SAND2000-3119C

Risk Assessment Methodology for Protecting Our Critical Physical Infrastructures

Betty Biringer[1]
Jeffrey J. Danneels[2]

Abstract

Critical infrastructures are central to our national defense and our economic well-being, but many are taken for granted. Presidential Decision Directive (PDD) 63 highlights the importance of eight of our critical infrastructures and outlines a plan for action. Greatly enhanced physical security systems will be required to protect these national assets from new and emerging threats.

Sandia National Laboratories has been the lead laboratory for the Department of Energy (DOE) in developing and deploying physical security systems for the past twenty-five years. Many of the tools, processes, and systems employed in the protection of high consequence facilities can be adapted to the civilian infrastructure.

Introduction

The risk assessment methodology presented here has been adapted to several of our critical infrastructures. Due to the sensitive nature of the work, the critical infrastructures assessed will not be identified.

Each critical infrastructure facility has a mission. The design of the facility and associated procedures assures the performance of the mission. Security systems should guarantee that the mission continues to be performed despite the intervention of anthropogenic threats.

[1]Systems Analyst, Systems Analysis and Development, Dept. 5845, Sandia National Laboratories, PO Box 5800, Albuquerque, NM 87185-0759; phone 505-844-3985, bebirin@sandia.gov
[2]Department Manager, Civilian Surety Programs, Dept. 5862, Sandia National Laboratories, PO Box 5800, Albuquerque, NM 87185-0781; phone 505-284-3897; jjdanne@sandia.gov

DISCLAIMER

DISCLAIMER

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

Analysis Methodology

The analysis methodology for assessing the vulnerability of critical facilities has seven basic steps:

- characterize facility.
- identify undesired events and critical assets.
- determine consequences of undesired events.
- define threats to the facility.
- analyze protection system effectiveness.
- estimate risks.
- suggest and evaluate upgrades to the system.

Figure 1 describes the order and sequence of the steps of the methodology.

Facility Characterization

An initial step in security system analysis is to characterize the facility operating states and conditions. This step requires developing a thorough description of the facility itself (the location of the site boundary, building locations, floor plans, and access points). A description of the processes within the facility is also required, as well as identification of any existing physical protection features. This information can be obtained from several sources, including facility design blueprints, process descriptions, safety analysis reports, environmental impact statements, and site surveys.

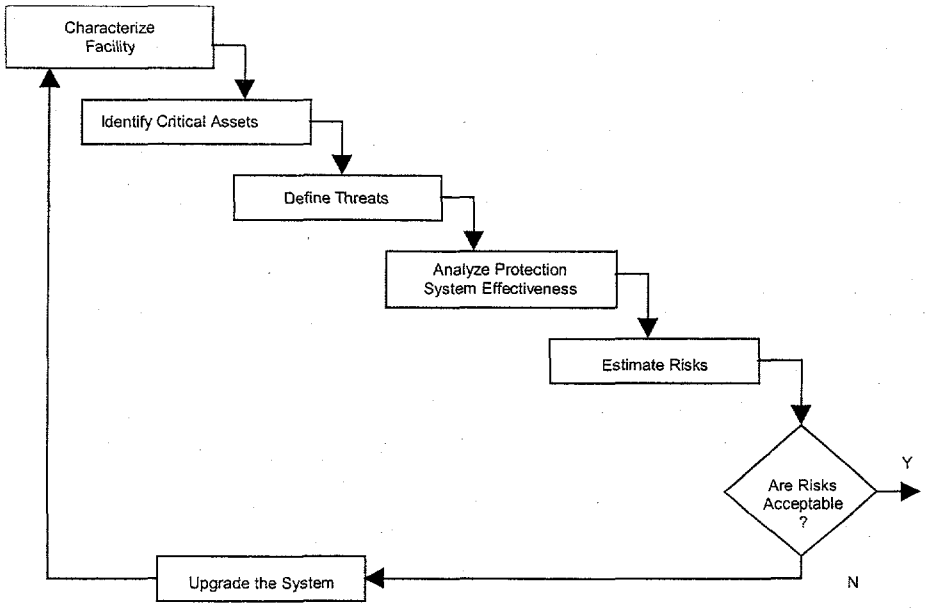

Figure 1. Analysis methodology.

