



*An Online PDH Course  
brought to you by  
CEDengineering.com*

## **Building Terrorism Mitigation – Site Layout and Design**

Course No: F05-002  
Credit: 5 PDH

---

Gilbert Gedeon, P.E.

---



Continuing Education and Development, Inc.

P: (877) 322-5800  
[info@cedengineering.com](mailto:info@cedengineering.com)

*This course was adapted from the Federal Emergency Management Agency (FEMA), Chapter 2 "Site Layout and Design Guidance", Publication FEMA 426 "Mitigating Potential Terrorist Attacks Against Buildings", which is in the public domain.*

**T**his chapter discusses site-level considerations for development. The intent of this guidance is to provide concepts for integrating land use planning, landscape architecture (vegetation, landforms, and water), site planning, and other strategies to mitigate the design basis threats as identified via the risk assessment. Integrating security requirements into a larger, more comprehensive approach necessitates achieving a balance among many objectives such as reducing risk; facilitating proper building function; aesthetics and matching architecture; hardening of physical structures beyond required building codes and standards; and maximizing use of non-structural systems.

The design community must work closely with building owners and operators to ensure that the optimal balance of all the above considerations is achieved; thus, coordination within the design team is critical. Many asset protection objectives can be achieved during the early stages of the design process when mitigation is the least costly and most easily implemented. Planners, architects, and landscape designers play an important role in identifying and implementing crucial asset protection measures while considering land use; site selection; the orientation of buildings on the site; and the integration of vehicle access, control points, physical barriers, landscaping, parking, and protection of utilities to mitigate threats.

It is important to remember that the nature of any threat is always changing. Although indications of potential threats may be scarce during the design stage, consideration should be given to accommodating enhanced protection measures in response to future threats that may emerge. Asset protection objectives must be balanced with other design objectives, such as the efficient use of land and resources, and must also take into account existing physical, programmatic, and fiscal constraints.

## **2.1 LAND USE CONSIDERATIONS**

Managing the many dimensions of land use (e.g., development, transportation, activities, and growth, etc.) is a well-established practice in the United States, with numerous regulations and other tools in use by state and local governments to influence the urban form. These tools range from private controls (e.g., deed restrictions and easements) to governmental mechanisms, including permitting, subdivision, land development regulations, and zoning. In addition, economic forces such as land market values, enterprise zones, insurance costs, tax incentives, and impact fees are major considerations in land use decision-making.

Many of these land use controls are significant factors of anti-terrorism and security. For example, zoning, subdivisions, and planned unit developments define urban configurations, which translate directly into potential terrorist attack opportunities because they provide protective clustering of some activities and defensive dispersion of others. Furthermore, performance-based zoning (in contrast to prescriptive zoning) can allow for greater freedom in land use by removing location-based use constraints in favor of simply assigning responsibility for any negative impacts directly to the land owner. The benefits of increased performance-based zoning's flexibility relies on the ability of the owner and/or operator to make informed decisions about the level of risk that they are willing to accept and how much risk they can mitigate through land use countermeasures.

As another example, a deed restriction limiting the use of an adjacent parcel to open space or recreation may present a security advantage in terms of setback, but such spaces may also make hostile surveillance and attack preparations difficult to detect or to discern from those of normal use. Impact fees on stormwater infrastructure may provide an economic incentive to implement low-impact development techniques. In addition to reducing infrastructure costs, managing stormwater on site can add security through retention facilities that also serve as vehicle barriers and blast setbacks. The design of on-site stormwater infrastructure can

also reduce the need for culverts, drainage pipes, manholes, and other covert site access and weapon concealment opportunities.

In some cases, permit and fee waivers can be used to promote public transportation, which can reduce urban sprawl and traffic congestion, thus helping to decrease the vulnerability of high-risk sites by curbing the flow of traffic and construction of new buildings in high-risk areas. Similarly, creation of an overlay zone (sub-zoning to address area-specific considerations) based on security requirements could firmly establish antiterrorism as a key design consideration, but it could also cause the “branding” of an area as dangerous or high risk, thus jeopardizing the success of any development nearby.

Land use tools for antiterrorism and security are generally derivative in nature and may not be initially obvious. Typically, land use documents contain a wealth of data that can be used to address antiterrorism and security objectives. These sources of information, and many more, are available through a variety of channels, including city, county, and metropolitan planning offices, emergency management offices, tax assessors, councils of governments, and other state and local agencies.

For land use design, designers should consider external and internal aspects. External aspects involve the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of adjacent activities, as well as the implications of these characteristics for the protection of the people, property, and operations on the site under consideration. Internal aspects include the amount of land available on the site for stand-off and the inherent ability of the site to accommodate the implementation of natural and manmade antiterrorism and security design features. It is important to recognize that conflicts sometimes arise between security-oriented site design and conventional site design. For example, open circulation and common spaces (which are desirable for conventional design) may be detrimental to certain aspects of security. Designers must balance protection priorities with the requirements of the Americans

with Disabilities Act Accessibility Guidelines (ADAAG), Uniform Federal Accessibility Standards (UFAS), National Fire Protection Codes (NFPC), and other applicable building codes and standards. To resolve these issues, coordination between the disciplines is critical to the design process.

Whether designing new buildings or evaluating existing ones, the designer should evaluate key protection measures to ensure they are appropriate, desirable, and cost-effective in terms of mitigating the risk of potential terrorist attacks. Security measures must be evaluated carefully to understand which measures are truly beneficial and which are not practical.

When making decisions about site antiterrorism and security, designers should consider the following factors:

- Building footprint(s) relative to total land available
- Building location(s) or, if undeveloped, suitable building location(s) relative to the site perimeter and adjacent land uses; distance between the perimeter fence and improved areas off site
- Access via foot, road, rail, water, and air; suitability to support a secure perimeter
- Current and planned infrastructure and its vulnerabilities, including easements, tunnels, pipes, and rights-of-way
- Infrastructure nodes that constitute single-point vulnerabilities
- Adjacent land uses and occupancies that could facilitate attacks or that are potential targets themselves and thus present collateral damage or cascading failure hazards (see Figure 2-1)
- Proximity to fire and police stations, hospitals, shelters, and other critical facilities that could be of use in an attack
- Natural hazards, susceptibility to subsidence or liquefaction, and other environmental considerations

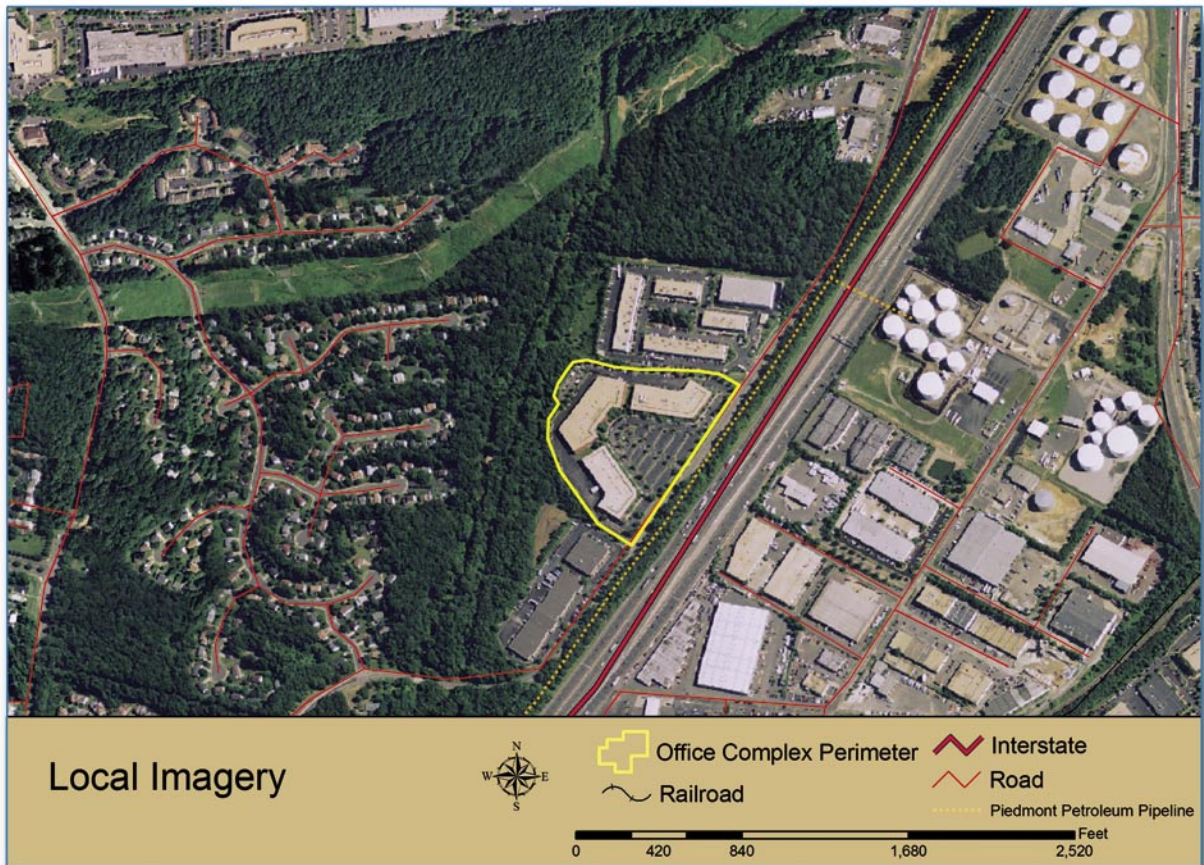


Figure 2-1 An example of using GIS to identify adjacent hazards. Note the large fuel storage and distribution facility (tank farm) in the vicinity of the office building being assessed.

- Presence of natural physical barriers such as water features, dense vegetation, and terrain that could provide access control and/or shielding, or suitability of the site for the incorporation of such features
- Topographic and climatic characteristics that could affect the performance of chemical agents and other weapons
- Observability from outside site boundaries; ability of vegetation in proximity to building or site to screen covert activity

## **2.2 SITE PLANNING**

The single most important goal in planning a site to resist terrorism and security threats is the protection of life, property, and operations. Decision-making in support of this purpose should be based first and foremost on a comprehensive assessment of the manmade threats and hazards so that planning and design countermeasures are appropriate and effective in the reduction of vulnerability and risk. It is important to recognize that a given countermeasure can mitigate one or more vulnerabilities, but may be detrimental to other important design goals. It is also important to think creatively and comprehensively about the security repercussions of common site planning and design decisions. This section will highlight several aspects of site design and will present some of the unique characteristics arising from their application to antiterrorism and security.

### **2.2.1 Site Design**

Because the economics of development dictate recovering the largest possible portion of square footage within most urban and rural sites, security concerns should be evaluated carefully. Conflicts sometimes arise between security site design and conventional site design. For example, open circulation and common spaces, which are desirable for conventional design, are often undesirable for security design. To maximize safety, security, and sustainability, designers should implement a holistic approach to site design that integrates form and function to achieve a balance among the various design elements and objectives. Even if resources are limited, significant value can be added to a project by integrating security considerations into the more traditional design tasks in such a way that they complement, rather than compete with, the other elements.

### **2.2.2 Layout and Form**

The overall layout of a site (e.g., the placement and form of its buildings, infrastructures, and amenities) is the starting point for development. Choices made during this stage of the design process will steer decision-making for the other elements of the site. A



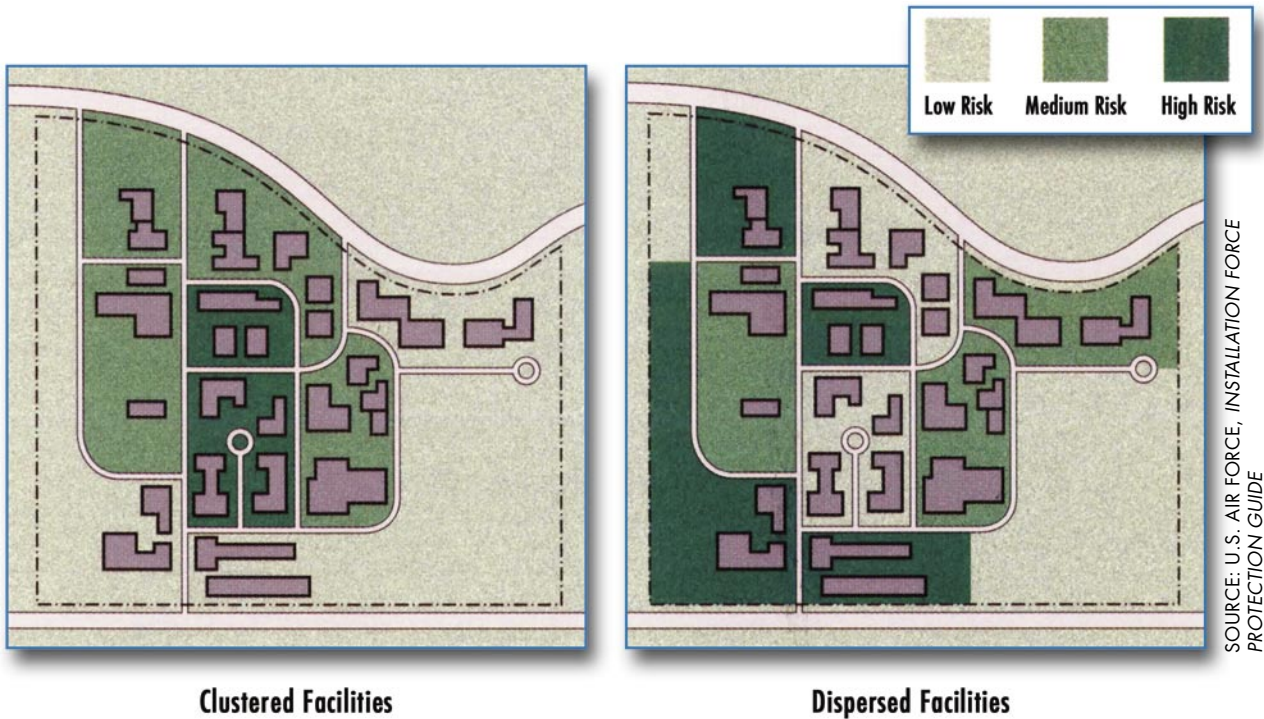
number of aspects of site layout and building type present security considerations and are discussed below.

