Transit Security Design Guidance - Infrastructure

Course No: F08-001

Credit: 8 PDH

Gilbert Gedeon, P.E.

Continuing Education and Development, Inc.
22 Stonewall Court
Woodcliff Lake, NJ 07677

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

U.S. Department
of Transportation

Transit Security Design Considerations

Final Report
November 2004

FTA Office of Research Demonstration and Innovation

FTA Office of Program Management

Prepared for the FTA by:

Research and Special Programs Administration

John A. Volpe National Transportation Systems Center
Cambridge, MA 02142-1093

FTA-TRI-MA-26-7085-05
DOT-VNTSC-FTA-05-02

6.0 Infrastructure

Generally, infrastructure is the set of underlying structural or institutional elements that provide the framework in which a structure or facility operates and functions. The components of infrastructure are the elements that enable and facilitate carrying out certain activities. Transit infrastructure in particular refers to all the stationary assets in a system, such as real estate, buildings, tunnels, and rail tracks.

Infrastructure design is only one element of a larger security program. The process begins with a TVA, which identifies potential threats and their severity, and estimates how vulnerable each asset is to these threats. Scenario and Consequence Analyses then evaluate the maximum extent of damage or injury in the event of an attack. Based on these evaluations, transit agency officials can then prioritize their concerns and determine the appropriate level of protection through countermeasures.

How is this chapter useful?

For **transit administrators** it is a resource for:

- Security design concepts to consider when procuring infrastructure assets
- Reviewing infrastructure design guidelines

For **operations or planning staff** it is a resource for:

- Identifying tools and techniques for hardening assets

For **engineers** it is a resource for:

- Reviewing current hardening practices and procedures

Agencies adopting any of the infrastructure design security measures described in this chapter should consider coordinating them with other transit system components, such as vehicles and emergency procedures, to develop a comprehensive security strategy.

Overlaps between access management and infrastructure protection are extensive. Many of the threats facing infrastructure can be greatly reduced by instituting appropriate access management measures. Since no transit security program can be completely effective at eliminating risk while still providing convenient and high quality service, infrastructure design should also include measures to prevent attacks or reduce their effects in the event that perpetrators are able to gain access. Refer to **Chapter 5: Access Management** for additional information. Note also that this chapter is specific to infrastructure; design-related security measures for other transit assets are covered in **Chapter 7: Vehicles** and **Chapter 8: Communications**.

This chapter provides further details on the concept of CPTED[30] by showing how agencies can use the physical design of infrastructure components to help detect and prevent attempted terrorist

[30] CPTED is a branch of situational crime prevention based on the premise that the proper design and effective use of the built environment can lead to a reduction in crime and an improvement in the quality of life. CPTED differs from other crime prevention strategies by using environmental factors, such as site plan, building layout, and other physical characteristics, to bring about behavioral effects that reduce the fear and incidence of crime. Refer to **www.cpted.com.au** and **www.cpted-watch.com** and to the *Security-Oriented Design Considerations for Transit Infrastructure"* section of the 1998 *FTA Transit Security Handbook* at **http://transit-safety.volpe.dot.gov/Publications/Default.asp** for additional information.

attacks in their systems, and minimize the damage from attacks that do occur. This chapter begins with an overview of the various categories of transit infrastructure, then continues with a description of:

- Infrastructure Characteristics
- Security Approaches for Types of Transit Infrastructure

6.1 Introduction to Security Design for Transit Infrastructure

6.1.1 Categories of Infrastructure

Infrastructure categories relating to all of the fixed sites and facilities within a system are summarized below and described in more detail in Section 6.3.

- Transit Stations are facilities used for boarding and alighting of transit passengers, and fare collection; they can be below-grade, at-grade, or elevated. Their high profile, large volumes of pedestrian traffic, and central locations integrated with surrounding uses, make them likely targets for terrorist attack.
- Transit Stops are usually smaller and more open than transit stations. They are typically on public land, where passengers can board buses and light rail vehicles; these include everything from elaborate shelters to mere signposts. Transit agencies often lack control over these sites, which, combined with their high level of accessibility, makes them difficult to secure against attack.
- Administrative Facilities and Operations Control Centers (OCCs) are used for the operations and administration of the transit system and may be co-located on a site with non-transit uses. Although most administrative facilities are not open to the public and can therefore maintain stricter access control, they have a critical role in the transit system and have value as strategic targets.
- Vehicle Maintenance Facilities are used for the repair and storage of transit vehicles; they include vehicle garages, yards, and repair facilities. They often contain a large number of assets to be protected, including some high-risk elements such as fuel storage areas or containers. Maintenance facilities can be designed to allow transit vehicles and maintenance staff to enter and exit freely, while preventing access by unauthorized vehicles and people.
- Elevated Structures refer to all above-grade bridges and track structures, including pedestrian bridges and overpasses. Their high visibility and structural complexity present particular challenges to securing them against terrorist attack.
- Tunnels are used for the passage of transit vehicles underground and, in limited cases, underwater. They are more secure when designed to prevent unauthorized access from

