determine the location of law enforcement and military forces along the route, the location of any forces that may be on training maneuvers, the potential tactics to be used for a recovery/recapture operation, and mobility factors for additional response force members. These forces may also be called upon for recapture/recovery operations.

SCENARIO DEVELOPMENT

To design and evaluate the PPS effectiveness, credible attack scenarios must first be developed. This involves assessing the vulnerable states of the MTS, determining all potential adversary actions, planning various adversary attacks, and then selecting the most credible scenarios for PPS evaluation.

Vulnerable States

In developing scenarios or strategies to commit an act against a moving target the analyst must think beyond the established ideas used to act against a fixed-site location. Historically, an adversary's success greatly depends on the MTS being stopped at the time of the attack. A moving target is difficult to gain control of and predictability factors are lost. It should be noted that the response force also has a difficult task of defending against adversaries during movement. Cover and concealment is strictly limited to response force accommodations; a safe egress is nearly impossible. In general, there are only two states for the MTS: rolling or stopped. Figure 1 illustrates in decision-tree form the details of these two states.

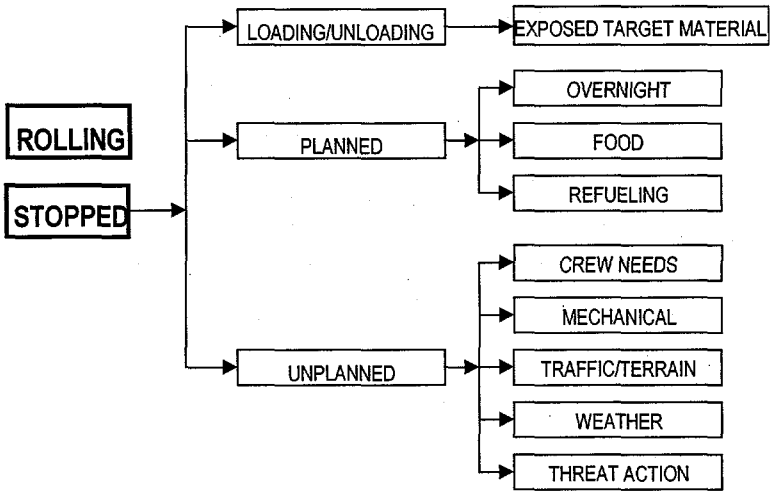

Figure 1. Vulnerable state decision tree

Adversary Actions and Planning

Fortunately for the analyst, the adversary has only a small set of specific actions to be accomplished. These are shown in decision tree form in Figure 2. Adversary planning must focus on the three key physical protection elements of the MTS: avoiding detection, minimizing delays and defeating response. The response force may be the only initial detection mode available. This may be especially true during daylight hours and in good weather conditions. But what occurs if the aforementioned conditions are not present? The analyst then determines what other detection systems are available and what their effectiveness is in relationship to the total system. In railcar transport, for example, the system may require a sensor capability that enunciates to a response force railcar, providing intruder detection.

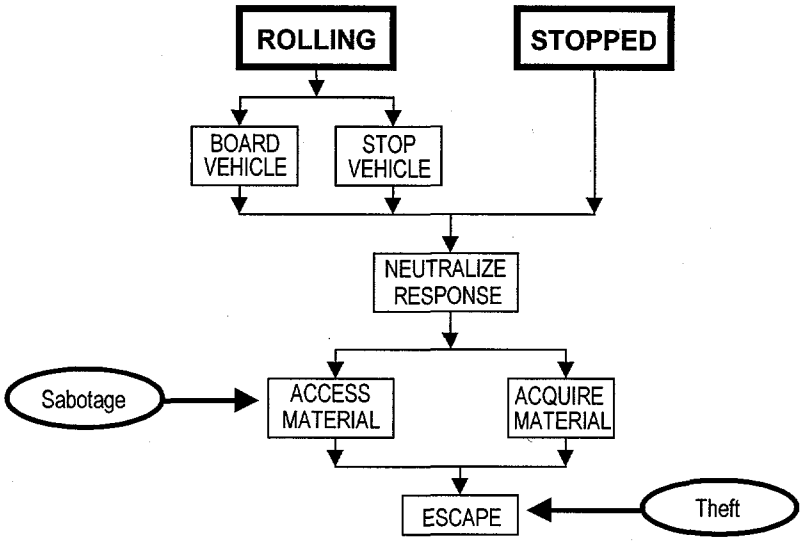

Figure 2. Adversary actions decision tree

In assessing physical protection system delays, the analyst must take into consideration the number of response force members immediately available. The number of additional response force members available at any given location along the route may vary as well as their response time. Each type of delay should be identified and annotated for future reference, then evaluated to determine defeat tactics and timing.