- **Building placement.** Depending on the site characteristics, the occupancy requirements, and other factors, buildings may be clustered tightly in one area, or dispersed across the site. Both patterns have compelling strengths and weaknesses.

Concentrating people, property, and operations in one place creates a target-rich environment, and the mere proximity of any one building to any other may increase the risk of collateral impacts. Additionally, the potential exists for the establishment of more single-point vulnerabilities in a clustered design than would exist in a more dispersed pattern. However, grouping high-risk activities, concentrations of personnel, and critical functions into a cluster can help maximize stand-off from the perimeter and create a “defensible space.” This also helps to reduce the number of access and surveillance points, and minimize the size of the perimeter needed to protect the facilities. Stand-off planning is discussed in detail in Sections 2.3 and 2.4. In addition, combining multiple uses also provides economic and environmental benefits such as opportunities to efficiently transfer heat from net heat-producing areas and activities to net heat-consuming ones, thus reducing energy costs.

In contrast, the dispersal of buildings, people, and operations across the site reduces the risk that an attack on any one part of the site will impact the other parts. However, this could also have an isolating effect, and reduce the effectiveness of on-site surveillance, increase the complexity of security systems and emergency response, and create a less defensible space.

To the extent that site, economics, and other factors allow, the designer should consolidate buildings that are functionally compatible and have similar threat levels (see Figures 2-2 and 2-3). For example, visitor screening areas, receiving/loading areas, and mailrooms constitute the innermost line of defense,

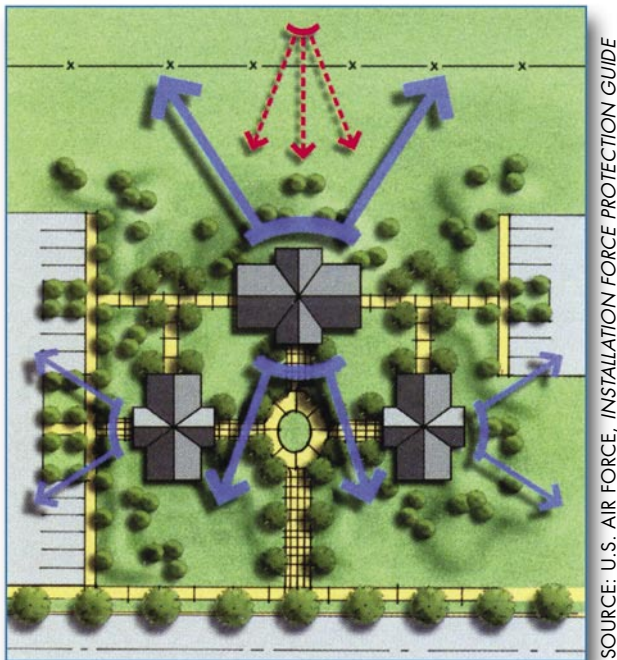


SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

**Clustered Facilities**

**Dispersed Facilities**

Figure 2-2 Clustered versus dispersed site layouts



SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

Figure 2-3 Clustering to enhance surveillance opportunities while minimizing views into the buildings

because they may be the first places where people and materials are closely inspected before being introduced into the facility. Logically, they should be physically separated from the key assets such as main operational areas and concentrations of people. It is also desirable to locate potential target buildings away from lower-risk areas in order to minimize collateral damage, should an attack occur.

- **Building orientation.** The orientation of a building can have significant impact on its performance, not only in terms of energy efficiency, but also in the ability to protect occupants. For the purposes of this discussion, the term “orientation” refers to three distinct characteristics: the building’s

spatial relationship to the site, its orientation relative to the sun, and its vertical or horizontal aspect relative to the ground.

A structure's orientation relative to its surroundings defines its relationship to that area. In aesthetic terms, a building can "open up" to the area or turn its back; it can be inviting to those outside, or it can "hunker down" defensively. The physical positioning of a building relative to its surroundings may seem subtle, but can be a greater determinant of this intangible quality than exterior aesthetics. Nevertheless, the proximity of a vulnerable façade to a parking area, street, adjacent site, or other area that is accessible to vehicles and/or difficult to observe can greatly contribute to its vulnerability. This illustrates one way in which protective requirements can be at odds with otherwise good design. A strong, blank wall with no glazing will help to protect the people, property, and operations within from a blast, but the lack of windows removes virtually all opportunity to monitor activities outside and take appropriate protective actions in a timely manner. Designers should consider such trade-offs early in the design process, in an effort to determine an acceptable level of risk.

The solar orientation of a building is a significant factor in energy consumption. By optimizing the positioning of the building relative to the sun, climate control and lighting requirements can be met while reducing power consumption. However, these energy conservation techniques present some important security considerations. For example, natural ventilation is an effective and time-tested technique for efficiently cooling buildings; however, the use of unfiltered outside air presents a major vulnerability to aerosolized chemical, biological, and radiological agents, in addition to accidental releases of hazardous materials. Additionally, awnings may become projectiles in a blast event, and the construction of operable windows may not be as blast-resistant as the frames of fixed windows. Similarly, the use of light shelves, skylights, clerestories, and atria can help meet illumination requirements while dramatically reducing

the need for electric lighting. However, day lighting relies inherently on the use of glazing, which has been shown to be one of the major hazards in blast events. In addition to ensuring the maximum setback possible for highly-fenestrated facades, designers should ensure that aperture sizes, glazing materials, films, and frames and connections are selected with blast-resistance as well as energy efficiency in mind.

- **Open space.** The incorporation of open space into site design presents a number of benefits. First and foremost is the ability to easily monitor an area and detect intruders, vehicles, and weapons. Closely related to this benefit is the stand-off value of open space; as discussed in Chapter 4, blast energy decreases as the inverse of the cube of the distance from the seat of the explosion, so every additional increment of distance provides increasingly more protection. In addition, pervious open space allows stormwater to percolate back into the ground, reducing the need for culverts, drainage pipes, manholes, and other covert site access and weapon concealment opportunities. Also, if the open space is impassible for vehicles (as in the case of a wetland or densely vegetated area), it can provide not only environmental and aesthetic amenities, but prevent vehicle intrusion as well.

Leaving significant amounts of open space, wetland, or other sensitive areas unimproved may present opportunities to reap economic benefits in the form of transferable development rights (TDRs). TDR is a market-based approach that provides incentives to developers to focus growth only where it is desired, making it profitable to refrain from developing open space and sensitive areas. By not maximizing the profit potential of their land, owners can receive “development right credits” that can be sold to developers elsewhere in the community, who will then be able to use those credits to intensify the use of their own land in ways that promote more sustainable growth.<sup>1</sup> Thus, in some cases, TDRs may be a windfall benefit of security-oriented development.

<sup>1</sup>U.S. EPA, *Smart Growth Policy Database*. <http://cfpub.epa.gov/sgpdb/sgdb.cfm>

### 2.2.3 Vehicular and Pedestrian Circulation

The movement of people and materials into, through, and out of a facility is determined by the design of its access, circulation, and parking systems. Such systems should be designed to maximize efficiency while minimizing conflicts between vehicle and pedestrian modes. Designers should begin with an understanding of the site's transportation requirements based on an analysis of how the facility will be used. This includes studying the number and types of access points that are required, the parking volume needed, pedestrian patterns, and the modes of transportation they will use. Several aspects of transportation planning can impact security and are discussed below.

- **Roadway network design.** Streets are generally designed to minimize travel time and maximize safety, with the end result typically being a straight path between two or more endpoints. Although a straight line may be the most efficient course, designers should use caution when orienting streets relative to buildings. Given that the energy transferred when one object strikes another is a function of its mass and its velocity, a bollard that can stop a 15,000-pound truck moving at 35 miles per hour may not be able to stop the same truck moving at 55 miles per hour. In developing a system of street alignments with protection in mind, the designer cannot determine the size or weight of a vehicle that will travel along the road, because that is a management decision. However, the designer can propose a roadway system to minimize vehicle velocity, thus using the roadway itself as a protective measure. This is accomplished through the use of the following strategies.

First, straight-line or perpendicular approaches to buildings should not be used, because these give vehicles the opportunity to gather the speed necessary to ram through protective barriers and crash into or penetrate buildings. Instead, approaches should be parallel to the façade, with berms, high curbs, appropriate trees, or other measures used to prevent vehicles from departing the roadway. A related technique for reducing vehicle speeds is the construction

of serpentine (curving) roadways with tight-radius corners. Existing streets can be retrofitted with barriers, bollards, swing gates, or other measures to force vehicles to travel in a serpentine path. Again, high curbs and other measures should be installed to keep vehicles from departing the roadway in an effort to avoid these countermeasures.

Less radical than these techniques are traffic calming strategies, which seek to use design measures to cue drivers as to the acceptable speed for an area. These include raised crosswalks, speed humps and speed tables, pavement treatments, bulbouts, and traffic circles. In addition to creating a more pedestrian-friendly environment, which increases “eyes on the street” surveillance, designing roadways to physically limit speeds can have the added benefits of increasing safety and, subsequently, lowering liability. Designers should be aware, however, that many of these techniques can have detrimental effects for emergency response, including slowing response time, interfering with enroute emergency medical treatment, and increasing the difficulty of maneuvering fire apparatus. They also may present problems for snow removal, and their outer ends should remain flat so that bicycles can proceed unimpeded. Finally, the distinction between speed humps, speed tables, and speed bumps is critical. Speed humps and tables are much gentler than speed bumps and can be constructed to “enforce” a specific speed range. Speed bumps have much more abrupt profiles and are only appropriate for low-speed applications, such as parking lots.

- **Parking.** There are three primary types of parking facilities, all of which present security trade-offs. Surface lots can be designed to keep vehicles away from buildings, but they consume large amounts of land and, if constructed of impervious materials, can contribute greatly to stormwater runoff volume. They can also be hazardous for pedestrians if dedicated pedestrian pathways are not provided. In contrast, on-street parking is often convenient for users and a source

of revenue for local governments, but this type of parking may provide little or no setback. Finally, garage structures provide revenue and can be convenient for users, but they may require structural measures to ensure blast resistance as well as crime prevention measures to prevent street crime. Although the cost of land suggests that the construction of a garage below a building (either underground or aboveground) may be the most economically viable approach for many developments, they can be highly vulnerable to vehicle-borne weapons, endangering the building above. If garages must be used, human security procedures (e.g., vehicle searches) and electronic systems (e.g., closed circuit television) may be necessary to ensure safety (see Section 2.7 for additional information).

#### **2.2.4 Infrastructures and Lifelines**

Providing power, gas, water, wastewater, and communications services is one of the most basic requirements of any development. At the site scale, all critical lifelines should have at least one layer of redundancy, or backup. By eliminating single-point vulnerabilities, designers reduce the chance that service will be interrupted if an attack damages or destroys a lifeline either outside the perimeter or on site. It is important to note that collocating a backup lifeline with its primary lifeline does not eliminate single-point vulnerability; only physical separation can substantially increase the likelihood of continuity of service. Designers should be aware that this could create the need for each type of infrastructure lifeline to cross the site perimeter at multiple locations, potentially complicating the process of managing utility easements and rights-of-way. Additional information on critical systems is also discussed in Chapter 3.

Additionally, all controls, interconnections, exposed lines, and other vulnerable elements of infrastructure systems should be protected from access and exploitation by surveillance and/or physical countermeasures. Service entrances and other secondary access points should be monitored and access-controlled; special

attention should also be paid to any locations where multiple systems or primary and backup systems come together, such as control rooms and mechanical spaces. Again, these facilities should be designed for maximum observability, including the use of opportunity reduction and target hardening strategies where appropriate, and should be equipped with adequate lighting and emergency communications capabilities wherever possible.

### **2.2.5 Landscape and Urban Design**

Designing to meet user needs while maintaining stewardship of the natural and built environments becomes increasingly more challenging when security requirements are factored in. Design principles should include an emphasis on mixed-use development; selection of low-impact development techniques and environmental stewardship; compatibility of context and relationship with adjacent uses, forms, and styles; establishment of scale and identity through aesthetic design; connectivity among buildings, uses, activities, and transportation modes; resource conservation; cultural responsiveness; and the creation of appealing public spaces. These objectives are generally achieved through the work of two closely related disciplines, landscape design and urban design. For the purposes of this document, these two domains are virtually overlapping and will, therefore, be addressed together.

- **Landscape design.** The implications of security for landscape design affect everything from plant species and building material selection to landform construction and wayfinding. Elements such as landforms, water features, and vegetation are among the building blocks of attractive and welcoming spaces, and they can also be powerful tools for enhancing security. These features can be used not only to define or designate a space, but also to deter or prevent hostile surveillance and unauthorized access. Vegetative groupings and landforms can even provide some level of blast shielding. Stands of trees, earthen berms, and similar countermeasures generally cannot replace setbacks, but they can offer supplementary protection. However, landscaping



can also have detrimental impacts for safety and security, and practitioners should consider the unique requirements of the project to ensure that the landscape design elements they choose will be appropriate and effective.

For example, thorn-bearing and sharp-leaved plant species (e.g., firethorn, Spanish bayonet, and pampas grass) can create natural physical barriers to deter aggressors. Although this technique can be highly effective, designers should consider the liability they may incur from injuries resulting from legitimate users inadvertently coming into contact with them. Additionally, although such plants can provide security for ground-level windows, they may also impede emergency egress.

