A SITE PLANNING AND DESIGN PROCESS FOR ANTITERRORISM PRACTICES

Wilbur L. Peart

ABSTRACT

This study explores a solution to a growing problem involving the landscapes of many prominent landmarks in America. The probability that terrorists will target and attack public and private sites has mandated increased security presence. The initial response was to surround sensitive facilities with barriers and guards. Thus, the images of these sites intended to be publicly open and welcoming are being transformed to seemingly modern fortresses. To date, the solution to the problem has focused on sophisticated engineering and electronics to help protect vulnerable architecture. Meanwhile, the potential contribution of the landscape architecture profession has not been fully recognized.

This thesis develops a planning process to guide the integration of site design and physical security. It describes the role of the landscape architect on design teams charged with the complex task of protecting against terrorism. The document provides the landscape architect with a flowchart, site images, and a step-by-step process that leads to reconciliation of conflicting needs. The thesis culminates with a conceptual schematic site design that demonstrates how the site planning and design process proposed in this thesis can be a mechanism to achieve both secure and socially desirable landscapes.

This thesis helps resolve the current dilemma of how to maintain an adequate degree of security while preserving a sense of openness on a site. The paper identifies functions specific to the landscape architecture profession that ease and improve collaboration on secure site design. It

identifies a niche that has the potential to increase the demand for landscape architectural services. Most importantly, the planning and design process proposed in this document fills a void in the existing literature by addressing the significance of landscape architecture in antiterrorism practices.

ACKNOWLEDGMENTS

This paper is the result of the contributions made by many people involved in the physical security and law enforcement professions. Special thanks are due to Mike Jones of the Division of Capitol Police, Richmond, Virginia, who provided expertise and a network of resources that were invaluable to the completion of this study. I would also like to thank my wife, Patricia, for her steadfast encouragement and patience during this project.

CONTENTS

LIST OF FIGURES

LIST OF CHARTS

Chapter I

INTRODUCTION

1.1 INTEGRATION OF DESIGN AND SECURITY

This thesis presents a process for site planning and design that protects buildings against terrorist threats. The document describes how to integrate the various tools and skills of a design team to create effective physical security without impairing the sense of openness and welcome that are desirable in site design. It identifies the roles of the architect, engineer, security consultant, and landscape architect, and it designates key points of group decision-making during the planning process. Planning documents are suggested to guide the integration of design and security. The thesis explores and demonstrates how and why the landscape architect is a critical member of a design team planning antiterrorism practices.

In recent years, America's vulnerability to terrorism has led to a heightening of physical security at many government and private facilities. The bombing of the Alfred P. Murrah Federal Building in Oklahoma in 1995 demonstrated that the United States is just as susceptible to terrorist attacks in the homeland as it is abroad. This trend is costing citizens a significant amount of tax revenue that could be used for other causes. But beyond this concern, the consequences are producing a much more complex dilemma that remains unsolved: how to achieve security without creating a fortress image. The landscape of many of our cherished landmarks is being defaced with ill-placed barriers, closed entrances, and intimidating armed guards. The dilemma has not gone unnoticed. Politicians, architects, and engineers have joined security consultants in solving the challenge. Several books have been written and technological solutions have been developed to enhance a building's survivability against a terrorist attack. Unfortunately, the role of the landscape architect in physical security has not been fully recognized. To date, there are no publications that identify the role of landscape architects in meeting this crisis. As a result, the visible presence of security continues to dominate the site image of many sensitive public and private landscapes.

1.2 ROLE OF LANDSCAPE ARCHITECTURE

Landscape architects are well trained in creating socially desirable outdoor spaces. Their experience in site design enables them to create landscapes that best fulfill the needs of a particular site's users. This paper proposes that an understanding of the social aspects of a site is fundamental to developing site designs that are both secure and desirable. The lack of this perspective results in intimidating site images such at the U.S. Capitol shown in figure 1. This photograph is one example of how the security signature of protected sites is contradicting our most basic beliefs – that the government is of the people and not against the people. Clearly, the security needs reflected in the example have overshadowed the needs for a socially desirable space. This paper will demonstrate that such dilemma can be resolved by an integration of design and security.

Figure 1 – Vehicular Entry at U.S. Capitol, Washington, DC

Beyond creating social benefits by the integration of design and security, landscape architects contribute to the creation of functional site designs. Their experience in site design not only accommodates the need for security, but also allows it to function in a more efficient and desirable manner. Conflicts between landscape design and security such as figure 2 shows can be avoided. (Voigt, 1999) In the example, the tree canopy of the ill-placed trees hampers the line of sight of the closed-circuit television cameras mounted on a pole. The circulation of pedestrians and vehicles on a site can be tailored to enhance access control. The integration of good landscape architectural principles into the design process can prevent undesirable circulation such as we see outside the U.S. White House in figure 3.

Figure 2 – Blocked Lines of Sight by Landscape Elements

Figure 3 – Pedestrian Circulation through Barriers

1.3 FRAMEWORK OF THE PAPER

The planning process developed as part of this thesis describes a method for creating safe, secure, and desirable public and private sites. Chapter II provides summarizes an in-depth study of physical security undertaken in the course of this thesis. The study included site visits to security-sensitive sites, interviews with security professionals, physical security and design training seminars, and an extensive literature review. Chapter II identifies relevant design strategies to enhance security, such as crime prevention through environmental design (CPTED). The tools of landscape architecture that can be used in security site planning are also identified. Chapter III draws on the preceding chapter to establish a method for integrating design and security. A design process flow diagram depicts how the integration occurs among key design team members with emphasis on the role of the landscape architect. Chapter IV translates the results of collaborative planning into design parameters the landscape architect can use for design development. Charts and examples show how user needs are integrated with the needs for physical security. The chapter provides a schematic site design derived from the proposed

planning process as a measure of its effectiveness. Finally, chapter V summarizes this research and suggests several ways the landscape architecture profession can best use the findings.

Chapter II
SECURITY PLANNING

2.1 INTRODUCTION

This thesis proposes a planning process that will integrate design tools with security measures. To facilitate an understanding of this integration, a foundation of principles, requirements, and current practices is required. The chapter will provide that foundation along with strategies to achieve this process. The presentation is applicable to private, commercial, and public facilities. The discussion focuses on antiterrorism, since planning for this contingency is the greatest challenge to the integration of security and design. (Karpiloff, 2000)

The proposed planning process builds upon two established methodologies: physical security and crime prevention through environmental design. Physical security strives to protect assets and prevent crime using human, physical, and psychological forces. Guards, physical barriers, electronic sensor and surveillance devices, and other security measures are used to establish a defensive posture around a protected asset. The physical presence of security elements is the foundation of the physical security doctrine.

According to Fennelly, security tools are used in "deterring the criminal attack, detecting the attack if it occurs so that authorities can respond, delaying the attack to allow time for an apprehension to be made or to frustrate the offender into leaving before crime success is achieved, and denying access to selected targets." (Fennelly, 1989, p14)

While these practices are effective, they produce long-term financial and social costs. Maintaining skilled guards and sophisticated security devices is expensive. (Foley, 2000, and Stevens, 2000) Although the visible signature is a deterrent to crime, it produces an undesirable fortress image for the public. It is "possible for armed guards and extensive security to turn away customers." (Crowe, 1991, p18)

Crime prevention through environmental design (CPTED) is a method that uses an understanding of how criminals operate to create places that pose a minimum opportunity for crime. The foundation of CPTED is the use of the built environment as a mechanism to minimize the chances of criminal activity. (Crowe, 1991) Architectural design can be manipulated to increase the opportunities for "natural" surveillance and also to increase the efforts of the criminal to commit a crime. (Jacobs, 1961) For example, building form, window placement, and entrance design can be situated to optimize surveillance by inhabitants, employees, or other bona fide site users. Protected assets can be positioned away from vulnerable areas of a building or a site in order to decrease "natural" accessibility to a sensitive element. The arrangement of interior and exterior spaces can be configured to create a sense of "territoriality," or ownership of an area. (Newman, 1972, p3) Natural surveillance, natural access control, and territoriality are achieved using the inherent characteristics of the built environment. Such strategies have been successful in reducing conventional crimes against property and persons with minimum deterioration of site image.

Terrorism is more complex than conventional crime. Terrorists are capable of a wider range of tactics and weapons than conventional criminals. Because they are mission- or cause-driven, terrorists are likely to accept greater risks. Terrorists' lethality and unpredictability also make them more difficult to defend against. (Hoffman, 1993) Appendix A provides a further discussion of terrorists. This thesis proposes to meet this challenge by merging the tools of physical security and those of CPTED, thus creating a site design that maximizes the strengths of each method and lessens its limitations. Some degree of physical security is necessary in order to produce deterrence, detection, delay, and denial of access to motivated and unpredictable intruders. Some visible presence of security is also beneficial in reducing fear by bona fide users. (Crowe, 1991) However, overprotected sites are financially and socially unacceptable. CPTED provides an opportunity to lessen the visible signature of physical security through design practices. This thesis proposes a security planning process that prudently applies the tools of both physical security and CPTED to attain a secure and desirable site. This strategy is seen as a favorable alternative to current antiterrorism practices, and he landscape architect has a critical role in executing it. The following discussion establishes the framework for the process.

2.2 PRINCIPLES OF SECURITY PLANNING

Security planning is a process that determines what physical security measures are required and an assesses where these forces are necessary. Sufficient forces must be provided to deter, detect, delay, and deny access to unauthorized entry. Granger cites this principle as being fundamental to "a good security plan." (Granger, 2000). **Deterrence** is a preventive tactic that aims to maximize the risks and effort required by a potential criminal to such a degree that the criminal would reconsider the desirability and feasibility of an attack. Various means, such as the presence of armed guards, physical barriers, warning signs, lights, and other psychological measures attain the effect. Security experts agree that deterrence is an essential component in physical security planning. Purpura cites the importance of deterrence in his book Security and Loss Prevention. In securing parking lots, Purpura's use of "uniformed patrols, lighting, and closed circuit television (CCTV)" provides an example of the use of human, physical, and psychological means to attain deterrence. (Purpura, 1984, p.187) Deterrence increases security by lessening the likelihood that a criminal will select a particular site for a crime.

Deterrence has become a premier objective in antiterrorism planning. For example, following the 1993 bombing of the World Trade Center (WTC), over sixty million dollars have been spent increasing that facility's physical security. According to the WTC security manager, the intent was to "make the terrorist select another site." (Karpiloff, 2000) Without proper integration between security and site design, this tactic often creates a fortress image of a site. For example, recent antiterrorism measures outside governmental facilities in Washington DC prompted an April 1999 Washington Post article to describe the city as "A Capital Under Siege." Although deterrence is needed to reduce the desirability of the site for a terrorist, excessive visible security measures lessen the desirability of the site for intended users. Thus, the degree of deterrence requires careful consideration. The process established in this thesis accomplishes deterrence while preserving the desirability of the site for intended users. This goal is attained by applying the CPTED concept of territoriality.

Territoriality uses design to impart a sense of control and ownership of a particular site. A hierarchy of spaces is designed to signal to an intruder that the area is controlled and that

unauthorized entry will cause a reaction. Physical means fulfill design functions such as privacy while at the same time they create obstacles to movement. These means include doors, walls, fences, and other horizontal and vertical elements that define a space. Subtle design clues such as changes in pavement, changes in elevation, the use of signage, and other techniques alert intruders that they are entering a controlled space.

> "These psychological barriers present no physical restriction, but discourage criminal penetration by making an obvious distinction between stranger and intruder . . . invasion into the space is conspicuous and comes under more intense surveillance." (DeChiara & Koppelman, 1984, p297)

By creating territoriality through the use of a hierarchy of spaces, the degree of deterrence can be tailored to the specific needs of each zone. In the book, Defensible Space: Crime Prevention Through Urban Design, Newman advocates the use of territoriality to deter crime in urban spaces. (Newman, 1972) In Situational Crime Prevention, Clarke cites several successful applications that confirm the utility of territoriality. (Clarke, 1992) This thesis proposes the concept of territoriality as a mechanism to integrate site design with security. Territoriality allows the need for deterrence in a particular zone to be met using site design tools such as berms rather than visually obtrusive barriers such as concrete jersey walls. A jersey wall, such as the ones shown in figure 3, is a heavy concrete barrier approximately 20 feet in length manufactured for highway use. In this manner, deterrence is accomplished without unnecessary visual disruption to the overall site image.

For territoriality to be successful, however, the intruder must be convinced that unauthorized entry will be detected. This requires the provision of reliable means of detection. **Detection** is a fundamental principle of physical security because it gives security forces the ability to identify the presence of a threat and to react in order to protect vulnerable assets on a site. Site design has a profound impact on detection. Poor site design can block lines of sight; conversely good site design can create conditions that will enhance detection. Site design that allows early detection precludes the intruder from attaining an advantage of surprise over security forces. "It is important for a perpetrator to be detected before he breaches the integrity of the facility." (Bell, 1994) Detection is achieved by physical means such as alarms or sensors and by human forces. Guards maintain close observation of an area, object, or entry point visually or by

the monitoring of electronic devices such as a closed-circuit television. To be effective, surveillance requires unobstructed lines of sight. Lines of sight are enhanced by careful integration of surveillance requirements with site design requirements. Site design requirements include the designation of activity areas and linkages. An activity area refers to user functions provided on a site, such as parking, sitting, or eating spaces. Linkages are paths or routes for vehicular or pedestrian movement, such as internal streets and walkways. The manner in which activity areas and linkages are positioned and aligned impacts the line of sight potential needed by security forces. The landscape architect uses a functional diagram to graphically depict activities and linkages. By integrating site design and security, opportunities are created to maximize detection.

This thesis will propose two strategies to attain detection. One strategy is referred to as continuous surveillance; the other borrows from the CPTED principle of natural surveillance. The two strategies differ in their requirements for direct lines of sight as well as in the intended beneficiaries of the surveillance potential. The options allow planners to adopt the technique that will best meet the security needs of a specific area of the site. Constant observation along fixed, unobstructed lines of sight is referred to as continuous surveillance. Continuous surveillance ensures that any intrusion into the protected area will be detected. It increases the control of the site and contributes to deterrence. The presence of fixed security posts, closed-circuit television cameras, and well-defined line of sight corridors are characteristics of continuous surveillance.

Various aspects of design impact the continuous surveillance strategy. Activity areas and linkages can be positioned and designed to enhance visibility by surveillance means and to minimize hiding opportunities. For example, parking areas can be positioned and designed to optimize detection. Because “it is difficult to see over a row of cars,” parking bays can be oriented to maximize lines of sight along the travel lanes. (Maurer, 2000) Similarly, walkways can be aligned and designed for unobstructed visibility along the route. The selection and placement of planting materials, the type and placement of lighting, and the positioning of entry points impact detection. Trees and other plant material should be sited to avoid restricting or blocking surveillance by a guard or closed-circuit television. Camera functioning is enhanced when the line of sight is beneath tree branching. Lighting in front of a fixed security post extends the range

of surveillance and reduces the guard's vulnerability that can result from silhouetting. Light placement and lighting levels are planned to ensure adequate detection by guards and CCTV, but care taken not to blind these security sources. (Voigt, 1999) Lighting levels vary depending on the detection requirement. User identification requires a sufficient lighting level for color rendition and image detail such as facial recognition. Image detection needs enough lighting to generate a shadow effect. (Cressman, 1999)

Continuous surveillance is enhanced when the site layout has a minimum number of entry points. (Zahm, 1996) A few closely monitored entry points reduce the likelihood that intruders can bypass surveillance. This requires careful integration between building architecture and site design. In addition, such integration allows doors and windows to be positioned to increase the opportunity for natural surveillance.

The natural surveillance strategy refers to detection resulting from the daily routine of site users, security forces, and passers-by. This concept is derived from Jacob's theory of "eyes on the street" as a result of citizens' daily activity. (Jacobs, 1961, p35) Routine observation occurs as a result of the positioning and design of activity areas and linkages on a site. Natural surveillance allows everyone at a facility to become involved in the security effort, not just the guards. Placing buildings so that windows overlook a parking lot or a walkway allows users to detect suspicious vehicles, persons or activities. Strategically positioned security posts allow guards to perform their security functions such as entry security while informally overwatching activity areas and linkages. Good surveillance increases the risk of detection for intruders and contributes to a reduction of fear by site users. (Zahm, 1996) Thus, natural surveillance achieved by the integration of design and security increases deterrence and also increases desirability of the site by bona fide users.

Continuous and natural surveillance together effectively achieve detection. These strategies require integration of building design, site design, and surveillance objectives. This thesis proposes that the development of a surveillance plan is a key step during the integration of design and security. During the program phase of site design, design agenda should include the designation of surveillance corridors to overwatch entry points, activity areas, and linkages. By

plotting these corridors on a surveillance plan, design needs are accomplished in a manner that maintains designated surveillance objectives. Carefully drawn surveillance plans are instrumental to detection and response by security forces.

Security forces respond to threats by employing two principles of physical security: delay and deny. **Delay** refers to practices designed to increase the difficulty of an intruder by slowing the approach or by requiring extra effort. By delaying the intruder, time is gained for the deployment of an appropriate response by security guards. “Responsiveness of a guard force is key to security.” (Jones, 1999) One strategy to attain delay is to establish successive layers of defense. A perimeter is normally “the first line of defense.” (NRC, 1995, p33) Physical security planners traditionally view the building wall as the second line of defense. A third layer of defense is that provided in the interior spaces. Human and physical controls such as guards and locks are used to enforce entry procedures and to control access to sensitive inner compartments. Successive layers of security work together to create a defense in depth. (Atlas, 1992) However, the traditional preponderant focus on these three layers often leads to a fortress-like appearance. Armed guards, bulky and ill-placed barriers, and closed entrances have destroyed a sense of openness characteristic of American public spaces. This thesis proposes that by integrating security and design, the principle of delay can be attained in a more desirable manner. The following paragraphs explain.

The perimeter is the edge of a controlled space. Control of the perimeter is accomplished by human, physical, and psychological means. Typically, the line is well defined by armed guards, fences or walls, closed circuit television, and other means that help deter, detect and delay penetration onto the site. The perimeter is designed to be distinguishable to intruders. Since it is also visible to intended users, it often creates a fortress image. An alternative strategy requires thinking beyond the common practice of establishing the visibly linear edge of a site. It requires consideration of risks based on a site’s intended users and their activities and linkages. This thesis proposes that by using a hierarchy of spaces referred to as zones, the principles of delay and denial can be accomplished without unnecessary damage to the overall site image. The establishment of zones is suggested as an effective means to attain a layer of defense. This

technique substitutes a more intricate pattern of security than the traditional 3-ringed circle system. (Fennelly, 1989)

Zones allow determination of control to based on the risks inherent to or issuing from a particular user group. By tracing the pattern of flow of risk-categorized users, and dividing them within zones, you give the designer far more flexibility. Designs become fluid rather than the stiff image resulting from traditional security practices. For example, visitors to a facility require a greater degree of control to ascertain their identity and purpose. Employees, on the other hand, require less due to visual recognition, security passes, and other means of verification. Zone design expedites access control of routine intended users such as employees. Zone elements can also sufficiently delay users to ensure adequate security screening. Control of zones is done through points of interface, which are designated areas security forces can closely screen and control users, and/or collect evidence for later use. The number and positioning of interface points are dependent on the site layout and the user risks. Because visitors generally pose greater risks, they will often be subjected to multiple points of interface that extend a greater distance from the protected area than that needed for routine users. Zones are linked and enforced by site design. For example, berms, retaining walls, and other means to delay access are positioned to channel users to and through interface points. Surveillance corridors in zones allow detection of unauthorized movement, activity, or attempts to bypass designated entry points.

A similar use of the concept of zones appears in military publications, such as Protection of Federal Buildings. (USN, 1988) This book, for example, identifies the utility of approach and blast zones in antiterrorism security. An approach zone refers to an ingress route leading onto a site. A blast zone is a "controlled area that surrounds a facility by a set standoff distance." (DOD, 1993, p58) This thesis extends that concept by advocating the establishment of zones based on the characteristics of user groups. Organizing site security based on specific user risks and functions allows security to be focused on those users who present the greatest risks and in those areas of the site where it is most needed. In addition, the number and types of zones can vary by location and function. A typical site may include, but is not limited to, the following zones: street, approach, drop-off, parking, emergency access, walkway, and building entrance zones. Details on these zones are contained in Chapters III and IV. The employment of zones changes the

appearance of a perimeter from a continuous barrier encircling a site to a series of cohesive areas. The principles of deterrence, detection, and delay are accomplished without unnecessary loss of openness. Channeling users through zones also increases the effective use of security forces.

The ability to **deny** access is a fundamental principle of physical security. It is the protection of vulnerable assets by human and physical means. Armed guards are trained to respond to criminal threats using apprehension or force if necessary. Security posts are strategically sited to allow quick response and reinforcement. Predetermined rapid response routes enable guards to reach an intercept point quickly or to reinforce another security effort. Site designs can extend the range of security by facilitating the employment of roving patrols. For example, pathways can be placed to ease patrol circulation, and lighting and planting plans tailored to complement their surveillance potential. Physical barriers enhance the defense of a site by channeling users to authorized areas, keeping them away from vulnerable spaces, facilitating apprehension by restricting their egress, and by hindering intelligence gathering or "casing" by criminals.

Barriers vary according to the intended security function. People barriers resist foot passage and channel pedestrians into controllable zones. This type of barrier includes building walls, doors, freestanding walls and fences, and other horizontal and vertical planes. Screening barriers such as walls, fences, or tall plantings prevent potential criminals from obtaining intelligence to aid their attack planning. Vehicle barriers confine vehicles to authorized areas, control and direct their speed and direction of movement, and deny vehicular penetration to vulnerable areas. Building and freestanding walls, berms and topographic depressions, and other vertical obstacles are used to deny vehicular passage. Blast-resistant barriers are measures such as choice of building framing, walls, and door and window design that decrease the loss of life and property due to an explosion. (NRC, 1995)

According to Brodie, barriers are effective means to "shield a target from observation by a criminal, to deter, delay or stop an aggressor, and to mitigate or lessen the force, strength or severity of an attack." (Brodie, 1996, p251)

The placement, design, and construction of defensive barriers dictate security's effectiveness as well as site image. For example, improperly sited barriers may block response routes by guards. Intended obstacles may be bypassed, overrun, or used as hiding places. From a design standpoint, oversized barriers contribute to a sense of beleaguerment. Thus, the close integration of physical security and design is essential in planning site defenses. This thesis proposes and orderly step-by-step system by which members of a design team achieve integration. (See Chapter III.) Appendix B provides a further discussion of barriers.

Sites are especially vulnerable to risks from close-in detonations of car-delivered bombs or bombs planted by intruders. These can produce the greatest degree of destruction and injury because of their proximity to the target. The vehicle bomb detonated only a few feet away from the Alfred P. Murrah Building in Oklahoma "claimed 168 lives including 19 children and wounded another 674 people." (OKC, 1996, ix) Consequently, controlling circulation close to buildings is a premier task in antiterrorism. One means of control is the establishment of a blast zone defined earlier. The design team determines the depth of the blast zone by combining the risk acceptance with an engineering analysis of the potential effects of a hypothetical explosive composition. This results in a model, referred to as a "design reference threat" that is used to determine blast resistance requirements such as vehicle barriers, structure framing, and blast-resistant windows. Risk acceptance is determined by the client based on recommendations and input provided by the design team. Risk acceptance stipulates that a facility should be capable of sustaining a design reference threat that consists of a specified size/type of explosive detonated at a specified distance from the protected area.