The characterization of a facility includes a description of building structures, traffic areas, infrastructure, terrain, weather conditions, historical data, and

operational states. When characterizing the facility, the first step is to gather information that depicts everything that could affect vulnerabilities. The types of documentation include:

- policy and procedure documents.
- unusual occurrence reports.
- existing threat assessment information.
- results from past security survey/audits.
- building blueprints and plans for future structures.
- site plans of detection, delay, assessment systems.
- operational procedures.

Once the documentation has been collected, the following information should be extracted to characterize the facility. Site plans can help identify:

- property borders.
- egress and regress routes to the facility.
- specific vulnerable areas in and around the facility, including routes outside the areas such as adjacent buildings that could be used to target the building.
- adjacent parking lots and related security countermeasures.
- building locations and characteristics (purpose of the building, who is allowed access, and operational conditions or states).
- existing physical protection features.

Operational conditions are described by:

- length and number of day and night shifts.
- activities typical to each shift and the associated security implications.
- number of employees/contractors, unions, visitors in the area during each shift and level of access to the facility during weekdays, weekends, and holidays.
- availability of security forces, to include local law enforcement.
- meteorological conditions for the region and time of the year.
- description of adjacent residential or commercial areas.

Facility structure information that is needed to characterize the facility includes type of materials used in construction and the location and type of doors, gates, entrance ways, utilities, windows, and emergency exits.

Procedural information that must be obtained includes:

- entry control procedures for visitors, deliveries, contractors, and vendors.
- emergency operations procedures for evacuation.
- entry control procedures.
- procedures used to evacuate facility personnel in the event an incident occurs.
- security procedures.
- policies related to alarm assessment and communication to responding security personnel or local law enforcement.

The overall mission and operations conducted at the facility must be clearly understood. In order to determine how the mission can be interrupted, it is necessary to understand what is required for the site to operate effectively. The operation and location of equipment and features that are important to the facility mission must be documented.

After facility characterization has been completed, the next step in the analysis process is to identify the undesired events and associated critical assets.

Undesired Events/Critical Assets Identification

Undesired Events. The undesired events must be established. Undesired events result in undesired consequences. Undesired events are site-specific and have adverse impacts on public health and safety, assets, mission, and publicity.

Critical Assets. The adversary could cause each undesired event to occur in several ways. A structured approach is needed to identify critical components for prevention of the undesired events. A logic model, like a fault tree, can be used to identify the critical components. The critical components and their locations become the critical assets to protect.

Fault Tree. Because the analysis methodology uses the fault tree as a primary tool for analyzing and describing the site vulnerabilities, an explanation of fault trees is thus included as a critical part of the methodology. Mastering the concepts of fault tree construction will enable decision-makers to create a fault tree that identifies the vulnerabilities of a particular site.

A fault tree is a logical tool. The tree itemizes critical assets, those that must function to prevent an undesired event. A tree shows scenarios involving critical assets that could produce an undesired event. The tree guides analysts in estimating the degree of risk associated with threats..

Consequence Determination

The next step is to categorize undesired events or loss of critical assets. The categories of consequences are similar to those used by the Department of Defense (DoD) [Mil Standard 882C]. The definitions have been modified to make them pertinent to civilian applications. The consequence values and categories are described in Table 1.

Consequence Category	Consequence Value
Catastrophic—results in death(s), total mission loss, or severe environmental damage	**VH**
Critical—results in severe injury/illness, major mission loss, or major environmental damage	**H**
Marginal—results in minor injury/illness, minor mission loss, or minor environmental damage	**M**
Negligible—results in less than minor injury/illness, less than minor mission loss, or less than minor environmental damage	**L**

Table 1. Consequence categories and associated values.