In assessing the defeat methods used by an adversary, the analyst considers the elements of detection, delay and response. Although the elements are the same as for a fixed site location, adversary methods vary due to the location and various states of the MTS. In detecting an adversaries' approach to a fix-site location, a protective perimeter may be used with manned portals for access and egress. Detection of adversary actions for an MTS is usually provided by response force personnel. In those instances where the MTS elements are equipped with sensor capabilities, detection may occur at the outside shell of a vehicle. If detection does not occur until the shell of the vehicle is attacked, then delay becomes critical to interrupting the adversaries successfully.

If a limited delay time exists for the adversary to acquire the target, then detection before the attack becomes critical to response force success. Early detection of adversary actions can be accomplished through the use of an aggressive surveillance detection program. A program of this nature includes: periodic route surveys, identifying choke points and danger zones, intelligence gathering, and rapid communications. Delay times for penetration of the vehicle are determined based on the amount of protective material (armor) available and the task times associated with penetrating the shell.

Defeating the response force can be accomplished through a series of acts, which include: ambush, overwhelming adversary numbers, and pre-positioned explosive devices. The response force training program should include practical exercises on these types of issues.

Credible Scenarios

In developing credible scenarios for an MTS, the analyst must have a clear understanding of what it takes to make a scenario successful. Scenarios should be designed to replicate the actual threat presented. If "theft" of material is the worst case, then the scenario requires the adversaries to have an attack position, with time allocated for material acquisition, and allow for egress. If the worst case is

sabotage of material, then the adversary objective of simply pre-positioning an explosive device with remote detonation may be all that is required to begin developing the scenario.

Next, the scenario should describe the type of equipment the adversary would need to accomplish their objective. Equipment could include: light and/or heavy weapons, hand and power tools, diversionary items like construction crew barriers, and a method for egress. In addition to the DBT identifying the number of adversaries and equipment, the difficulty factor of their use and ability to acquire them should be included.

Finally, the analyst determines the plausibility of the scenario. Is the scenario realistic enough to be considered in the analysis? A general rule in developing an MTS attack scenario (actually any scenario) is to keep it simple to implement.

SYSTEM EFFECTIVENESS EVALUATION

PPS Options

The options available to the PPS analyst to counter adversary actions include: 1) primary response force numbers, weapons and tactics; 2) vehicle speeds, dispersion, camouflage and armor; and 3) system communications and delays. As illustrated in Figure 3, the designer should look at the application of each PPS option against every specific adversary action in a scenario, and then select those combinations which will provide the system with the highest effectiveness.