Security forces typically prevent intrusion into a blast zone by providing perimeter security. This usually results in the encirclement of a building or the entire facility with people and vehicle barriers. This thesis proposes the use of an intercept zone as an alternative strategy. The intent of this zone is to channel pedestrian and vehicle traffic to a few points on the site where security is focused. In this concept, initial security screening takes place outside the blast zone. Circulation beyond this point(s) proceeds along well-defined corridors. The corridors are designed to project a pleasing image to the user. Control in the corridors is achieved using unobtrusive but continuous surveillance and barriers to maintain user integrity. Channeling

circulation to a few points allows the efficient use of security forces and the use of site design techniques such as grading to preserve the blast zone, both of which lessen the visible signature of security.

Street design and traffic flow are important off-site influences on physical security. The need for vehicle barriers increases on urban grid sites because such sites are exposed on all sides. The street pattern may also add to a site's vulnerability due to possible attacks from adjacent properties. T-junctions formed by cross streets, alleys, or driveways of adjacent facilities, large open urban intersections, or adjacent spans of open space can be high-speed avenues of approach and escape. Businesses that draw truck traffic create an opportunity for terrorists in trucks to blend in unnoticed. Streets without medians allow a sufficient turning radius for a bomb-laden vehicle to make a sudden wide turn in a high-speed terrorist attack. Thus, it is important to assess security requirements beyond the boundary of the protected site. The landscape architect's expertise in street design is vital in mitigating risks from the public street zone and adjacent properties. For example, street medians can be designed as barriers and entrances drives aligned to prevent a high-speed approach from the street.

Internal traffic control also influences physical security. Channeling traffic controls speed, increases surveillance, and decreases the opportunity for criminals to use vehicles to carry out a crime. By manipulating road alignment, lane widths, and curb height, vehicles are slowed and/or contained. For example, a roadway with multiple horizontal curves or curves with small turning radii, vertical curves such as a peak or sag in the roadway, or a combination such as a reverse bank curve will slow traffic, affording safety and physical security. (Gray, 1986, and Strom & Nathan, 1993) Controlling vehicle speed allows more time for surveillance, and it decreases the kinetic energy of a vehicle, thus lessening the resistance strength needed for a vehicle barrier. Street design can create opportunities for vehicle barriers without defacing the site image with bulky obstacles. For example, the height of barrier curbs can be extended to serve as obstacles in areas where such design does not present hazards to pedestrians. "It is difficult to drive over a 6-8" curb," (Lindsey, 1999) These "deep curbs" can be reinforced with berms or depressions. The alignment of vehicular routes impacts on the employment of closed-circuit television. A CCTV line of sight is enhanced by a head-on image in daylight, but blinded by approaching headlights

at night. (Voigt, 1999) Vehicles can be routed to avoid access to areas vulnerable to property theft and to other vulnerable areas such as an entrance lobby or a mission-critical utility element such as antennas or electrical controls. Vehicle control by routing can also avoid interference with sensitive electronic intrusion detection sensors, and can preclude the use of vehicles as climbing devices. Circulation design effects the difficulty in establishing and maintaining physical security, the convenience to users, and the image of the site. Careful integration between circulation and security planning increase opportunities to detect, delay, and deny.

The extent of the security effort depends on risk assessment. Risk assessment is the process through which the security consultant identifies threats that may jeopardize a protected asset. Protected assets may include persons, equipment, spaces containing sensitive data, and elements such as heating, ventilation, and air conditioning (HVAC) or communications links. Risks include natural disasters, such as earthquakes or floods. Criminal threats include personal or property crimes, such as assault or theft. Sites are influenced by local crime conditions such as gang violence. Some facilities are subject to specific risks because of their function, such as abortion clinics. Facilities may be vulnerable to sabotage, espionage, vandalism or attacks by disgruntled employees, or attacks by terrorists. Terrorists may target one very important person (VIP) at the facility, such as a judge or a company executive. A public facility may be targeted by terrorists because of the site's symbolic importance, for example, government services buildings, shrines, museums, and monuments. (NRC, 1995, p51) Risk assessment is an important step in physical security planning. Security consultants are aided in risk assessment by various law enforcement agencies. For example, the Federal Bureau of Investigation (FBI) provides up-to date information on terrorist activities and tactics.

Risk assessment guides decision making in antiterrorism planning. The assessment determines the extent of human, physical, and psychological forces and means needed to achieve physical security. Since security cannot guarantee safety and protection, the client must determine what risks are acceptable. This in turn determines security requirements. These requirements guide site design. Thus, risk acceptance is an important step in the design process. Landscape architects will be better prepared to understand risk assessment provided by security consultants if they understand how terrorists operate. Appendix A provides a basic framework

for this understanding. Since terrorism is a complex and dynamic crime, additional study and experience will enhance landscape architect's ability to counter terrorists' tactics.

2.3 CONCLUSION

The planning process outlined in this document provides a means for members of the design team to better integrate their respective skills and tools. The preceding discussion will allow landscape architects to speak a common language with security members on the team. The strategies proposed in this chapter will help landscape architects to produce a site design that contributes to security while also maintaining the desirable social aspects of a site.

Chapter III

METHODOLOGY FOR INTEGRATING DESIGN AND SECURITY

3.1 INTRODUCTION

This chapter presents a way to integrate security with the CPTED principles cited in the previous chapter. This will be accomplished by establishing a framework for decision making. The proposed planning process can integrate the efforts of an antiterrorism design team consisting of, but not limited to, architects, landscape architects, structural and civil engineers, security consultants, and law enforcement representatives. This thesis proposes that the traditional site design planning process used by those in the design professions such as landscape architecture and architecture is a suitable mechanism that can be modified to guide this integration. Using a flowchart, this chapter will illustrate how the traditional process can incorporate the principles and requirements cited in the preceding chapter. The flowchart will show who integrates with whom and the results of the action. The tasks of the various members of the design team will be identified with emphasis on the role of the landscape architect.

This chapter goes beyond existing writings such as Fennelly's Effective Physical Security and Clarke's Situational Crime Prevention that rely on checklists to suggest integration. (Fennelly, 1992 and Clarke, 1992) This thesis proposes that by depicting how integration actually occurs, the ability of the design team to achieve more efficient, effective, and desirable site design will be enhanced. Such planning will avoid costly retrofit to correct oversights. (Cressman, 1999)

3.2 PROGRAM DEVELOPMENT

The traditional design process involves four phases: programming, design development, construction, and postconstruction. Programming provides an understanding of what functions the site design must satisfy. Motloch defines programming as "the definition and analysis of human needs." (Motloch, 1991, p296) A "program" lists the design requirements in a concise, legible manner. Using the program, the design team is able to coordinate solutions to site design

requirements. Because of the importance of programming in the design process, this thesis will focus on the programming phase.

The proposed programming process involves four major group decision points: assessing client needs, determining a design program audit, determining blast protection requirements, and determining design parameters. These decision points are explained in the following discussion and illustrated in chart 1 as a flowchart.

Program development for antiterrorism planning begins by **assessing the client's needs.** The client's goals and objectives influence the degree of accessibility, the intended users, and the activities to be accommodated on the site. For example, a site with restricted access such as a military installation presents security requirements different from one intended to have some degree of openness to the public (such as a courthouse). The profiles of the intended users of each site are also different. The activities to be supported by the site design also affect security. For example, visitor parking at a sensitive site produces risks different from a similar site that is restricted to official vehicles. In some cases, an advisory body may dictate security requirements in order to ensure protection of high-risk individuals, agencies, or sites. Understanding the client in terms of goals and objectives is fundamental to prudent security planning. Assessing the client's needs is the first point of decision making among the members of the design team.

The design team uses the guidance conveyed by the client to deduce tasks to be supported by the site design. This is accomplished by restating the client's goals and objectives in terms of design and security requirements. Formulating design requirements begins by an identification of user functions. The landscape architect maps out exterior activities and linkages deemed necessary to fulfill the client's needs. An activity refers to the various uses of a site, such as parking, seating, etc. A linkage refers to elements of circulation, such as a walkway and building entrance or an entrance drive. Close coordination between the landscape architect and architect occurs in order to link building requirements with outdoor space requirements. Graphically depicting activities and linkages on a functional diagram similar to the one shown in chart 2 is useful to understand how the site is intended to function. A functional diagram illustrates functional relationships to be satisfied later by site design. (Motloch, 1991)

Security requirements evolve from an identification of the protected assets and a risk assessment. Protected assets may include persons, equipment, spaces, elements, or data the loss of which could jeopardize the safety and functioning of the client. The security consultant assesses the client in order to identify who or what needs to be protected. The consultant also formulates a risk assessment. The assessment accounts for risks associated with a specific site location, the client's function, and the intended design agenda. For example, risks may be brought about by a site location in a hostile foreign country such as an embassy, or a domestic site location in a high crime area. Inherent risks associated with the client's function, for example the susceptibility of a high profile individual like a judge, to criminal or terrorist attacks are also assessed.

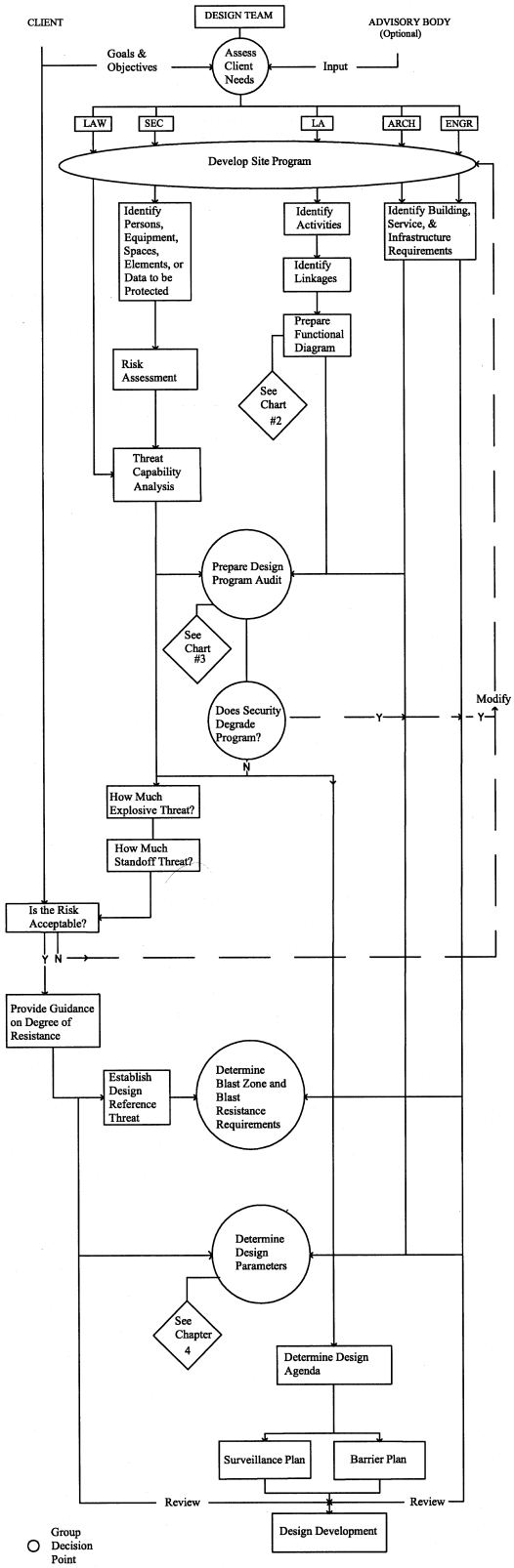
The security consultant and the designers merge risks with site design by the preparation of a **design program audit.** In this phase of decision making, intended users are categorized by user profile based on the risks associated with a particular user group. For example, visitors present a different set of security risks than routine users such as employees. Each user profile is assessed in terms of risk from the user and risks to the user. Risk from the user refers to threats that jeopardize the safety and functioning of the client. Risk to the user refers to threats to the safety of the intended user such as susceptibility to personal or property crimes. Zones are then associated with the activities and linkages of each user group. Security requirements are then developed by zone to ensure security is focused where it is needed. The functional diagram is studied to determine prearranged points or areas that will enhance security response to threats. These points or areas are referred to as "points of interface," and are established in each zone based on the risks and circulation of the user group. The degree of control at each point of interface is specified as the degree of control necessary to achieve a certain level of security in the zone. During this evaluation, the site layout is reviewed to determine how the site design can be adapted to complement security efforts. For example, a prospective walkway may be realigned to improve surveillance in a particular zone. The result of this phase of decision making is expressed in a chart referred to as a "design program audit." The design program audit establishes the risks and degree of control necessary to ensure physical security in each zone of a site. Chart 3 provides an example of a design program audit.

The next phase of program development involves decisions concerning **blast protection requirements.** Blast protection is required on sites that are susceptible to attacks using explosives. The risks of the site are assessed considering threats from skilled terrorists, activist groups, and disgruntled individuals. Blast protection requirements are determined through interaction among the security consultant, site designers, and engineers. The landscape architect's role in this phase involves the alignment and positioning of parking areas, walks, and internal roads. Building setback, offsite influences such as perpendicular drives, and other site design factors are evaluated in order to determine the limits of a blast zone. The landscape architect uses the blast zone as a guide to modify site design to improve blast resistance. For example, a berm or freestanding wall may be positioned to serve as a barrier for blast protection.

The final phase of program development is the establishment of **design parameters.** Design parameters transform the security requirements into a design agenda, a "to do" list for the landscape architect. This step involves an identification of security goals and objectives for each user profile and zone. The landscape architect develops site design tasks or agenda to correspond to these security requirements. Design parameters guide the execution of design development phase. Chapter IV provides a discussion and an example of design parameters.

CHART 1 - PROGRAM DEVELOPMENT

FLOW DIAGRAM



REMARKS

The **client and advisory bodies** such as a governmental agency, community committee, or private interest group provide the design team with desires and concerns that will impact on design decisions. The **design team** consists of an architect (ARCH), landscape architect (LA), security consultant (SEC), engineers (ENGR), representatives from the Federal Bureau of Investigation or other law enforcement agencies (LAW), and other members as required by the project.

The design team prepares a program. A **program** identifies the requirements to be met by the site design. The program reflects input received from the client, advisory body, and members of the interdisciplinary design team. The landscape architect identifies requirements as **activities and linkages** to satisify user needs. Examples of activities include parking, walkways, outdoor seating, etc. Linkages are vehicular roads or pedestrian walkways to, from, and between activity areas. Activities and linkages are graphically depicted in functional diagrams such as Chart #2.

The security consultant identifies **persons, equipment and other assets** requiring protection. A **risk assessment** is conducted to identify risks that may threaten the protected assets. Aided by law enforcement, **threat capability** is analyzed by security consultants in terms of the availability of weapons, past tactics, and site chararacteristics that may increase a site's vulnerability to a risk. For example, a protected asset may be susceptible to a specific tactic(s), such as a terrorist act using a vehicle bomb, particularly if the site has a high-speed avenue of approach.

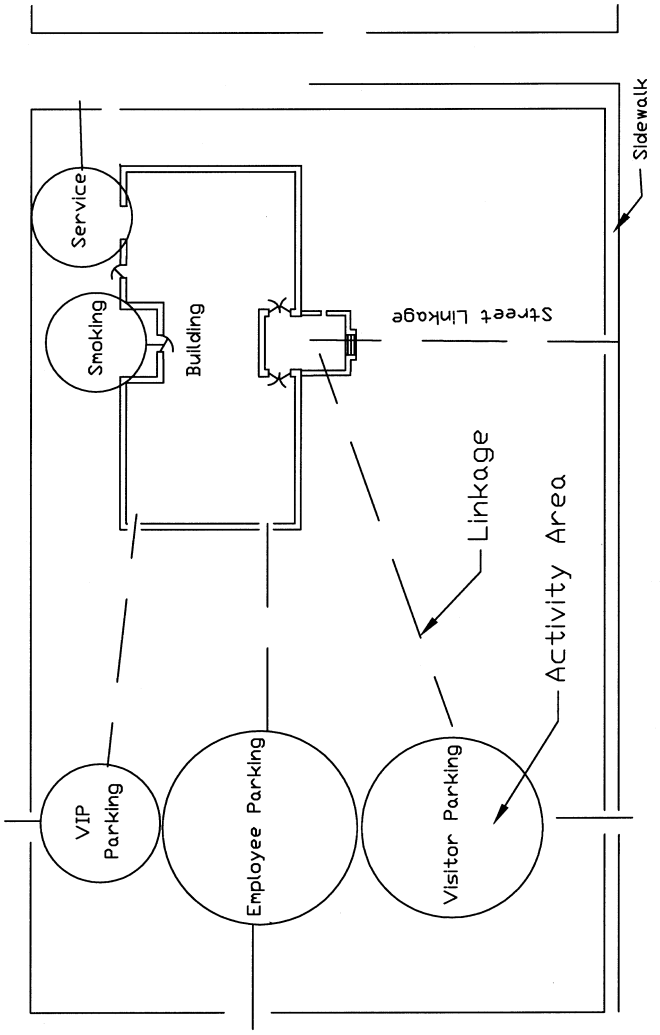
The **design program audit** is conducted by designers and security members. The activity and linkage of each user type are identified, and user types are compartmentalized into zones. The types of users are dependent on the facility, but may include visitors arriving in vehicles, employees arriving in vehicles, very important persons (VIPs), service personnel, Americans with disabilities, street pedestrians, etc. Zones are established for each user type depending on the activities and linkages required. Each user profile is then analyzed separately. The risk associated with each zone is analyzed, and the need for interface and control determined. A chart is prepared similar to Chart #3.

The risk assessment and threat analysis are the basis for **risk acceptance**. Risk acceptance is the client's decision regarding the degree of resistance the facility must be able to sustain against the risk(s) identified by the security consultant. Risk acceptance for **explosive threats** or **standoff attacks** such as sniper fire or a shoulder-launched missile determines the degree of site hardening required. Guidance on the degree of resistance is transformed into a **design reference threat**. A design reference threat is used as a model for calculating the blast zone and blast resistance requirements. A **blast zone** is a planning envelope established around a building/facility to ensure sufficient distance from a potential detonation point to attain the required resistance determined by the risk acceptance. The blast zone serves as a planning tool for the placement of barriers to protect the facility. **Blast resistance** can be accomplished by free-standing blast barriers and/or blast hardening such as window treatments, facade hardening, and other structural techniques.

Design parameters are developed to respond to the program audit and blast requirements. Security consultants specify security goals and objectives for each user in each zone. Design agenda prepared by the landscape architect identifies design options that can meet the security goals and objectives.

The end products of program development are the **surveillance** and **barriers plans**. The surveillance plan is a consolidated plan depicting the surveillance requirements for each user. Similarly, the barrier plan reflects the consolidated barrier requirements. Both of these plans are used to guide **design developmen**t.

CHART 2 - FUNCTIONAL DIAGRAM EXAMPLE



The functional diagram is a planning tool prepared by the landscape architect to identify intended activities and linkages of the site. The diagram displays the relative location of various areas of a site and how these areas are linked. For more on the functional diagram, see chapter III.

CHART 3 - DESIGN PROGRAM AUDIT *

User Profile	Risk Assessment: Risks **to** User	Risk Assessment: Risks **from** User	Point of Interface / Degree of Control: Street Zone	Approach Zone	Dropoff Zone	Parking Zone	Intercept Zone	Emergency Zone	Walkway Zone	Building Entrance	Special Provisions
Visitor in Vehicle	Variable	High		1 M	2 H	3 L	4 H		5 M	6 H	Crowd Control
Employee in Vehicle	Variable	Moderate		1 M		2 M	H		M	3 H	Threat Condition
Very Important Persons in Vehicles	High	Low		1 H		H			H	2 H	Threat Condition
Service Personnel	Variable	High	L	1 H		2 H				3 H	Threat Condition
Emergency Responders	Low	Low to Moderate		1 L-M				H		2 H	
Special Users	High	Low		1 M		2 H				3 H	Threat Condition
Street Pedestrians	Variable	Moderate	L-M	2 M			3 H		4 M	5 H	Crowd Control
Outdoor Space Users	Variable	Low								1 H	
Adjacent Land Users	Variable	Variable	L-M				H				

* The headings and subheadings in this chart provide the structure for a design program audit. The annotations under the various subheadings, i.e., user profile, risks to user, risks from user, and the degree of control and point of interface for each zone, are intended as examples. The actual annotations (such as high, 1, M) would be determined during program development based on the specifics of the users and the site.

Risk Assessment. Risk assessment is analyzed for each user profile and recorded in two subcategories: "risk to users" and "risk from users." Risk to users refers to the susceptibility of users to personal or property crimes while at the facility. For example, users may be subject to assault, sabotage, or theft of property. Risks from users refers to the threat brought to the facility by users of a particular profile. For example, parking and accessibility of visitors may increase the risk of criminal or terrorist threat to the facility. Variable risk indicates the classification is dependent on the local crime rate.

Point of Interface. Point of interface refers to prearranged points or zones for security to respond to perceived threats. The numbers reflect the number of interface points needed to control a particular user, i.e. there are 6 interface points for visitors in vehicles. The same numbers are shown the charts and overlays in Chapter 4, i.e., interface point #1 in this chart for the approach zone of visitors in vehicles is the same as the one shown for this user group in Chapter 4.

Degree of Control. Degree of control is a general classification in the hierarchy of security. The classification varies by user profile, by risk assessment, and by zone. Low (L) control indicates a zone that has at least natural surveillance, and may or may not have perimeter barriers, depending on the risk assessment. Moderate (M) control indicates a zone with continuous surveillance or a zone enclosed with barriers sufficient to at least delay entry by unauthorized users. High (H) control indicates a zone with continuous surveillance and enclosed with barriers sufficient to deny access to unauthorized users or objects.

Special Provisions. Special provisions refers to conditions or situations that may increase the risks and/or the degree of control. For example, demonstrators may crowd a security post and reduce its effectiveness. Similarly, a bomb threat may increase the degree of control of a particular zone. In such situations, the degree of control or points of interface may be modified.

Chapter IV

DESIGN PARAMETERS TO GUIDE DESIGN DEVELOPMENT

4.1 INTRODUCTION

Programming provides a means of identifying those design and security requirements that must be integrated during the site design process. The process establishes security goals and objectives to safeguard intended users on the site. The product of programming is a set of design parameters that serve as guidelines for the design development phase of site design. These parameters transform security requirements into a design agenda. Programming leads to the preparation of security goals and objectives, a design agenda, and surveillance and barrier plans. Matrices and overlays such as the ones shown in chapter 4 are useful tools to guide the development of design parameters.

4.2 SECURITY GOALS AND OBJECTIVES

The first step is to identify the aims (goals) and tasks (objectives) of security for each user group in every one of the zones that the user encounters. Goals identify the overall aim or intent of the security effort in each particular zone. For example, preliminary entry screening of visitors arriving by vehicle and vehicle control may be deemed as necessary goals in order to detect and respond to potential threats. Objectives are specific tasks that can be measured in order to ascertain the satisfaction of a security goal. For example, the degree of continuous surveillance provided by a site design may be one measurable entity (among others) that can indicate how well security is able to conduct preliminary entry screening and vehicle control. The identification of security goals and objectives provides a framework to guide designers during site design.