The consequence values are very high (VH), high (H), medium (M), or low (L), based on the severity of the consequence. The goal is to estimate the relative consequence value associated with each undesired event.

Threat Definition

Threat. Before a vulnerability analysis can be completed, a description of the threat is required. This description includes the type of adversary, tactics, and capabilities (number in the group, weapons, equipment, and transportation mode). Also, information is needed about the threat to estimate the likelihood that they might attempt to accomplish the undesired events.

Defining the Threat. The specific type of threat to a facility is referred to as the design basis threat (DBT). The DBT is often reduced to several paragraphs that describe the number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit.

Specific tasks must be completed in conducting a threat analysis. These steps include:

- interview organizations possessing threat information.
- profile the threat.

The types of organizations that may be contacted during the development of a DBT description include local, state, and federal law enforcement (to include searching source material) and related intelligence agencies. Local authorities should be able to provide reports on the type of criminal activities that are occurring and analytical projections of future activities. As an example, an environmental group may have previously only demonstrated at a facility but recently has announced plans to commit acts of sabotage that would disrupt normal operations.

A review of literature may be conducted to include past incident reports associated with the site, local periodicals, professional journals, and other related material. Other information to be collected includes:

- incident reports analysis data. This could include criminal reports, intelligent reports, and other historical data.
- employee data. Establish the number of personnel at the facility and types of positions. Employee numbers vs. the number of contractors, visitors, and vendors. The reviews should identify any problems that may have occurred with any of the groups. Incidents such as domestic violence problems, union disputes, downsizing, and other problems should be identified.

In profiling the threat, various questions must be answered. Some of these questions are:

1. What are the major types of crime that have occurred in the last year?
2. Has there been any terrorist-type activity in any of the areas owned or operated by the organization?
3. Are law enforcement organizations aware of any groups that may pose a threat

to the site?

4. What type of knowledge can be gained about the facility?
5. What types of background checks are conducted?
6. Have employees been involved in any type of adverse activities?
7. What categories of insiders are allowed access to the facility?

Based on the historical data received from the various groups, the DBT is formulated. Developing a specific threat table from the information is helpful in establishing the DBT.

Likelihood of Attack. After the threat spectrum has been described, the information can be used together with statistics of past events and site-specific perception to categorize threats in terms of likelihood that each would attempt an undesired event. The DoD standard definitions [Henry Shelton 1998] were modified in order to be used to categorize the threats. The modified DoD definition is based on the following characteristics:

Existence—threat is assessed to be present or able to gain access.

Capability—the threat is assessed to have, or has demonstrated, the level of capability to conduct the attack.

Intentions—recent demonstrated activity or stated or assessed intent to conduct such activity exists.

History—demonstrated activity exists over time.

Targeting—current credible information indicates that the threat is preparing for a specific attack.

These definitions have been used to describe threat security levels. The results of the categorization are used to estimate the likelihood that the threat would undertake the undesired events. These values are considered to be relative estimates and are used primarily for priority ranking of threat likelihood of attack. Figure 2 defines the process for estimating likelihood of attack.