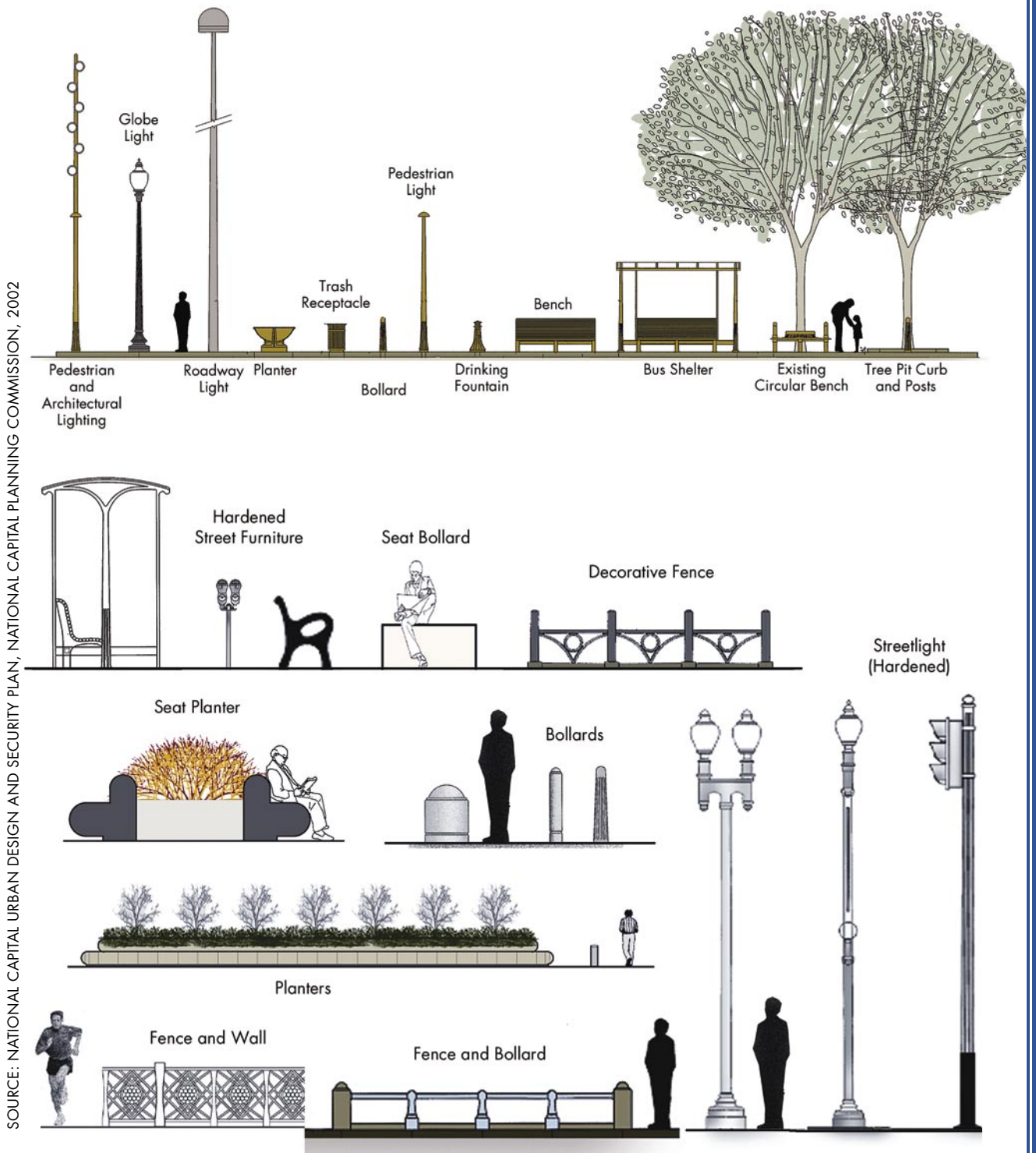
With careful selection, placement, and maintenance, landscape elements can provide visual screening that protects sensitive operations, gathering areas, and other activities from surveillance without creating concealment for covert activity. However, dense vegetation in close proximity to a building can screen illicit activity and should be avoided. Additionally, thick ground cover such as English ivy or vegetation over 4 inches tall such as monkey grass can be used to conceal bombs and other weapons; in setback clear zones, vegetation should be selected and maintained with eliminating concealment opportunities in mind. Similarly, measures to screen visually detractive components such as transformers, trash compactors, and condensing units should be designed to minimize concealment opportunities for people and weapons.

- **Urban design.** Through urban design, practitioners seek to create vibrant, inviting, and functional places for people to live, work, and play. To protect people, property, and operations, and to reduce liability, security should be considered a necessary aspect of these characteristics. If people do not feel safe, they will not use a place and, if a place is not used as intended, it will fail to fulfill its purpose. This failure can, in turn, result in a net loss to the community in terms of social, economic, and environmental sustainability.

Numerous urban design elements present opportunities to provide security. The scale of the streetscape should be appropriate to its primary users, and it can be manipulated to increase the comfort level of desired users while creating a less inviting atmosphere for users with malicious intent. However, even at the pedestrian scale, certain operational requirements must be accommodated. For example, although efficient pedestrian and vehicle circulation systems are important for day-to-day living, they are also critical for emergency response, evacuation, and egress. Furthermore, despite an emphasis on downsizing the scale of the streetscape, it is critical to maintain the maximum stand-off distance possible between vehicles and structures.

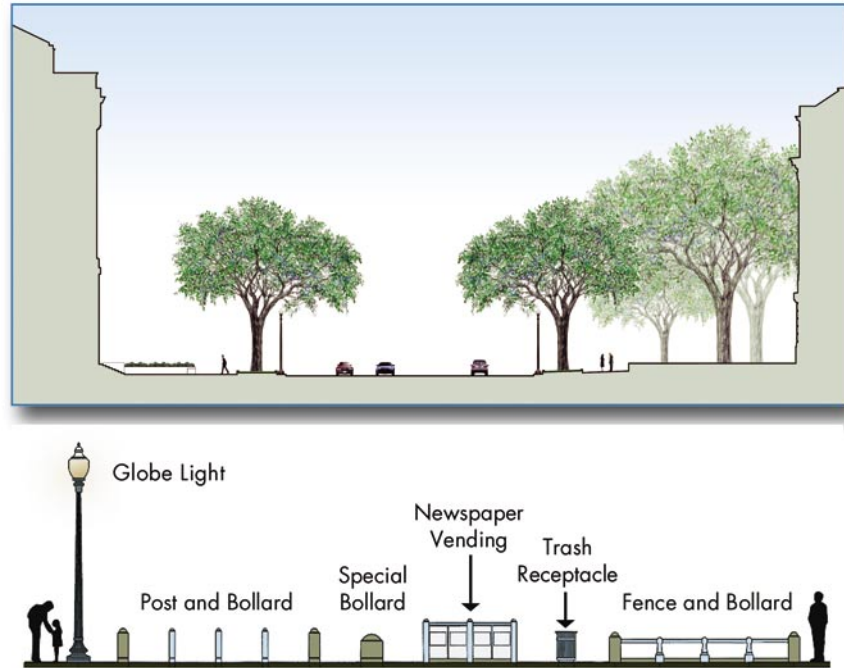
At the site perimeter, walls and fences used for space definition may be hardened to resist the impact of a weapon-laden truck; however, planters, bollards, or decorative boulders could accomplish the same objective in a much more aesthetically pleasing manner. Such an approach also creates permeability, which would allow pedestrians and cyclists to move more easily through the space. Additional information on protective barriers is included in Section 2.4.1.

Similarly, street furniture (e.g., mailboxes, bus stop shelters, light poles, works of art, street trees, planters, bicycle racks, seating, newspaper boxes, kiosks, and trash receptacles) can be used to enhance security (see Figure 2-4). For example, bus stop shelters can be designed to allow for easy surveillance and detection of suspicious activity and objects. Hardened versions of everyday items, such as light poles, planters, benches, street trees (of appropriate size and type), and even water fountains can serve as vehicle barriers. These items maintain stand-off while creating a line of protection that is virtually transparent and highly permeable at the pedestrian scale. Note that in-ground installation of bollards, fences, and any other anti-ram measures should be preceded by an assessment of soil conditions and underground utilities in the immediate vicinity.



SOURCE: NATIONAL CAPITAL URBAN DESIGN AND SECURITY PLAN, NATIONAL CAPITAL PLANNING COMMISSION, 2002

Figure 2-4 Streetscape security elements



SOURCE: NATIONAL CAPITAL URBAN DESIGN AND SECURITY PLAN,  
NATIONAL CAPITAL PLANNING COMMISSION, 2002

Figure 2-4 Streetscape security elements (continued)

A main challenge for the design community is to reach the desired level of protection without turning the building or facility into a bunker or fortress. In other words, they are required to incorporate subtle and aesthetically pleasing security measures when involved in urban design projects. Below are some rules of thumb that should be taken into consideration when designing an urban landscape with a security component:

- Security measures must not impede access to public entrances or pedestrian flow on adjacent sidewalks.
- Landscape elements in the form of grassed plinths, trees, plantings, fountains, and pools are appropriate, but must be designed as integral parts of a building and its setting as much as possible.
- Miscellaneous decorative elements such as flag poles, fountains, pools, gardens, and similar features may be located within an accessway to slow movement or restrict access.

- Trees planted along the inside edge of a public sidewalk and adjacent to pedestrian and vehicular accessways can serve dual aesthetic and barrier purposes.
- The design of bollards, fences, light posts, and other streetscape and landscape elements should form an urban ensemble that helps to create a sense of unity and character.
- Security devices must be designed and located to establish consistent, rhythmic patterns along the street, particularly where a number of elements are used in combination to reduce visual street clutter.
- Security devices must not obstruct pedestrian movement or access by emergency vehicles; therefore, the use of bollards, posts, and chains may be inappropriate when this function is required.

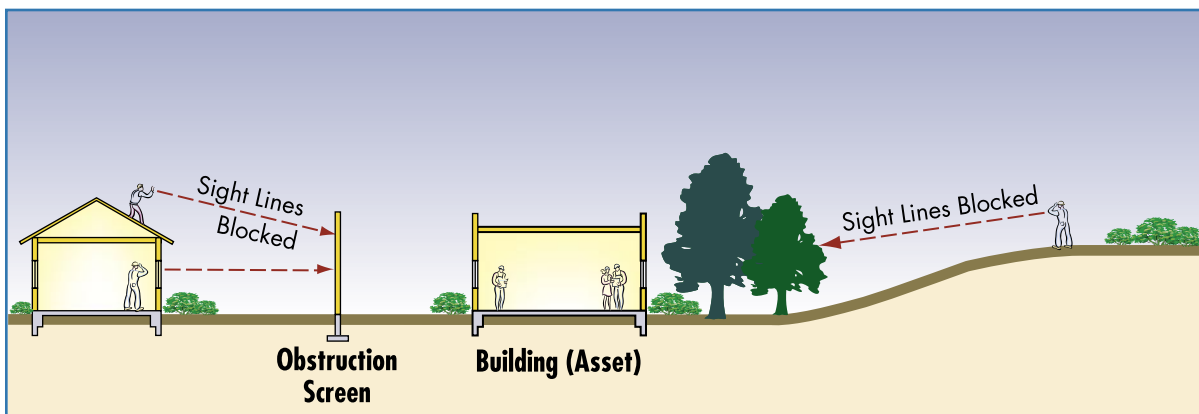
No discussion of using landscape and urban design for security would be complete without a discussion of design-oriented crime prevention strategies such as Crime Prevention Through Environmental Design (CPTED). This approach to design is based on evidence that the design and form of the built environment can influence human behavior. Specifically, CPTED seeks to create a physical environment that discourages criminal activity by incorporating territoriality cues, natural access controls, natural surveillance, support for legitimate activities, and ongoing property maintenance into landscape and urban design. Section 2.12 is a brief overview of CPTED.

Closely related to, but not synonymous with, CPTED is situational crime prevention. This approach encompasses many CPTED principles; however, it focuses on managerial and user behavior factors that affect opportunities for criminal behavior in a specific setting for a specific crime, whereas CPTED focuses on changing the physical design aspects of environments to deter criminal activity. More akin to CPTED is the defensible space approach, in which the emphasis is on structuring the physical layout of space so that its residents are able to establish a sense of ownership and control over common areas in the community. Both of these proactive approaches to crime prevention have merit; designers should care-

fully evaluate the unique requirements of each design problem to identify the most appropriate strategy.

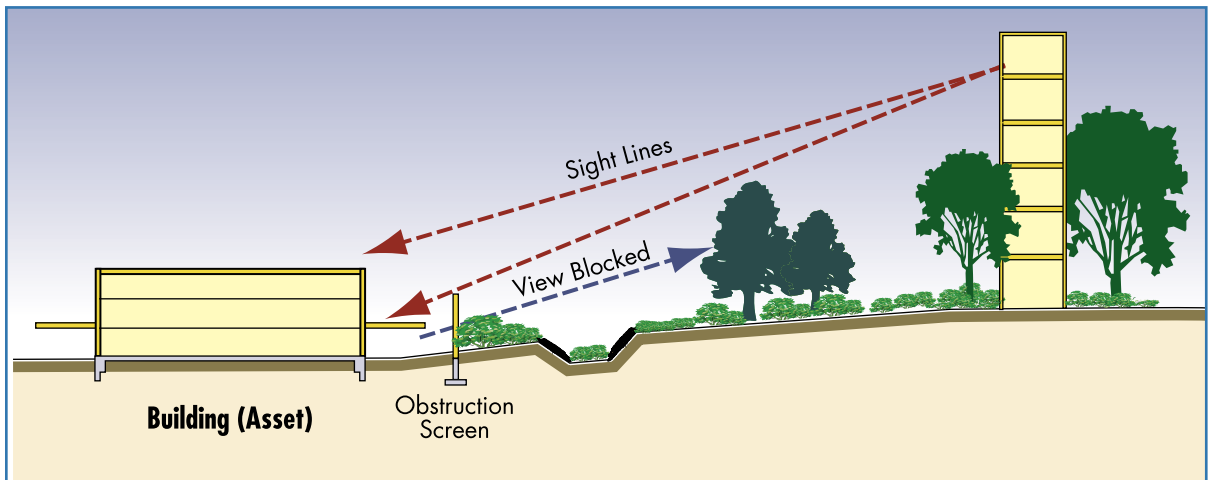
Landscape and urban design inherently define the “line of sight” in a space. Operational security is not a traditional element of master planning, but managing the threat of hostile surveillance is a significant consideration in protecting people, property, and operations. These techniques seek to deny aggressors a “line of sight” to a potential target, either from on or off site. This increases the protection of sensitive information and operations by using stand-off weapons (see Figures 2-5 and 2-6). In addition to the use of various screening options, anti-surveillance measures (e.g., building orientation, landscaping, screening, and landforms) can also be used to block sight lines.