4.3 DESIGN AGENDA

The second step is to identify every task the landscape architect must undertake to reach the goals and meet the objectives just identified. The landscape architect begins by reviewing the security goals and objectives for each user in each zone. These tasks may include a range of site design facets, such as the selection, positioning, or construction of a particular design element. During this process, the landscape architect evaluates the site layout in order to position design elements to complement security. For example, an entrance drive or a walkway can be positioned or aligned to ensure continuous surveillance. Another design task may require decisions on construction issues, such as grading and hardscape details. For example, a berm may be created to channel traffic, or the height of a wall may be manipulated to resolve a surveillance requirement. The development of a design agenda provides useful guidelines for the design development phase of site design.

4.4 SURVEILLANCE AND BARRIER PLANS

The final step is to collect all the landscape architecture tasks into a surveillance plan and barrier plan. A surveillance plan depicts intended line-of-sight corridors that must be maintained in order to ensure effective detection. Barrier plans show the relative location and functions of the various barriers to counter risks and to channel users for more effective physical security. Plotting the surveillance and barrier plans on separate overlays is a useful way to organize these requirements into usable forms. For example, the landscape architect can identify those areas of the site where plantings will conflict with surveillance lines of sight. With such information, plantings, parking layouts, and other site design elements can be manipulated to improve detection. Similarly, the barrier plan overlay allows the landscape architect to identify site design options that fulfill barrier requirements. For example, grading may be adjusted or a wall positioned to meet a barrier requirement.

A separate surveillance and barrier overlay is prepared for each user group such as visitors in vehicles, employees in vehicles, and street pedestrians because each of these users present a different set of risks. The security consultant reviews each overlay to ensure it meets

the stated security goals and objectives. A composite of all overlays shows the complete surveillance plan and barrier plan for the site. The “overlay methodology” in design was originated by McHarg as a way to blend program requirements with environmental features. (McHarg, 1992) For example, McHarg advocates the technique to lessen the impact of siting a building on the existing terrain and drainage pattern of a site. Similarly, the overlay technique is a useful method to reconcile physical security requirements with site design elements.

The development of design parameters is a useful tool to guide the subsequent design development process. The integration of design and security helps to fulfill the requirements for defense in depth without damage to the site image.

4.5 DESIGN PARAMETER EXAMPLE

The following presents how to develop design parameters using a hypothetical site as an example. The example is based on a set of site users including visitors in vehicles, employees in vehicles, very important persons, service providers in vehicles, emergency responders such as fire and rescue, special users such as sallyport, utility vehicle, and other site specific users, street pedestrians, outdoor space users, and adjacent land users. Each example identifies the security goals and objectives and the corresponding design agenda. Preparing a chart similar to the one shown for each user group below is a useful way to record the security and design decisions. Following each example chart is a brief discussion of design options and an overlay showing how surveillance and barrier requirements for the example are satisfied. The surveillance and barrier plans for the hypothetical site produced from a composite of all the overlays are shown in paragraph 4.6.

4.5.1 Design Parameters for Visitors in Vehicles (See parts A, B, and chart 4)

PART A- DEVELOPING DESIGN AGENDA FOR VISITORS IN VEHICLES

User	Zone	Security		Design Agenda
		Goals	Objectives	
Visitor in Vehicle	Approach Zone (Interface Point #1)	* Preliminary entry screening of users	*Maintain continuous surveillance * Respond to perceived threat	* Designate continuous surveillance corridor * Provide lighting level for image detection * Provide means for rapid response by security
		* Vehicle control	*Delay attempt for forced vehicular entry into another zone	* Position entrance, channel traffic, and/or provide vehicle barrier to hinder high speed approach to building from entrance
	Dropoff Zone (Interface Point #2)	* Intermediate screening with minimum difficulty to user * User safety and convenience	* Maintain continuous surveillance of dropoff and parking for disabled users (ADA)	* Designate continuous surveillance corridor * Provide lighting level for image detection * Position ADA parking near dropoff
		*Protection of facility	* Minimize vulnerability to blast	* If dropoff is within blast zone, contain vehicles to dropoff zone with vehicle barrier and use blast resistant barrier to protect building
		* Vehicle control	* Detect and respond to suspicious activity	*Position dropoff for rapid response by security * Position dropoff near facility but outside blast zone when possible
	Parking Zone (Interface Point #3)	* Safety of users	* Maintain natural surveillance	* Designate natural surveillance corridor * Provide lighting level for image detection
		* Protection of facility	* Minimize vulnerability to blast * Detect and respond to suspicious activity	* Provide means for rapid response by security * Provide blast resistant barrier if parking is within the blast zone and if required by the risk * Place parking outside the blast zone when possible

User	Zone	Security		Design Agenda
		Goals	Objectives	
Visitor in Vehicle	Intercept Zone **(Interface Point #4)**	* Intermediate entry screening of users	* Maintain continuous surveillance * Detect and respond to suspicious users	* Designate continuous surveillance corridor * Provide lighting level for user identification * Establish people barrier to prevent bypass of intercept zone * Provide route for rapid response by security * Establish enclosed entry point for channeled passage of visitors
		* Vehicle control	* Deny vehicular access into blast zone	* Establish vehicle barrier to prevent vehicular entry into blast zone
	Walkway Zone **(Interface Point #5)**	* Passive monitoring of users * Safety of users	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for image detection * Place stopping points such as seating areas within the walkway
		* User control	* Contain users to authorized zone * Detect and respond to suspicious users or activities	* Use people barrier or clear space expanse to channel users * Use vehicle barrier and/or ramp design to deny vehicular access to ADA ramp * Provide route for rapid response by security * Provide direct ADA-accessible route to building entrance without detours or hiding places

		Security		
User	Zone	Goals	Objectives	Design Agenda
Visitor in Vehicle	Building Entrance Zone (Interface #6)	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification * Place stopping points such as seating areas within the continuous surveillance corridor
			* Slow approach of users	* Use people barrier to channel users to interface point
			* Detect and defend against unauthorized entrance	* Provide route for rapid response by security
			* Deny vehicular access into building entrance	* Establish vehicle barrier to deny vehicle access to entrance zone

PART B - DESIGN OPTIONS FOR VISITORS IN VEHICLES

Approach Zone. The visitor entrance should be outside the blast zone when possible, as shown in chart 4. A separate vehicular entrance allows security to be tailored to the particular profile of visitors in vehicles, as, for example, visitors in automobiles without prearranged security passes. If an unexpected or suspicious vehicle such as a large truck were to enter the zone, security would respond to the perceived threat. If the risk warrants, an overhead barrier can limit the height of authorized vehicles that can enter the zone. Moderate control (M) is achieved by continuous surveillance. If the zone is within the blast zone or the risk warrants, vehicle barriers such as deep curbs, road alignment, berms, ditches, or other obstacles can channel traffic or limit access of a vehicle into the blast zone. Offsetting the entrance and directing traffic away from the building are examples of road alignment techniques to increase security. Depending on the risk assessment, interface point #1 may be configured as a fixed security post, a gate, or an alert mechanism associated with a rapid response route from a nearby security post. The lighting level permits security guards to detect the presence of vehicles or pedestrians in the zone by visual or electronic means.

Dropoff Zone. The ADA dropoff zone should be positioned near the facility for user convenience. The zone includes the dropoff area and ADA parking. Both should be outside the blast zone when possible and/or separated from vulnerable facility elements by a blast resistant barrier such as a wall, berm, a lower risk building, or another horizontal or vertical plane. The protected building's perimeter wall(s) can be blast-hardened as an alternative or supplemental security measure. Because of its proximity to the protected facility, the zone is a high-control (H) area. Control is achieved by continuous surveillance, vehicle barriers to deny access into the blast zone, or a blast-resistant barrier if sited within the blast zone. Surveillance is achieved by positioning of the ADA parking spaces near interface point #2. Control at interface point #2 may be achieved by a fixed security post or visual or electronic surveillance associated with a rapid response route from a nearby security post. Vehicle barriers for this function may consist of deep curbs with an ADA curb ramp, bollards, or antiram walls or fences placed in the intercept zone. Direct linkage to the walkway zone should be provided through the barriers, but without permitting vehicular passage. This can be accomplished by walkway spacing, bollards, planters,

or other similar vertical obstacles. The blast-resistant barrier may be provided as a free-standing wall or as a blast-resistant façade of the protected building. Lighting of the spaces should permit the detection and monitoring of vehicles and pedestrians in the zone by visual or electronic means.

Parking Zone. Visitor parking may be provided as surface or structure parking (aboveground or underground). Surface and aboveground spaces should ideally be outside the blast zone and/or separated from vulnerable facility elements by a blast-resistant barrier such as a wall, berm, a lower-risk building, or another vertical surface. The protected building's perimeter wall(s) can be blast-hardened as an alternative or supplemental security measure. If parking is under a protected building, a blast-resistant barrier should partition the parking zone from the protected area. Low control (L) of visitor parking is achieved by positioning and by designing surface parking to allow natural surveillance. This requires consideration of parking aisle placement, alignment, plant selection, and plant placement. Control at interface point #3 may be achieved by a fixed security post, by roving patrol, or by a rapid response route from a nearby security post. Response routes may be surface or underground. Low control of structure parking is achieved by designs that allow visibility into the structures by visual and/or electronic means. Depending on the risk assessment and positioning, a people barrier and/or vehicle barrier may be necessary to control ingress into a parking zone. Surface and structure parking should be sited and designed for rapid response by security guards. Lighting of the spaces should permit the detection and monitoring of vehicles and pedestrians by visual or electronic means.

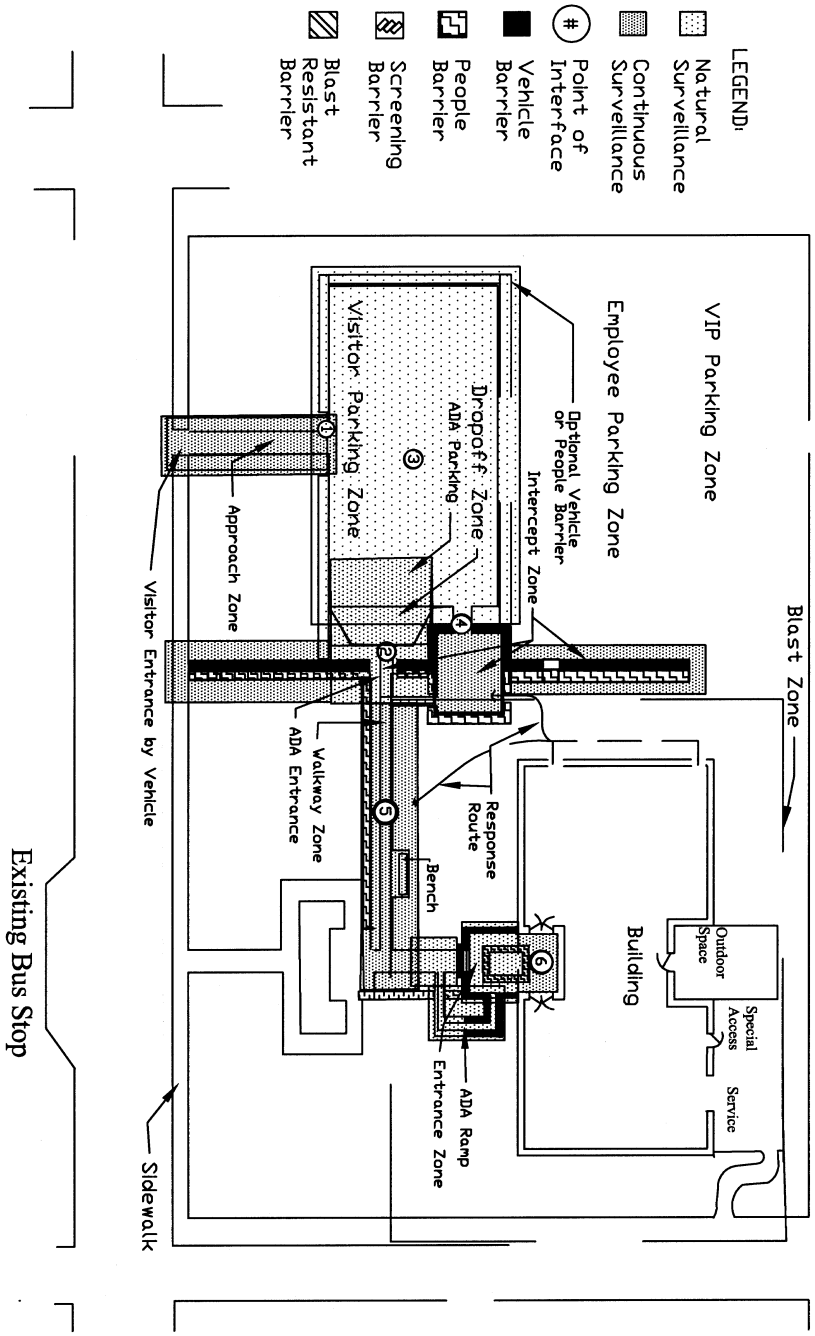
Intercept Zone. The intercept zone serves as a high control (H) area for intermediate screening. Offset placement of the zone allows interception of risks before they jeopardize the building. The remote location permits design to restore a sense of openness along the walkway to the building. Ideally, the zone is positioned at least at the edge of the blast zone. The zone is linear, consisting of vehicle and people barriers that deny access except at an authorized entry point(s). One barrier may serve as both a people and vehicle obstacle, depending on its physical characteristics. Vehicle barriers may consist of an antiram wall or fence, berm, ditch, or other obstacle capable of denying vehicular access into the blast zone. People barriers may consist of an anti-climb wall or fence, ditch, or another obstacle that will deny foot passage. A clear space along each side of

the barrier(s) allows continuous surveillance to detect efforts to bypass or defeat the barrier. For visitors, the intercept zone includes an enclosed entry point to channel users to interface point #4. Visitors attempting to enter through interface point #2 will be intercepted. The zone is positioned for continuous surveillance by security using visual or electronic means. Control at the interface point can be achieved by a fixed security post or by a rapid response route from a nearby security post. The lighting level should be sufficient to allow facial recognition for security screening and evidence collection and to allow detection of suspicious elements such as an unexpected or unauthorized package, camera, or other prohibited objects. The enclosed entry point can be configured as a design amenity or element such as a pavilion or plaza.

Walkway Zone. The walkway zone is a linkage between the intercept and building entrance zones. It includes an ADA-accessible walkway and stopping points along the route, such as seating areas. An ADA ramp maybe required along the walkway and/or at the building entrance, depending on the topography. Such ramps should deny vehicle access. This can be accomplished by right-angle alignment of the ramp, the use of reinforced cheek walls to narrow the ramp width, or the use of vertical obstacles along the ramp. Such design should not create unnecessary difficulty or danger to the ADA users. The walkway should provide a direct route without the need or opportunity for detour. The walkway should be well defined to channel users along the intended path. Moderate control (M) is achieved by a continuous surveillance corridor and/or people barrier. An expansive clear space and/or people barrier can be used to contain screened users to the walkway zone and to prevent nonscreened users from entering the zone. Such clear space should be of sufficient depth to allow security to detect attempted passage. People barriers for this function include planting beds, low hedges, a low wall or retaining wall, or other elements that delay foot movement. Depending on the site layout and the risk, people barriers may be on one or both sides of the walkway. Clear space along the walkway enhances safety of users and security surveillance by preventing hiding opportunities. Interface point #5 extends the length of the walkway. Continuous surveillance allows passive monitoring of users and response to suspicious activity or persons. Lighting should be sufficient for user safety and image detection by security guards.

Building Entrance Zone. The entrance zone is a high control (H) area in which positive access control is achieved by continuous surveillance and barriers. Visitors are channeled to control their direction and speed of movement to interface point #6 using people barriers. The entrance zone includes designated stopping points such as seating, but such points should be within the continuous surveillance corridor. Examples of people barriers for this zone include planters, low walls, sculptures, or other vertical obstacles. Vehicle barriers extend around the zone's perimeter to deny forced entry by vehicle. Examples of vehicle barriers for this function include retaining walls, steps, ramps, elevated plazas, or other vertical obstacles. Depending on the selection, vehicle barriers can double as people barriers. Control of interface point #6 can be achieved by a fixed security post, access control mechanisms such as locks and doors, and interior access control devices. The lighting level should allow facial recognition for access control and evidence collection and to allow the detection of suspicious or prohibited objects.

CHART 4 – SURVEILLANCE AND BARRIER PLANS FOR VISITORS IN VEHICLES



EXTRACT FROM CHART 3	Point of Interface / Degree of Control
Street Zone	
Approach Zone	1 / M
Dropoff Zone	2 / H
Parking Zone	3 / L
Intercept Zone	4 / H
Emergency Zone	
Walkway Zone	5 / M
Building Entrance	6 / H

4.5.2 Design Parameters for Employees in Vehicles (See parts A, B, and chart 5)

PART A - DEVELOPING DESIGN AGENDA FOR EMPLOYEES IN VEHICLES

User	Zone	Security Goals	Security Objectives	Design Agenda
Employee in Vehicle	Approach Zone (Interface Point #1)	* Entry screening	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting for image detection
			* Respond to perceived threat	* Provide means for rapid response by security
			* Minimize disruption to offsite traffic due to entry screening	* Provide space for vehicle stacking based on access control delay, employee traffic, and street conditions
	Parking Zone (Interface Point #2)	* Safety of users	* Maintain natural surveillance	* Designate natural surveillance corridor * Provide lighting level for image detection
			* Detect and respond to suspicious activity	* Provide means for rapid response by security
		* Protection of facility	* Delay access to unauthorized users	* Isolate parking from other users by people barrier and/or by placement
			* Minimize vulnerability to blast	* Place parking outside the blast zone when possible * Provide blast resistant barrier if parking is within the blast zone and when required by the risk
	Intercept Zone	* Vehicle control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for image detection
			* Deny vehicular access into blast zone	* Establish vehicle barrier to prevent vehicular entry into blast zone

User	Zone	Security		Design Agenda
		Goals	Objectives	
Employee in Vehicle	Walkway Zone	* Passive screening of users * Safety of users	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
		* User control	* Delay infiltration by unauthorized users * Contain users to authorized zone	* Provide direct route to building entrance without detours or hiding places * Use people barrier to channel users to entrance and to delay access by unauthorized users
	Building Entrance Zone **(Interface Point #3)**	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
			* Detect and defend against unauthorized entrance	* Use people barrier to channel users to interface point * Provide separate entrance

PART B - DESIGN OPTIONS FOR EMPLOYEES IN VEHICLES

Approach Zone. The employee entrance should be outside the blast zone when possible, as shown in shown in chart 5. A separate vehicular entrance allows security to be tailored to the particular profile of employees in vehicles, as, for example automobiles with prearranged security passes and/or access to magnetic card operated gates. The zone may be operational only during shift change periods and between shifts by prearrangement. If the risk warrants, an overhead barrier can limit the height of authorized vehicles that enter the zone. Moderate control (M) is achieved by continuous surveillance. Depending on the number of employees, such surveillance may allow visual recognition of employees during their approach. If the zone is within the blast zone or the risk warrants, design options are similar to those discussed for the visitor approach zone. Provisions should be made for safe movement to and from the street and sufficient space for stacking of cars awaiting entry and exit. Depending on the risk assessment, interface point #1 may be configured as a fixed security post or a gate, and it may be associated with a rapid response route from a nearby security post. The lighting level is similar to that for the visitor approach zone.

Parking Zone. Employee parking may be provided as surface or structure parking. Design options for placement are similar to the visitor parking zone. Moderate control (M) is achieved by positioning and the use of people barriers to delay access by intruders. Examples of people barriers for this function include dense medium-height hedges, a wall, fence, and other vertical obstacles to at least delay passage by intruders. Natural surveillance requires similar considerations as visitor parking. Control at interface point #2 may be achieved by roving patrol or associated with a rapid response route from a nearby security post. The lighting level is similar to that for the visitor parking zone.

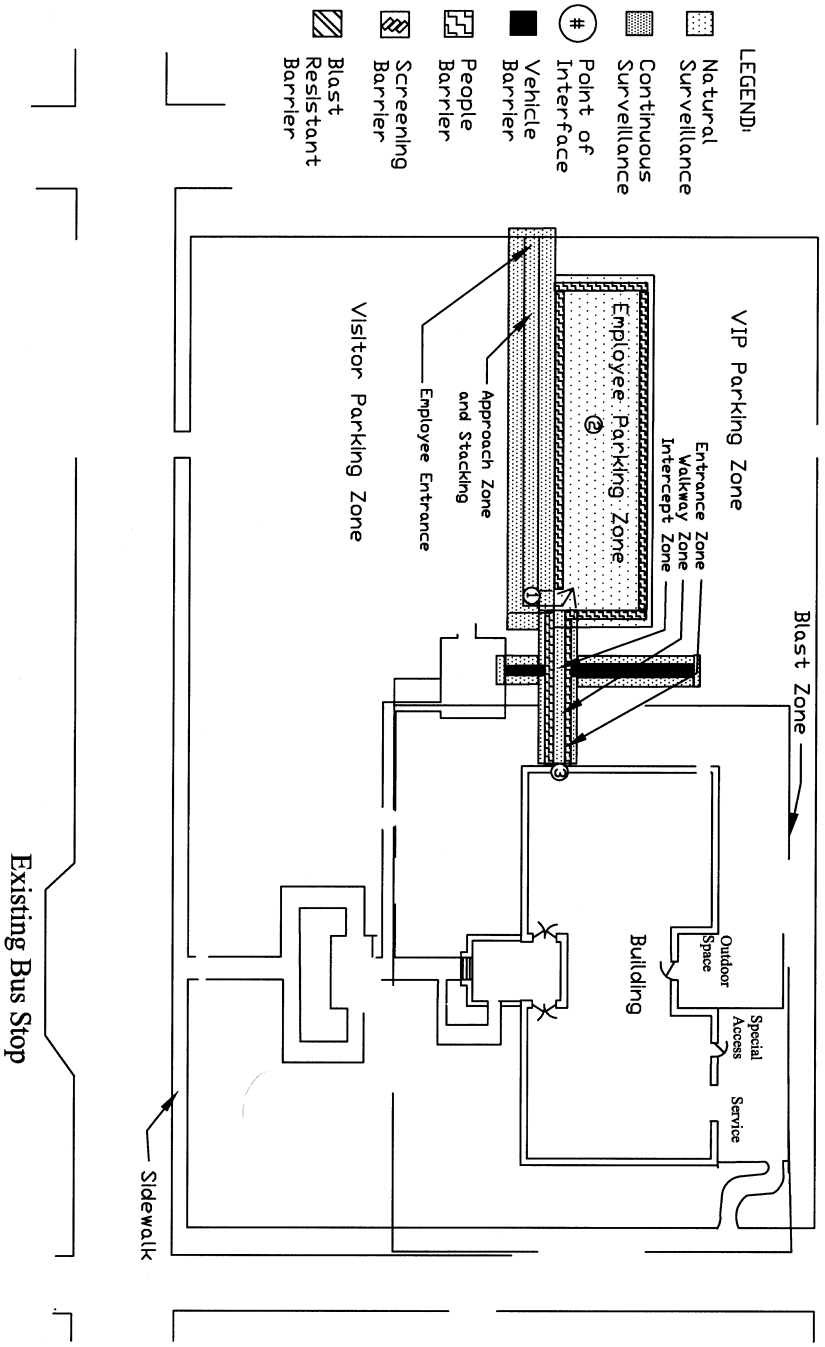
Intercept Zone. The intercept zone is a high control (H) area that denies vehicular and foot access into the blast zone. The options for the barriers are similar to those identified for the visitor's intercept zone. Ideally, the zone is positioned at least at the edge of the blast zone. Requirements for clear space and surveillance are similar to the visitor intercept zone.