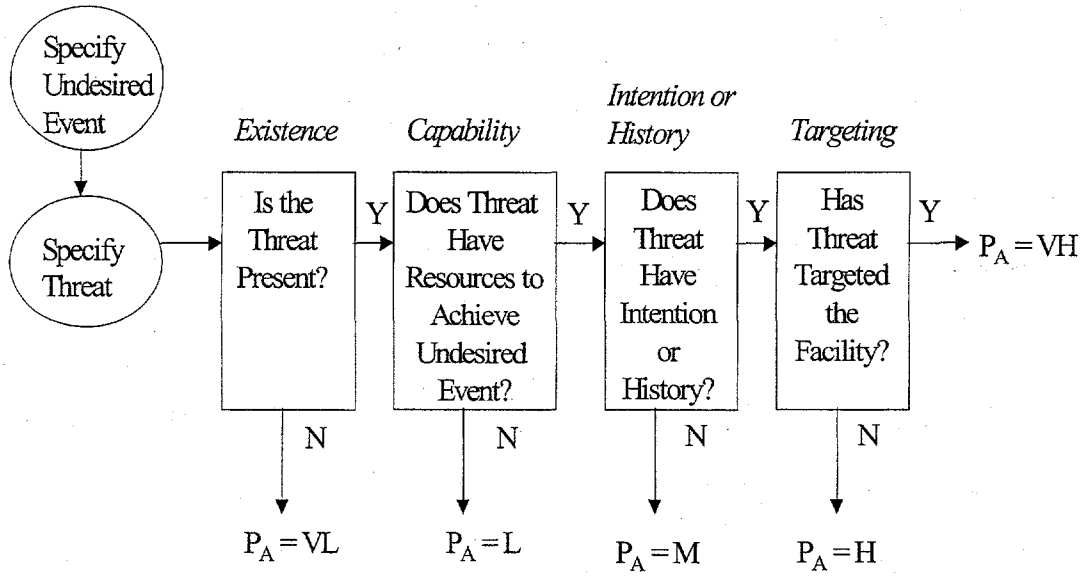

Figure 2. Process for estimating likelihood of attack, P_A.

Protection System Effectiveness Analysis

Figure 3 describes the design and analysis process outline that can be used when estimating physical protection system effectiveness. The physical protection features must be described in detail before the security system effectiveness can be evaluated. An effective security system must be able to detect the adversary early and delay the adversary long enough for the response to arrive and stop the adversary before the mission is accomplished. In particular, an effective security system provides effective:

- detection.
- delay.
- response.

These security system functions (detection, delay, and response) must be integrated to ensure that the adversary threat is stopped before the mission is accomplished.