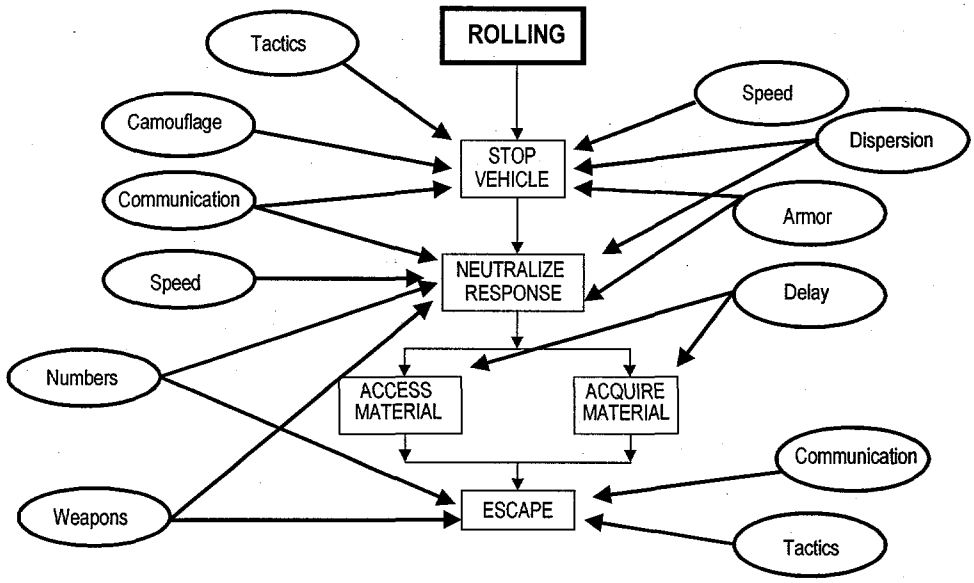

Figure 3. Physical protection system options

Engagement Analysis Methods

Once the PPS is defined, an engagement analysis should be performed for each credible scenario. The analyst has at least six generic methods for analyzing engagements, which will be discussed in detail in a subsequent paper. The six methods are: 1) expert judgement, 2) stochastic estimation techniques such as the ASSESS Neutralization Module, 3) battle board or tabletop modeling exercises, 4) computerized wargaming, 5) force-on-force exercises, and 6) actual engagements. It is preferable to use more than one technique to analyze each engagement, and compare the results from each method for consistency.

Risk Estimation and Upgrades

Several methods of risk analysis, such as the DOE risk equation with the graded safeguards table target consequence values, could be used to complete the system effectiveness evaluation. In general, however, the results of the engagement analysis can be used. If the PPS has low losses in each scenario, then it is acceptable. If the system has high losses, the analyst must determine the problem and implement changes as follows: determine the main cause of loss, implement a PPS option to counter it, and then reevaluate the system. The upgrade-analyze-evaluate process is continued until the system wins most of the time.

EXAMPLES

Previous Incidents

MTS case studies are available for nearly any type of scenario. As an example, the US Department of Energy studied attacks that have occurred on armored vehicles carrying money. Research indicated that in most cases the adversaries had either the aid of an insider or spent considerable time conducting surveillance and gathering intelligence on the organization's operation. Additional research conducted by several international transportation associations indicates that employees who act as insiders often hold positions of authority and know the routes, materials being shipped, and security systems being employed.

Analysis Example

As a generic example, consider an SNM convoy design consisting of three vehicles, one of which is transporting a potential theft target. The strategy is denial. The first vehicle is a police escort without radio contact with the transporter or response force vehicle. The transporter carries the target and two unarmed drivers. The response force, consisting of 15 armed guards, follows the transporter in a standard military truck. This MTS lost every theft scenario engagement to a six-man terrorist team.

The upgraded system retained the police vehicle as a route surveillance escort, but added a three-man response team and communications to the vehicle. The response strategy was changed to containment. The target transporter was replaced by an armored vehicle with access delays and two armed drivers with communications who could also function as a response team. The single response-force vehicle was replaced with four dispersed, camouflaged escort vehicles, each with armor, communications, and a three-man response team. Each response team included one sniper. The system effectiveness in all scenarios rose to greater than 90 percent.

SUMMARY AND CONCLUSIONS

In summary, an MTS is simpler to analyze but harder to protect. Credible adversary attack scenarios should be developed, and engagements during these scenarios between the response forces and the adversary should be evaluated with more than one analysis technique. In designing and upgrading the PPS for the MTS, apply generic protection concepts to each step of adversary action that are difficult to defeat, i.e., increase system effectiveness.

In practice, detection and assessment are performed by the PRF, usually resulting in a probability of assessed detection of an attack of 1.0. Route planning and surveillance, with appropriate communications, can reduce the likelihood of an ambush. Enhanced delay systems should provide sufficient delays for the PRF to contain an adversary. It is desirable for PRF numbers to be much greater than the threat equivalent, with superior weapons, a high level of training, and response vehicles incorporating speed, mobility, and armor.

As discussed, the vulnerability analysis process is a systematic means to evaluate the physical protection systems for SNM at a fixed location, and has direct applications to the various modes of transportation. It is imperative that the analysts understand that differences between a fixed and mobile PPS do exist and should be considered, but by following a proven process a comprehensive report can be created that is defensible, as well as practical and understandable. The end result is an analysis that future improvement decisions and financial expenditures can be based upon.

REFERENCES

1. Sandia National Laboratories, The International Training Course: Physical Protection of Nuclear Facilities and Materials, Vol. III. *Evaluating the Physical Protection System Design,* Albuquerque, NM, March 1998.

2. B. Erkilla, D. Fidler, J. Larson, and J. Markin, *Guidelines for Material Protection, Control and Accounting Upgrades at Russian Facilities,* US Department of Energy, Washington, DC, December 1998.

3. International Atomic Energy Agency, INFCIRC/225/Rev.4: *The Physical Protection of Nuclear Material and Nuclear Facilities*, Vienna, Austria, March 1999.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.