passenger platforms and at-grade entrances, while allowing transit vehicles to pass freely. Proper design can also facilitate evacuation in an emergency.

- Right-of-Way, Track, and Signals include all land and equipment dedicated to the movement of transit vehicles between stations. Like tunnels, a design goal is to allow transit vehicle movement while preventing access by unauthorized people or vehicles.
- Remote and Unmanned Structures capture all other physical assets. This category includes power substations and communications relays, and the like, which are not necessarily located on rights-of-way or in stations. These may be owned or controlled by other agencies or companies. Design features that take into account their remote locations and lack of consistent or continuous staff presence can improve their security.

6.2 Infrastructure Characteristics

This section describes transit property design elements that planners, designers, and administrators should consider when selecting a facility location and/or designing a new or renovating existing facilities to protect them against potential terrorist attacks. Characteristics include:

- Site layout
- **Interior layout**
- **Structural engineering**
- **Architectural features**
- **Systems and services**

6.2.1 Site Layout

The physical characteristics of a site have a major impact on which security measures are possible and appropriate in safeguarding a facility. Some of these elements, such as building location, landscaping, and site circulation are under the control of the transit agency; while off-site features, such as topography and abutting uses, are not. Some on-site characteristics such as topography and vegetation are under limited control of the transit agency.

This section describes the factors a transit agency might consider when determining where to locate a facility and how to design the site. These include site selection, building placement, access points to the site, on-site vehicle circulation, and relevant factors to mixed-use facilities.

Site layout can be conducive to incorporating measures that protect personnel, riders, and other assets from attacks, and to limiting unauthorized access to the property. In addition, a facility's site design should enable security measures to be scaled and adapted in response to changing threat levels over time.

6.2.1.1 Site Selection

The unique characteristics of a site influence their appropriateness for different types of transit facilities, and have a direct effect on security. Relevant security issues for agencies include obstacles hindering outward surveillance, amount of available land, natural buffers, and the existence of nearby elevated vantage points.

Planners should consider the impact of the following site elements on site security when evaluating a property:

- Natural features (such as a stream or swamp)
- Manmade features (such as a pipeline or neighboring building)
- Existing easements
- General characteristics of abutting properties and access control
- Access to public roads
- Proximity to private roads

Natural Features

Natural elements, such as rolling hills and steep terrain, can provide hiding places for aggressors and hinder visual surveillance by security personnel. High points on the site elevate buildings where they are easily visible from off-site and therefore vulnerable to weapons fire from unsecured areas. Agencies should consider avoiding topography and vegetation that prevents clear lines of sight from the site to avoid making it easy for potential attackers to approach the site without notice.

Dense trees and shrubbery present similar challenges. Portions of sites (especially larger sites) are often left in their natural state, which can include steep terrain and dense vegetation. This occurs for a variety of reasons including unsuitable terrain, zoning or environmental regulations, and land banking for future use. Where these situations exist, agencies should consider perimeter protection to separate those areas from the developed portion of the site, to prevent them from being used for a covert approach to valuable assets. Refer to Section **6.2.1.2** for details on using unobstructed space as a strategy and Section **6.2.1.3** for access management strategies.

Some natural features benefit site security. For example a stream, especially one with a sunken bed, can be an effective barrier against vehicles trying to gain unauthorized access to the property. When incorporated strategically into site layout, these features can supplement access management strategies, however, agencies must be careful not to create security gaps where such features intersect with perimeter fences and other security measures (i.e., a person might use a streambed to crawl under a fence or wall where they intersect).

Manmade Features

Manmade features may present challenges to security. For example, storm drains and utility tunnels could enable someone to gain covert access to the property.

Existing Easements

Existing easements on the property might grant non-transit personnel the right to enter the property without prior approval from the transit agency. Agencies should make efforts to be familiar with the location of existing easements, especially in relationship to the location of critical assets.