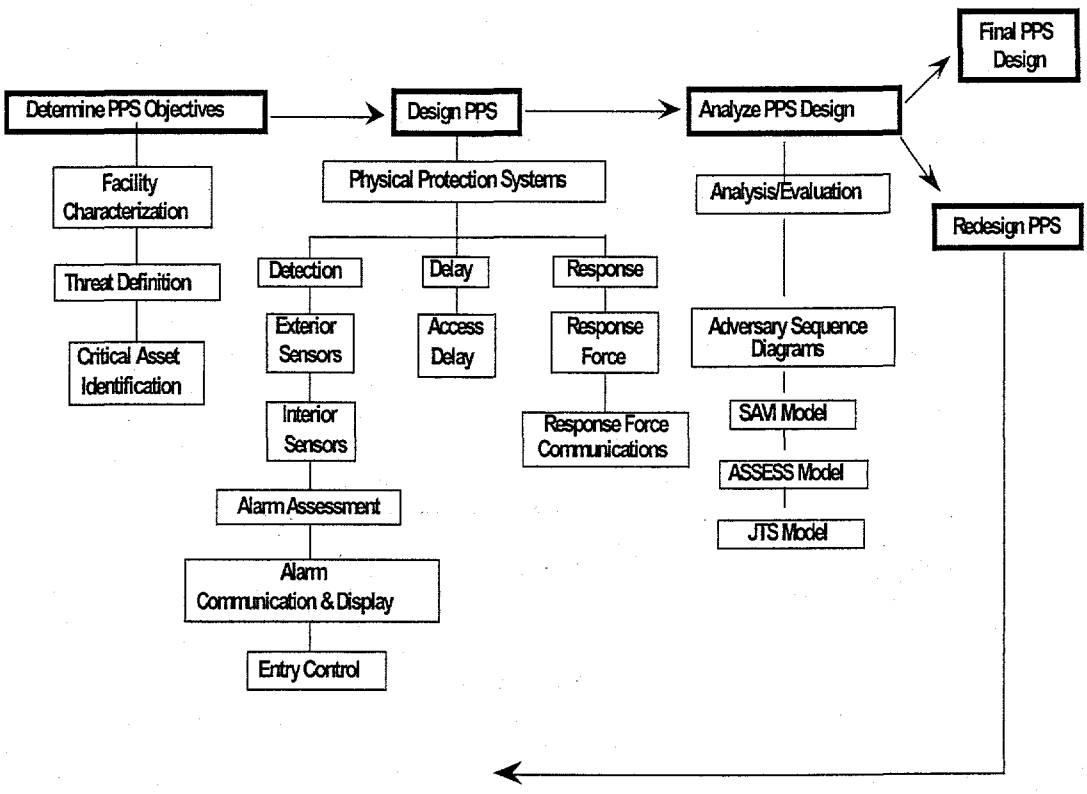

Figure 3. Design and Evaluation Process Outline (DEPO).

Detection. The first required function of a security system, is the discovery of adversary action and includes sensing covert or overt actions. In order to discover an adversary action, the following events must occur:

- sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm.
- information from the sensor and assessment subsystems is reported and displayed.

- someone assesses information and determines the alarm to be valid or invalid (If determined to be a nuisance alarm, detection has not occurred.).

Methods of detection include a wide range of technologies and personnel. Entry control, a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband, is included in the detection function of physical protection. Entry control, in that it includes locks, may also be considered a delay factor in some cases. Entry control to various layers of the system should be designed to filter and reduce the population that has access as they approach the target. Only those individuals who need direct access to the target should be allowed through the final entry control point. Searching for metal (possible weapons or tools) and explosives (possible bombs or breaching charges) is required for high-security areas. This may be accomplished using metal detectors, x-ray (for packages), and explosive detectors. Security police or other personnel also can accomplish detection. Personnel can contribute to detection if they are trained in security concerns and have a means to alert the response force in the event of a problem.

An effective assessment system provides two types of information associated with detection: (1) information about whether the alarm is a valid alarm or a nuisance alarm, and (2) details about the cause of the alarm, i.e., what, who, where, and how many. The effectiveness of the detection function is measured by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

Delay. The second required function of a security system. It impedes adversary progress. Delay can be accomplished by fixed or active barriers, (e.g., doors, vaults, locks) or by sensor-activated barriers, e.g., dispensed liquids, foams. The security police force can be considered an element of delay if personnel are in fixed and well-protected positions. The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element.

Response. The third requirement of security systems, comprises actions taken by the security police force (police force or law enforcement officers) to prevent adversarial success. Response consists of interruption and stopping the adversary. The measure of response effectiveness is the time between receipt of a communication of adversarial actions and the interruption and ability to stop the action. The effectiveness measures for response communication are the probability of accurate communication and the time required to communicate. The effectiveness measure of this function is the response force engagement effectiveness. Interruption is defined as the response force arriving at the appropriate location to stop the adversary's progress. It includes the communication to the response force of accurate information about adversarial actions and the deployment of the response force. Deployment describes the actions of the security police force from the time communication is received until the force is in position to stop the adversary. The effectiveness measure is the probability of deployment to the adversary location and the time required to

deploy the response force. The effectiveness measures for stopping the adversary are security police force equipment, training, tactics, and cover capabilities.

Protection System Effectiveness. Analysis and evaluation of the security system begin with a review and thorough understanding of the protection objectives and security environment. Analysis can be performed by simply checking for required features of a security system, such as intrusion detection, entry control, access delay, response communications, and a response force. However, a security system based on required features cannot be expected to lead to a high-performance system unless those features, when used together, are sufficient to ensure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a security system.

The Adversary Sequence Diagram (ASD) is a graphical representation of physical protection system elements along paths that adversaries can follow to accomplish their objective. For a specific physical protection system and threat, the most vulnerable path can be determined. This path with the least physical protection system effectiveness establishes the effectiveness of the total physical protection system. An ASD is developed for a single critical asset associated with an undesired event.