Depending on the circumstances, landforms can be either beneficial or detrimental to anti-surveillance. Elevated sites may enhance surveillance of the surrounding area from inside the facility, but may also allow observation of on-site areas by adversaries. Buildings should not be sited immediately adjacent to higher surrounding terrain, unsecured buildings owned by unfamiliar parties, or vegetation, drainage channels, ditches, ridges, or culverts that can provide concealment. For high-risk buildings, it may be necessary to provide additional protection by creating a clear zone immediately adjacent to the structure that is free of all visual obstructions or landscaping (see Figure 2-7). The clear zone fa-



SOURCE: U.S. AIR FORCE, INSTALLATION  
FORCE PROTECTION GUIDE

Figure 2-5 Blocking of sight lines



SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

Figure 2-6 Improper building siting and view relationships

Facilitates monitoring of the immediate vicinity and visual detection of attacks. Walkways and other circulation features within a clear zone should be located so that buildings do not block views of pedestrians and vehicles. If clear zones are implemented, it may be necessary to implement other anti-surveillance measures.

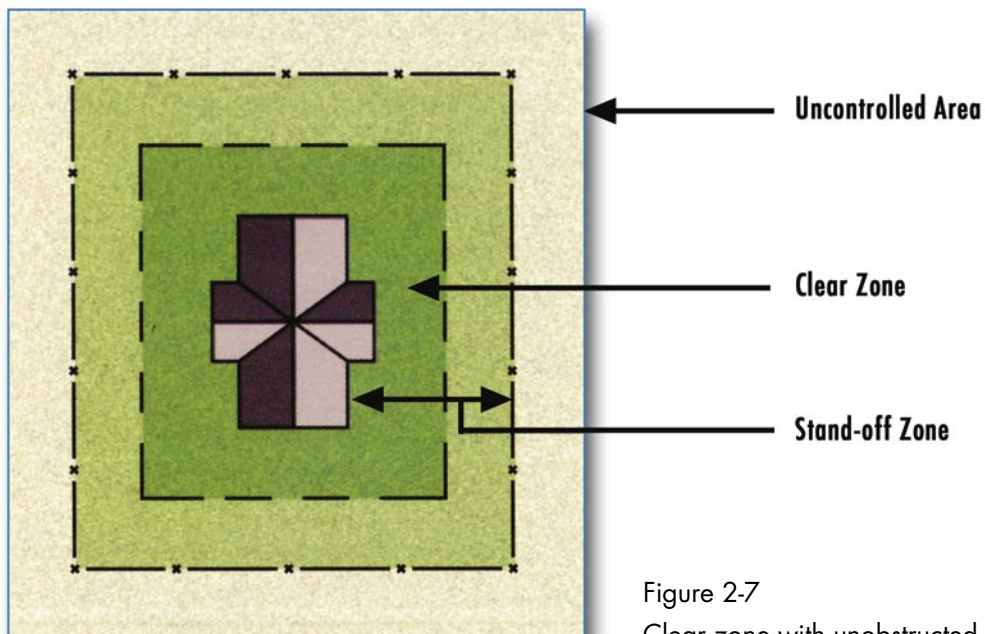


Figure 2-7 Clear zone with unobstructed views

SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

## 2.3 STAND-OFF DISTANCE

Many different measures can be used to provide site design protection. Distance is the most effective and desirable tool because other measures vary in effectiveness, are more costly, and often have unintended consequences. For example, a blast wall can become the source of fragmentation if an explosion occurs in close proximity to it. The most cost-effective solution for mitigating explosive effects is to ensure the explosions occur as far away from the buildings as possible. Stand-off distance and the effects of blast are discussed in Section 4.2.

The distance between an asset and a threat is referred to as the stand-off distance, as shown in Figure 2-8. There is no ideal stand-off distance; it is determined by the type of threat, the type of construction, and desired level of protection. The primary design strategy is to keep terrorists away from inhabited buildings (see Figure 2-9). Although sufficient stand-off distance is not always possible in conventional construction, maximizing the distance may be the most cost-effective solution. Maximizing stand-off distance also ensures that there is opportunity in the future to upgrade buildings to meet increased threats or to accommodate higher levels of protection. Stand-off distance must be coupled

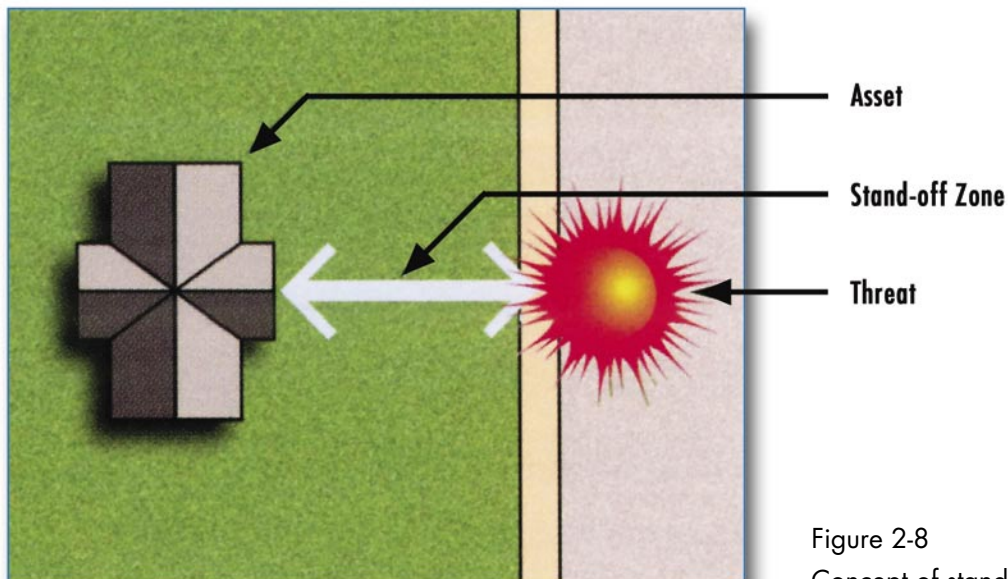


Figure 2-8  
Concept of stand-off distance

SOURCE: U.S. AIR FORCE, *INSTALLATION FORCE PROTECTION GUIDE*



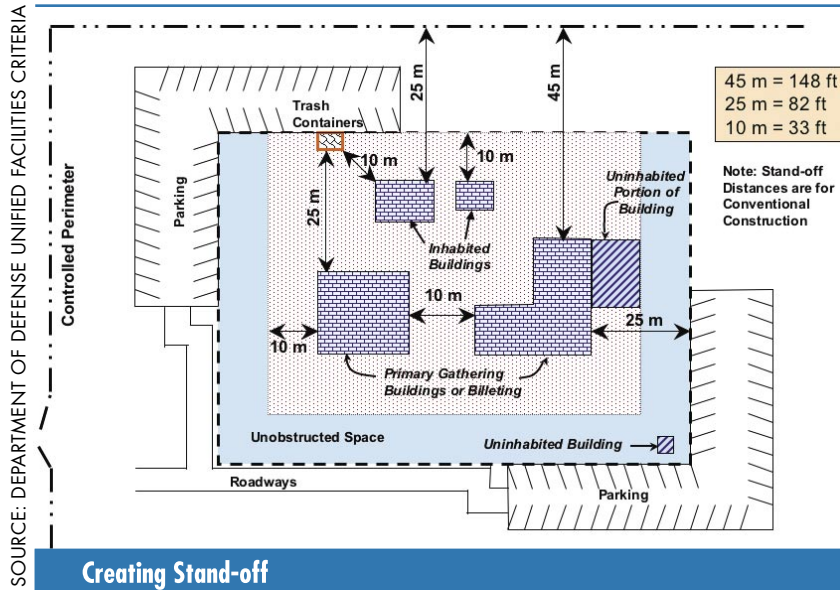
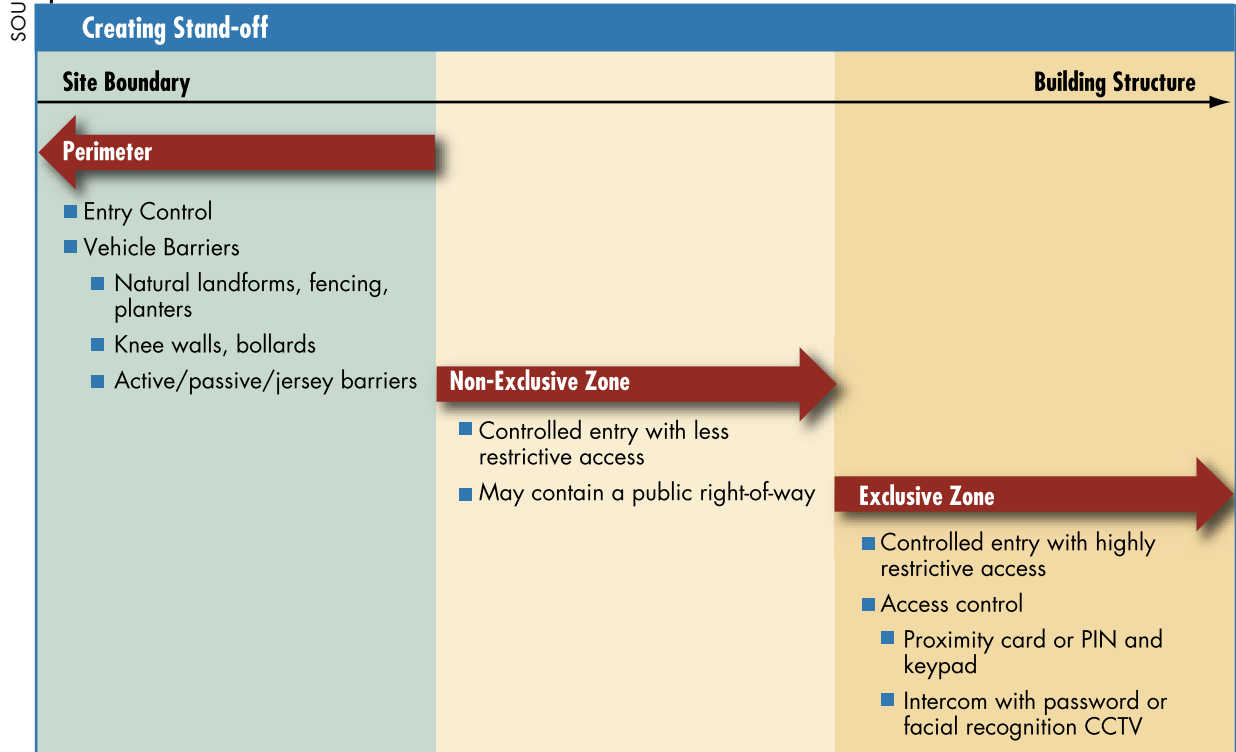


Figure 2-9  
Stand-off distance and building separation



with appropriate building hardening, as discussed in Chapters 3 and 4, to provide the necessary level of protection to assets. Considerations for stand-off distance are as follows:

- The first mode of site protection is to create “keep out zones” that can ensure a minimum guaranteed distance between an explosion (e.g., from a vehicle) and the target structure.

- The perimeter line is the outermost line that can be protected by the security measures incorporated during the design process. It is recommended that the perimeter line be located as far as is practical from the building exterior. Many vulnerable buildings are located in urban areas where only the exterior wall of the building stands between the outside world and the building occupants. In this case, the options are obviously limited. Often, the perimeter line can be pushed out to the edge of the sidewalk by means of bollards, planters, and other obstacles, as discussed earlier in this chapter. To push this line even further outward, restricting or eliminating parking along the curb often can be coordinated with local authorities. In some extreme cases, elimination of loading zones and the closure of streets are an option.
- “Keep out zones” can be achieved with perimeter barriers that cannot be compromised by vehicular ramming. A continuous line of security should be installed along the perimeter of the site to protect it from unscreened vehicles and to keep all vehicles as far away from critical assets as possible.
- When selecting a site for a building, consider its location relative to the site perimeter. Maximize the distance between the perimeter fence and developed areas, providing as much open space as possible inside the fence along the site perimeter.
- The following critical building components should be located away from main entrances, vehicle circulation, parking, and maintenance areas. If this is not possible, harden as appropriate:
  - Emergency generator, including fuel systems, day tank, fire sprinkler, and water supply
  - Normal fuel storage
  - Telephone distribution and main switchgear
  - Fire pumps
  - Building control centers
  - UPS systems powering critical functions

- Main refrigeration systems if critical to building operation
- Elevator machinery and controls
- Shafts for stairs, elevators, and utilities
- Critical distribution feeders for emergency power

## **2.4 CONTROLLED ACCESS ZONES**

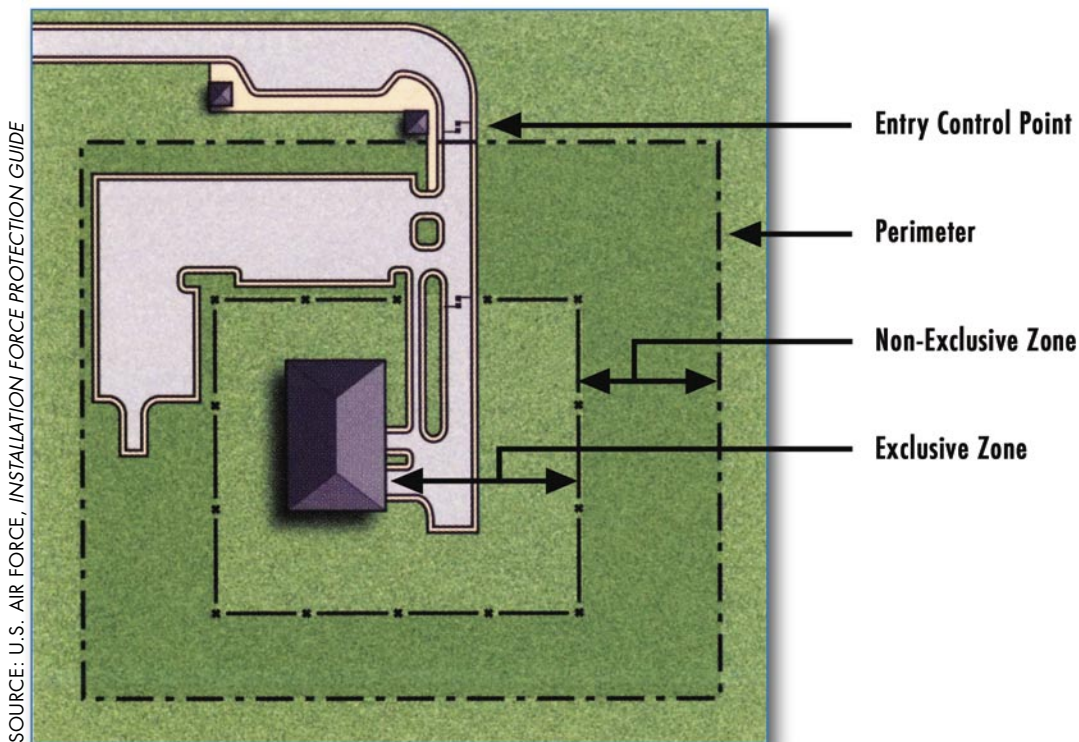
One method to attain the appropriate level of protection and ensure stand-off distance between assets and potential threats is with the creation of a controlled access zone. These zones attempt to limit access to the area immediately surrounding a building. Access to a controlled zone can be restricted by the installation of a physical barrier. Although a controlled access zone is one of the best methods of providing stand-off, such issues as site limitations, building siting, and property line restrictions do not always allow this zone to be created. For additional references, see building placement information in Section 2.2.2.