Abutting Properties

While a transit agency may be able to design its property to meet agency security needs, it may have little or no control over neighboring properties. Site planners should therefore consider the characteristics of all nearby properties in the site selection process and layout of the transit property to avoid undermining even the best on-site security precautions.

Factors to take into account include topography, vegetation, buildings, and rooftops that can provide vantage points for aggressors. An additional consideration is what access controls, if any, exist on abutting properties. For example, if an adjacent building is a federal agency with tight security and access controls, this fact may mitigate concerns about the proximity of the building to the transit site. In contrast, an abutting public park, for instance, could be seen as a legitimate security concern—both for positive reasons (open areas provide clear views of approaching persons or vehicles) and negative reasons (open, public access is offered to a wide range of individuals). Agencies should consider these issues in addition to other non-security issues when acquiring property for transit agencies. Purchasing the abutting properties outright as a buffer or for less critical uses is also an option.

Access to Public Roads

Avoid siting critical facilities in such a way that vehicles may have direct routes between public roads and critical facilities. However, the site layout should neither preclude nor complicate access via public roads for emergency vehicles, nor should it inhibit emergency egress for passengers and/or employees.

Proximity to Private Roads

Agencies should be aware of any private roads close to the property that might introduce threats to the facility, the types of traffic attracted by adjacent uses and facilities, and traffic use of private roads near the facility.

6.2.1.2 Building Placement

Appropriate placement and orientation of buildings and other structures on the site is a major component of an effective security strategy to protect against damage from terrorist attacks. Agencies should consider the impact of the following building elements on site security: unobstructed space, standoff distances, and building orientation.

Unobstructed Space

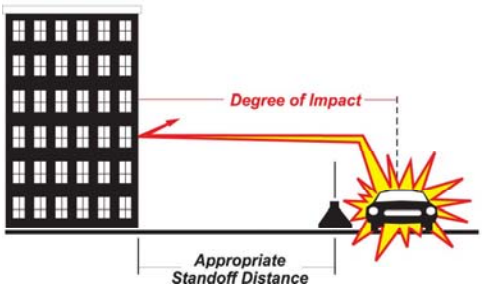
Unobstructed space is an area around an asset, usually a building, which provides clear visibility around the asset.

Agencies should consider surrounding buildings and equipment by unobstructed space to facilitate surveillance of the property and prevent the concealment of explosives and other harmful devices next to structures. For buildings, federal standards for unobstructed space call for an area 10 meters (33 feet) wide adjacent to a building.[31] This may not always be possible, particularly in dense urban areas, calling for alternate measures to accommodate existing conditions.

Standoff Distances

Standoff distances are minimum distances between a building, or other asset, and a secured perimeter barrier established to protect the asset from blast damage. Standoff distances limit the proximity of a terrorist or explosive to the asset. The appropriate standoff distances are determined by the size of a potential explosive and the critical value of the asset. Standoff distances help minimize damage from an explosive attack.

Figure 6-1 illustrates the impact of standoff distances on building security.



Standoff distances help minimize damage from an explosive attack.

Figure 6-1. Standoff Distance

The area within the standoff distance, excluding unobstructed space, can be landscaped with trees, shrubbery and other features. If agencies use this area, wherever possible they should avoid inhibiting the security function of the space; activities such as parking should be avoided. If parking within the standoff distance is needed, agencies should consider parking access control measures. If threat levels increase, they should consider temporarily prohibiting parking. Agencies should also consider restricting bicycle parking within standoff distances as threat levels rise, especially where bicycle lockers are used since they might conceal bombs or weapons.

Building Orientation

Building orientation can be used to protect or shield external vulnerable features of a building from an attack. Vulnerable features include entrances, windows, lobby areas, drop-off areas, loading docks, and other miscellaneous openings.

Agencies should consider orienting buildings and other critical assets so that clear lines of sight between their vulnerabilities and uncontrolled areas or vantage points is avoided. On-site vantage points include publicly accessible areas such as lobbies and parking lots, which may have less

[31] UFC 4-101-01, Department of Defense, *Minimum Antiterrorism Standards for Buildings*, (31 July 2002).

stringent security measures. For example, entrances to critical buildings should not directly face a public street from which an aggressor could fire a weapon at the lobby. When orienting assets, the site planner should keep in mind that the aggressor does not have to be in the secured area to attack a person or asset within the secured area; likely origins of attacks from which a terrorist could fire a weapon or detonate an explosive include nearby buildings, hilltops, roadways, or other uncontrolled areas outside the transit property perimeter.

6.2.1.3 Access Points to the Site

Control over how and where vehicles and pedestrians approach and enter a transit property is a crucial factor in site security.