Employees transit the intercept zone at an entry point separate from visitors to avoid infiltration. Rather than entering an enclosed entry point like visitors, employees may enter directly into the walkway zone. The lighting level is sufficient to allow facial recognition for security screening and evidence collection and to allow detection of suspicious elements such as unauthorized or prohibited objects.

Walkway Zone. The walkway is a moderate control (M) zone that provides a direct route to the building entrance. Employee walkway zones may also be used to link workspaces at multibuilding facilities. Moderate control (M) is achieved by a continuous surveillance corridor and a people barrier. An expansive clear space and/or or people barriers are used to contain employees to the walkway zone and to authorized stopping points and to prevent unauthorized users from entering these spaces. People barriers for this function include dense medium-height hedges, a wall, a fence, or other vertical obstacles to at least delay passage by intruders. Clear space along the walkway provides safety for users and security surveillance by preventing hiding opportunities. Continuous surveillance allows passive screening of employees and response to suspicious activity or persons. Lighting should provide for user safety and for visual recognition by security.

Building Entrance Zone. The entrance zone is a high control (H) area in which positive access control is achieved by continuous surveillance and people barriers. Employees are channeled through a separate entrance using people barriers such as planters, low walls, or other vertical elements. Control of interface point #3 can be achieved by a fixed security post, access control mechanisms such as locks and doors, and interior access control devices. Lighting requirements are similar to those for the visitor entrance zone.

CHART 5 – SURVEILLANCE AND BARRIER PLANS FOR EMPLOYEES IN VEHICLES



EXTRACT FROM CHART 3	Point of Interface / Degree of Control
Street Zone	
Approach Zone	1 / M
Dropoff Zone	
Parking Zone	2 / M
Intercept Zone	2 / H
Emergency Zone	
Walkway Zone	3 / M
Building Entrance	3 / H

4.5.3 Design Parameters for Very Important Persons (VIPS) in Vehicles (See parts A, B, and chart 6)

PART A – DEVELOPING DESIGN AGENDA FOR VIPS IN VEHICLES

User	Zone	Security		Design Agenda
		Goals	Objectives	
Very Important Person	Approach Zone Interface Point #1)	* Access control with minimum delay * Safety of users	* Maintain continuous Surveillance * Expedite screening	* Designate continuous surveillance corridor * Provide lighting level for user identification * Provide separate entrance
			* Deny access to unauthorized users	* Provide means for rapid response by security * Use overhead vehicle barrier to limit access to automobiles only
	Parking Zone	* Safety of users	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for image detection
			* Deny access to unauthorized users	* Isolate parking from other users by people and vehicle barrier
	Walkway Zone	* Access control * Safety of users	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
			* Avoid infiltration by unauthorized users	* Use people barrier to channel users to entrance and to deny access to unauthorized users
	Building Entrance Zone (Interface Point #2)	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
			* Detect and defend against unauthorized entrance	* Use people barrier to channel users to interface point
		* Expeditious routing to interior spaces	* Minimize delay in access control	* Provide separate entrance to a secure interior corridor

PART B - DESIGN OPTIONS FOR VIPS IN VEHICLES

Approach Zone. The VIP entrance should be separate from other vehicular circulation to reduce the opportunity for infiltration by unauthorized users. VIPs will be in automobiles with prearranged security passes and/or access to magnetic card operated gates. High control (H) is achieved by continuous surveillance and a gate. Interface point #1 may be configured as a fixed security post or a gate, and IT may be associated with a rapid response route from a nearby security post. The lighting level should be sufficient for facial recognition for access control.

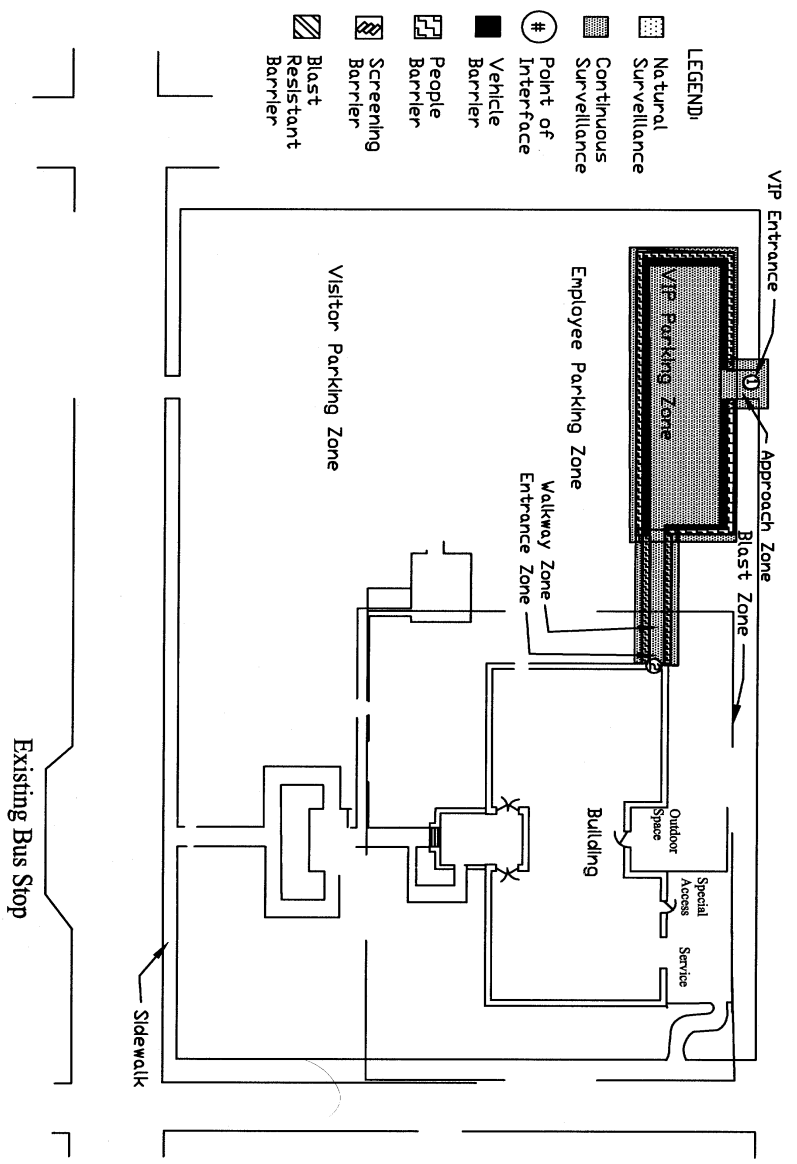
Parking Zone. VIP parking may be provided as surface or structure parking. The parking should be placed near the facility for expeditious routing to interior spaces, as shown in chart 6. High control (H) is achieved by the use of continuous surveillance and people and vehicle barriers to deny access by intruders. Such barriers may consist of anticlimb, antiram walls or fences or by other vertical obstacles that prevent covert or forced entry by person or vehicle. Continuous surveillance requires consideration of parking aisle placement and alignment and avoidance of all obstructions to lines of sight. The lighting level is similar to that used for the visitor parking zone.

Walkway Zone. The walkway is a high control (H) zone that provides a direct route to the building entrance. Control is achieved by a continuous surveillance corridor and a people barrier. People barriers are used to deny entrance to unauthorized users. People barriers for this zone are similar to those described for the parking zone above. Continuous surveillance allows identification and monitoring of VIPs enroute to the building. This can be accomplished by a fixed security post and/or a closed-circuit television. Lighting should provide for user safety and user identification by security guards.

Building Entrance Zone. The entrance zone is a high control (H) area in which positive access control is achieved by continuous surveillance and people barriers. VIPs are channeled through a separate entrance using people barriers such as planters, low walls, or other vertical elements. Control of interface point #2 can be achieved by a fixed security post, access control mechanisms

such as locks and doors, and interior access control devices. Lighting requirements are similar to those for the visitor entrance zone. The VIP entrance may be linked to secure interior corridors.

CHART 6 – SURVEILLANCE AND BARRIER PLANS FOR VERY IMPORTANT PERSONS (VIPS) IN VEHICLES



EXTRACT FROM CHART 3 / Degree of Control \ Point of Interface	
	Street Zone
H / 1	Approach Zone
	Dropoff Zone
H	Parking Zone
	Intercept Zone
	Emergency Zone
H	Walkway Zone
H / 2	Building Entrance

4.5.4 Design Parameters for Service Providers in Vehicles (See parts A, B, and chart 7)

PART A - DEVELOPING DESIGN AGENDA
FOR SERVICE PROVIDERS IN VEHICLES

User	Zone	Security		Design Agenda
		Goals	Objectives	
Service Provider in Vehicle	Street Zone	* Early warning	* Maintain natural surveillance	* Designate street frontage adjacent to service zone as a natural surveillance corridor * Ensure street lighting level adequate for image detection
		* Traffic safety	* Minimize disruption to offsite traffic due to vehicle maneuvering	* Position entrance and make street provisions for traffic safety
	Approach Zone (Interface Point #1)	* Preliminary entry screening	* Maintain continuous surveillance * Respond to perceived threat	* Designate continuous surveillance corridor * Provide lighting level for user identification * Provide means for rapid response by security
		* Vehicle control	* Deny attempt for forced vehicular entry from zone	* Channel traffic and/or provide vehicle barrier to hinder high speed approach to building
			* Minimize disruption to offsite traffic due to entry screening	* Accommodate vehicle maneuvering in approach zone * Provide ample stacking space
	Parking Zone (Interface Point #2)	* Protection of facility	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for image detection
			* Deny access to unauthorized persons	* Provide blast resistant barrier if parking is within blast zone and when required by the risk * Isolate zone from other vehicles and pedestrians
			* Minimize vulnerability to blast	* Place parking outside blast zone when possible
		* Safety of persons and equipment	* Prevent accidents and property crimes	* Provide means for rapid response by security * Provide ample space for safe maneuvering

		Security		
User	Zone	Goals	Objectives	Design Agenda
Service Provider in Vehicle	Building Entrance Zone (Interface Point	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
			* Detect and defend against unauthorized entrance	* Isolate service area from facility by positioning or interior people barrier

Street Zone. The street zone fronting the service entrance presents a facility risk and a traffic hazard. Trucks comprise a significant risk due to their ability to carry large amounts of explosives. Truck traffic can also endanger pedestrians and street traffic. Since it is a public right-of way, control is normally limited to low control (L) achieved by natural surveillance. If the risk warrants and is approved by local agencies, medium control can be achieved by restricting parking in the vicinity of the service zone. Modifications to the street may be required to enhance traffic safety. Examples of such provisions include left-turn lanes, speed control, ample driver line of sight for entry and exit, and offset of the entrance from the street intersection for safety. Coordination is effected with local public agencies to achieve a lighting level sufficient to detect the presence of vehicles or pedestrians in the zone by visual or electronic means.

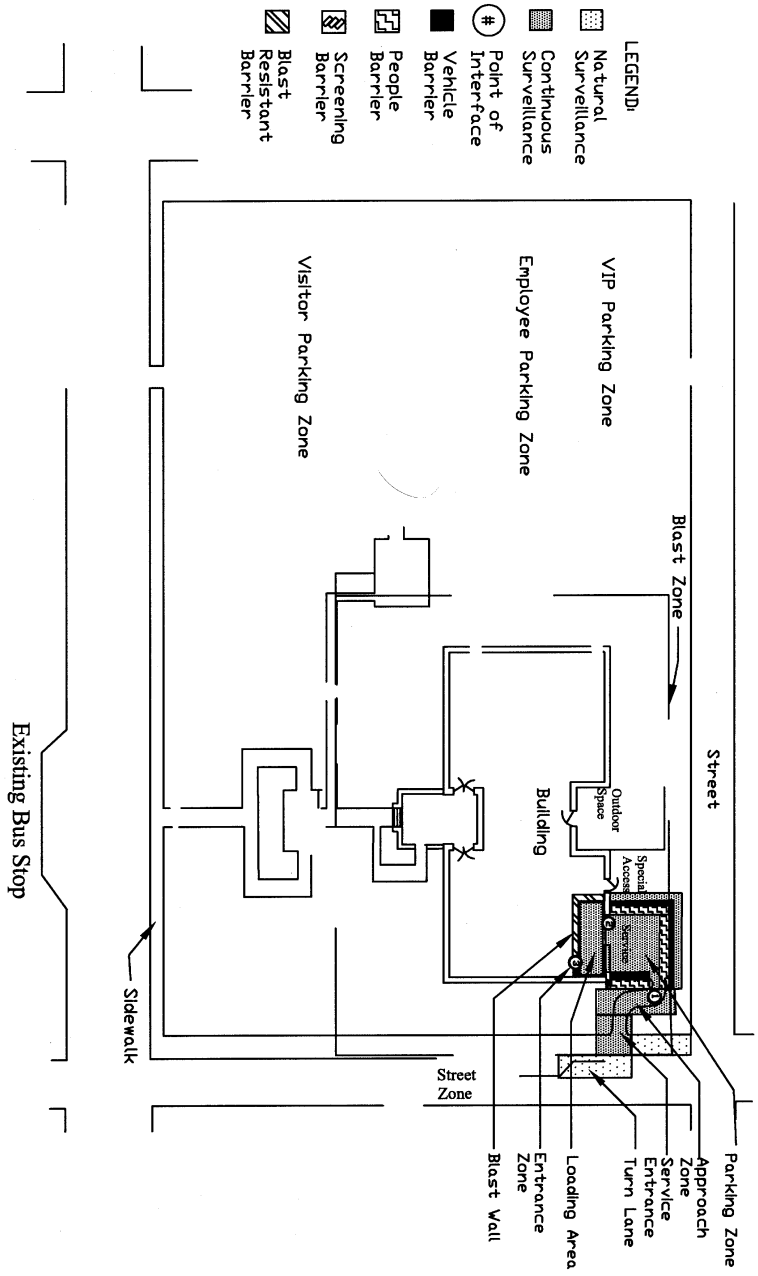
Approach Zone. The service entrance should be designed with stacking and maneuvering space sufficient to accommodate the number and size of vehicles. A vehicle turn-around or waiting area may be included for service vehicles denied entry or awaiting entry approval. The entrance should be outside the blast zone when possible. A separate service entrance allows security to be tailored to a particular user profile, e.g., users in vans or trucks. High control (H) is achieved by continuous surveillance, vehicle barriers, and procedural measures such as scheduled delivery. Vehicle barriers for this function can include curb depth, road alignment to slow speed and channel traffic, anti-ram walls or fences, berms or ditches, or obstacles to deny forced entry to the building. Depending on the risk assessment, interface point #1 may be configured as a fixed security post or a gate and it may be associated with a rapid response route from a nearby security post. The lighting level is similar to that used for the visitor approach zone.

Parking Zone. Service parking may be provided as surface or internal bays. Ideally the zone is outside the blast zone. High control (H) is achieved by positioning of the zone and the use of vehicle and people barriers to deny access to intruders. When the risk warrants and space permits, the zone may be positioned at a remote area of the site or at a site separate from the protected facility. Depending on the positioning, vehicle barriers may include antiram walls or

fences, berms or ditches, or other such obstacles to vehicle traffic. People barriers include anticlimb fences or walls to deny access to unauthorized persons in order to prevent property crimes such as vandalism, sabotage, or property theft. Depending on the selection, barriers may deny access to vehicles and people. When the zone is within the blast zone, the facility should be protected by a free-standing, façade, and/or an internal blast-resistant barrier. The parking zone should have sufficient space for turning, backing, and temporary parking. Continuous surveillance allows passive monitoring of users and response to suspicious persons or activities. Interface point #2 may be a fixed security post and/or a roving patrol. The lighting level should permit the image detection by visual or electronic means.

Building Entrance Zone. The entrance zone is a high control (H) area requiring access control and includes the loading area and the entrance to the protected facility. Control is achieved by continuous surveillance, people barriers and/or the use of a separate service building. Control of interface point #3 can be achieved by a fixed security post, access control mechanisms such as locks and doors, and interior access control devices. The lighting level should be sufficient for user identification and evidence collection.

CHART 7 – SURVEILLANCE AND BARRIER PLANS FOR SERVICE PROVIDERS IN VEHICLES



EXTRACT CHART 1 / Point of Interface / Degree of Control	
L	Street Zone
H 1	Approach Zone
	Dropoff Zone
H 2	Parking Zone
	Intercept Zone
	Emergency Zone
	Walkway Zone
H 3	Building Entrance

4.5.5 Design Parameters for Emergency Responders in Vehicles (See parts A, B, and chart 8)

PART A – DEVELOPING DESIGN AGENDA
FOR EMERGENCY RESPONDERS IN VEHICLES

User	Zone	Security		Design Agenda
		Goals	Objectives	
Emergency Responder in Vehicle	Approach Zone (Interface Point #1)	* Early warning	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
		* Expeditious access control	* Provide rapid emergency response	* Provide ample entrance to accommodate emergency vehicle maneuvering
		* Operational continuity during emergency	* Maintain security during emergency	* Provide emergency backup lighting
	Emergency Zone	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridors for each emergency zone * Provide emergency backup lighting
			* Allow escorted access on emergency response routes	* Use active vehicle barriers to allow vehicular access into blast zone * Designate emergency response routes to major building entrances
		* Safety of facility users	* Provide safe evacuation of facility users	* Provide evacuation routes that do not interfere with emergency responders
	Building Entrance Zone (Interface Point #2)	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification and evidence collection * Provide emergency backup lighting
			* Provide for rapid entry by emergency responders	* Provide ample space for access and maneuvering of emergency persons and equipment
			* Deny access to unauthorized persons	* Provide means for access control

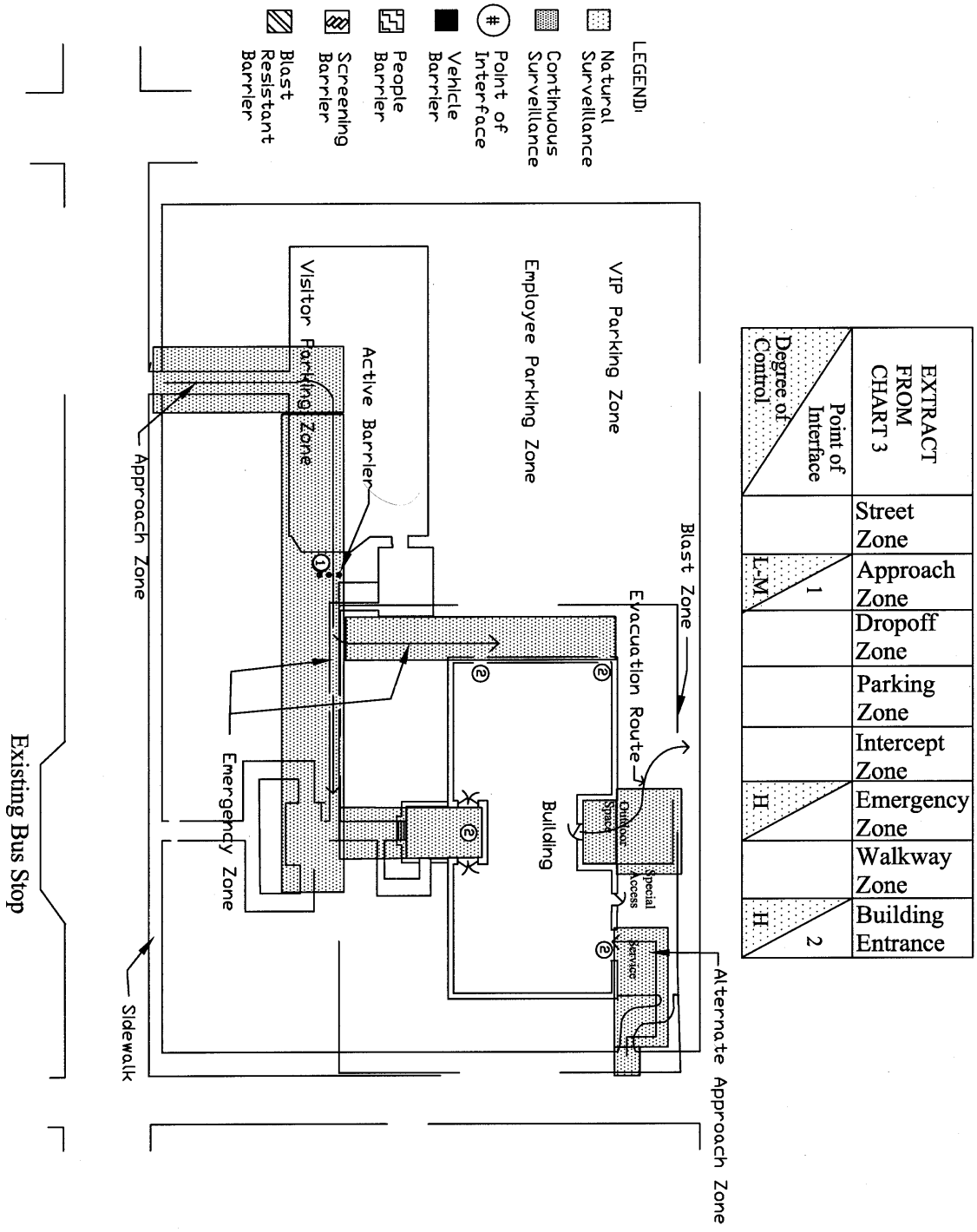
Approach Zone. The emergency responder entrance should afford expeditious access to the building. The entrance may coincide with other entrances such as the visitor entrance as long as access can be granted rapidly. Low control (L) depends on continuous surveillance and procedural measures such as visual recognition of emergency vehicle markings, sirens, flashing lights, and other warning signals. Verification of the presence of an emergency situation allows security guards to confirm and anticipate an emergency response. Low control allows for expeditious movement to the emergency area of the facility. If the risk warrants, stationing a temporary guard in the approach zone can achieve a moderate level (M) of control. During an emergency, security guards may deny entrance to all but emergency responders to avoid the potential for intruders to infiltrate during the chaos. The lighting level for the approach zone coincides with the respective entrance. If a separate emergency responder entrance is established, the lighting level should allow user identification. In both cases, the approach zone should be equipped with emergency backup lighting.

Emergency Zone. The emergency zone consists of avenues of approach that allow vehicular passage by emergency responders. It also includes provisions for evacuation routes for facility users. Routes for emergency responders should be designated for each major entrance. Access to the route requires high control (H) since such access permits movement within the blast zone. High control is achieved by continuous surveillance and vehicle barriers that deny access to unauthorized users. Such barriers must be active or removable to allow access to emergency responders when required. Examples of active barriers include hydraulic bollards, gates, or other movable obstacles. Active (and passive) barriers are discussed in appendix B. Depending on the availability of security forces, control can also be achieved by escorting emergency responders within the blast zone. Evacuation routes should allow rapid, safe passage of facility users away from the area of the emergency. Such routes should not interfere with the emergency responder routes.

Building Entrance Zone. The entrance zone is a high control (H) area requiring access control. Provisions should allow for emergency egress and for security that denies ingress of

unauthorized persons. Control at interface point #2 (several may be designated) can be achieved by continuous surveillance, separate building entrances reserved for emergency responders, temporarily stationed security guards, and/or people barriers such as emergency doors or gates. The lighting level should be sufficient for user identification and evidence collection.