For high-risk building sites, there is a broad range of “controlled access” elements in security design. Controlled access may range from a complete physical perimeter barrier (full control), to relatively minimal anti-vehicle protection with full pedestrian access, to simply monitoring the perimeter with electronic means.

A good way to ensure appropriate stand-off distance is by establishing controlled zones. These zones define minimum distances between assets and potential threats through the installation of barriers (such as bollards, planters, fountains, walls, and fences), as explained in Section 2.2.5. The barriers are designed to withstand assaults by terrorist vehicles; however, their placement must be designed to allow for access by fire and rescue vehicles in the event of an emergency. Selection of barriers is based on operational considerations related to vehicle access and parking. Good design principles for high-risk buildings endorse the complete surround of a building with a stand-off zone that has perimeters set at distances that consider threat levels, desired level of protection,

building construction, and land availability. Entry into a controlled area should only be through an entry control point.

Controlled access zones may be exclusive or non-exclusive, as shown in Figure 2-10. An exclusive zone is the area surrounding a building within the exclusive control of the building. Anyone entering an exclusive zone must have a purpose related to the building. A non-exclusive zone is either a public right-of-way or an area related to several buildings. Someone entering a non-exclusive zone could be headed for any building within that area. Public access areas outside a downtown building would typically be considered non-exclusive. As explained previously, these measures may not be applicable for all buildings. They are intended for those who need security measures due to their function or location.



SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

Figure 2-10 Exclusive and non-exclusive zones

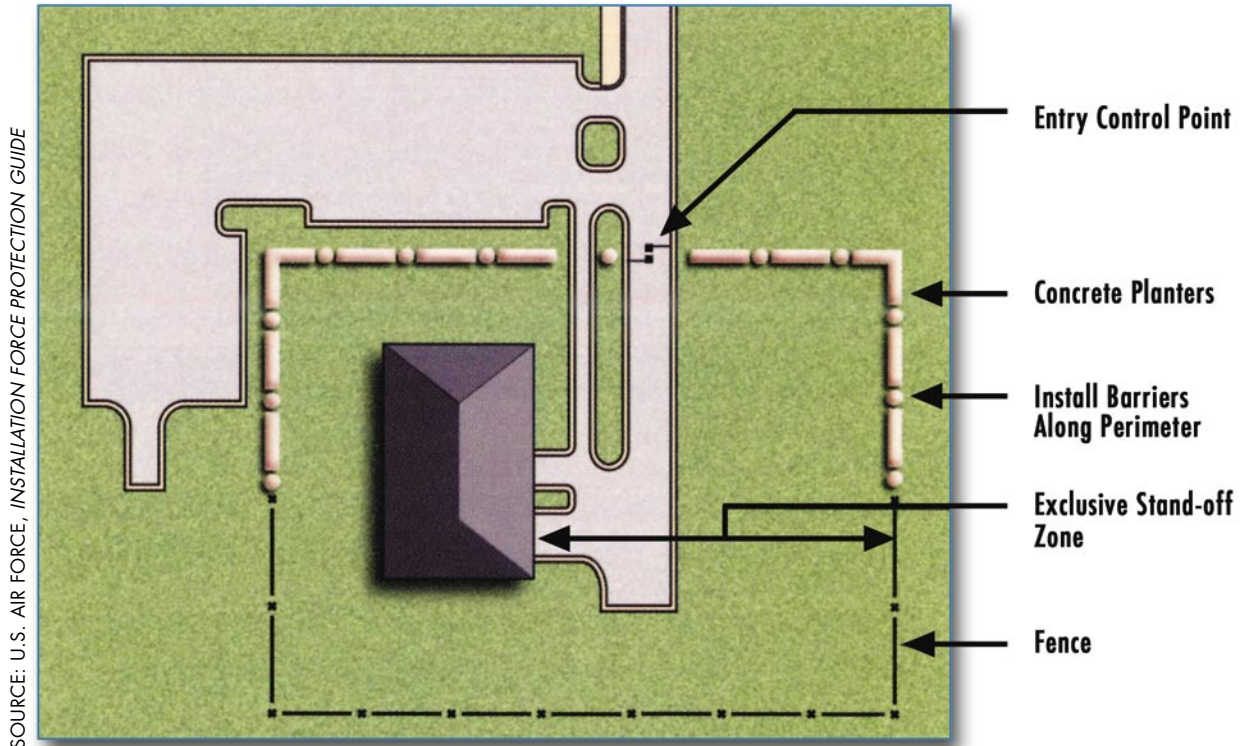
### **2.4.1 Physical Protective Barriers**

A physical barrier is a means of establishing a controlled access area around a building or asset. Physical barriers can be used to define the physical limits of a building or campus and can help to restrict, channel, or impede access and constitute a continuous obstacle around the site. Physical barriers can create a psychological deterrent for anyone planning an unauthorized entry and they can delay or prevent passage into a site. This is especially true of barriers against forced entry by vehicles. The type of barriers utilized can have a direct impact on the number and type of security posts that may be needed to ensure site security. Utility areas (such as water sources, transformer banks, commercial power and fuel connections, heating and power plants, or air conditioning units) may require these barriers for safety standards.

As explained in Section 2.2.5, a number of elements may be used to create a physical barrier, some natural and some manmade. Natural barrier elements include rivers, lakes, waterways, steep terrain, mountains, barren areas, plants, and other terrain features that are difficult to traverse. Manmade elements include fencing, walls, buildings, bollards, planters, concrete barriers, and fountains. Selection of elements must consider the level of security desired and the type of threat most likely to occur. Some perimeter security elements are shown in Figure 2-11.

Fencing is a common means of establishing a physical protective barrier to protect a controlled area. The type of fencing used depends primarily on the threat and the degree of permanence. It may also depend on the availability of materials and the time needed for construction. Fencing may be erected for other uses besides impeding personnel access, such as obstructing views, serving as a means to defeat stand-off weapon systems (e.g., rocket-propelled grenades), and serving as a barrier to hand-thrown weapons (e.g., grenades and firebombs).

Fencing may be used to augment or increase the security of existing barriers that protect restricted areas. Examples include the creation an additional barrier line and an increase in the existing



SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE

Figure 2-11 Application of perimeter barrier elements

fence height. It is important to recognize that fencing provides very little delay when it comes to motivated aggressors, but it can act as a psychological deterrent when an aggressor is deciding which building to attack. The following are commonly used fencing types:

- **Chain-link.** Generally, chain-link fencing is used for protecting permanent limited and exclusion areas. Chain-link fence (including gates) is typically 6-foot high fence fabric, mounted on steel poles that may include a top guard or outrigger. Chain-link fences are usually 9-gauge or heavier, galvanized wire with mesh openings not larger than 2 inches per side and have twisted and barbed selvages at the top and the bottom.
- **Anti-climb (CPTED) fence.** Although different styles of anti-climb fences are available, most consist of vertical bars with horizontal supports designed to make climbing difficult.

- **Barbed wire.** Standard barbed wire is twisted, double-strand wire, with four-point barbs spaced an equal distance apart along the strand. Barbed wire fencing (including gates) intended to prevent human trespassing should not be less than 6 feet high and must be affixed firmly to posts not more than 6 feet apart. Barbed wire may be used as a top guard or outrigger on a standard chain-link fence.
- **Barbed tape or concertina.** A barbed taped obstacle fabricated from 0.025-inch stainless steel tape with barbed clusters. Barbed tape can be deployed, tangle-free, for fast installation without supporting fence posts.
- **Triple-standard concertina wire.** This type of fence uses three rolls of stacked concertina; one roll is stacked on top of two other rolls that run parallel to each other while resting on the ground, forming a pyramid. This fence has been used effectively in lieu of a chain-link fence.
- **Tangle-foot wire.** Tangle-foot wire is an obstruction fence constructed of barbed wire or tape set up outside a single perimeter fence or in the area between double fences to provide an additional deterrent to intruders. Wire or tape is supported on short metal or wooden pickets spaced at irregular intervals of 3 to 10 feet and at heights between 6 and 12 inches. The wire or tape should be criss-crossed to provide a more effective obstacle. The space and materials available govern the depth of the field. Liability issues should be considered when installing a tangle-foot wire.
- **Cable.** Cable or wire rope can be used as a separate, temporary barrier or it may be attached to chain-link or anti-climb fences to provide additional crash resistance.

When necessary, a top guard should be installed on all perimeter fences and may be added to interior enclosures for additional protection. A top guard is an overhang of barbed wire or tape along the top of a fence, facing outward and upward at approximately a 45-degree angle. Placing barbed wire or tape above it can further enhance the top guard. Top guard supporting arms are perma-

nently affixed to the top of fence posts and increase the overall height of the fence. Three strands of barbed wire spaced 6 inches apart must be installed on the supporting arms. (Due to liability issues in some locations, the top guards will not be allowed to face outward where the fence is adjacent to public areas.)

Clear zones should be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the ground adjacent to it. A clear zone of 20 feet or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or manmade features. When possible, a clear zone of 50 feet or more should exist between the perimeter barrier and structures within the protected area, except when the wall of a building constitutes part of the perimeter barrier. Roads within the clear zone should be as close to the perimeter barrier as possible without interfering with it. The roads should be constructed to allow effective road barriers to deter motor movement of unauthorized personnel. When barriers enclose a large area, a perimeter road should be provided for security patrol vehicles on the interior.

Fences may be augmented with additional security systems, such as motion sensors and closed circuit camera systems.

Because barriers can be compromised through breaching (cutting a hole through a fence) or by nature (berms eroded by the wind and rain), they should be inspected and maintained at least weekly. Security personnel should look for signs of deliberate breaches, holes in and under barriers, natural debris building up against barriers, and the proper functioning of locks.

#### **2.4.2 Other Perimeter Barriers**

The exterior of a building may form a part of a perimeter barrier. Brick or block masonry or cast in place concrete walls may act as part of a perimeter barrier. They must be at least 7 feet high and should have a barbed wire top guard, depending on the threat and application. The windows, active doors, and other designated openings should be pro-



tected with fastening bars, grilles, or chain-link screens, and window barriers should be fastened from the inside. If hinged, the hinges and locks must be on the inside to facilitate emergency egress.

Barrier walls designed to resist the effects of an explosion can, in some cases, act to reduce the pressure levels acting on the exterior walls of buildings. They may not, however, enhance security because they prohibit observation of activities occurring on the other side of the wall. In this case, a plinth wall (anti-ram knee wall) with a fence may be an effective solution to combine anti-ram capability and observation.

Consideration should also be given to the improvement of a defensive posture should threat levels increase. A number of temporary or semi-permanent measures may be effective. Expedient methods include blocking access routes with heavy vehicles or temporarily blocking roads surrounding a building to create a form of controlled access area. Figure 2-12 is an example of closing streets to restrict access around a building.

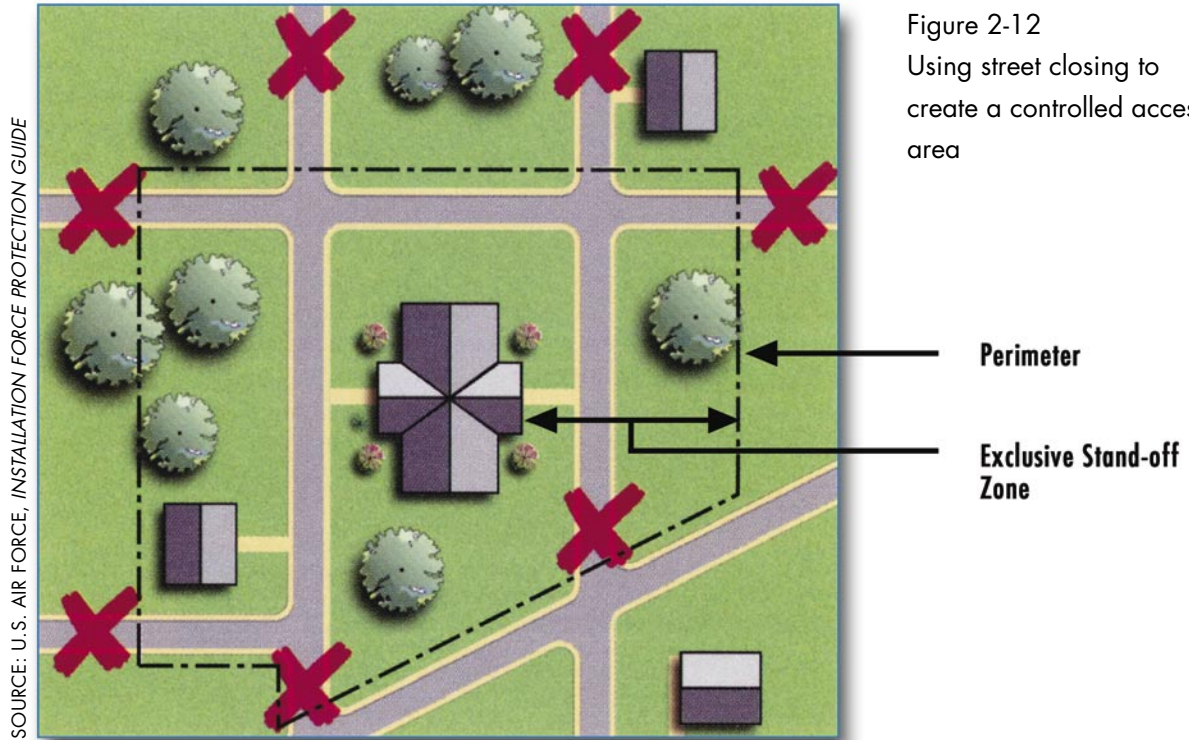


Figure 2-12  
Using street closing to  
create a controlled access  
area

Typically, street closures exclude vehicles, but allow access by pedestrians with proper credentials. The use of street closures must be balanced against minimum circulation/access requirements and fire protection considerations.