Key concerns include number and location of access points, dedicated entrances or areas, and speed-control approaches.

Number and Location of Access Points

Access points are the means by which people enter and exit a site. The quantity and location of access points depends on a number of factors, including directions from which people will be approaching the site, method of approach (car, on foot, etc.), and the volume and timing of people or vehicles the entrances must accommodate. The type of facility plays a role as well; a large transit station, for example, may need several entrances to function smoothly, while a maintenance yard may have only one entrance for vehicles and pedestrians.

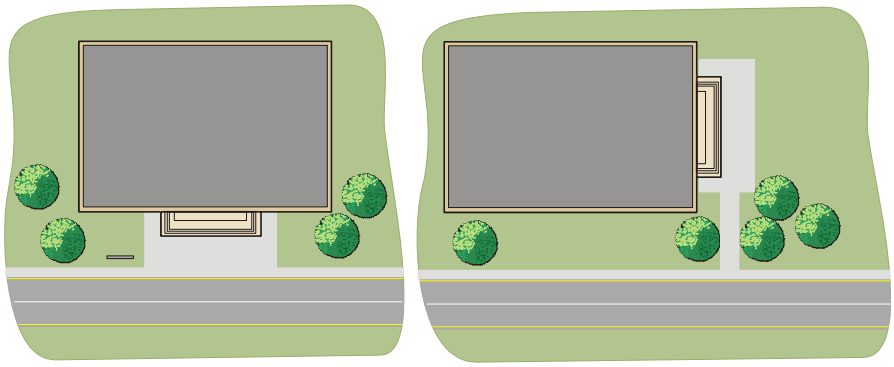
A facility with fewer entrances is generally easier to secure. Agencies should consider designing a site with the minimum number of entrances needed to satisfy the requirements of its daily operations. In areas where local safety regulations require emergency entrances and exits, these points should be secured in a manner that prevents unauthorized everyday access while still meeting safety criteria; this often requires advanced coordination with emergency responders to ensure they will have access to the property through all entrances. As threat levels vary, some access points to sites or buildings can be closed off, to channel movement by less vulnerable assets.

Agencies should consider locating facility entrances at points that reflect their user population, while facilitating security. Facilities with heavy public use, such as transit stations, should have access points that maximize convenience and capacity, while facilities used less frequently by the public can have less convenient entrances without generating a significant negative impact on facility operations (see Figure 6-2).

Dedicated Entrances or Areas

At facilities with different types of users accessing the site, it may be appropriate to have specific entrances and areas within the site dedicated to particular users. The goal of this strategy is to segregate traffic that presents different security threats, and therefore requires different degrees of access management. Transit staff, for example, pose less of a threat than anonymous transit riders

or delivery vehicles, and agencies should consider allowing their staff to access a site more easily and park their vehicles nearer to sensitive assets.



Entrances should be oriented away from (right) rather than facing (left) uncontrolled areas such as roadways, provided that such orientation does not impinge on access by disabled persons and maintains safe, convenient pedestrian access.

Figure 6-2. Building Entrance Location

Delivery vehicles pose a particularly high threat to at-risk facilities, because of their large payload and authorization to enter sites. For these reasons, agencies should consider separate delivery entrances with a dedicated access road that admits vehicles directly to receiving areas or loading docks (and away from vulnerable assets) wherever possible. If a dedicated roadway is not practical, a designated route through the site could serve the same purpose. Any delivery vehicle parked inappropriately, or seen driving outside the designated route, would be noticed more easily and generate the appropriate response from security personnel.

Many facilities may already have segregated entrances. Commercial and industrial facilities typically segregate entrances to satisfy a variety of needs such as maneuverability, aesthetics, and traffic flow. If existing facilities have segregated access routes, they should be evaluated and upgraded to address the concerns discussed in this chapter. When initiating or reconfiguring access points, planners and designers should also maintain safe, convenient access routes for pedestrians, persons with disabilities, and cyclists as well.

Speed-Control Approaches

Agencies should consider designing roadway alignments to impede high-speed vehicle approaches to site access points and assets such as buildings. This prevents an attacker from using a fast moving vehicle to ram through perimeter security or destroy an asset in a collision. Roadways approaching gates or assets can force a vehicle to pass through sharp curves that can only be negotiated at low speed. Staggered concrete or water-filled barriers or indirect roadway alignment lined with dense low shrubbery or other barriers are examples of obstacles to high-speed approaches. These methods limit the approach speed, while preserving clear views of the roadway from security checkpoints and building lobbies.