CHART 8 – SURVEILLANCE AND BARRIER PLANS FOR EMERGENCY RESPONDERS



Point of Interface / Degree of Control	EXTRACT FROM CHART 3
	Street Zone
L-M 1	Approach Zone
	Dropoff Zone
	Parking Zone
	Intercept Zone
H	Emergency Zone
	Walkway Zone
H 2	Building Entrance

4.5.6 Design Parameters for Special Users (See parts A, B, and chart 9)

PART A – DEVELOPING DESIGN AGENDA FOR SPECIAL USERS

User	Zone	Security		Design Agenda
		Goals	Objectives	
Special Users (transport of prisoners etc.)	Approach Zone (Interface Point #1)	* Preliminary screening	* Maintain continuous surveillance * Respond to perceived threat	* Designate continuous surveillance corridor * Provide lighting level for image detection * Provide means for rapid response by security guards
		* Vehicle control	* Delay attempt for forced vehicular entry from zone	* Position entrance, channel traffic, and/or provide vehicle barrier to hinder high-speed approach to building from entrance
	Parking Zone (Interface Point #2)	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
			* Deny access to unauthorized persons	* Isolate zone from other vehicles and pedestrians using vehicle and people barriers
		* Protection of persons and property	* Respond to perceived threat	* Provide means for rapid response by security guards
	Building Entrance Zone (Interface Point #3	* Access control	* Detect and defend against unauthorized entry	* Designate continuous surveillance corridor * Provide lighting level for user identification * Provide people barriers to deny access to unaulhorized persons

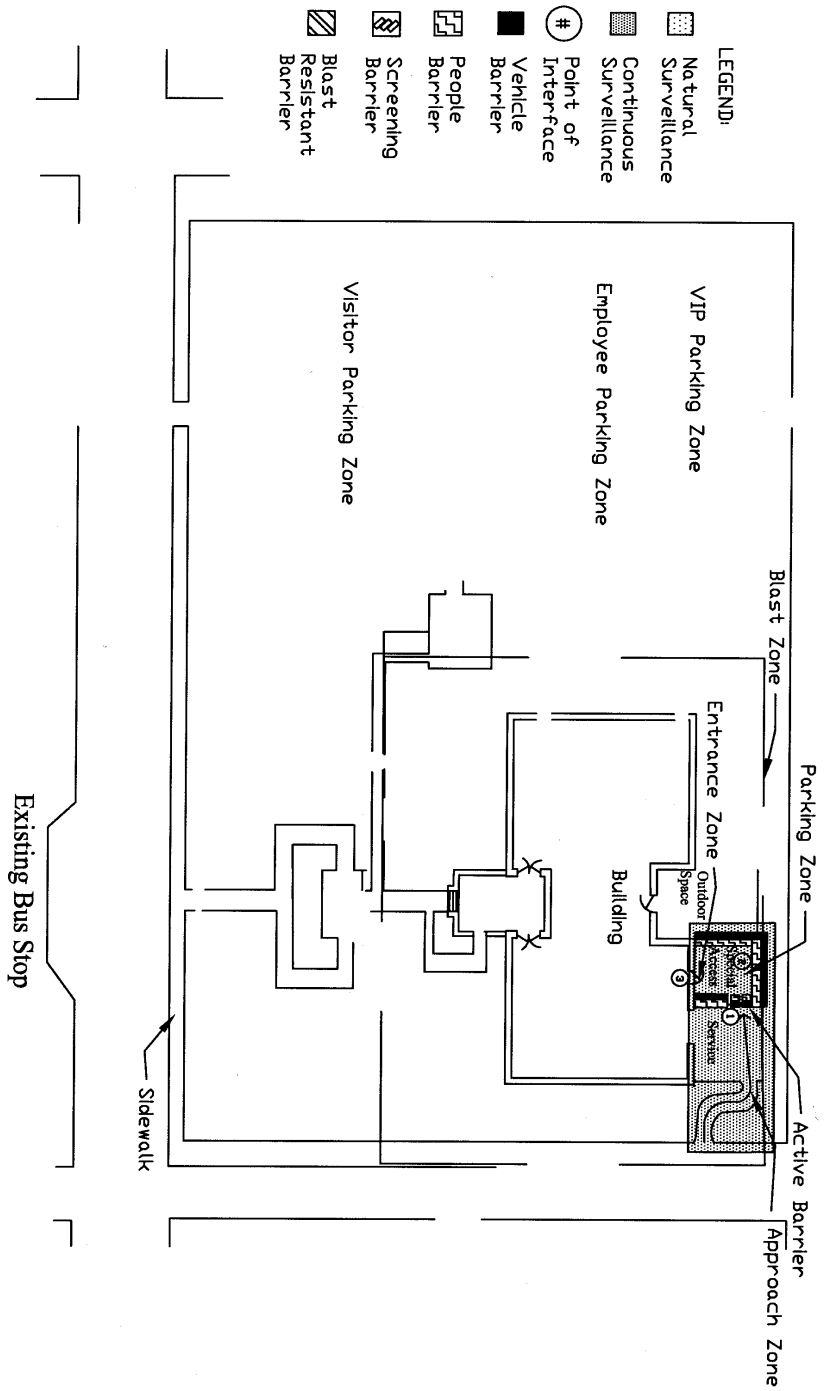
Approach Zone. The special user entrance should be designed with maneuvering space sufficient to accommodate the number and size of special users. A separate entrance allows security to be tailored to a particular user profile, e.g., users with prearranged security passes and/or access to magnetic card operated gates. Moderate control (M) is achieved by continuous surveillance, vehicle barriers, and procedural measures such as scheduled entrance. Vehicle barriers for this function can include deep curbs, road alignment to slow speed and channel traffic, antiram walls or fences, berms or ditches, or other obstacles to delay forced vehicle entry to the building. Depending on the risk assessment, interface point #1 may be configured as a fixed security post or a gate and it may be associated with a rapid response route from a nearby security post. The lighting level is similar to that for the visitor approach zone.

Parking Zone. Special user parking may be provided as surface or internal bays. High control (H) is achieved by the use of vehicle and people barriers to deny access to intruders. Depending on the positioning, vehicle barriers may include antiram walls or fences, berms or ditches, or other such obstacles to vehicle traffic. An active vehicle barrier allows access to authorized users only. People barriers include anticlimb fences or walls to deny access to all unauthorized persons to prevent property crimes such as vandalism, sabotage, or property theft. Depending on the selection, these barriers may also deny access to vehicles. The parking zone should have sufficient space for turning, backing, and parking. For facilities that have requirements for a sallyport to transfer high-risk prisoners, the sallyport itself may comprise a special user zone. A sallyport is a controlled entrance for high-risk activities such as the loading and unloading of prisoners. Continuous surveillance allows passive monitoring of users and response to suspicious persons or activities. Control at interface point #2 may be achieved by a fixed security post and/or by roving patrol. The lighting level should permit the image detection by visual or electronic means.

Building Entrance Zone. The entrance zone is a high control (H) area requiring access control. This is achieved by continuous surveillance and people barriers. Control of interface point #3 can be achieved by a fixed or temporary security post, access control mechanisms such as locks and

doors, and/or interior access control devices. The lighting level should be sufficient for user identification and evidence collection.

CHART 9 – SURVEILLANCE AND BARRIER PLANS FOR SPECIAL USERS



EXTRACT FROM CHART 3 — Point of Interface / Degree of Control	
	Street Zone
M / 1	Approach Zone
	Dropoff Zone
H / 2	Parking Zone
	Intercept Zone
	Emergency Zone
	Walkway Zone
H / 3	Building Entrance

4.5.7 Design Parameters for Street Pedestrian Users (See parts A, B, and chart 10)

PART A – DEVELOPING DESIGN AGENDA FOR STREET PEDESTRIAN USERS

User	Zone	Security		Design Agenda
		Goals	Objectives	
Street Pedestrian	Street Zone (Interface Point #1)	* Early warning	* Maintain natural Surveillance	* Designate natural surveillance corridor * Ensure street lighting level adequate for image detection
		* User control	* Detect and respond to unauthorized or suspicious activity	* Provide means for rapid response by security guards * Provide through passage for pedestrians and minimize occurrence of pedestrian generators that increase facility risk
	Approach Zone (Interface Point #2)	* Preliminary screening	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for user identification
			* Detect and respond to unauthorized activity or suspicious users	* Use people barriers to channel pedestrian traffic through approach zone
	Intercept Zone (Interface Point #3)	* See visitor in vehicle	* See visitor in vehicle	* See visitor in vehicle
	Walkway Zone (Interface Point #4)	* See visitor in vehicle	* See visitor in vehicle	* See visitor in vehicle
	Building Entrance Zone (Interface Point # 5)	* See visitor in vehicle	* See visitor in vehicle	* See visitor in vehicle

PART B - DESIGN OPTIONS FOR STREET PEDESTRIAN USERS

Street Zone. Events in the street zone that may serve as early warning can occur on the street and public sidewalk. The zone may have low or moderate control, depending on the risk. For low control (L) facilities, natural surveillance is used to detect suspicious activity such as an illegally parked vehicle. Security guards can respond to perceived threats in the street zone (interface point #1). For moderate control, natural or continuous surveillance and restrictions on activities that increase risk, such as street parking, vehicle stopping, loitering, mass transit terminals, street vendors, and other such activities may suffice. Such restrictions require coordination with local agencies.

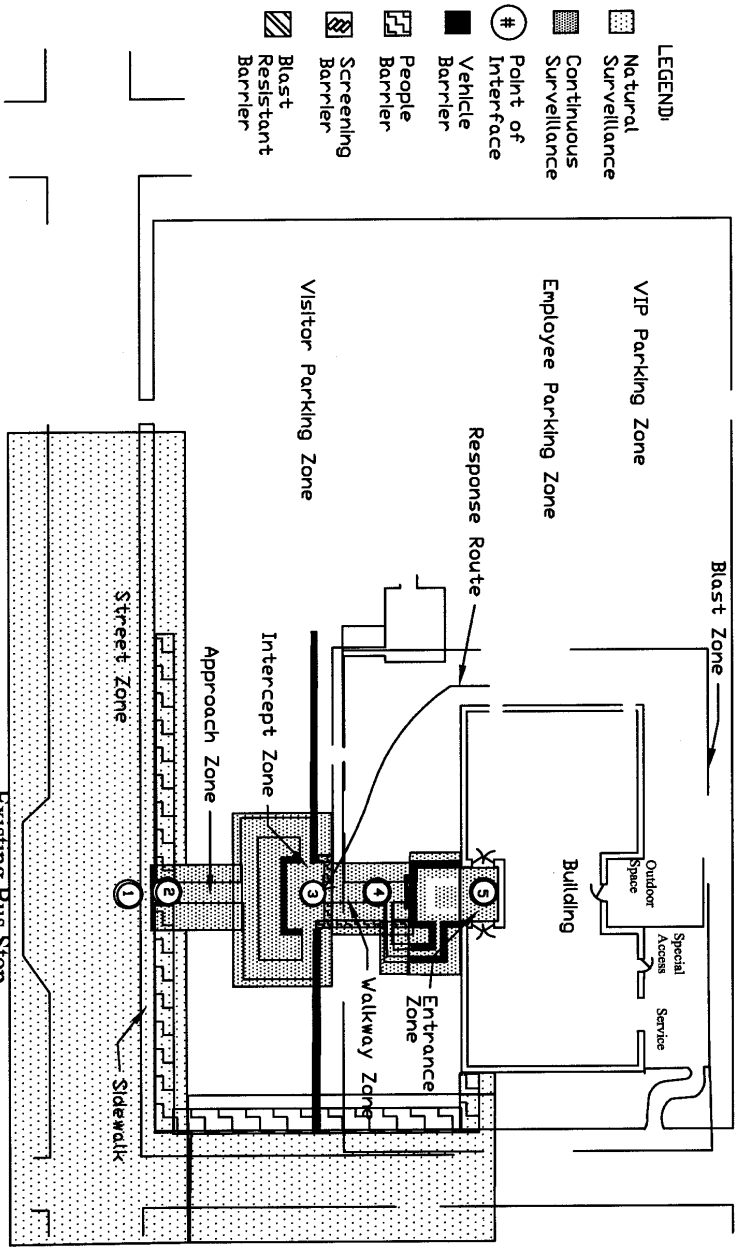
Approach Zone. Street pedestrian users include a mix of people such as visitors, tourists, employees, or other persons arriving at the facility on foot. These users are channeled from the street zone into the approach zone using people barriers. These include planting beds, low walls or fences, planted berms or ditches, and other obstacles that will delay foot passage. People barriers and continuous surveillance provide moderate (M) control. Depending on the risk assessment, interface point #2 may be configured as a fixed security post, roving security, a gate, or association with a rapid response route from a nearby security post. The lighting level permits security guards to detect the presence of vehicles or pedestrians in the zone by visual or electronic means.

Intercept Zone. The intercept zone serves as a high control (H) area for intermediate screening. The function and design of this zone is similar to that discussed for the visitor's in vehicle intercept zone. Interface point #3 may be configured as a change in elevation or a channeled path with right-angle turns or curves. These options can also be combined with vehicle barriers to deny vehicular access.

Walkway Zone. The walkway zone is a linkage between the intercept and building entrance zones. The moderate control (M) zone includes the walkway and stopping points along the route such as seating areas. The function and design of the walkway zone are similar to visitors' walkway zone, and is controlled at intercept point #4.

Building Entrance Zone. The entrance zone is a high control (H) area in which access control is achieved by continuous surveillance and barriers. Control is exercised from interface point #5 by a fixed security post, doors, and other security measures. At the entrance zone, users may be segregated according to user profile for building entry, for example, visitors and employees. A designated entrance may be assigned to correspond with the entry requirements of the user profile. Other design considerations for this zone are similar to those discussed for the visitor arriving by vehicle.

CHART 10 – SURVEILLANCE AND BARRIER PLANS FOR STREET PEDESTRIAN USERS



EXTRACT FROM CHART 3 / Degree of Control / Point of Interface	
L-M 1	Street Zone
M 2	Approach Zone
	Dropoff Zone
	Parking Zone
H 3	Intercept Zone
	Emergency Zone
M 4	Walkway Zone
H 5	Building Entrance

4.5.8 Design Parameters for Outdoor Space Users (See parts A, B, and chart 11)

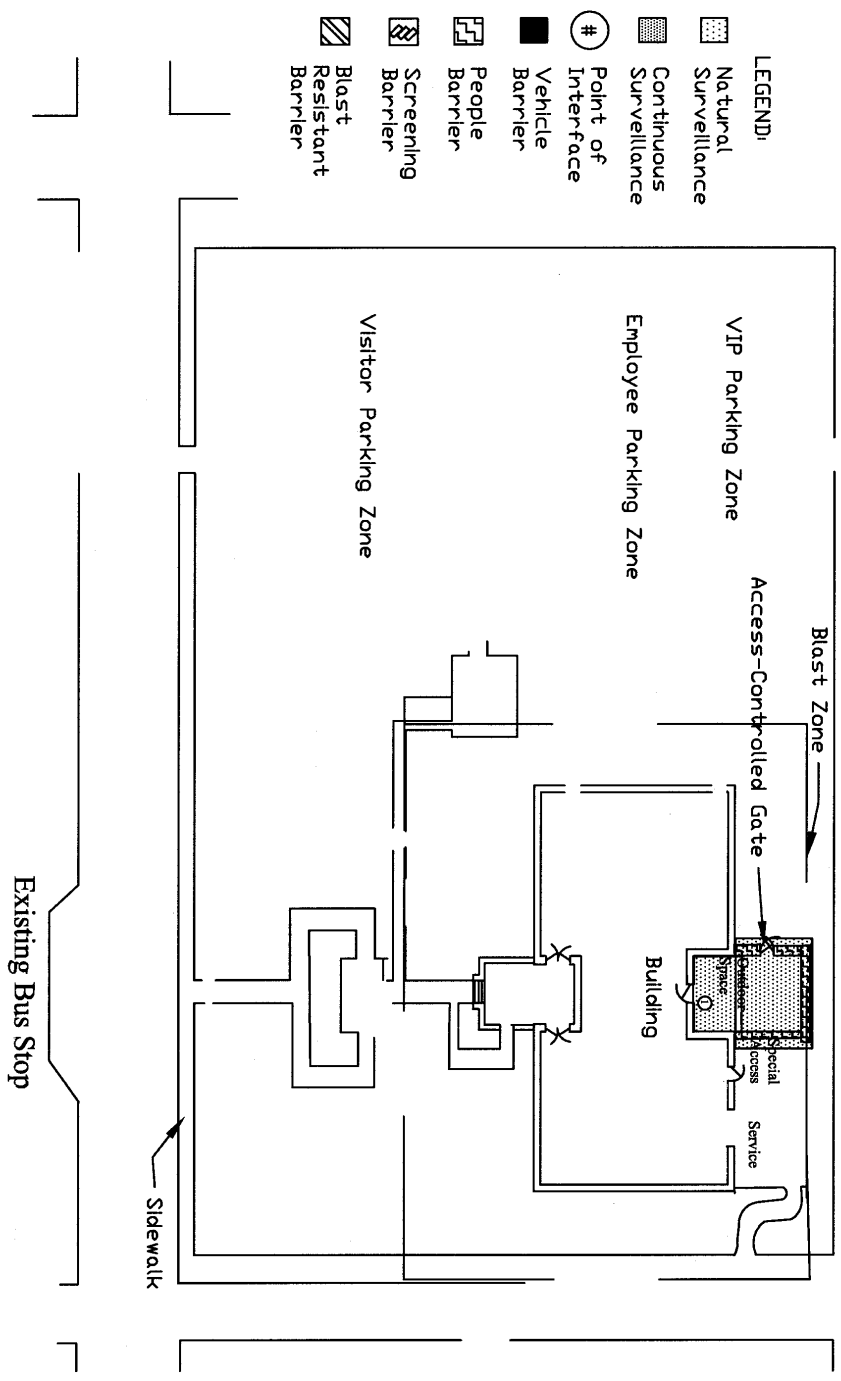
PART A – DEVELOPING DESIGN AGENDA FOR OUTDOOR SPACE USERS

User	Zone	Security		Design Agenda
		Goals	Objectives	
Outdoor Space Users	Building Entrance Zone Interface Point #1)	* Access control	* Maintain continuous surveillance	* Designate as continuous surveillance corridor * Provide lighting level for image detection
		* Safety to users	* Deny access to unauthorized users	* Provide social outdoor space for facility users at designated building entrances * Use people barriers to deny access to unauthorized users * Provide evacuation route using active people barrier

PART B - DESIGN OPTIONS FOR OUTDOOR SPACE USERS

Building Entrance Zone. Outdoor space uses include a variety of social spaces that may serve as a facility amenity. Examples include sitting, eating, smoking, and other gathering spaces not included as part of a walkway zone. Interface point #1 at the entrance zone is a high control (H) point requiring access control. This is achieved by continuous surveillance and people barriers. Continuous surveillance can be achieved using electronic means. People barriers consist of an anticlimb wall or fence with an access-controlled gate to allow for emergency evacuation. The lighting level should be sufficient for image detection.

CHART 11 – SURVEILLANCE AND BARRIER PLANS FOR OUTDOOR SPACE USERS



EXTRACT FROM CHART 3 / Degree of Control / Point of Interface	
	Street Zone
	Approach Zone
	Dropoff Zone
	Parking Zone
	Intercept Zone
	Emergency Zone
	Walkway Zone
H / 1	Building Entrance

4.5.9 Design Parameters for Adjacent Land Users (See parts A, B, and chart 12)

PART A – DEVELOPING DESIGN AGENDA FOR ADJACENT LAND USERS

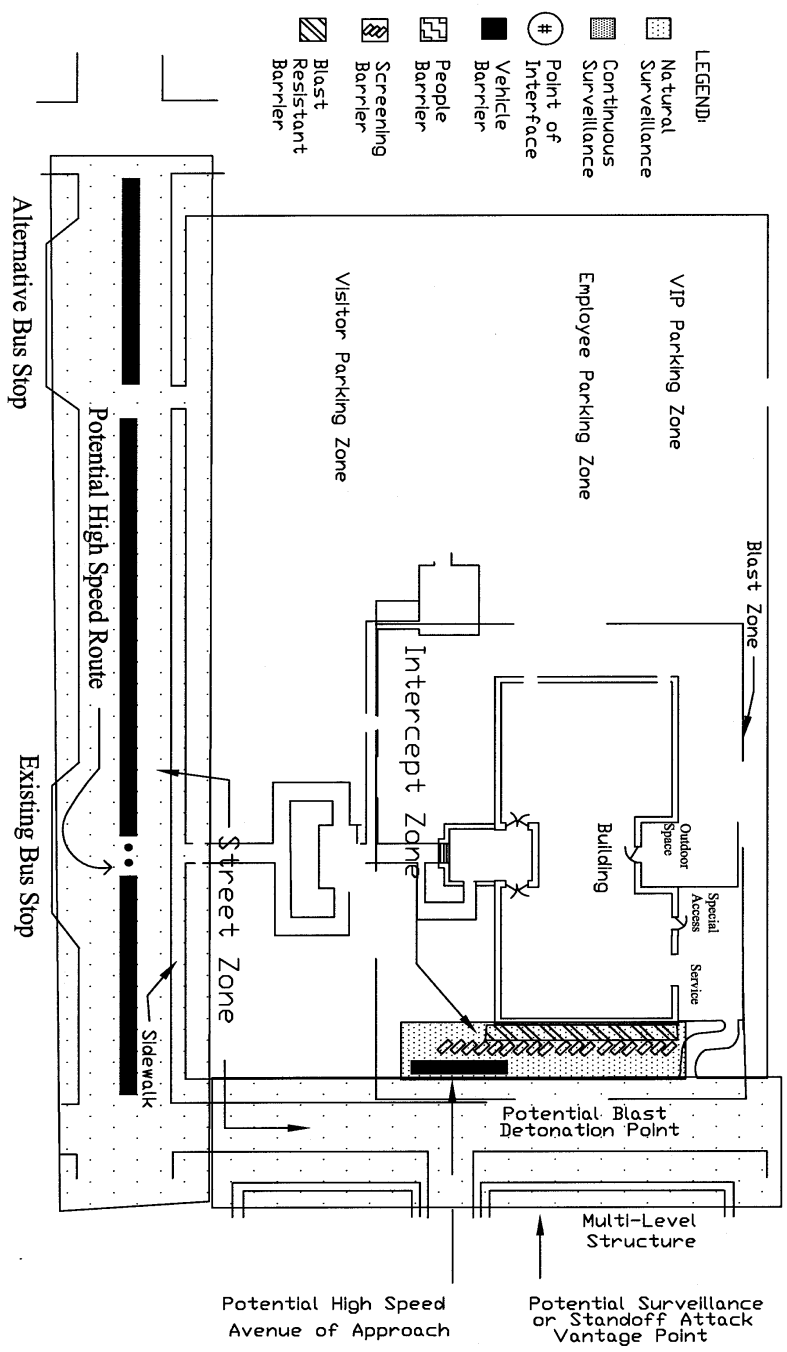
User	Zone	Security		Design Agenda
		Goals	Objectives	
Adjacent Land Users	Street Zone	* Early warning	* Maintain natural surveillance	* Designate natural surveillance corridor * Ensure street lighting level adequate for image detection
		* Access control	* Delay attempt for forced entry from zone	* Provide vehicle barriers to hinder high-speed avenue of approach from offsite
		* Protection of facility	* Minimize vulnerability to offsite risk	* Remove or relocate offsite risk generators
		* Safety to users	* Avoid security equipment and practices that can hinder or harm street users and adjacent land users	* Use street design and traffic control measures that provide safety and reduce interreference with users
	Intercept Zone	* Access control	* Maintain continuous surveillance	* Designate continuous surveillance corridor * Provide lighting level for image detection
			* Deny forced entry by vehicles	* Provide vehicle barriers to prevent high-speed approach from offsite land uses
		* Protection of facility	* Minimize vulnerability to blast	* Provide blast resistant barrier to minimize blast effects from offsite points
			* Minimize vulnerability to offsite vantage points that provide observation or attack means	* Provide screening barrier to obstruct line of sight from offsite vantage points

PART B - DESIGN OPTIONS FOR ADJACENT LAND USERS

Street Zone. Adjacent land users may have a variety of activities that can endanger the facility. Examples include land uses that promote trucking, sites that provide maneuvering space for high- speed approaches such as perpendicular drives or loading docks, wide streets without medians, streets with adjacent dropoff lanes such as bus stops, adjacent open spaces that allow vehicle maneuvering or hiding opportunities, vantage points for observation or stand-off attack by criminals or terrorists such as public-accessible multilevel rooftops or parking garages, and other possible risk generators. The street zone is a low (L) or moderate (M) control zone depending on the risk. Control is achieved by natural surveillance and vehicle barriers. In some cases, control can be achieved by relocating or removing a risk (such as a bus stop) to a more favorable site. Vehicle barriers for control include elevated or deep curb medians, street planters, bollards, trees, light standards, reinforced benches, or other obstacles that can of delay high-speed vehicular access from the street. Coordination is effected with local agencies for use of vehicle barriers and to ensure the lighting level is sufficient for image detection.