If a secured area requires a limited exclusion area on a temporary or infrequent basis, it may not be possible to use physical structural barriers. A limited exclusion area may be established with additional security posts, patrols, and other security measures during the period of restriction. Temporary barriers (including temporary fences, jersey barriers, and vehicles) may also be used.

### **2.4.3 Anti-ram Vehicle Barriers**

Vehicle barriers are a traditional anti-ram solution that prevents vehicle access for pedestrian protection and building security. Vehicle barriers are considered either passive barriers, which are stationary (e.g., fixed bollards, concrete walls, planters, berms), or active barriers, which can typically be retracted or moved out of the way to allow passage (such as retractable bollards, crash beams, and rotating plates). Passive barriers are used to create perimeter or edge protection; active barriers are applicable to roadways, driveways, or entry control points where they can be lowered or raised to prevent passage.

Passive barriers typically consist of bollards, which are concrete filled steel pipes that can be placed every few feet along the curb of a sidewalk to prevent vehicle intrusion (see Figure 2-13). In order to resist the impact of a vehicle, the bollard needs to be fully embedded into a concrete strip foundation that is several feet deep. The height of the bollard above ground should be higher than the bumper of the vehicle, typically 39 to 40 inches. The spacing of the bollards is based on several factors, including Americans with Disabilities Act (ADA) requirements, the minimum width of a vehicle, and the number of bollards required to withstand the impact. As a rule of thumb, the center to center spacing should be between 3 and 5 feet to be effective. The foundation should be designed according to site soil conditions.

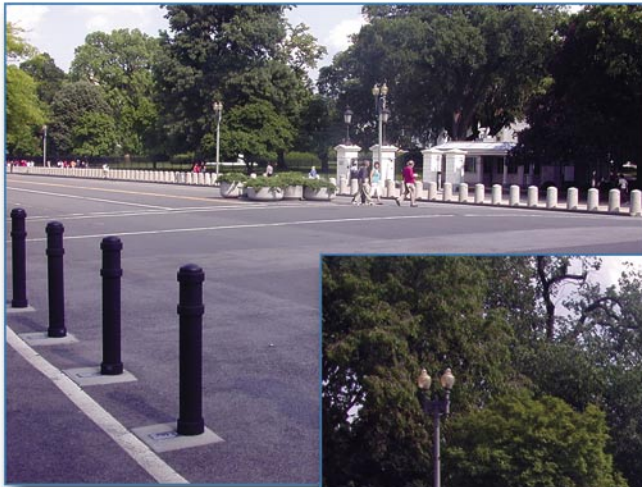


Figure 2-13  
Sample bollard applications



An alternative to a bollard is a plinth wall, which is a continuous low wall constructed of reinforced concrete with a buried foundation. The bollard or plinth wall is designed by equating the kinetic energy of the vehicle at impact with the strain energy absorbed by the barrier and the vehicle.

The foundation of the bollard and plinth wall system can present challenges. For effectiveness, the barriers need to be placed as close to the curb as possible. The property line of buildings often does not extend to the curb. Therefore, a permit may be required by the local authorities to place barriers with foundations near the

curb. To avoid this, building owners are often inclined to place bollards along the property line, which significantly reduces the effectiveness of the barrier system because it reduces the stand-off distance. Sometimes a basement may exist below the pavement that extends to the property line. Embedding a barrier foundation into the basement foundation wall or through the basement roof may introduce water infiltration issues and structural foundation design complications.

Another problem that can arise is below ground utilities that may be close to the pavement surface. Their exact location along the length of the perimeter may not be known. This can be a strong deterrent to selecting barriers with foundations as a solution. For high-risk buildings, it is recommended that these issues be resolved so that a proper anti-ram solution is worked out and installed.

#### **Barrier Design Considerations**

The effectiveness of a barrier is based on the amount of energy it can absorb versus the amount of kinetic energy,  $KE$ , imparted by a head-on vehicle impact:

$$KE = \frac{Mv^2}{2}$$

where  $M$  is the mass of the vehicle and  $v$  is the velocity at the time of impact with the barrier. The angle of approach reduces this energy in non-head-on situations and the energy absorbed by the crushing of the bumper also reduces the energy imparted to the barriers. Because the velocity is squared in this equation, a change in velocity affects the result more than a change in vehicle weight. For this reason, it is important to review lines of approach to ensure that a vehicle does not have a long, straight road to pick up speed before impact.

The vehicle weight used for the design of barriers typically ranges from 4,000 pounds for cars up to 40,000 pounds for trucks. Impact velocities typically range from 30 mph for slanted impact areas (i.e., where the oncoming street is parallel to the curb) up to 50 mph where there is straight-on access (i.e., where the oncoming street is perpendicular to the curb).

For lower-risk buildings without straight-on vehicular access, it may be more appropriate to install surface mounted systems, such as planters, or use landscaping features to deter an intrusion threat. An example of a simple, but effective, landscaping solution is to install a wide permanent planter around the building with a wall that is as high as a car or truck bumper. Individual planters mounted on the sidewalk resist impact through inertia and friction between the planter and the pavement. It can be expected that the planter will move as a result of the impact. Furthermore, to reduce displacement, the planter may be positioned several inches below the pavement surface. A roughened, grouted surface also will improve performance. The objective is to keep the displacement less than the building setback.

In high security sites and at points where access must be provided through an anti-ram perimeter, active or operational anti-ram systems are required. Off-the-shelf products are available that are rated to resist various levels of car and truck impacts (see Figure 2-14). Solutions include crash beams, crash gates, surface mounted plate systems, retractable bollards, and rotating wedge systems.



Figure 2-14 Examples of active and passive vehicle barriers

The following are some security considerations for sites requiring security measures (see also Sections 2.4.1 and 2.4.2):

- Design and select barriers based on threat capabilities.
- If the limited availability of land precludes the creation of an exclusive zone, the use of screening surrounding the building is an alternative.
- Use a combination of barriers. Some barriers are fixed and obvious (fences and gates), while others are passive (sidewalks far away from buildings, curbs with grassy areas, etc.).
- Where physical barriers are required, consider using landscape materials to create barriers that are soft and natural rather than manmade.
- Vehicles can be used as temporary physical barriers if they are placed in front of buildings or across access roads.

- Maintain as much stand-off distance as possible between potential vehicular bombs and the building:
  - Provide traffic obstacles near entry control points to slow down traffic.
  - Consider vehicle barriers at building entries and drives.
  - Offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed.
  - When possible, position gates and perimeter boundary fences outside the blast vulnerability envelope.
  - If the threat level warrants, provide a vehicle crash resistance system in the form of a low wall or earth berm.
- Provide passive vehicle barriers to keep stationary vehicle bombs at a distance from the asset.
  - Use high curbs, low berms, shallow ditches, trees, shrubs, and other physical separations to keep stationary bombs at a distance.
  - Do not allow vehicles to park next to perimeter walls of the secured area. Consider using bollards or other devices to keep vehicles away.

## **2.5 ENTRY CONTROL AND VEHICULAR ACCESS**

If a perimeter barrier is employed, it will be necessary to provide points of access through the perimeter for building users (i.e., employees, visitors, and service providers). An entry control point or guard building serves well as the designated point of entry for site access. It provides a point for implementation of desired/required levels of screening and access control; an example is shown in Figure 2-15. The objective of the entry control point is to prevent unauthorized access while maximizing the rate of authorized access by foot or vehicle. These measures are not required for all sites and buildings; they are only required for those considered at high risk.

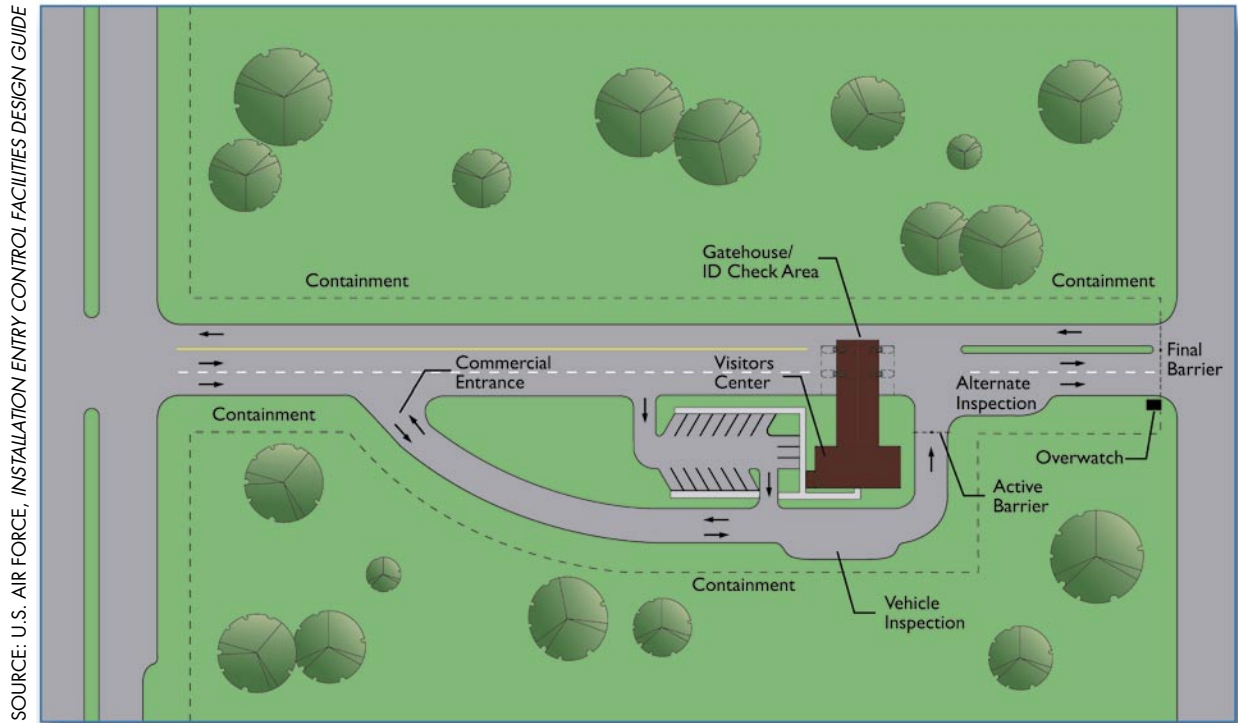


Figure 2-15 Combined multi-user gate

Location selection for vehicular access and entry control for a building starts with an evaluation of the anticipated demand for access to the controlled site. An analysis of traffic origin and destination, and an analysis of the capability of the surrounding connecting road network, including its capacity to handle additional traffic, should then be performed. Expansion capacity should also be considered. The analysis should be coordinated with the state and local departments of transportation.

The existing terrain can have a significant impact on the suitability of a potential entry control point site. Flat terrain with no thick vegetation is generally preferred. A gentle rise in elevation up to the entry control guard building allows for a clear view of arriving vehicles. Consider how existing natural features such as bodies of water or dense tree stands may enhance perimeter security and vehicle containment. Entry control spatial requirements vary, depending on the type, the traffic demand, and the necessary security measures.

In commercial buildings or campuses, more than one type of entry may be required to accommodate the three basic types of traffic (site personnel, visitors, and commercial traffic). Active perimeter entrances should be designated so that security personnel can maintain full control without creating unnecessary delays in traffic. This could be accomplished with a sufficient number of entrances to accommodate the peak flow of pedestrian and vehicular traffic, and adequate lighting for rapid and efficient inspection. Some entrances may be closed during non-peak periods, and should be securely locked, illuminated during hours of darkness, and inspected periodically. Additionally, warning signs should be used to warn drivers when gates are closed. Doors and windows on buildings that form a part of the perimeter should be locked, lighted, and inspected regularly.

The following measures should be considered in the design of entry control points:

- Design entry roads to sites and to individual buildings so that they do not provide direct or straight-line vehicular access to high-risk buildings. Route major corridors away from concentrations of high-risk buildings.
- Design access points at an angle to oncoming streets so that it is difficult for a vehicle to gain enough speed to break through the stations.
- Minimize the number of access roads and entrances into a building or site.
- Designate entry to the site for commercial, service, and delivery vehicles, preferably away from high-risk buildings whenever possible.
- Design the entry control point and guard building so that the authorization of approaching vehicles and occupants can be adequately assessed, and the safety of both gate guards and approaching vehicles can be maintained during periods of peak volume.



- Approach to the site should be designed to accommodate peak traffic demand without impeding traffic flow in the surrounding road network.
- Provide pull-over lanes at site entry gates to check suspect vehicles. When necessary, provide a visitor/site personnel inspection area to check vehicles prior to allowing access to a site or building.
- Design active vehicle crash barriers (e.g., road alignment, retractable bollards, swing gates, or speed bumps) as may be required to control vehicle speed and slow incoming vehicles to give entry control personnel adequate time to respond to unauthorized activities.
- Design the inspection area so that it is not visible to the public, when necessary. Place appropriate landscape plantings to accomplish screening.
- Consider current and future inspection technologies (e.g., above vehicle and under vehicle surveillance systems, ion scanning, and x-ray equipment).
- Provide inspection bays that can be enclosed to protect inspection equipment in the event of bad weather.
- Design inspection areas that are large enough to accommodate a minimum of one vehicle and a pull-out lane. They should also be covered and capable of accommodating the inspection of the undercarriage plus overhead inspection equipment.
- If space is available, provide traffic queuing for vehicles needing authorization.
- Consider providing a walkway and turnstile for pedestrians and a dedicated bicycle lane.
- If possible, provide a gatehouse for the workstations and communications equipment of the security personnel. It may also serve as a refuge in the event of an attack.
- Provide some measure of protection against hostile activity if ID checking is required between the traffic lanes.

