SAND96-3028C
SAND--96-3028C

SPIE 2934A-18

Security systems engineering overview

CONF-961113--21

Basil J. Steele

Sandia National Laboratories
PO Box 5800, MS 0768
Albuquerque, NM 87185-0768

ABSTRACT

Crime prevention is on the minds of most people today. The concern for public safety and the theft of valuable assets are being discussed at all levels of government and throughout the public sector. There is a growing demand for security systems that can adequately safeguard people and valuable assets against the sophistication of those criminals or adversaries who pose a threat. The crime in this country has been estimated at $70 billion in direct costs and up to $300 billion in indirect costs. Health insurance fraud alone is estimated to cost American businesses $100 billion. Theft, warranty fraud, and counterfeiting of computer hardware totaled $3 billion in 1994. A threat analysis is a prerequisite to any security system design to assess the vulnerabilities with respect to the anticipated threat.

Having established a comprehensive definition of the threat, crime prevention, detection, and threat assessment technologies can be used to address these criminal activities. This talk will outline the process used to design a security system regardless of the level of security. This methodology has been applied to many applications including:

- government high security facilities
- residential and commercial intrusion detection and assessment
- anti-counterfeiting/fraud detection technologies (counterfeit currency, cellular phone billing, credit card fraud, health care fraud, passport, green cards, and questionable documents)
- industrial espionage detection and prevention (intellectual property, computer chips, etc.)
- security barrier technology (creation of delay such as gates, vaults, etc.).

2. PROCESS OF SYSTEM DESIGN AND ANALYSIS

The design of an effective physical security system (PSS) requires a methodical approach in which the designer weighs the objectives of the PSS against available resources, and then evaluates the proposed design. Without this kind of careful assessment, the PSS could waste valuable resources on unnecessary security or, worse yet, fail to provide adequate security at critical points of the facility. For example, maximum security measures at a facility's main vehicle sally port would be wasted if entry were also possible through an unguarded gate at the cafeteria loading dock.

The Design Evaluation Process Outline is shown in Figure 1. This process will be discussed with a basic explanation of how the steps are applied.

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL 85000.
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy

DISCLAIMER

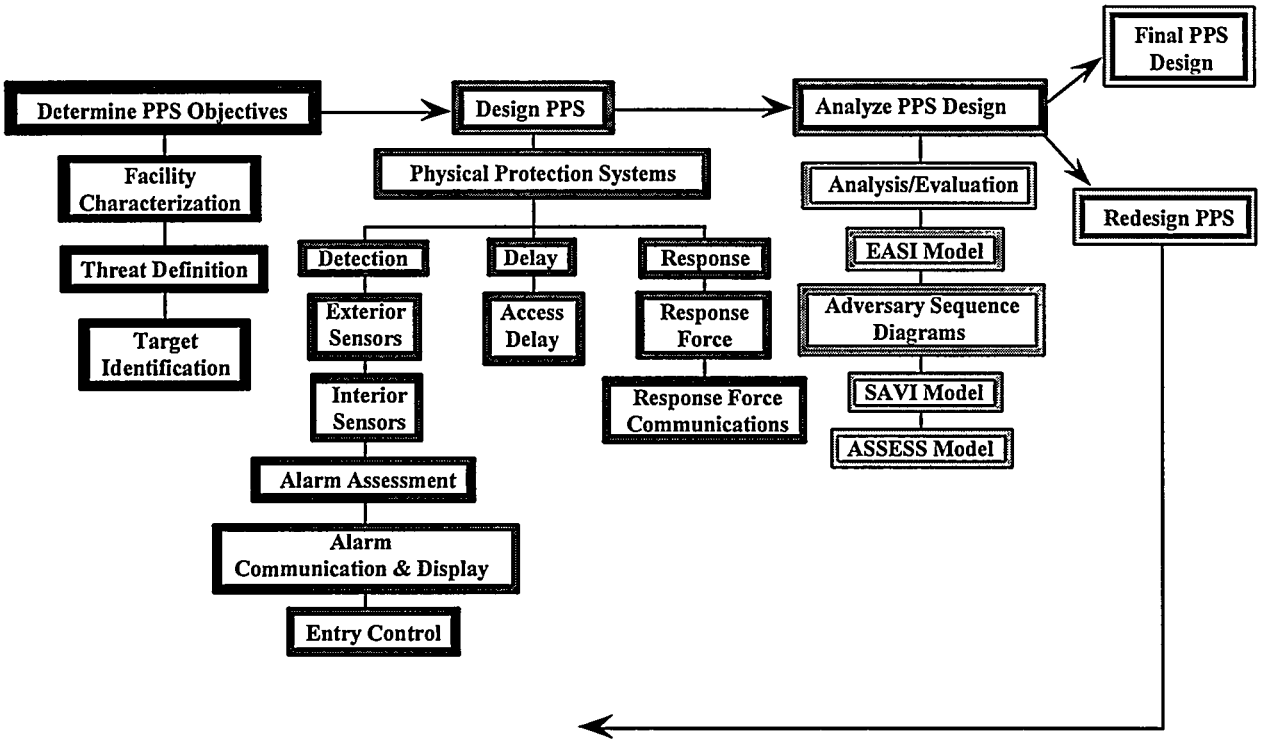

Figure 1. Design Evaluation Process Outline

3. DETERMINE THE OBJECTIVES

The first step in the development of a security design is to determine the objectives of the security system. To formulate these objectives, the designer must:

- characterize (understand) the facility operations and conditions,
- define the threat, and
- identify potential adversary targets.