Approaches that allow a vehicle to approach a gate or checkpoint unseen can be avoided using speed bumps, speed tables, and similar traffic-calming techniques as speed controls, although they are less effective because they still allow a vehicle to accelerate. Similarly, agencies should consider avoiding clear straight approaches that allow high-speed acceleration toward lobby entrances, fuel storage, or other sensitive areas.

Vehicle barriers such as this and other access control measures assist in managing vehicles approaching a submerged access point.

6.2.1.4 On-Site Vehicle Circulation

Controlling how vehicles and pedestrians move about within a transit property may also be a useful security measure. Designers might consider dedicated circulation routes for certain users and routes that limit high-speed approaches to assets on the site. The sophistication of a circulation plan depends on the size of the site, the diversity of activities, and the types of users at the site.[32] This should include drivers, pedestrians, cyclists, etc. When selecting a facility site, an agency should consider how the property accommodates the circulation needs of both its everyday functions as well as its security concerns.

Key concerns include parking areas and drop-off areas.

Parking Areas

Agencies should consider locating general parking in open lots or dedicated garages with access control systems. Vehicles should be parked beyond standoff distances that are sufficient to protect vital structures. Agencies should avoid locating parking under a transit building or on its rooftop. If this is unavoidable, agencies should consider stricter access controls, surveillance, or detection measures.

Depending on the type of facility, planners may segregate visitor or commuter parking from that of authorized personnel, especially at sites with substantial public activity. A separate visitor parking lot may be located near the visitors' entrance to buildings, but design measures (discussed above) can be used to protect the entrance from high-speed approaches or attacks from the parking lot.

Drop-Off Areas

Passenger drop-off areas should be located where vehicles pose a minimal threat to assets. If possible, they should be outside the required standoff distance, and should not provide clear lines of sight to openings, windows, lobbies, HVAC intakes, or other external building vulnerabilities. When

[32] For information about access control concerns such as perimeter vehicle inspection, access to parking, parking and traffic controls, vehicle registration, towage and access control systems, refer to *Chapter 5: Access Management*.

it is impractical to have the drop-off area outside the standoff distance, designers may consider monitoring the drop-off area for suspicious activity or devices with additional surveillance.

Agencies should consider locating drop off areas away from areas of concern, such as a station platform, especially when the drop-off area is within the standoff distance. Depending on passenger volumes, the agency can also consider providing a shuttle bus to bring passengers or visitors from remote parking areas to a closer point. All drop-off areas should be in an open space, not under a covered entryway or building overhang, and they should not be in areas that would concentrate a blast toward a building or other sensitive assets.

6.2.1.5 Particular Considerations for Mixed-Use and Intermodal Facilities

Mixed-use facilities are buildings or parcels of land that incorporate more than one use. They are addressed in this chapter because mixed-use transit stations – those that combine transit facilities with residential, commercial or other space – are becoming a popular model in the United States. In addition, transit agencies' administrative offices are often located in buildings shared with other tenants.

Intermodal facilities are characterized by the multiple modes that meet at the location. They enable transfers or connections between bus, rail, or light rail and/or ferry lines. These facilities enable seamless transportation throughout one's journey by facilitating movement between the modes at the site.

Challenges

Securing mixed-use facilities presents unique problems because other uses will be in close proximity to transit facilities, and the transit agency's control over the entire site is typically limited. The result is that traditional access management techniques and security-oriented site design may not be possible. This is especially true for retail facilities and historic sites that integrate transit space, because of the abundance of non-secure public space surrounding the station.

Strategies

Options for addressing security concerns in mixed-use facilities vary depending on the included uses. When administrative offices share space with other tenants, security options are usually limited to access control and intrusion detection. Many office buildings have a security system for the entire building that incorporates access control, intrusion detection, and surveillance. Standoff distances for blast protection and vehicle barriers (other than for parking control) are not commonly found at commercial office properties.

Transit stations integrated into commercial, recreational, or historic facilities should focus on strategies for detection of attempted attacks. Security options for these sites include:

- CCTV and other surveillance methods
- Attack detection (fire, chemical release, explosion)

- Intrusion detections (intrusion into restricted areas such as mechanical rooms)
- Evacuation plans

A transit agency should work with the owners of the surrounding spaces to develop a security plan that meets all parties' needs. If such cooperation fails, and if the facility is judged to be at a high risk for attack, the transit agency may want to evaluate relocating to another facility.