Intercept Zone. The intercept zone protects the facility from offsite land uses that may provide vantage points for criminals or terrorists. High control is achieved by vehicle barriers, screening barriers, and/or blast resistance barriers such as blast-hardened walls or free-standing blast walls. Screening barriers may consist of walls, fences, tall shrubs or trees, lower-risk buildings, or other obstructions to the line of sight from potential offsite vantage points. Blast-resistant barriers are used to mitigate vulnerability to blast when the street, street parking, open spaces, or other uncontrolled spaces fall within the blast zone.

CHART 12 – SURVEILLANCE AND BARRIER PLANS FOR ADJACENT LAND USERS



EXTRACT FROM CHART 3 — Degree of Control / Point of Interface	
L-M	Street Zone
	Approach Zone
	Dropoff Zone
	Parking Zone
H	Intercept Zone
	Emergency Zone
	Walkway Zone
	Building Entrance

4.6 IMPORTANCE OF SURVEILLANCE PLAN AND BARRIER PLAN

This thesis proposed that there are two elements that are fundamental to the prudent integration of security and design. These are the surveillance plan and the barrier plan. These documents occur as end products of the program phase of site planning and design. Created by the landscape architect, each plan is a composite overlay showing key design agenda produced for all user zones that is necessary for effective integration. The security consultant reviews these documents and identifies gaps in coverage. After the design team accepts these plans, the security consultant uses the information to determine equipment and personnel requirements. The landscape architect uses the graphic plans to guide design development. For example, areas where plantings will be restricted by surveillance requirements are readily identifiable on the surveillance plan. Similarly, the landscape architect uses the barrier plan to determine the need for and placement of walls and fences and grading to create berms as well as other ways to meet barrier requirements. Engineers study the barrier overlay to identify the plans' impact on structural building requirements. For example, coordination between the engineer and landscape architect for a freestanding wall may lessen the structural hardening of the building. While these plans provide vital information, they do not mandate design. Rather, they are guide the development of secure and desirable site designs. An activity area or a linkage may be modified during design development to improve either a security or design function. For example, an entrance drive may be shifted to better meet a surveillance requirement; at the same time a route may be found that also makes the site more welcoming. Such changes must always comply with the security goals and objectives of the zone.

The composite surveillance and barriers plans for the site example are shown in charts 13 and 14.

CHART 13 – SURVEILLANCE PLAN FOR EXAMPLE SITE

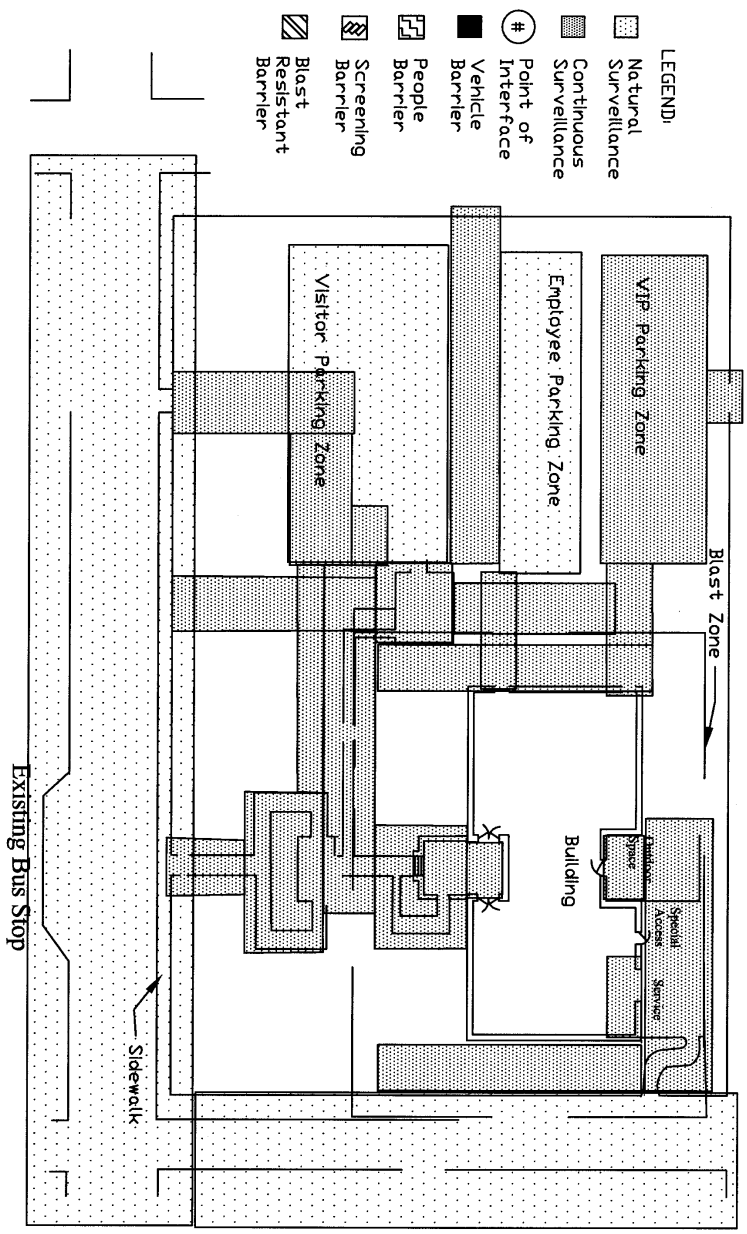
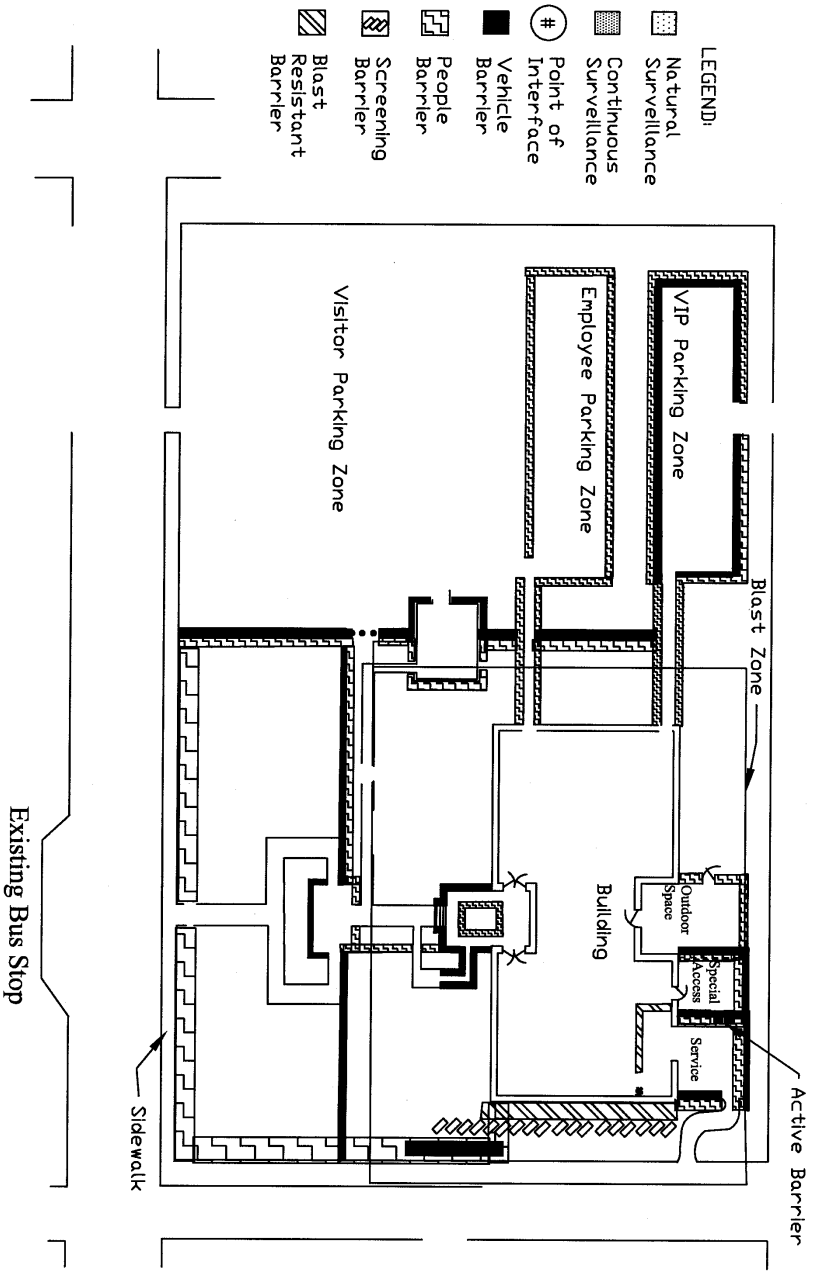


CHART 14 – BARRIER PLAN FOR EXAMPLE SITE



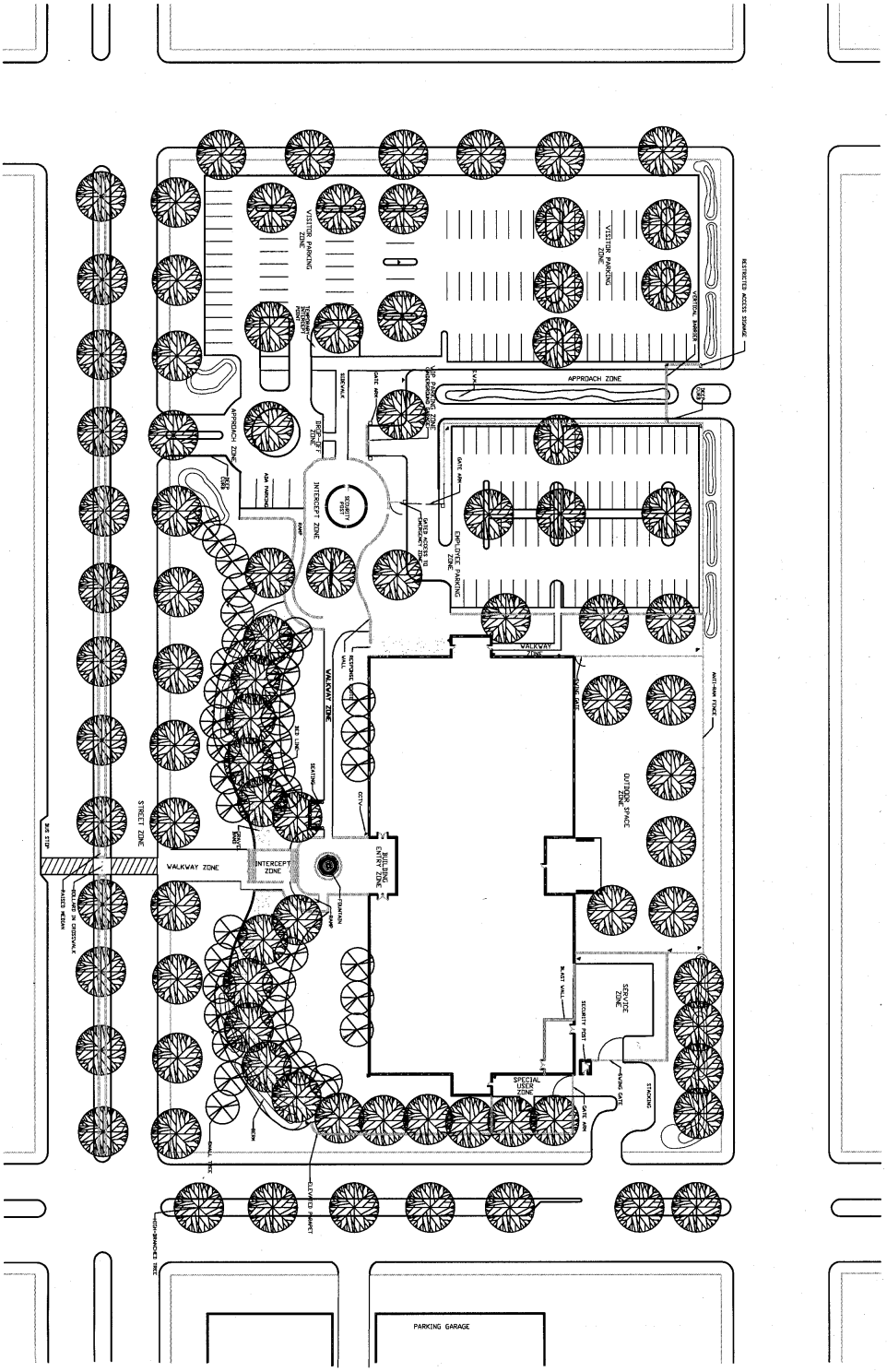
4.7 APPLICATION OF DESIGN PARAMETERS

This section provides a proposed schematic site design that demonstrates the concept of design parameters proposed by this thesis. Chart 15 is one design solution to fulfill the security goals and objectives identified for the example site used in preceding discussion. Although the example is hypothetical, it addresses issues that are frequently encountered in antiterrorism planning.

For this problem, the design is a new project in a typical urban grid setting. The client's needs require safeguard to protect intended users from risks associated with terrorists. The intended users include visitors who will be arriving by vehicles and on foot. Provisions for employee and very important person parking are required, as well as service accommodations. The topography will require grading to achieve accessibility for disabled users. In this situation, the architect and landscape architect sited the 4-story building to take advantage of grading, parking, and other planning concerns. The client desires sufficient outdoor space for employees' leisure and recreation. The client accepts security posts, but desires to minimize the number and signature of such elements.

The design team followed the design process described in this thesis. Chart 2 represents the activity and linkage functions identified by the landscape architect. Chart 3 depicts the design program audit that responds to this case. Chart 15 incorporates the surveillance and barrier plan produced by the design agenda in paragraph 4.6. The design solution for each user zone follows the chart, along with photographs to convey the design intent. In the solutions, security requirements do not dictate design nor do they impose a fortress appearance. Rather, the integration of security and design allows the development of a secure and socially acceptable site. Similar results are achievable by using the programming process described in this thesis.

CHART 15 – SCHEMATIC DESIGN FOR EXAMPLE SITE



4.7.1 Design Solution for Visitors in Vehicles

Approach Zone. The design agenda for this zone stated the requirement for vehicular control of visitors entering the site. Key agenda were to prevent a high-speed vehicular assault, slow traffic, and allow continuous surveillance. A point of interface between visitors and security should be established in the zone. Using this guidance, the scheme for the approach zone evolved as follows.

Visitors proceed through a traffic circle that pleasingly slows their speed, routes them past a nearby security post, and directs them to an offset parking area. Deep curbs and berms flank the roadway to subtly keep visitors in vehicles outside the blast zone. Figure 4 illustrates a similar deep curb. The ramp providing ADA access doubles as a vehicular barrier. Disabled users have the convenience of close-in parking and dropoff amenities without jeopardizing site security.

High-branched trees were placed to provide design interest without interfering with line of sight in the zone. Landscaping in the medians and other spaces in the zone are to be planted with ground cover or grass. (These are not shown due to the scale of the drawing.) The security post is positioned near the approach zone to allow visual screening and rapid response when interception is deemed necessary. The post's offset placement, however, reduces the security signature. Site image is further maintained by integrating the security post in an architectural element such as the one shown in figure 5. A temporary intercept point is provided for use when threat conditions warrant. In such situations, space is provided for guards to stop and inspect a vehicle. The traffic circle affords space for waiting vehicles and turn-around opportunity during these times.

The above design evolved from the design agenda that manifested during the planning process of the design team. The functions of the rectangular approach zone formulated during planning were subsumed into a traffic circle configuration without a compromise of security. The design adapted landscape elements to meet the design agenda in a user–friendly environment.

Figure 4 – Deep Curb

Figure 5 – Architectural Security Post Facade

Parking Zone. The visitor parking zone is positioned outside the blast zone as depicted in the development of the design agenda. Ninety-degree angled parking stalls are oriented for optimum surveillance along the travel lanes of the zone. This perspective allows visual surveillance of vehicular and pedestrian movement in the travel lanes from the security post. Parking medians were positioned to break up the expansiveness of the parking area, to provide opportunity for high-branched shade trees, and to afford an opportunity for CCTV points to augment visual surveillance of the more distant parking areas. The parking layout provides for easy detection and response by roving security guards. In this example, an assumed low crime rate did not warrant enclosing the zone with a people barrier.

Visitors walk to a central pedestrian walkway leading to the building entrance. The walkway and landscaping is designed to allow passive monitoring of the visitors throughout this journey. Visitors are isolated from other users in a pleasing but effective manner using landscape design.

.

Intercept Zone. The primary design agenda for the intercept zone are to deny vehicular access into the blast zone and to afford an intercept point for remote screening of visitors walking to the building entrance. A stormwater management (SWM) element and a deep curb along the edge of the employee parking zone fulfill the vehicular barrier requirement in a subtle but effective manner. Figure 6 illustrates an example of the SWM element envisioned for this site. These same discourage passage by visitors departing the parking zone on foot and encourage the use of the pleasing walkways leading through the intercept zone. Attempts to bypass the intercept zone will be detected by CCTV and/or visual surveillance from the security post. As visitors near the security post, they are channeled by low walls such as shown those shown in figure 7, allowing close-in screening by guards. The security post is enclosed in one-way glass to further reduce the security signature.

Figure 6 – Stormwater Management Barrier

Figure 7 – Barrier Walls

Walkway Zone. The walkway zone channels visitors from the parking zone to the building entrance without opportunity for infiltration by other users. A broad planting bed about 50 feet in width flanks an open walkway corridor. This planting bed consists of small low-branched trees, dense plantings of woody shrubs, vine-type ground covers, and a backdrop of high-branched trees. As shown in figure 8, this design produces a visually pleasing scene that enhances the arrival experience of visitors. Seating areas offer additional welcoming amenities. Low plantings along the building façade, such as those suggested in figure 9, prevent hiding places or surveillance obstructions.

Figure 8 – Planting Bed Barriers

The dense planting bed presents a barrier that is undesirable to foot passage. A band of gravel similar to that shown in figure 10 is placed in the bed to reinforce the barrier. The audible signature of movement through this gravel will alert guards. This planting bed composition adequately contains users to the authorized zone and delays infiltration by unauthorized users. A clear corridor is maintained along the walkway zone to facilitate the safety of users and continuous surveillance. The walkway and seating areas are strategically aligned with the security post and CCTV coverage for easy surveillance. A guarded, direct route allows rapid response of security forces from interior security posts.

Figure 9 – Planting for Line of Sight

Figure 10 – Band of Gravel

Building Entrance Zone. Access control is the primary security function of the building entrance zone. This is achieved by continuous surveillance, slow approach, and barriers to forced entry.

The design example employs elevated surfaces as barriers and channeling devices. The steps and ramp leading to the elevated terrace form the perimeter of the zone. The low antiram wall surrounding the fountain presents an obstacle to a high-speed approach. The fountain channels visitors while affording an attractive visual and audible amenity. Figure 11 illustrates a typical fountain structure.

Figure 11 – Fountain Structure

4.7.2 Design Solution for Employees in Vehicles

Approach Zone. The design agenda for this zone require smooth controlled access for routine use by employees. In this design, an extended approach zone is provided to accommodate vehicle stacking. While employees pause to engage the card-activated gate arm, security guards have the opportunity for visual recognition from the nearby post. CCTV along the approach zone affords early warning and rapid response to perceived threats or suspicious vehicles.

Intercept Zone. The intent of the intercept zone is to deny vehicular access into the blast zone and to afford an intercept point screening of employees. The design places the intercept zone prior to the parking zone. Although this layout is different from the functional plan derived during the planning process, the design agenda elements are accomplished. Employees progress through passive screening by CCTV in the approach zone. The point of intercept occurs as employees pause to activate the gate arm that controls access to the parking zone. This arrangement allows security guards to conduct visual recognition from the nearby post and to interrupt employee movement only when required. The gate arm and deep curb deny employees access into the blast zone prior to screening.

Parking Zone. The design agenda for this zone requires isolation of users, barriers to prevent vehicular penetration into the blast zone, and provisions for rapid security response. An antiram fence similar to figure 12 encloses the zone and doubles as a vehicle and people barrier. Since the parking zone is within the blast zone, 5-foot high wall is used to mitigate effects should a bomb be detonated in an employee's car. Added blast protection results from the vertical barrier in the approach zone that denies access to van and trucks that can carry large explosives. A turn-around is provided for vehicles exceeding the height limit.

Figure 12 – Antiram Fence

Walkway Zone. Employees are channeled to a separate entrance that is isolated from other users. CCTV outside the building entrance allows security guards to confirm an employee by visual recognition without disrupting their daily routine.

Building Entrance Zone. Access control is the primary security function of the building entrance zone. This design achieves this agenda by allowing continuous surveillance and by using card-activated doors.

4.7.3 Design Solution for Very Important Persons in Vehicles

Approach Zone. Design agenda for this zone specify a separate entrance, access control, and expeditious screening. In this design, the approach zone is shared with employees. This alternative meets the security requirements implied by a separate entrance using a defense layer consisting of a warning sign, CCTV, and a vertical barrier. The warning sign identifies the entrance as restricted access. Guards use CCTV to confirm the identity of VIPs in the approach zone and to monitor their movement to ensure their safety. The vertical barrier limits the size of authorized vehicles that can physically enter the zone. This final section of the approach zone segregates employees from VIPs prior to entry into the parking zone.