Characterization of facility operations and conditions requires developing a thorough description of the facility itself which should include the location of the site boundary, building locations, building interior floor plans, and access points. A description of the procedures within the facility is also required, as well as identification of any existing physical security features. This information can be obtained from several sources, including facility design blueprints, departmental procedures, security post orders, and maintenance records. In addition to acquisition and review of such documentation, a tour of the site under consideration and interviews with facility personnel are necessary. This provides an understanding of the physical security requirements for the facility as well as an appreciation for the programmatic, operational, and safety constraints which must be considered. Compromises must usually be made on all sides so that operation can continue in a safe and efficient environment while physical security is maintained.

Next, a threat definition for the facility must be made. Information must be collected to answer three questions about the adversary:

1. What class of adversary is to be considered?
2. What is the range of the adversary's tactics?
3. What are the adversary's capabilities?

Adversaries can be separated into three classes: insiders, outsiders, and outsiders in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be considered. **Deceit** is the attempted defeat of a security system by using false authorization and identification; **force** is the overt, forcible attempt to overcome a security system; and **stealth** is the attempt to defeat the detection system and exit the facility covertly.

Important capabilities for the adversary include his knowledge of the PSS, his level of motivation, any skills that would be useful in an escape attempt, the speed with which the attack is carried out, and his ability to obtain and carry tools and weapons. Since it is not generally possible to test and evaluate all possible capabilities of an unknown adversary, the designer and analyst must make assumptions. These assumptions can be based on published information about human performance and the tested vulnerabilities of physical security elements.

Finally, target identification should be performed for the facility. All credible escape scenarios should be considered, including the defeat or by-passing of security system components or barriers, breaching of structural features, or use of facility features as climbing or bridging aids, use of force or stealth, or the defeat of procedures by deceitful means such as forged gate passes. The credibility of escape scenarios usually depends on identification of key features or vulnerabilities in the security system. These targets should become the focal points of the physical security system design.

The natural focus of security system design is to increase security at those features or areas that are most obvious and likely to be used by the defined threat. Each improvement moves the attention of the potential adversary to the next easier path of opportunity. The cost of each proposed improvement can be measured against the reduction in vulnerability to determine its worthiness for consideration. As the level of vulnerability decreases, we eventually reach the point of "acceptable risk" below which we are willing to accept the vulnerability because additional security is not worth the cost.

Given the information obtained through facility characterization, threat definition, and target identification, the designer can determine the security objectives of the PSS. An example of a security objective might be to "interrupt a knowledgeable and motivated person from removing valuable assets from a bank vault."

4. DESIGN THE SECURITY SYSTEM

The next step in the process is to determine how best to combine such elements as sensors, cameras, fences, barrier systems, procedures, communication devices, and response force personnel and weaponry into a security system that can achieve the security objectives. The resulting security design should meet these objectives within the operational, safety, and economic constraints of the facility. The primary functions of a security system are detection and assessment of an adversary, delay of that adversary, and response by the appropriate authorities, while continuing to maintain an efficiently operating institution.

Certain general guidelines should be observed during the security design. A security system generally is more effective if detection is accomplished early in the breakout attempt, and delay mechanisms are placed to interrupt the escapee's progress and expose him to response force action. In addition, there is close association between detection (exterior or interior) and assessment. The designer should be aware that "**detection without assessment is not detection.**" Another close association is the relationship between response and response force communications. A response force cannot respond unless it receives a reliable communication system call for a response.

These and many other particular features of PSS components help to ensure that the designer takes advantage of the strengths of each piece of equipment and uses equipment in combinations that complement each other and protect any weaknesses.

4.0 ANALYSIS AND EVALUATION

Analysis and evaluation of the security design begins with a review and thorough understanding of the security objectives that the designed system must meet. This analysis can be completed simply by checking for required features of a PSS such as detection, access control, delay, response communications, and a response force. However, a security design based on required features cannot be expected to lead to a high performance system unless those features, when used together, are sufficient to assure adequate levels of security. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a security system.

The end result of this phase of the design and analysis process is a **system vulnerability assessment.** Analysis of the PSS design will either find that the design effectively achieved the security objectives or it will identify weaknesses. If the security objectives are achieved, then the design and analysis process is completed. However, the PSS should be analyzed periodically to ensure that the original security objectives remain valid, that the threat definition remains current, and that the security system continues to meet them.

If the PSS is found ineffective in the system vulnerability assessment, vulnerabilities in the system can be identified. The next step in the design and analysis cycle is to redesign or upgrade the initial security system design to correct the noted vulnerabilities. It is possible that the PSS objectives also need to be re-evaluated. An analysis of the redesigned system is performed. This cycle continues until the results indicate that the PSS meets the security objectives.

5.0 SUMMARY

Detection, delay, and response are all required functions of an effective physical security system. These functions must be performed in order and within a length of time that is less than the time required for the adversary to complete his task, such as an inmate making good his escape. An effective correctional physical security system has several specific characteristics. A well-designed system provides protection-in-depth, minimizes the consequence of component failures, and exhibits balanced protection. In addition, a design process based on performance criteria rather than feature criteria will select elements and procedures according to the contribution they make to overall system performance.