Intermodal facilities can be somewhat easier to protect than mixed-use facilities because they are under the control of a transit agency or multiple transport agencies. The advantage is that all transit agencies have similar security concerns, making it easier to implement a comprehensive security plan. The high level of transient pedestrian traffic through intermodal stations, however, creates increased risk because it is easier for an attacker to access the site and the large amount of people make it an attractive target for an attack.

In order for the facility to work efficiently, agencies should consider balancing the need to accommodate the large numbers of people smoothly with the impositions created by security measures.

6.2.2 Interior Layout

The interior layouts of the buildings and other structures on the site may also support the detection and deterrence of harmful activity by establishing protective barriers around sensitive assets and by enabling effective surveillance within the structure. In addition, providing the necessary access routes and emergency equipment enables successful facility evacuation and emergency response.

This section describes the factors a transit agency might consider when designing the interior layout of the site. These include asset shielding, surveillance, and emergency routes.

6.2.2.1 Asset Shielding

A building's layout can be used to shield critical areas such as a central-control room, or vulnerable areas such as a station platform packed with people, from an attack at the outer edge of the site.

Agencies should consider using special reinforced materials between valuable features and easily accessible areas, such as lobbies, mailrooms, and loading docks, or locating these areas at a distance from each other. For example, designers may consider positioning a control room at the center of a building, behind layers of other non-public areas, and at a distance from a likely detonation point in case of an attack. Within a room, planners may be able to reduce the vulnerability of personnel and critical equipment by positioning them away from windows and doors. Critical assets might be dispersed so that they cannot be disabled by a single attack, and locate redundant or back-up systems in a different building, or even at a different site, if possible.

Agencies should consider using a facility's layout to help enforce zones for each type of activity taking place, to safeguard the nonpublic areas of a site. Public areas such as train platforms or lobbies can be separated from non-public spaces intended only for staff; and access management elements (such locked doors, checkpoints, etc.) may help prevent unauthorized movement between the zones. Agencies can insulate particularly sensitive non-public facilities from the public using other, less critical non-public spaces.

Agencies should also consider making pedestrian movement within the facility consistent with the access management tools in place. Signage and other pedestrian flow controls can direct public users away from non-public spaces. Separate entrances and routes can be used for the public and staff within the building wherever possible; this minimizes the opportunity for someone to gain unauthorized access to secure areas of the facility.

6.2.2.2 Surveillance

Public spaces can be designed to facilitate surveillance—a key CPTED principle—with large fields of vision and no blind spots or hiding spaces.

With clearly identified and understood zones of activity, staff and the public can more easily identify unauthorized people and suspicious behavior. Designers should try to avoid creating blind corners, isolated passageways, as well as columns and other sightline obstructions.

6.2.2.3 Emergency Routes

Emergency routes within, to, and from all areas of the building serve two purposes: evacuation of staff and the public, and access by responding agencies. Appropriate emergency routing is critical to safety and can vastly reduce the impact of an unexpected event.

Agencies should consider making emergency routes an integral element of a building's design and factor in the following principles:

- Locating corridors and stairways making up the routes away from likely areas of attack and reinforcing them to resist damage in an explosion or fire.
- Devising evacuation routes that are clearly marked, unobstructed, and adequately sized for the occupancy level of the building.
- Designing routes and protected "safe areas" to accommodate wheelchair users and other occupants with special needs.
- Providing multiple evacuation routes, in case the primary exit becomes damaged or blocked.
- Locating critical routes and systems that are logical and consistent with other buildings and the surrounding area, since during an emergency, authorities must be able to quickly access to the building and the on-site emergency equipment.

6.2.3 Structural Engineering

Structural engineering, or structural design, is the design of a building's internal support system. Structural design includes the selection of a framing method or structural system, as well as the selection and sizing of structural members, based on loading and architectural requirements. Structural members include beams, columns, the foundation, floor slabs, connections of these elements to each other, and other ancillary components.

Building design (structural and architectural) can contribute to infrastructure security by minimizing the extent and depth of damage in an attack. Structural integrity can help mitigate blast and fire damage to the building; protect inhabitants; protect equipment, property, and records; allow critical operations to function immediately after an attack; and allow rescue operations in and around the building preserved after an attack.