Parking Zone. The design agenda for this zone requires isolation of users and continuous surveillance. Unauthorized users are denied access to an underground parking structure by a gate arm that is under continuous surveillance from the security post. VIP identity is accomplished by the use of the card-activated gate arm, and it is confirmed by security surveillance. The single point of entry to the parking zone requires the negotiation of a sharp turn, preventing forced entry attempts.

Walkway and Building Entrance Zones. An underground tunnel is used to link the parking zone to the building entrance. In this manner, VIPs remain in a secure corridor, lessening the need for subsequent access control.

4.7.4 Design Solution for Service Providers in Vehicles

Street Zone. A turning lane satisfies the requirement for traffic safety of service vehicles entering the site. High-branched trees enable drivers to maintain lines of sight when entering and exiting the site. The security post enables guards to conduct natural surveillance of the zone while performing other security functions assigned to the post.

Approach Zone. Service traffic is channeled on a reverse curve drive before arrival at a security gate. A berm and antiram wall prevent a forced entry into the service area. The approach zone has sufficient space to allow vehicles to wait for security checks.

Parking Zone. A clear space is maintained between the wall enclosing the parking zone and the tree plantings in order to prevent aggressors from using the tree branches as a climbing aid. Since the parking zone is within the blast zone, a blast-resistant wall forms the façade of this section of the building. The security post is positioned to allow continuous surveillance of the parking zone.

Building Entrance Zone. The building entrance zone is enclosed with a blast resistant wall. The proximity of the security post ensures the zone is secure at all times.

4.7.5 Design Solution for Emergency Responders in Vehicles

Approach Zone. The site design should provide expeditious access for emergency responders without jeopardizing the remainder of site security. This design accomplished this agenda by placing a drop curb and a swing gate in close proximity to the security post. Security guards open the gate to allow emergency responders to enter the blast zone in emergency situations such as rescue or fire.

Emergency and Building Entrance Zones. Clear space along the façade of the building provides emergency responder routes to each major building entrance.

4.7.6 Design Solution for Special Users

Approach Zone. The approach zone for special users is collocated with that of service users. This allows the security post to simultaneously control access and function as an intercept point for both the special user parking zone and the service provider parking zone.

Parking and Building Entrance Zones. The special user parking zone is positioned along the side of the building to take advantage of the security provided by the wall and screening located in that area. A gate arm controls access to the parking zone. Ample space is provided for maneuvering of vehicles. The layout allows for continuous surveillance of the parking zone and the building entrance using CCTV and/or mirrors.

4.7. 7 Design Solution for Street Pedestrians

Street Zone. The design agenda for the street zone necessitate provisions for natural surveillance and limitation of pedestrian street activity. The street frontage of the site is designed as a clear space to facilitate surveillance. High-branched trees along the street contribute to the site image without blocking lines of sight. CCTVs are employed to maintain passive surveillance of pedestrian traffic along the public sidewalk.

Approach Zone. Pedestrians are channeled to a central walkway by use of planted berms and walls. These barriers also prevent vehicular assault along the street frontage. The width of the ramp providing ADA access is limited to 5 feet to prevent its use by a vehicle. A clear space along the length of the walkway ensures continuous surveillance.

Intercept and Walkway Zone. Opportunity for intercept occurs as pedestrians slow to transit the two sets of steps in the approach zone. Security guards use visual or CCTV means to detect suspicious persons or activities. The surrounding walls and plantings establish a subtle but effective perimeter in which security guards can contain a threat.

Building Entrance Zone. The building entrance zone functions as described previously for the visitors arriving in vehicles.

4.7.8 Design Solution for Outdoor Space Users

Building Entrance Zone. A large open space fulfills the agenda for controlled social space and evacuation. A fence similar to that depicted in figure 13 achieves control of the space. The fence has sufficient height to delay penetration. The people barrier is reinforced by a clear space to prevent climbing aids and ensures continuous surveillance. The fence design avoids intermediate supports that could also aid climbing. A locked gate provides an emergency evacuation exit from the site when required.

4.7.9 Design Solution for Adjacent Land Users

Street Zone. The design agenda specify control of adjacent activities that could jeopardize the protected site. A street median was installed to limit high-speed vehicular assaults from offsite points. A median such as the one depicted in figure 14 contributes to the site image while posing an obstacle to pedestrian and vehicular traffic.

Intercept Zone. The site design should mitigate the risk of forced entry attacks and information gathering by potential aggressors from offsite vantage points. In this example, the intercept zone consists of an elevated parapet and high-branched trees to offset the shallow setback along the side of the building near the street. Figure 15 illustrates the kind of elevated parapet envisioned for this site. This vertical structure will serve as a blast-resistant wall. The elevated surface enhances the use of trees for screening from observation by persons at offsite vantage points such as the parking garage.

Figure 13 – People Barrier

Figure 14 – Street Median

Figure 15 – Elevated Parapet

4.8 CONCLUSION

Chapter 4 demonstrates that the use of design parameters can be effective tools to guide the schematic design of security-sensitive sites. The chapter shows how security goals and objectives are used to generate design agenda. The surveillance plan and barrier plan derived from the design agenda were used as a framework to guide design development. The functional intent of the agenda influenced design decisions, but did not instill rigid rules. A careful analysis of the schematic site design proposed in chart 15 reveals the presence of the surveillance and barrier overlays.

Deriving a design solution that is attentive to the requirements of specific user zones succeeds in developing a secure design. In the proposed design solutions to the example site, the form of the zones was changed to achieve a desirable site image without compromising the design agenda. This demonstrates the need for flexibility when integrating security and design. Such flexibility allowed a reduction in the security signature of the barriers. It maintained defense in depth, but avoided the need for bulky ill-placed barriers. This design demonstrates

that by finding a balance between the need for visible deterrence and the need for a desirable site image a secure but welcoming site evolves.

Chapter V

SUMMARY AND CONCLUSIONS

5.1 A PLANNING PROCESS FOR ANTITERRORISM PRACTICES

This study has proposed the creation of two new tools instrumental to prudent integration of security and design: the surveillance plan and the barrier plan. These documents are end products of the program phase of site planning and design.The paper recognizes the importance of integrated planning by the design team. The thesis makes two significant contributions to a challenging task plaguing the design and security professions. First, the proposed method fills a current void in the literature since it shows step by step exactly addressing how to achieve integration of site design with physical security. This was accomplished by combining the tools of the landscape architecture profession with physical security principles and crime prevention through environmental design concepts. A procedural flowchart was used to that critical points of collaboration in the planning process. The traditional design tool commonly referred to as programming was suggested as a mechanism to merge goals and objectives of the client, security enforcers, and designers. The thesis showed how the integration of design and security can actually occur and gave examples of proposed group output documents to guide design development. The method will enable the design team to better integrate their respective skills and tools to achieve synergistic results.

A second major contribution of the paper is the establishment of the landscape architect as a vital member of an antiterrorism design team. This role emerged from wide recognition of the need to minimize the damage to site images in the process of establishing physical security. The paper describes how landscape architects can use their experience in creating and modifying site design to meet user needs. This role is an integral part of a proposed antiterrorism strategy that organizes security efforts according to risks specific to each group of users. The paper discussed how a landscape architect’s understanding of the functional and social requirements of a site can contribute to the development of desirable site images with built-in physical security.

5.2 ANALYSIS OF THE PROPOSED PLANNING PROCESS

The purpose of the proposed planning process is to counter terrorism in a more effective manner than current practice. The landscapes of many sensitive public and private sites are being fortified with an intrusive and seemingly omnipresence of security. In many instances, recent efforts have transformed the perimeters of some facilities into "frightened architecture." (deBecker, 1999) Perimeters have been lined with 10,000-pound planters and reinforced bollards. Technological solutions such as improved structural methods, blast-resistant glass, and electronic surveillance and intrusion systems are costing billions. Security improvements to the World Trade Center alone cost sixty million dollars. (Karpiloff, 1999) Routine users such as employees and the public can hardly miss the telltale signs of this security at places that were once open and welcoming. A recent Washington Post article describes the situation occurring in Washington DC, as, "a capital under siege." (Wash. Post, 1999)

This paper proposed a planning process that integrates site design with physical security and crime prevention through environmental design. The method will not only improve the effectiveness of antiterrorism, but it helps reverse the current trend described above. This alternative has the potential to reduce not only financial costs, but social costs as well. Such effectiveness is attainable by recognizing that site design is a tool that can lessen the need for unnecessary visible signs of security. Landscape architects have a premier role in implementing this process.

The planning process presented in this thesis is conceptual. The method evolved from a perspective founded on research and experience in both physical security and design. The findings and lessons were applied in the schematic site design presented in chapter 4. The hypothetical situations solved in that design are typical of those posed by many existing sites. A measure of the success of this design can be made by comparing photographs of typical existing semi solutions with the alternatives proposed by the schematic site design.

Landscape architects recognize that a visitor's first impression on at site is an important aspect of site design. Figure 1 depicted the vehicular entry to the U.S. Capitol. Security is afforded by large bulky planters intended to channel vehicles and prevent a forced entry into the

site. This is typical of security posts found at many existing sites. Figure 16 compares the existing solution at the Capitol with an image similar to that conveyed in the example schematic site design. By using a barrier plan to outline the type and relative location of barriers at an entry, the landscape architect is able to develop a secure and desirable solution. The schematic design shows hypothetical entry which uses a curved road layout, deep curbs, berms, and an ADA ramp to achieve channeling. Curved entrances lower the speed of the vehicle so that bulky obstacles are not required. Thus, effective channeling can be done using subtler and less expensive methods. Integrating design and security enables the security post to be embedded in an architectural element so as to make it almost disappear into the pattern as "part of the woodwork." Such techniques have also proved successful in lessenig the security signature at Disney World. (Clarke, 1992, p250)

Landscape plantings are common site design amenities. Landscape architects are well trained in selecting and positioning such plantings in a manner that meets user needs. By proper integration, their experience can be used to avoid situations such as the one depicted in figure 17. Conflicts between design and security can be prevented during planning by use of a surveillance plan that outlines line-of-sight requirements. The design solution in the figure is more effective because it avoids redundant security posts and surveillance equipment. The reduced security signature also prevents the social costs associated with a fortress appearance.

The selected examples used for comparison reveal a viable alternative to current antiterrorism practices. Surveillance and barrier plans can be valuable tools to guide design development. They enable planners to concentrate security where it is needed. The design agenda produced while developing these output documents gives designers the flexibility to choose among various design elements to satisfy security requirements. As a consequence, site design itself becomes a valuable physical security tool. Landscape architects possess vast experience in using site design to attain functional and social objectives. Therefore, it stands to reason that landscape architects should be vital members on an antiterrorism team.

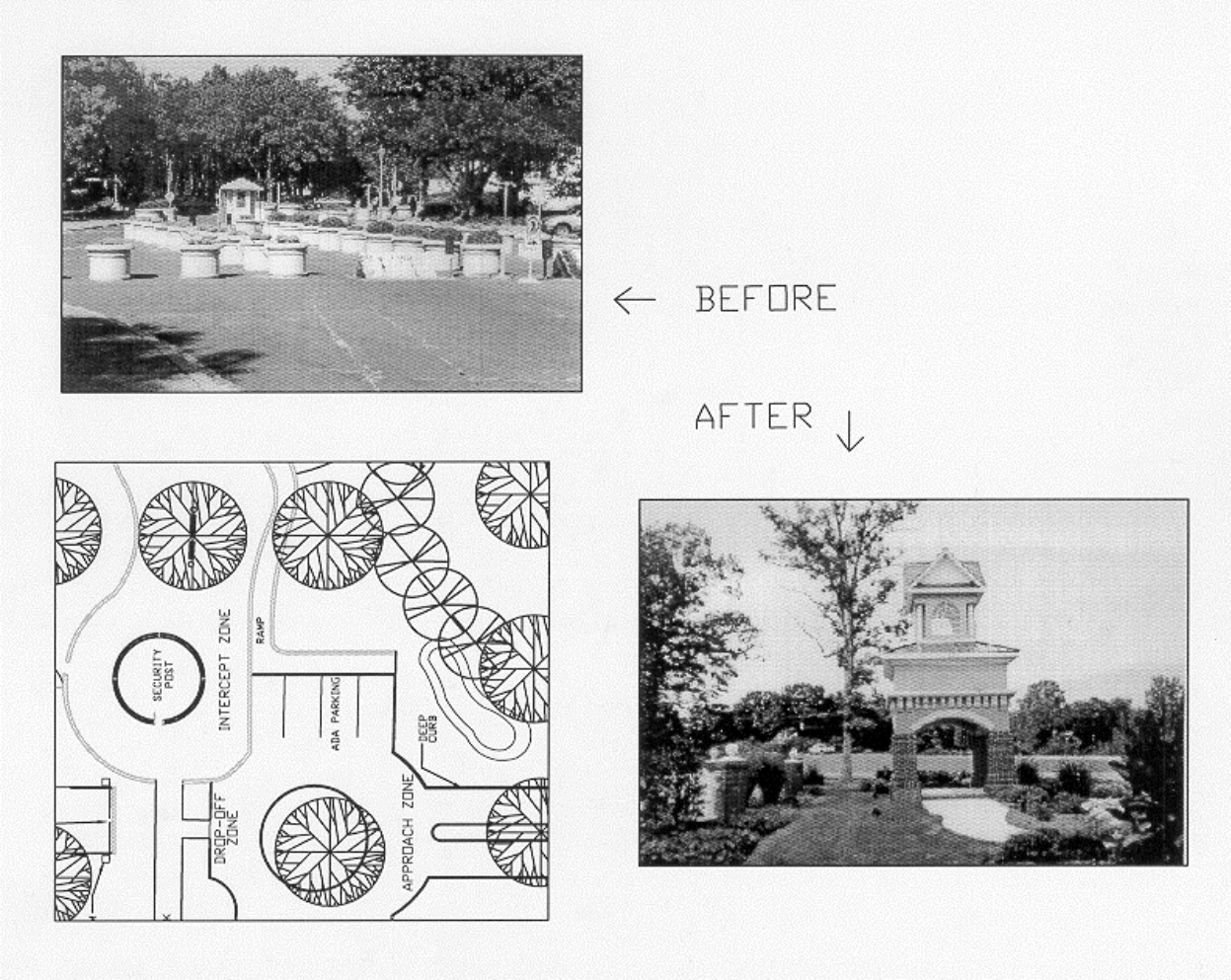


Figure 16 – Comparison of Barriers

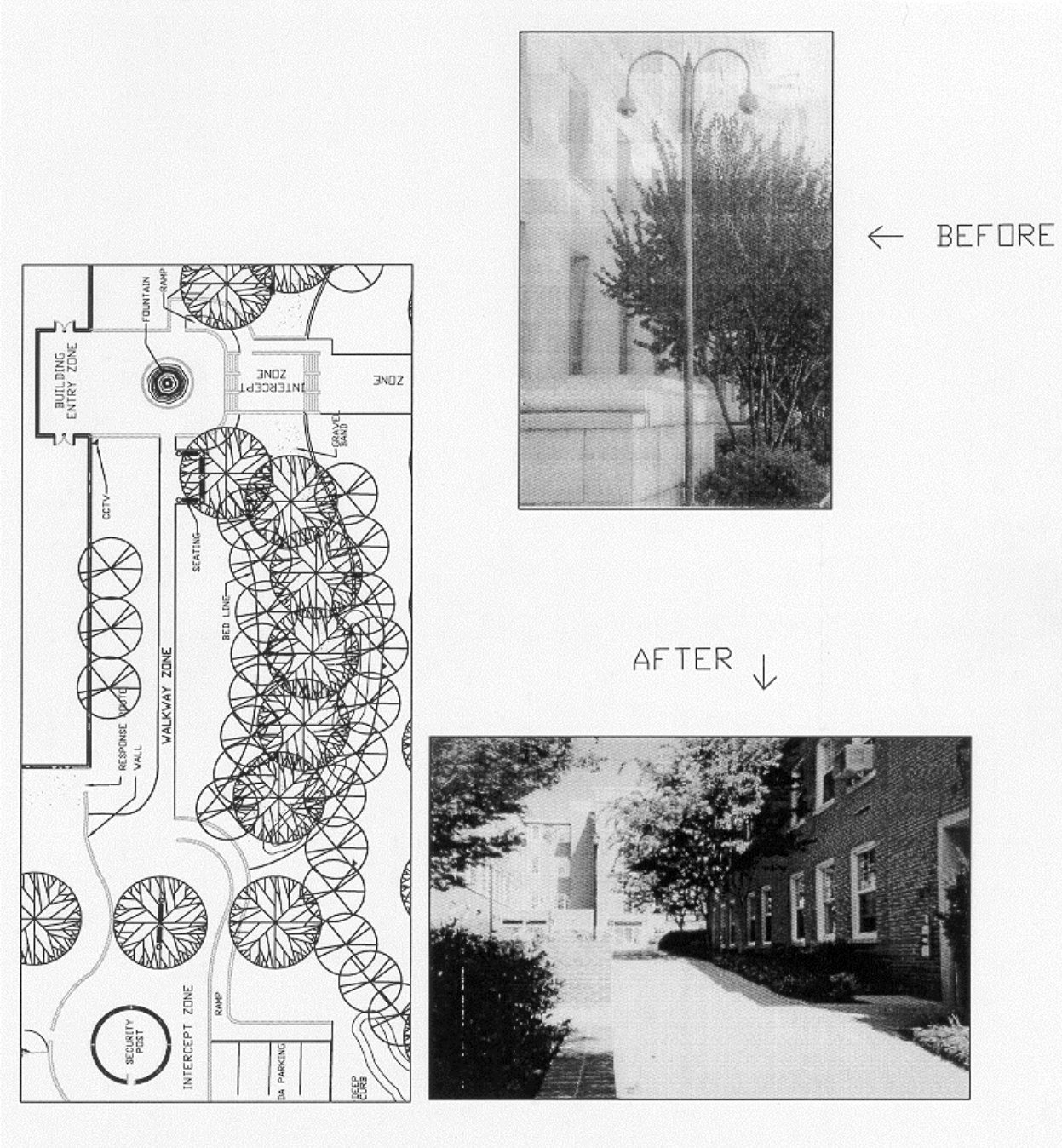


Figure 17 – Comparison of Surveillance

5.3 SIGNIFICANCE TO THE LANDSCAPE ARCHITECTURE PROFESSION

The need for increased security to counter terrorism and other crimes is an unfortunate, but necessary reality. As such, security should become an integral design program requirement for any site design intended for public use. The successful integration of security and design requires a unique skill set. Landscape architects who are trained in physical security and crime prevention through environmental design have an advantage in the transformation of security goals and objectives into design agenda. The development and marketing of such skills has the potential of launching a new specialty within the landscape architecture profession.

The landscape architecture profession is a dynamic field with many facets, ranging from environmental to urban design issues. This thesis has identified another viable niche for landscape architects. A respected practicing security consultant acknowledged, "I know of only a handful of landscape architects that understand security concerns." (Strauchs, 2000) With successful marketing, landscape architects can potentially become leaders in the new and challenging field of security design. This added skill can be combined with their previous repertoire of site design tools to give landscape architects to ability to better preserve the social desirability aspects of a site without sacrificing security.

5.4 RECOMMENDATIONS

In order to capitalize on the professional opportunities suggested by this study, several tasks are recommended. The landscape architecture profession should conduct a training seminar aimed at promoting security design. The forum should inform and encourage practicing landscape architects to seek design opportunities involving physical security. Second, a marketing program should be launched by the profession aimed at the inclusion of landscape architects on design teams involving security issues. The effort should be directed towards government, commercial, and private clients. Security consultant firms should be informed of the help that landscape architects can provide in solving security issues. Finally, education and training in physical security and crime prevention should become required courses in landscape architecture education programs. A course in "Crime Prevention Through Environmental Design" (CPTED) could inform future landscape architects on their roles in reducing crime. Elective courses or seminars in physical security should include security lighting, security

fencing, and the employment of electronic security devices such as closed-circuit televisions and detection sensors. Collectively, the fulfillment of these recommendations can enhance the profession by establishing landscape architects as key members on future design teams tasked to integrate design with security.

Appendix A

THREAT TACTICS

Security experts agree that understanding a threat is essential to establishing an effective defense. " A knowledge of the adversary could reveal vulnerability to various forms of defense and counterattack." (Kellen, 1982, p3) Accordingly, familiarity with terrorist tactics is an important part of the antiterrorism planning done by a design team. The knowledge forms common ground upon which each team member can stand to make an individual contribution to achieve a synergistic effect. This section aims to provide a framework for understanding terrorist tactics.

Terrorists are capable of a wide range of tactics and weapons to attack targets important to their cause. Past terrorist incidents involved the use of guns, explosive or incendiary bombs, and sophisticated detonating mechanisms. Tactics also include actions such as hostage taking or kidnapping. However, since "bombs account for 70 percent of all terrorist attacks," this discussion will focus on that threat without forgetting the remaining 30 percent. (VDES, 1999, p3) Explosives are the most common terrorist weapons due to their proven reliability as an effective, inexpensive, easily acquired terrorist device. (VDES, 1999) Bombs of various sizes can be configured from a range of dangerous materials, many of which are commonly available. Site design is a useful mechanism to assist in the defense against hand-delivered and vehicle-delivered bombs.

Destructive effects of explosives result from the outward energy force, fragments, and thermal effects. Surfaces closest to the detonation point sustain the greatest damage, often resulting in progressive collapse of structural elements.

Blast pressure moves the lower floor systems and shears connections between columns and floor beams. The progressive collapse of the lower part of the structure causes failure of the upper floors creating a pancake type collapse in a matter of seconds. As the over-pressure strikes hardened objects such as exterior walls, the energy is reflected into oncoming pressure, increasing the strength of the blast. As outward pressure moves away, a temporary vacuum effect

is created, causing negative pressure which hurls debris producing further damage. The smooth reflective surface of glass façades amplifies the effect of blast pressure and contributes to a significant amount of injuries by flying glass. (VDES, 1999)

Adjacent facilities can also sustain damage and depending on their proximity can contain the blast. Understanding the dynamics of bomb effects is useful in site design. Site design can ameliorate these effects by the positioning of buildings and roads on the site, by using design elements such as freestanding walls or berms to absorb blast, and by creating barriers to control access to vulnerable areas.

Terrorists gain entry to a site using various tactics. They can enter and exit covertly by blending in with visitors, using break-and-enter tactics similar to those of a conventional property offender, or coaxing an insider. (DOD, 1993) Stealth and disguise allow the aggressor to plot an attack or gain entry to plant a remote- or time-activated bomb. Small, lethal bombs can be hidden in hand-carried objects such as briefcases or packages. They can be emplaced at the most vulnerable area of a target, making detection difficult. "The FBI statistics show that there is only a 20 percent chance of finding such a planted bomb." (VDES, 1999, p35) Site design can improve success in countering covert tactics. For example, devising means to segregate and channel site users increases the likelihood that security guards will detect disguised terrorists and suspicious activity.

Terrorists use forced-entry tactics to overcome obstacles and other security defense. An intruder can overcome an obstacle by going over, under, or through it. (DOD, 1993) Quick access is obtained by scaling barriers that are not under surveillance, by going through gaps at the base of fences or between obstacles, or by bridging. Any horizontal obstacle less than 10 feet wide is vulnerable to bridging. (Fennelly, 1989) Security planners counter these tactics by designating clear spaces along barriers to facilitate surveillance. Clear space is defined as a corridor free of visual obstructions. Landscape architects must, in turn, develop site plans that facilitate continuous surveillance of these clear spaces. The employment of anticlimb and antiram obstacles also increases security.