- For high security buildings, provide a final denial barrier to stop unauthorized vehicles from entering the site. Most individuals who may attempt to enter without authorization are lost, confused, or inattentive, but there are also those whose intent may be to “run the gate.” A properly designed final denial barrier will take into account both groups, safely stopping the individuals who have made an honest mistake, but providing a properly designed barrier to stop those with hostile intentions.
- Design the barrier system to impede both inbound and outbound vehicles. The system should include traffic control features to deter inbound vehicles from using outbound lanes for unauthorized access. Barrier devices that traverse both roadways should be included in the design. The safety features discussed above for inbound lanes should also be provided in the outbound lanes.

## **2.6 SIGNAGE**

Wayfinding is an important function of design that illustrates the importance of coordination among practitioners and community planning, public works, transportation, law enforcement, and fire-rescue organizations. The ability of users to navigate an unfamiliar environment is important for its success on a day-to-day basis, but will become critical in an emergency situation. In addition to overt prompts such as landmarks, architectural elements, and clear, consistent signage and maps, users will subconsciously rely on cues from their surroundings to help them select a path to safety. Similarly, emergency responders will depend in part on these design elements in order to navigate the scene.

Signs are an important element of security. They are meant to keep intruders out of restricted areas; however, inadequate signs can create confusion and defeat their primary purpose. Confusion over site circulation, parking, and entrance locations can contribute to a loss of site security. Signs should be provided off site and at entrances. There should be on-site directional,

parking, and cautionary signs for visitors, employees, service vehicles, and pedestrians. Unless required, signs should not identify sensitive areas. A comprehensive signage plan should include the following:

- Prepare signs for each entry control building.
- Prepare entry control procedures signs, which explain current entry procedures for drivers and pedestrians.
- Prepare traffic regulatory and directional signs, which control traffic flow and direct vehicles to specific appropriate points.
- Consider using street addresses or building numbers instead of detailed descriptive information inside the site.
- Minimize the number of signs identifying high-risk buildings; however, a significant number of warning signs should be erected to ensure that possible intruders are aware of entry into restricted areas.
- Minimize signs identifying critical utility complexes (e.g., power plants and water treatment plants). Post clear signs to minimize accidental entry by unauthorized personnel into critical asset areas.
- Install warning signs that are easy to understand along the physical barriers and at each entry point.
- Warning signs must use both (or more) languages in areas where two or more languages are commonly spoken. The wording on the signs should denote warning of a restricted area. The signs should be posted at intervals of no more than 100 feet and should not be mounted on fences equipped with intrusion-detection equipment. Additionally, the warning signs should be posted at all entrances to limited, controlled, and exclusion areas.
- Locate variable message signs, which give information on site/organization special events and visitors, far inside site perimeters.

## **2.7 PARKING**

Parking restrictions can help to keep potential threats away from a building. In urban settings, however, curbside or underground parking is often necessary and sometimes difficult to control. Mitigating the risks associated with parking requires creative design measures, including parking restrictions, perimeter buffer zones, barriers, structural hardening, and other architectural and engineering solutions. Operational measures may also be necessary to inspect or screen vehicles entering parking garages. The following considerations may help designers to implement sound parking measures for buildings that may be at high risk:

- Locate vehicle parking and service areas away from high-risk buildings to minimize blast effects from potential vehicle bombs.
- Restrict parking from the interior of a group of buildings.
- If possible, locate visitor or general public parking near, but not on, the site itself.
- Restrict parking within the secured perimeter of an asset from unauthorized personnel.
- Locate general parking in areas that present the fewest security risks to personnel.
- If possible, design the parking lot with one-way circulation to facilitate monitoring for potential aggressors.
- Locate parking within view of occupied buildings.
- Prohibit parking within the stand-off zone.
- When establishing parking areas, provide emergency communication systems (e.g., intercom, telephones, etc.) at readily identified, well-lighted, closed circuit television monitored locations to permit direct contact with security personnel.
- Provide parking lots with closed circuit television cameras connected to the security system and adequate lighting capable of displaying and videotaping lot activity.

- Request appropriate permits to restrict parking in curb lanes in densely populated areas to company-owned vehicles or key employee vehicles.
- Provide appropriate setback from parking on adjacent properties if possible. Structural hardening may be required if the setback is insufficient. In new designs, it may be possible to adjust the location of the building on the site to provide adequate setback from adjacent properties.
- If possible, prohibit parking beneath or within a building.
- If parking beneath a building is unavoidable, limit access to the parking areas and ensure they are secure, well-lighted, and free of places of concealment.
- Do not permit uninspected vehicles to park under a building or within the exclusive zone. If parking within the building is required, the following restrictions may be applied:
  - Public parking with ID check
  - Company vehicles and employees of the building only
  - Selected company employees only, or those requiring security
- Apply the following when parking inside a building is necessary and the building superstructure is supported by the parking structure:
  - Protect primary vertical load carrying members by implementing architectural or structural features that provide a minimum 6-inch stand-off from the face of the member.
  - Design columns in the garage area for an “unbraced length” equal to two floors, or three floors where there are two levels of parking.
- For all standalone, aboveground parking garages, maximize visibility for surveillance into, out of, and across the garage.

- Employ express or non-parking ramps, sending the user to parking on flat surfaces.
- Avoid dead-end parking areas, as well as nooks and crannies.
- Design landscaping that does not provide hiding places. It is desirable to locate plantings away from parking garages and parking lots to permit observation of pedestrians.

Additional parking considerations include:

- Stairways and elevator lobby design should be as open as code permits. The ideal solution is a stair and/or elevator waiting area totally open to the exterior and/or the parking areas. Designs that ensure that people using these areas can be easily seen (and can see out) should be encouraged. If a stair must be enclosed for code or weather protection purposes, glass walls can be used to deter potential attacks. Potential hiding places below stairs and within and around stairwells should be closed off.
- Elevator cabs should have glass backs whenever possible. Elevator lobbies should be well-lighted and visible to both patrons in the parking areas and the people outside the building.
- Pedestrian paths should be designed to concentrate activity to the extent possible. For example, bringing all pedestrians through one portal rather than allowing them to disperse to numerous access points improves the ability to see and be seen by other users. Limiting vehicular entry/exits to a minimum number of locations is also beneficial.

## **2.8 LOADING DOCKS AND SERVICE ACCESS**

Loading docks and service access areas are commonly required for a building and are typically desired to be kept as invisible as possible. For this reason, special attention should be devoted to these service areas in order to avoid undesirable intruders. Design criteria for loading docks and service access include the following:

- Separate (by at least 50 feet) loading docks and shipping and receiving areas in any direction from utility rooms, utility

mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.

- Locate loading docks so that vehicles will not be allowed under the building. If this is not possible, the service should be hardened for blast. Loading dock design should limit damage to adjacent areas and vent explosive forces to the exterior of the building.
- If loading zones or drive-through areas are necessary, monitor them and restrict height to keep out large vehicles.
- Avoid having driveways within or under buildings.
- Significant structural damage to the walls and ceiling of the loading dock may be acceptable; however, the areas adjacent to the loading dock should not experience severe structural damage or collapse. Provide adequate design to prevent extreme damage to loading docks. The floor of the loading dock does not need to be designed for blast resistance if the area below is not occupied and/or does not contain critical utilities.
- Provide signage to clearly mark separate entrances for deliveries.

## **2.9 PHYSICAL SECURITY LIGHTING**

Security lighting should be provided for overall site/building illumination and the perimeter to allow security personnel to maintain visual-assessment during darkness. It may provide both a real and psychological deterrent for continuous or periodic observation. Lighting is relatively inexpensive to maintain and may reduce the need for security personnel by reducing opportunities for concealment and surprise by potential attackers. Lighting is particularly desirable for sensitive areas of a site such as pier and dock areas, vital buildings, storage areas, and vulnerable control points in communications, power, and water distribution systems. It facilitates detection of unauthorized personnel and makes the job of an attacker more difficult.

At entry control points, a minimum surface lighting average of 4 horizontal foot-candles will help ensure adequate lighting for pedestrians, islands, and guards. Where practical, high-mast lighting is recommended, because it gives a broader, more natural light distribution, requires fewer poles (less hazardous to the driver), and is more aesthetically pleasing than standard lighting. Lighting of the entry control point should give drivers a clear view of the gatehouse and, for security personnel, it gives a clear view of the drivers and vehicles.

The type of site lighting system used depends on the overall requirements of the site and the building. Four types of lighting are used for security lighting systems:

- **Continuous lighting** is the most common security-lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light. Two primary methods of using continuous lighting are glare projection and controlled lighting:
  - The glare projection security-lighting method lights the area surrounding a controlled area with high-intensity lighting. It is a strong deterrent to a potential intruder because it makes him or her very visible while making it difficult to see inside the secure area. Guards are protected by being kept in comparative darkness while being able to observe intruders at a considerable distance. This method should not be used when the glare of lights directed across the surrounding territory could annoy or interfere with adjacent operations.
  - Controlled lighting is best when there are limits to the lighted area outside the perimeter, such as along highways. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit the particular need. This method of lighting may illuminate or silhouette security personnel.



- **Standby lighting** has a layout similar to continuous lighting; however, the lights are not continuously lit, but are either automatically or manually turned on when suspicious activity is detected or suspected by security personnel or alarm systems.
- **Movable lighting** consists of manually operated, movable searchlights that may be lit during hours of darkness or as needed. The system normally is used to supplement continuous or standby lighting.
- **Emergency lighting** is a backup power system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source such as installed or portable generators or batteries. Consider emergency/backup power for security lighting as determined to be appropriate.

## **2.10 SITE UTILITIES**

Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. Additional information on mechanical systems is presented in Section 3.4. To minimize the possibility of such hazards, apply the following measures:

- Where possible, provide underground, concealed, and protected utilities.
- Provide redundant utility systems to support site security, life safety, and rescue functions.
- Consider quick connects for portable utility backup systems if redundant sources are not available.
- Prepare vulnerability assessments for all utility services to the site, including all utility lines, storm sewers, gas transmission

lines, electricity transmission lines, and other utilities that may cross the site perimeter.

- Protect water treatment plants and storage tanks from waterborne contaminants by securing access points, such as manholes. Maintain routine water testing to help detect waterborne contaminants.
- Minimize signs identifying critical utility complexes (e.g., power plants and water treatment plants). Provide fencing to prevent unauthorized access and use landscape planting to conceal aboveground systems.
- Locate petroleum, oil, and lubricant storage tanks and operations buildings downslope from all other buildings. Site fuel tanks at an elevation lower than operational buildings or utility plants. Locate fuel storage tanks at least 100 feet from buildings.
- Locate the main fuel storage away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).
- Provide utility systems with redundant or loop service, particularly in the case of electrical systems. Where more than one source or service is not currently available, provisions should be made for future connections. In the interim, consider “quick connects” at the building for portable backup systems.
- Decentralize a site’s communications resources when possible; the use of multiple communications networks will strengthen the communications system’s ability to withstand the effects of a terrorist attack. Careful consideration should be made in locating, concealing, and protecting key network resources such as network control centers.
- Place trash receptacles as far away from the building as possible; trash receptacles should not be placed within 30 feet of a building.
- Conceal incoming utility systems within building and property lines, and give them blast protection, including burial or proper encasement, wherever possible.

- Consider incorporating low impact development practices to enhance security, such as retaining stormwater on site in a pond to create stand-off, instead of sending into the sewer system.
- Locate utility systems at least 50 feet from loading docks, front entrances, and parking areas.
- Route critical or fragile utilities so that they are not on exterior walls or on walls shared with mailrooms.
- Where redundant utilities are required in accordance with other requirements or criteria, ensure that the redundant utilities are not collocated or do not run in the same chases. This minimizes the possibility that both sets of utilities will be adversely affected by a single event.
- Where emergency backup systems are required, ensure they are located away from the systems components for which they provide backup.
- Mount all overhead utilities and other fixtures weighing 31 pounds (14 kilograms) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This standard does not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards.
- To limit opportunities for aggressors placing explosives underneath buildings, ensure that access to crawl spaces, utility tunnels, and other means of under building access is controlled.

All utility penetrations of a site's perimeter barrier, including penetrations in fences, walls, or other perimeter structures, should be sealed or secured to eliminate openings large enough to pass through the barrier. Typical penetrations could be for storm sewers, water, electricity, or other site

utility services. Specific requirements of various openings are discussed below:

- All utility penetrations of the site’s perimeter should be screened, sealed, or secured to prevent their use as access points for unauthorized entry into the site. If access is required for maintenance of utilities, secure all penetrations with screening, grating, latticework, or other similar devices so that openings do not allow intruder access. Provide intrusion detection sensors and consider overt or covert visual surveillance systems if warranted by the sensitivity of assets requiring protection.
- Drainage ditches, culverts, vents, ducts, and other openings that pass through a perimeter and that have a cross-sectional area greater than 96 square inches and whose smallest dimension is greater than 6 inches should be protected by securely fastened welded bar grilles. As an alternative, drainage structures may be constructed of multiple pipes, with each pipe having a diameter of 10 inches or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. Ensure that any addition of grills or pipes to culverts or other drainage structures is coordinated with the engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.
- Manhole covers 10 inches or more in diameter must be secured to prevent unauthorized opening. They may be secured with locks and hasps, by welding them shut, or by bolting them to their frame. Ensure that hasps, locks, and bolts are made of materials that resist corrosion. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available. If very high security is required, manhole covers that resist shattering after being artificially “frozen” by an aggressor should be considered.