This section focuses on blasts and fires, describing engineering concepts for structural integrity and strategies for minimizing damage. The concepts discussed include:

- Blast loads
- Blast damage
- Progressive collapse
- Blast mitigation
- Fire damage

The sections of most building codes relating to structural components address service loads and methods to determine the proper size of structural members and their connections. Service loads specified in building codes are based on the location and intended use of the proposed structure, and include:

- *Minimum dead load*: the weight of the structure
- *Live load*: variable loads such as people, cars, furniture, etc.
- *Earth load*: earth pressure on buried structures, retaining walls, foundations, etc.
- *Wind load*: pressure applied to the structure by wind
- *Snow load*: the weight of snow on a building
- *Seismic load*: loads induced on structural members during an earthquake

Building codes do not usually address "blast loads"; the force exerted on a building from the detonation of an explosive device.

Blast loads are different from the usual types of service loads considered by a structural engineer when designing a building. Service loads are relatively predictable in their magnitude and placement on the structure. In contrast, blast loads are much greater in magnitude, are unpredictable in size and placement. However, there are certain engineering strategies that agencies can use to enable a building to maintain its structural integrity after some of its components have been compromised or completely destroyed in a blast.

6.2.3.1 Blast Management

Blast Loads

A bomb exploding at ground level produces a hemispherical shock wave. As with other waves, such as sound waves, the shock wave can reflect off objects, concentrate in confined areas such as tunnels, or change direction. This is important to understand because once the skin of a building is breached, the shock wave can travel or ripple through a building's corridors as the energy in the wave dissipates.

Table 6-1. Bomb Size and Blast Range

Type of Explosive	Explosive Capacity in TNT Equivalents	Lethal Air Blast Range
Pipe Bomb	5 lbs. (2.3 kg)	
Briefcase, Backpack, or Suitcase Bomb	50 lbs. (23 kg)	
Compact Sedan (in trunk)	500 lbs. (227 kg)	100 ft. (30 m)
Full Size Sedan (in trunk)	1,000 lbs. (454 kg)	125 ft. (38 m)
Passenger or Cargo Van	4,000 lbs. (1,814 kg)	200 ft. (61m)
Small Box Van (14 ft box)	10,000 lbs. (4,536 kg)	300 ft. (91 m)
Box Van or Water/Fuel Truck	30,000 lbs. (13,608 kg)	450 ft. (137 m)
Semi-trailer	60,000 lbs. (27,216 kg)	600 ft. (183 m)

Source: Transportation Security Working Group, "Terrorist Bomb Threat Standoff (Card)," Government Printing Office (1999).

A bomb or other explosive device produces a blast that creates a blast load. Explosions cause damage by the generation and propagation of heat, pressure, and flying debris (shrapnel). An explosion is a rapid, often violent, release of energy that produces a rapid release of gases and heat. The rapid release of gases compresses the air immediately around the bomb, creating a shock wave. This shock wave, or pressure wave, propagates through the air outwards from the explosion. When this shock wave encounters an object, such as a building or a trash receptacle, it exerts a force on that object. The magnitude of these forces can be tremendous: a 74 mph wind (threshold hurricane wind speed) produces a pressure of approximately 21 psf (0.1480 psi); in contrast, according to Tod Rittenhouse, "the blast pressures exerted on the building façade in the Oklahoma City bombing were on the order of 4,000 psi."[33] Ranges for various types of explosives are further described in Table 6-1.

The blast load striking a building or other object depends on the amount and quality of explosive detonated and the distance of the explosion from the building. Maximizing standoff distances is important; the farther away an explosion, the weaker its effects. As the shockwave radiates away from the explosion, the magnitude of the shockwave decreases and the duration of the shockwave increases. (See Figure 6-3.)

[33] "Designing Terrorist-Resistant Buildings," Tod Rittenhouse, *Fire Engineering* (November 1995).

The peak magnitude of the shockwave increases by a reflection factor as it encounters the face of a building. This increase in magnitude is analogous to ocean waves rising as they strike a sea wall and the water "piles up" against the wall. The reflection factor varies with the incident angle (the angle at which the shockwave hits the building). The increase is maximized when the direction of wave travel is perpendicular to the building. This can increase the pressures by an order of magnitude.

Explosive materials vary in their efficiency (energy released per pound of material). In calculating blast loads, current practice expresses all explosives in terms of an equivalent weight of TNT, regardless of the actual explosive material used. Information for determining blast load magnitudes in relation to building hardening design is available through the Department of Defense, General Services Administration, and in other security-related publications.

Damage from Blasts

The main threat to the structural integrity of a building is blast force, regardless of whether the explosion occurs inside or outside the building. The primary vulnerability is the overloading of the structural system by blast loads that cause the system to fail and the building to collapse.