Terrorists can go through an obstacle using cutting tools, explosives, or the kinetic force of a vehicle. A suicide bomber can drive a bomb-laden vehicle on a high-speed avenue of approach to get close to or into a building. Straight, unobstructed routes are conducive to such high-speed tactics. Terrorists have chosen this tactic to attack American targets internationally on six occasions during the period 1990-1998. (Dunne, 1999) Some combatants use guns or other devices to overcome or distract security guards. "In the bombing incident in Narobi, the assailants used a flash-bang grenade to distract guards." (Dunne, 1999) In a July 1979 incident, "four Palestinian terrorists armed with machine guns and grenades shot their way into the Egyptian Embassy in Ankara, and threatened to blow up the embassy." In 1974, a lone gunman entered the Philippine embassy in the nation's capital, wounded an embassy official, and seized the ambassador. (Jenkins, 1982, p29 and 35) Alternatively, "a moving attack . . . can result from an innocent unknowing citizen or coerced driver, who delivers the bomb to the target." (ASCE, 1999, p2-5) Countering forced entry tactics is the premier challenge for the design team. Landscape architects are tasked to devise defense in depth while maintaining a sense of public openness.

A standoff attack can be launched by using a gun or other weapon that is effective from a remote site. Weapons such as rocket-propelled launchers allow an attack on a public space from a distance without fear of intervention. Terrorists have chosen this tactic on eight occasions during the period 1990-1998. (Dunne, 1999) A bomb-laden vehicle can be parked or stopped outside a facility and "detonated remotely or by a timing device after the driver has escaped," as was the case in the 1995 bombing of the Alfred P. Murrah Building in Oklahoma. Alternatively, a terrorist can break into an unoccupied vehicle belonging to a bona fide user and hide explosives there. (ASCE, 1999, p2-5) Site layout, street design, and the use of blast and screening barriers are useful means to counter standoff threats.

A growing concern is the use of weapons of mass destruction (WMD) such as chemical or biological agents, and nuclear devices. (Gavin, 1999) WMDs enable the revolutionary to destroy a large area and kill large numbers of people. The shock and fear of the mere threat of such weapons is as disruptive as their effects are lethal. Evacuations necessitated by a bomb hoax not only satisfy the terrorist's desire for public attention, but also are costly to the facility in terms of lost work time and the deployment of emergency services. " A bomb hoax is a destructive

device." (Jones, 1999) Of the more than 1200 federal facilities surveyed by the U.S. Justice Department in 1995, greater than 70 percent received bomb threats that year, causing over 100 evacuations. (DOJ, 1995) In forging a response, the temptation to overreact must be avoided. Not only does this further the accomplishment of the goal of terrorism, but it also diminishes the image of the site.

Despite terrorism being a "low probability-high impact threat," domestic attacks have happened in the U.S. and will happen again. (Jones, 1999) "The threat is real." (Watson, 1999) Antiterrorism requires a more integrated and concerted approach to physical security than defense aimed to counter conventional criminals. Modern technology and a range of tactics make the terrorist more lethal and less predictable than the conventional criminal. (Hoffman, 1993) The response of terrorists to deterrence varies with the terrorist's cause and commitment and the resources of supporters. In some cases terrorists may select softer targets. However, when the mission justifies it, terrorists have demonstrated the ability to attack facilities despite the visible presence of heavy security. Prudent antiterrorism must create built environments that use inherent design elements as security devices to complement traditional physical security measures. This goal requires integration between design and security during each phase of the design process.

Appendix B

THE EMPLOYMENT OF BARRIERS

Effective barrier employment requires close coordination between the security consultant and the landscape architect. This thesis proposes to accomplish this effect by the preparation of a barrier plan. A barrier plan designates the location and function of barriers on a site. The document is a useful for finding a balance between the need for security and the need for a desirable site image. Designers can choose from a myriad of site design techniques those that will fulfill barrier requirements and minimally degrade site image. For example, circulation can be rerouted to reduce the need for extensive vehicle barriers. The barrier plan is an important pat of the integration of security and design. The development of an effective barrier plan requires the landscape architect to understand key aspects of barrier employment. The following paragraphs help form this foundation.

A planner must consider an intruder's ability to go over, under, or through the barrier. "A fence provides only seconds of delay." (DOD, 1993 and Granger, 2000) The resistance of fences and walls is increased by the use of anticlimb surfaces. Landscape architects can develop anticlimb surfaces by designing fences and walls that avoid gaps exceeding two inches in order to prevent foot and hand holds. (Green, 1981) Structural supports can also be designed to reduce the number of horizontal elements that can serve as ladders. People barriers should have a 9-foot height to serve as a deterrent and to provide resistance to entry by an intruder. Such fences and walls should be placed away from trees, poles, or buildings that could serve as climbing aids. (USN, 1988) Barriers with opaque surfaces such as walls should be avoided in situations where blocked surveillance will hinder security. By understanding these key facets of wall and fence employment, landscape architects are better poised to detail site designs that will contribute to the security effort.

Aside from their usefulness in restricting movement, barriers also provide spatial definition. For example, low walls, hedges, shrubs with thorns, spines, or prickly foliage, and broad plantings of dense low shrubs help define zones. Landscape architects can use spatial definition to signal the limits of authorized zones. By doing so, security guards can easily detect

intrusion through such well-defined spaces or through bands of open space. This effect increases the effectiveness of security forces and lessens the need for fencing and other more obtrusive means of restricting movement on a site.

The provision of vehicle barriers is especially dependent on close integration among the landscape architect, the security consultant, and engineers. Landscape architects are responsible for establishing building and street linkage during site layout. The standoff distance between a building and a road is perhaps the most important single factor on the blast resistance of a structure. Roughly, "doubling the standoff distance diminishes a given blast's effectiveness by a factor of 8." (VDES, 1999, p16) Road alignment, building placement, and vehicle barriers are design techniques to achieve standoff. Where possible, internal road design should direct vehicular traffic away from vulnerable areas such as building entry points and key structural supports in a building. When this is not possible, engineers use other methods to achieve blast resistance. For example, a blast wall may be placed to lessen the effects of a potential blast. Designing entrances and pathways that require right-angled turns discourages or at least slows a vehicular attack. "Direct straight alignment of roads to buildings should be avoided." (Lindsey, 1999)

Vehicle barriers can also control access and channel traffic on the site. Vehicle arrest systems are often used to control access to an approach zone and/or to a parking zone. These mechanical barriers extend across the travel lanes and may be either active or passive devices. An active system presents a vertical obstruction to a vehicle until the device is deactivated to allow authorized passage. Conversely, a passive system allows uninterrupted passage until a system is engaged to present an obstacle to unauthorized entry. Both systems can be operated from a fixed security post at the entry point or from a remote location. (Delta, 2000) Vehicle arrest systems are typically designed as traffic gate arms, mechanical gates, hydraulic or air-activated bollards, or surface-mounted barricades that rise from the roadway. These barriers are selected and designed according to their ability to absorb the kinetic energy of a vehicle crash. "Barriers are designed to arrest a vehicle of a specific gross weight going at a specified speed." (USN, 1988, p35) This thesis proposes that the integrated efforts of a design team can better use vehicle barriers. Landscape architects can contribute their skills in site layout and street design to slow

and control vehicles. This control lessens the need for bulky engineered barriers and channels vehicles for better detection, delay, and denial.

Landscape architects also influence barrier effectiveness by site grading. Proper grading can avoid washouts under security fencing that create gaps for intrusion. Grading can preserve natural obstacles such as ravines or forested areas and create barriers such as berms or depressions. Such obstacles provide "natural access control." (Newman, 1972) Convex or concave terrain hinders vehicle movement by creating "hang-up or nose-in failure." Hang-up failure occurs when the bottom of a vehicle catches on an obstacle; nose-in failure occurs when the front end of a vehicle catches or collides with the vertical plane of an obstacle. (Bekker, 1969, p162) If berms are sited and designed with sufficient height, these obstacles also help absorb blasts and lessen blast effectiveness. (ASCE, 1999) Grading can provide for steps, ramps, and terraces that are useful as obstacles. Such design elements slow, channel, and restrict foot and vehicle passage. This thesis proposes that grading skills are valuable tools to achieve an unnoticed but effective barrier defense.

Appendix C

BIBLIOGRAPHY

(Cited Works)

1. American Society of Civil Engineers (ASCE Task Committee). 1999. Structural Design for Physical Security-State of the Practice. ASCE, Reston, Va.

2. Atlas, Randall. 1992. "Architectural Design and Security." ASIS Facility Security Design Workshop, Miami, Fla. July 17

3. Bell, Alan. "Physical Security Not Just Bars and Guards." www.terrorism.net/pubs/aran3.htm

4. Brodie, Thomas. 1996. Bombs and Bombing-A handbook to Detection, Disposal, and Investigation for Police and Fire Departments. Charles Thomas Publisher, Springfield, Ill.

5. City of Oklahoma (OKC). 1996. Final Report - The Alfred P. Murrah Federal Building Bombing. Fire Protection Publications, Stillwater, Ok.

6. Clarke, Ronald. 1992. Situational Crime Prevention. Harrow and Heston Publishers, NY

7. Cressman, Robert. 1999. Interview. Robert C. Byrd Federal Building, Charleston, WVa. October 29

8. Crowe, Timothy. 1991. Crime Prevention Through Environmental Design. Butterworth-Heinemann, Mass.

9. De Becker, Gavin. 1999. "Fear and Public Anxiety vs. Actual Risk." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

10. DeChiara, Joseph and Koppelman, Lee. 1984. Time-Saver Standards for Site Planning. McGraw-Hill Co., NY.

11. Delta Scientific (Delta). 2000. A Discussion of the Background, Operation, Selection, and Installation of a Vehicle Arrest System. Brochure Packet, Delta Scientific Corp. February 18

12. Department of Defense (DOD). 1993. Military Handbook Design Guidelines for Physical Security of Facilities. MIL-HBBK-1013/1A; DOD. Approved for Public Release. June 28

13. Department of Justice (DOJ). 1995. Vulnerability Assessment of Federal Facilities. DOJ, Wash., DC.

14. Dunne, James, Department of State. 1999. "NBC Domestic Preparedness." Presentation at WMD Training Seminar, Chesterfield, Va. October 25

15. Fennelly, Lawrence. 1989. Handbook of Loss Prevention and Crime Prevention; 2nd Ed. Butterworth-Heinemann, Boston, Mass.

16. Fennelly, Lawrence. 1992. Effective Physical Security. Butterworth-Heinemann, Boston, Mass.

17. Foley, David. 2000. "Guard Force Management." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

18. Gavin, David, FBI. 1999. "Overview of WMD Incidents and Investigation Protocols;" Presentation at WMD Training Seminar, Chesterfield, Va. October 25

19. Granger, Joseph. 2000. "Threats and Vulnerabilities." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

20. Gray, Kenneth. 1986. "Vehicle Access Control As Related to Countermeasures Against High Speed Car-Bombing Attack." ASIS Conference on Security Installation Against Car-Bomb Attack, Wash., DC. May 15

21. Green, Gion. 1981. Introduction to Security. Butterworth Publishers, Boston, Mass.

22. Hoffman, Bruce. 1993. Future trends in Terrorist Targeting and Tactics. RAND, Santa Monica, Ca.

23. Jacobs, Jane. 1961. The Death and Life of Great American Cities. Vintage Books, NY

24. Jenkins, Brian. 1982. Terrorism and Beyond-An International Conference on Terrorism and Low-Level Conflict. RAND, Santa Monica, Ca. December

25. Jones, Michael. 1999. Interview. Division of Capitol Police. Richmond, Va. September 23

26. Karpiloff, Douglas. 1999. "Balancing Security and Openness on a Day-to-Day Basis"Presentation at WMD Training Seminar, Chesterfield, Va. October 25

27. Karpiloff, Douglas. 2000. "Exterior Access Control." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

28. Kellen, Konrad. 1982. On Terrorists and Terrorism. RAND, Santa Monica, Ca.

29. Bekker, M.G. 1969. Introduction to terrain-vehicle systems. Univ. of Michigan Press, Ann Arbor, Mi.

30. Kyle, Thomas and Aldridge, James. 1992. Security Closed Circuit Television Handbook. Charles C. Thomas Publisher, Springfield, Ill.

31. Lindsey, David. 1999. Interview. U.S. Bureau of Engraving. Wash., DC. November 17

32. Maurer, Richard. 2000. "Access Control Strategies." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

33. McHarg, Ian. 1992. Design with Nature. John Wiley & Sons, NY

34. Motloch, John. 1991. Introduction to Landscape Design. Van Nostrand Reinhold, NY

35. National Research Council (NRC). 1995. Protecting Buildings from Bomb Damage. National Academy Press,Wash., DC

36. Newman, Oscar. 1972. Defensible Space: Crime Prevention Through Urban Design; Collier Books, NY

37. Purpura, Philip. 1984. Security & Loss Prevention. Butterworth Publishers, Boston, Mass.

38. Strom, Steven and Nathan, Kurt. 1993. Site Engineering for Landscape Architects. 2d Ed. Van Nostrand Reinhold, NY

39. United States Navy (USN). 1988. Protection of Federal Buildings. Department of Navy, Wash., DC

40. Virginia Department of Emergency Services (VDES). 1999. Public Safety Response to Terrorism. Commonwealth of Virginia. April

41. Voigt, Ronald. 1999. Interview. U.S. Justice Department, Wash., DC. November 17

42. Zahm, Diane. 1996. "Crime Prevention Through Environmental Design Seminar"

43. Washington Post (Wash.). 1999. "A Capital Under Seige." TheWashington Post. April 17 Ed.

44. Watson, Larry. FBI. 1999. "Protection of Federal Facilities." Presentation at ASIS Conference, Wash., DC. May

Appendix D

RELATED REFERENCES

(Studied During Research)

1. Acke, Theodore. 1999. "Crime Prevention Through Environmental Design." Seminar, Blacksburg, Va.

2. American Architectural Foundation (AAF). 1998. Human Experiences with Architecture. AAF, Wash., DC

3. American Bar Association (ABA). 1973. The American Courthouse Planning and Design for the Judicial Process. American Bar Association and AIA Joint Committee of Design of Courtrooms and Court Facilities

4. American Institute of Architects (AIA). 1996. Justice Facilities Review 1997. AIA, Wash., DC

5. Banks, Phillip. 2000. "Security Hardware." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

6. Bodino, Barbara, Ambassador. 1999. "Balancing Security and Openness on a Day-to-Day Basis." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

7. Booth, Norman. 1983. Basic Elements of Landscape Architectural Design. Waveland Press, Ill.

8. Brown, Carter, Commissioner of Fine Arts. 1999. "Public Expectations and the Design Process." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

9. Buildings and Economic Development (BED). 1997. Federal Building Security. Hearing before Subcommittee on Public Buildings and Economic Development, April 24, 1996. USGPO, Wash., DC

10. Campbell, Robert. "Public Expectations and the Design Process;" Presentation at "Balancing Security and Openness Symposium; Wash., DC; November 30, 1999

11. Carpenter, Philip; Walker, Theodore; and Lanphear, Frederick. 1975. Plants in the Landscape. W.H. Freeman Co., San Francisco, Ca.

12. Cohen, Bonnie and Peck, Robert, Department of State and GSA (respectively). 1999. "Where Do We Go From Here." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

13. Committee on Government Operations (COGO). 1991. Location and Construction of a Federal Courthouse in Orange County, CA. Hearing before the Government Activities and Transportation Subcommittee. USGPO. Wash., DC. June 17

14. Cummings, Barbara, Consular. 1999. "Public Expectations and the Design Process." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

15. Department of State (DOS). 1999. Foreign Building Operations. DOS Publication 10650. Released November

16. Department of State (DOS). 1999. Political Violence Against Americans. DOS Publication 10625.

17. Department of State (DOS). 1999. State Department Actions to Accountability Review Board (Africa Bombing). April. www.state.gov

18. DePasquale, Salvatore. 2000. "Security Design." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

19. Duda, David, CPP. 2000. "Interior/Exterior Sensor Technologies." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

20. Federal Emergency Management Agency (FEMA). Backgrounder: Terrorism. www.fem.gov

21. Friedburg, Paul. 1999. "The Design Community's Search for Security Solutions." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

22. General Accounting Office (GAO). 1988. Domestic Terrorism-Prevention Efforts in Selected Federal Courts and Mass Transit Systems. Report to the Chairman, Subcommittee on Civil and Constitutional Rights. GAO/PEMD-88-2. June

23. General Services Administration (GSA). 1996. Facilities Standards for the Public Buildings Service. PBS-PQ100.1. June 14

24. General Services Administration (GSA). 1999. "Federal Buildings and U.S. Courthouses." Public Building Service Website

25. Giffin, Gordon, Ambassador. 1999. "Balancing Security and Openness on a Day-to-Day Basis." Presentation at "Balancing Security and Openness Symposium,Wash., DC. November 30

26. Grassie, Richard and Betts, Curt. 1995. "Prevention Techniques." ASIS Conference on Domestic Terrorism Awareness Prevention and Planning, Arlington, Va. July 12

27. Hampson, John, Department of State. 1999. "International/Domestic Terrorism Overview." Presentation at WMD Training Seminar, Chesterfield, Va. October 25

28. Harris, Charles and Dines, Nicholas. 1998. Time-Saver Standards for Landscape Architecture: Design and Construction Data. 2nd Ed., McGraw-Hill, NY

29. Hemphill, Charles, Jr.1971. Security for Business and Industry. Dow-Jones-Irwin, Ill.

30. Hoffman, Bruce and Donna. 1998. The Rand-St.Andrews Chronology of International Terrorists Incidents, 1995. RAND, Santa Monica, Ca.

31. Hoffman, Bruce and Riley, Kevin. Undated. Domestic Terrorism-National Assessment of State and Local Preparedness, RAND, Santa Monica, Ca.

32. Hopf, Peter. 1979. Handbook of Building Security Planning and Design. McGraw-Hill, NY

33. Johnson, Carol. 1999. "The Design Community's Search for Security Solutions." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

34. Judicial Coordinating Committee (JCC). 1981.The Michigan Courthouse Study. Judicial Coordinating Committee of the Supreme Court of the State of Michigan. Thompson-Shore Inc., Dexter, Mi.

35. Judicial Council of Virginia (JCOV). 1987. Virginia Courthouse Facility Guidelines. March

37. Lynch, Kevin. 1994. Site Planning. The MIT Press, Cambridge, Mass.

36. Moynihan, Daniel Patrick, U.S. Senate. 1999. "Call for a National Conversation." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

37. Mozingo, Louise. 1995. "Public Space in the Balance." Landscape Architecture. February

38. National Trust for Historic Preservation (NTHP). 1976. A Courthouse Conservation Handbook. Preservation Press

39. Newman, Morris. 1996. "Playing It Safe." Landscape Architecture. May. pp50-55

40. Office of the Coordinator of Counterterrorism. 1997. Designation of Foreign Terrorist Organizations. www.state.gov/www/global/terrorism/; Oct 8

41. Office of Technology (OTA). 1992. Technology Against Terrorism – Structuring Security. OTA-ISC-511. OTA, Congress of the U.S., Wash, DC

42. Panasonic Video Imaging Systems Co. (Panasonic). 1999. "Covert Surveillance Cameras." Advertisement 726, Security Management, Vol.38. July. p144

43. Peck, Robert, GSA. 1999. "Where Do We Go From Here?" Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

44. Pierce, Charlie, R.A. 2000. "CCTV Technologies." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

45. Public Buildings Service (PBS), General Services Administration. Undated. "Federal Building and U.S. Courthouse. Website

46. Reid, Sue. 2000. Crime and Criminology. McGraw Hill, Boston, Mass.

47. Schultz, Donald. 1978. Principles of Physical Security. Gulf Publishing Co., Houston, Tx.

48. Scotti, Anthony. 1999. On The Lookout for Suspicious Signals. www.terrorism.net/pubs/scotti.html

49. Security Resource Net (SRC). Undated. Bomb Threats and Physical Security Planning. his.org/Library/Terrorism/bombthreat.html

50. Seger, Karl. 1990. The Anti-Terrorism Handbook. Presido, Ca.

51. Simon, Jeffery. 1990. U.S. Countermeasures Against International Terrorism. RAND, Santa Monica, Ca.

52. Smith, Joseph.1999. "Blast Analyses and Mitigation." ASIS Conference on Security in Federal Facilities, Wash., DC. May 4

53. Sorensen, Severin. 2000. "CPTED." ASIS Conference on Physical Security: Technology and Applications, Miami, Fla. January 31

54. Stanton, Michael. 1999. "Public Expectations and the Design Process." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

55. Stauchi, John. 1998. "Steps Towards an Effective Prevention Program." ASIS Conference on Prevention. July 12

56. Sulzbach, Edward. 1999. "The Psychology of Terrorism." Presentation at WMD Training Seminar, Chesterfield, Va. October 25

57. The Terrorist Research Center (TRC). Undated. "The Threat of Domestic Terrorism." URL: http//www.terrorism.com

58. United States Army (USA). 1979. FM 19-30 Physical Security. HQ, U.S. Army. March

59. United States Army (USA). 1987. FM 5-34 Engineer Field Data. HQ, U.S. Army. Approved for Public Release. June 8

60. United States Marine Corps (USMC). 1989. FMFM 7-14A The Individual's Guide for Understanding and Surviving Terrorism. Headquarters United States Marine Corps, Wash., DC

61. United States Marine Corps (USMC). 1990. FMFM 7-14 Combating Terrorism. Headquarters United States Marine Corps, Wash., DC

62. Woodlock, Douglas. U.S. Justice. 1999. "Balancing Security and Openness on a Day-to-Day Basis." Presentation at "Balancing Security and Openness Symposium, Wash., DC. November 30

63. Woodruff, Ronald. 1974. Industrial Security Techniques. Charles E. Merrill Publishing,Columbus, Oh.

64. Zahm, Diane. 1995. "Crime Proofing Design." Landscape Architecture. Feb. pp120

65. Zahm, Diane and Crowe, Timothy. 1994. "Crime Prevention through Environmental Design." Land Development. Fall

VITA

Wilbur L. Peart

Wilbur L. Peart was born December 4, 1953 in Alexandria, Louisiana. He received a bachelor of science degree from Northeast Louisiana University and entered the U.S. Marine Corps as a commissioned officer in 1975. His military training programs included basic and advanced field artillery and nuclear, biological, and chemical warfare training. During his 20-year service, his duty assignments as battery commanding officer, battalion operations officer, and battalion executive officer entailed physical security and military tactical responsibilities. While stationed in Japan, he was responsible for the planning and supervising of physical security for an entire U.S. Marine Corps' military installation.

Returning to civilian life, he earned a bachelor of landscape architecture degree from the University of Maryland in 1998, where he received an American Society of Landscape Architecture (ASLA) award for his academic accomplishments. He then entered the master's program in landscape architecture at Virginia Polytechnic Institute and State University in September of 1998 with a concentration in structural building design and crime prevention through environmental design. Since completing his course work in May 2000, he has been employed at a landscape architecture firm located in Northern Virginia where he has planned security for two multifamily housing developments. He is a member of the American Society of Industrial Security (ASIS) and the American Society of Landscape Architecture (ASLA).

Wilbur Peart and his wife currently reside in Herndon, Virginia. The couple has two children.