Computer codes such as Systematic Analysis of Vulnerability to Intrusion (SAVI) and Analytic System and Software for Evaluating Safeguards and Security (ASSESS) can be used to determine the most vulnerable path. ASSESS or Joint Tactical Simulation (JTS) can be used to estimate response force effectiveness.

Computer tools used for the prediction of blast effects are grouped into various categories depending upon how the calculations are made, how the blast and structural calculations are combined, and the relative distance of the explosive from the target. Blast prediction and structural response calculations may be based on first principles (basic principles of physics and mechanics) or may be semiempirical solutions. First-principle tools solve equations, which describe the basic laws of physics and chemistry. These basic laws are conservation of matter, conservation of momentum, and conservation of energy. In addition, the programs also need equations describing the physical behavior of the structure and structural materials to stress and strain and the laws describing the relationship between stress and strain in the structural materials. Semiempirical tools are developed through analysis of test results and use simplified models of the laws of physics.

Risk Estimation

Risk. For this study, risk is quantified by the following equation:

$R = P_A * (1-P_E) * C$

where:

R = risk associated with adversary attack.

P_A = likelihood of the attack.

P_E = probability security system is effective against the attack.
$(1 - P_E)$ = probability that the adversary attack is successful (also the probability that security system is not effective against the attack).
C = consequence of the loss from the attack.

Note that the dimension of R is a function of the dimension of the consequence, C. If consequence is a nondimensional value, risk will also be nondimensional, but risk is always in the same units as consequence, i.e., if consequence is expressed in dollars, risk is in dollars. Likewise, if consequence is expressed as loss of life or property or a dollar amount, risk is expressed in the same dimension.

Upgrades and Impacts

System Upgrades. If the estimated risk for the threat spectrum is judged to be unacceptable, upgrades to the system may be considered. The first step is to review all assumptions that were made that affect risk. All assumptions concerning undesired events, target identification, consequence definition, threat description, estimation of likelihood of attack, and safeguards functions should be carefully reevaluated. Upgrades to the system might include retrofits, additional safeguard features, or additional safety mitigation features.

The upgraded system can then be analyzed to calculate any changes in risk due to change in likelihood of attack, system effectiveness, or consequence values. If the estimated risk for the upgraded system is judged to be acceptable, the upgrade is completed. If the risk is still unacceptable, the upgrade process of assumption review and system improvement should be repeated until the risk is judged to be acceptable.

Upgrade Impact. Once the system upgrade has been established, it is important to evaluate the impacts of the system upgrade on the mission of the facility and the cost. If system upgrades put a heavy burden on normal operation, a trade-off would have to be considered between risk and operations. Budget can be the driver in implementing security upgrades. A trade-off between risk and total cost may have to be considered.

When balance is achieved in the level of risk and upgrade impact on cost, mission, and schedule, the upgraded system is ready for implementation. At this point, the design/analysis process is complete.

Methodology Summary

An analysis methodology for assessing the vulnerability of critical facilities has been described. The basic steps of the methodology are:

1. Characterization of the physical features, operations, and operating conditions of the facility.

2. Identification of undesired events and associated critical assets. Which events are to be prevented, and what are the critical assets to protect to prevent such events.
3. Determination of consequences of undesired events.
4. Definition of DBT to critical facilities including adversary type, tactics, number in group, weapons, equipment, and transportation mode. Further estimate likelihood of attack for undesired events for threat spectrum.
5. Analysis of protection system effectiveness. Develop ASD for critical assets associated with undesired events. Use analytic tools to estimate probability that protection system will prevent undesired events for threat spectrum.
6. Estimation of risk for threat spectrum using:

   $$\text{Risk} = P_A * (1.0 - P_E) * C$$

7. If risk level is acceptable, analysis is complete.
8. If risk level is not acceptable, suggest and evaluate system upgrades. Determine upgrade impact on cost, schedule, and mission.

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.

References

Military Standard 882 C, DoD Standard Definitions.
Shelton, Henry H, Chairman of Joint Chiefs of Staff, Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, March 17, 1998.