## **2.1.1 SUMMARY OF SITE MITIGATION MEASURES**

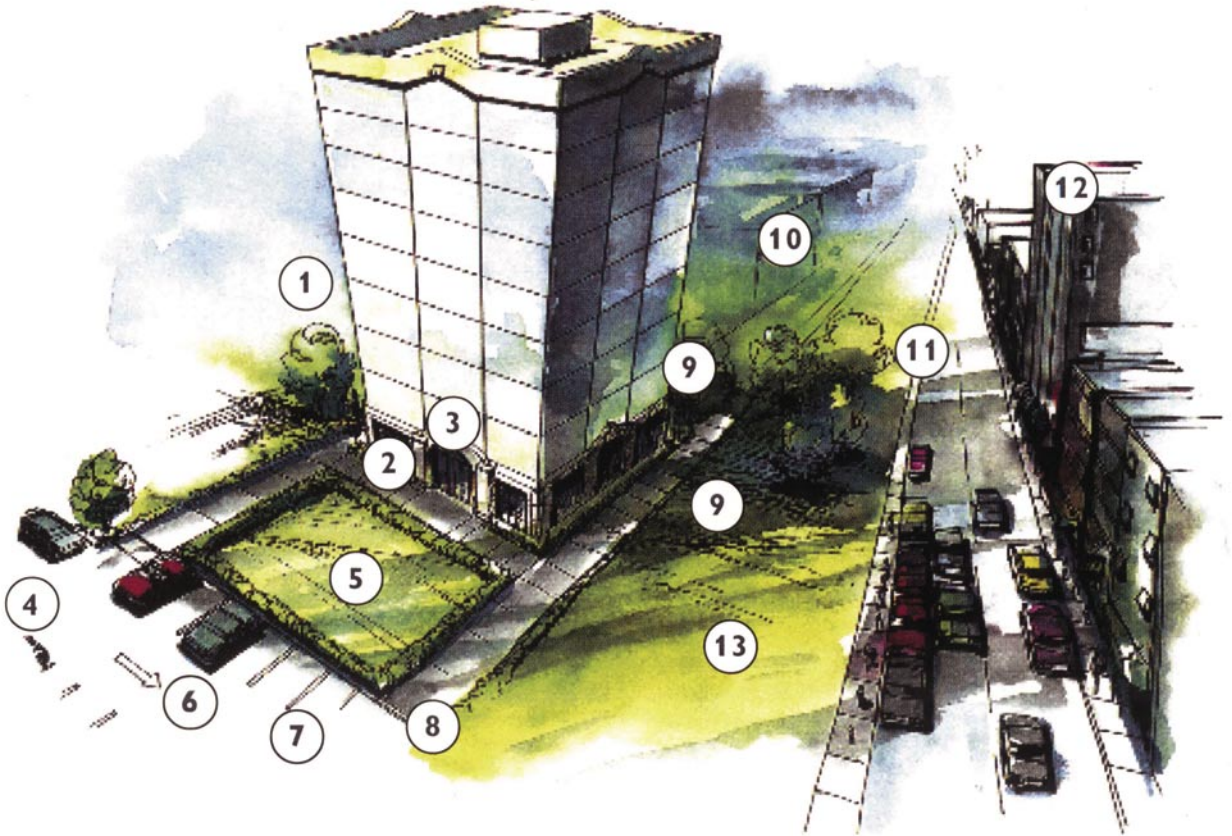
A general spectrum of site mitigation measures ranging from the least protection, cost, and effort going to the greatest protection, cost, and effort is presented below. Detailed discussions of individual measures can be found earlier in the chapter. This is a nominal ranking of mitigation measures. In practice, the effectiveness and cost of individual mitigation measures may be different for specific applications. Figure 2-16 is a graphic summary of site mitigation measures to protect building occupants. Table 2-1 correlates mitigation measures to specific threats.

**Less Protection  
Less Cost  
Less Effort**

- Place trash receptacles as far away from the building as possible.
- Remove any dense vegetation that may screen covert activity.
- Use thorn-bearing plant materials to create natural barriers.
- Identify all critical resources in the area (fire and police stations, hospitals, etc.).
- Identify all potentially hazardous facilities in the area (nuclear plants, chemical labs, etc.).
- Use temporary passive barriers to eliminate straight-line vehicular access to high-risk buildings.
- Use vehicles as temporary physical barriers during elevated threat conditions.
- Make proper use of signs for traffic control, building entry control, etc. Minimize signs identifying high-risk areas.
- Identify, secure, and control access to all utility services to the building.
- Limit and control access to all crawl spaces, utility tunnels, and other means of under building access to prevent the planting of explosives.
- Utilize Geographic Information Systems (GIS) to assess adjacent land use.
- Provide open space inside the fence along the perimeter.
- Locate fuel storage tanks at least 100 feet from all buildings.
- Block sight lines through building orientation, landscaping, screening, and landforms.
- Use temporary and procedural measures to restrict parking and increase stand-off.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much stand-off distance as possible from potential vehicle bombs.
- Separate redundant utility systems.
- Conduct periodic water testing to detect waterborne contaminants.
- Enclose the perimeter of the site. Create a single controlled entrance for vehicles (entry control point).
- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed circuit television cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate stand-off for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Do not site the building adjacent to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. For better stand-off, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or through street closings.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.
- Install active vehicle crash barriers.

**Greater  
Protection  
Greater Cost  
Greater Effort**

SOURCE: U.S. AIR FORCE, INSTALLATION FORCE PROTECTION GUIDE



1. Locate assets stored on site, but outside the building within view of occupied rooms in the facility.	8. Minimize vehicle access points.
2. Eliminate parking beneath buildings.	9. Eliminate potential hiding places near the building; provide an unobstructed view around building.
3. Minimize exterior signage or other indications of asset locations.	10. Site building within view of other occupied buildings on the site.
4. Locate trash receptacles as far from the building as possible.	11. Maximize distance from the building to the site boundary.
5. Eliminate lines of approach perpendicular to the building.	12. Locate building away from natural or manmade vantage points.
6. Locate parking to obtain stand-off distance from the building.	13. Secure access to power/heat plants, gas mains, water supplies, and electrical service.
7. Illuminate building exteriors or sites where exposed assets are located.	

Figure 2-16 Summary of site mitigation measures

Table 2-1: Correlation of Mitigation Measures to Threats\*

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
<p>■ The symbols indicate which of the protective measures shown in the left-hand column can be effective in countering the types of threats indicated across the top of the chart.</p>									
<b>LAND USE CONSIDERATIONS</b>									
Locate high-risk land uses in the interior of the site	■	■	■	■	■				
Consolidate high-risk land uses	■	■	■	■	■				
Include stand-off areas in land area requirements	■	■		■	■				
Consider effects of off-property development	■	■	■		■				
<b>SITE PLANNING</b>									
Maximize distance from perimeter fence and developed areas	■	■	■	■	■			■	
Site critical facilities on higher ground	■	■	■	■	■			■	■
Avoid areas with adjacent high terrain or structures			■	■	■			■	■
Avoid areas with adjacent dense vegetation			■	■	■				
Avoiding low-lying topographic areas			■	■	■			■	■
Provide separation between facilities	■	■	■	■	■		■		
Site facilities within view of other occupied facilities						■			
Cluster facilities with similar threat levels	■	■		■	■				
Create complexes to enhance surveillance opportunities	■	■	■	■	■				
Eliminate vehicle parking from interior of building complexes	■	■							
High surrounding terrain			■	■	■				
Distance from non-building facilities	■	■	■	■	■	■		■	■
Areas that provide concealment		■	■	■	■	■			



Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Earth berms		■	■	■	■				
Bodies of water	■	■	■	■	■	■			
Depressions			■	■	■				
Protect against unwanted surveillance			■	■	■	■			
“Defensible space”		■	■			■			
Vehicle access	■	■							
Dense thorn-bearing vegetation			■			■			
Vegetation screens		■	■	■	■	■			
Location of trash receptacles							■		
<b>STAND-OFF DISTANCE</b>									
Stand-off zone	■	■		■	■	■			
<b>CONTROLLED ACCESS ZONES</b>									
Exclusive zone/Non-exclusive zone	■	■				■			
Clear zone	■	■				■			
Fencing and physical barriers	■	■	■	■	■	■			
Active barriers	■	■	■	■	■	■			
Passive barriers	■	■	■			■			
<b>ENTRY CONTROL AND VEHICULAR ACCESS</b>									
Minimize access roads	■	■				■	■		
Control points	■	■	■	■	■	■			

Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Active monitoring	■	■	■	■	■	■	■	■	■
Provide enhanced protection at property entrances	■	■	■	■	■	■			
Include pull-over lanes at checkpoints to inspect vehicles	■	■	■	■	■	■			
Avoid straight-line vehicular access to high-risk resources	■	■							
Avoid straight-line entry approach roads	■	■							
Locate vehicle parking areas far from high-risk resources	■	■							
Provide separate service and delivery access	■	■							
Route major corridors away from high-risk resources	■	■		■	■				
Locate high-risk resources remote from primary roads	■	■		■	■				
Minimize directional identification signs	■	■	■	■	■	■			
Limit vehicular access to high-risk resources	■	■	■	■	■	■			
<b>SIGNAGE</b>									
Minimize signage	■	■	■	■	■	■	■	■	■
<b>PARKING</b>									
View of parking		■							
Parking under a building		■							
Parking at interior of facility		■							
Parking near high-risk areas		■							

Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Parking in exclusive zone		■							
One-way circulation	■	■	■			■			
<b>LOADING DOCKS AND SERVICE ACCESS</b>									
Loading/unloading docks		■					■		
Driveways under facilities	■	■							
<b>PHYSICAL SECURITY LIGHTING</b>									
Lighting		■	■			■			
<b>SITE UTILITIES</b>									
Provide protection at culverts, sewers, and pipelines					■	■			■
Provide protection at concrete trenches, storm drains, and duct systems					■	■			■
Provide and check locks on manhole covers					■	■			■
Minimize signs identifying utility systems					■	■			■
Provide fencing at critical utility complexes						■			■
Use landscape planting to conceal aboveground systems						■			■
Install utilities underground	■	■	■	■	■	■	■		
Locate fuel/lube storage downslope and away from facilities	■	■	■	■	■	■	■		
Provide redundant utility systems and loop service	■	■	■	■	■	■	■		
Provide utility “quick disconnects” for portable backup systems	■	■	■	■	■	■	■		

Table 2-1: Correlation of Mitigation Measures to Threats\* (continued)

	Moving Vehicle Bomb	Stationary Vehicle Bomb	Exterior Attack	Stand-off Weapons Attack	Armed Attack	Covert Entry	Mail and Supplies Bombs	Airborne Contamination	Waterborne Contamination
Decentralize communications resources	■	■	■	■	■	■	■		
Use multiple communications networks	■	■	■	■	■	■	■		
Conceal and protect network control centers	■	■	■	■	■	■	■		
Public address system			■		■			■	■
Underground utilities	■	■	■	■					■
Redundant utilities	■	■	■	■	■				■
Quick disconnects	■	■	■	■	■				
Remote fuel storage	■	■	■	■	■				

\* Adapted from U.S. Air Force, *Installation Force Protection Guide*.

## **2.12 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)**

CPTED is a crime reduction technique that has several key elements applicable to the analysis of building function and site design against physical attack. It is used by architects, city planners, landscape and interior designers, and law enforcement with the objective of creating a climate of safety in a community by designing a physical environment that positively influences human behavior. Although CPTED principles are not incorporated into the assessment process presented herein, it is useful to briefly discuss CPTED because it is often entwined with terrorism protection measures. Indeed, many antiterrorist design approaches are similar to those found in CPTED.

CPTED concepts have been successfully applied in a wide variety of applications, including streets, parks, museums, government buildings, houses, and commercial complexes. The approach is particularly applicable to older buildings that were designed and constructed 30 to 60 or more years ago. Security issues were almost nonexistent at the time, and technology was dramatically different. As a result, building designs are not always compatible with today's more security-conscious environment.

According to CPTED principles, depending upon purely conventional physical security measures (e.g., security guards and metal detectors) to correct objectionable behavior may have its limitations. Although employing these measures will no doubt increase the level of physical security, in some cases physical security measures employed as standalone actions may lead to a more negative environment, thereby enhancing violence. In short, employing standalone physical security measures may fail to address the underlying behavioral patterns that adversely affect the particular environment. CPTED analysis focuses on creating changes to the physical and social environment that will reinforce positive behavior.

CPTED builds on three strategies:

- Territoriality (using buildings, fences, pavement, signs, and landscaping to express ownership)
- Natural surveillance (placing physical features, activities, and people to maximize visibility)
- Access control (the judicious placement of entrances, exits, fencing, landscaping, and lighting)

A CPTED analysis of a building evaluates crime rates and stability, as well as core design shortcomings of the physical environment (e.g., blind hallways, uncontrolled entries, or abandoned areas that attract problem behavior). The application of CPTED principles starts with a threat and vulnerability analysis to determine the potential for attack and what needs to be protected. Protecting a building from physical attack by criminal behavior or terrorist activity, in many cases, only reflects a change in the level and types of threats. The CPTED process asks questions about territoriality, natural surveillance, and access control that can:

- Increase the effort to commit crime or terrorism
- Increase the risks associated with crime or terrorism
- Reduce the rewards associated with crime or terrorism
- Remove the excuses as to why people do not comply with the rules and behave inappropriately

The CPTED process provides direction to solve the challenges of crime and terrorism with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods.

CPTED concepts can be integrated into expansion or reconstruction plans for existing buildings as well as new buildings. Applying CPTED concepts from the beginning usually has minimal impact on costs, and the result is a safer building. Each

building, facility, and community should institute measures appropriate for their own circumstances because there is no single solution that will fit all situations.

Many CPTED crime prevention techniques for a building complement conventional terrorism and physical attack prevention measures. For example, as part of the CPTED strategy of improving territoriality, buildings are encouraged to direct all visitors through one entrance that offers contact with a receptionist who can determine the purpose of the visit and the destination, and provide sign-in/sign-out sheets and an identification tag prior to building access. These CPTED measures are similar to and complement physical security entry control point stations.

However, in some cases, CPTED techniques can conflict with basic physical security principles. The CPTED strategy of natural surveillance calls for locating parking in areas that allow ease of monitoring. A design that locates parking close to a building or office also reduces vehicle stand-off and could create a vulnerability of the building structure to a vehicle bomb. In cases where CPTED techniques conflict with security principles, designers should seek innovative solutions tailored to the unique situation.