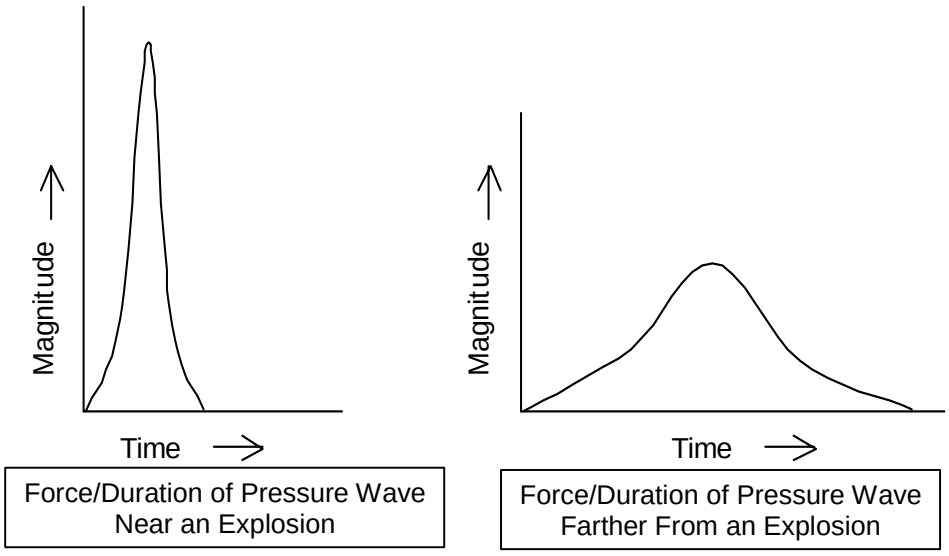


Figure 6-3. Variation of Explosive Pressure and Duration with Distance from Explosion

Blast damages are classified as either direct (those that occur in the explosion) or indirect (those that occur as a subsequent consequence of direct damage).

- Direct Damage
  - A hole in the ground or foundation.
  - Localized damage to the building's façade (bricks, windows, signs, etc.).

    - Damage or removal of a structural member or members (a beam, column or other structural element) directly caused by the blast.
- Indirect Damage
    - Flying shards of glass: Glass shards thrown from a window can cause serious injury to people, even if they are several feet from the window that shattered.
    - Flying debris: If the force of the explosion breaches the building's façade (building skin, curtain wall), the energy not absorbed by the façade can hurl furniture and other light objects. These "missiles" can cause injury, damage property, and rupture service systems such a gas, water, electric and communications.
    - Progressive collapse: If a blast directly destroys a column or beam locally, other structural members may fail. This can start a chain reaction of failures that results in damage disproportionate to the blast and collapse of the entire building.

Progressive Collapse

The worst-case consequence of blast damage related to structural engineering is progressive collapse. This is the disproportionately large collapse of a building or structure from an explosion, caused by the loss of one or more structural members, resulting in only localized damage. Progressive collapse occurs because most buildings are designed to carry the required loads, based on the assumption that all structural members are in place.

Two types of progressive collapse are possible:

- Pancaking is the stacking of floors on top of each other. It occurs when an explosion destroys a structural member or members, causing the floor directly above the destroyed members to collapse, which causes the next floor above it to collapse, and so on.
- Cascading is the collapsing of a series of bays (the section of a building between two rows of columns) from the destruction of one or a few bays. Cascading occurs when an explosion destroys a bay, or bays, causing the adjacent bay or bays to collapse in succession.

Progressive collapse occurs in stages, as summarized below. A complete discussion of progressive collapse is beyond the scope of this report; for more details refer to the latest edition of ASCE Standard ANSI/ASCE 7, *Minimum Design Loads for Building Structures.*

Beams (Including Girders)

Beams are horizontal structural members that support the floor slab. They carry gravity loads and are typically supported by columns or girders. Transfer beams or girders can support floor slabs, other beams and other columns. Beams and girders also provide lateral support to columns to prevent the columns from buckling.

When an explosion destroys a column, the supported beams lose their support at the destroyed column and become cantilever beams. If the beams are connected to the remaining columns with non-rigid connections (connections unable to transfer bending loads from a beam to a column), all beams previously supported by the destroyed column will collapse along with the floor slabs those beams support. This can extend through several stories. The loss of these beams can also reduce the lateral stability of the adjacent columns not damaged by the initial blast, causing those columns to fail, followed by more beams, and so on.

Floor Slabs

Floor slabs are typically designed to carry gravity loads. Sometimes the slabs are designed as diaphragms and are part of the lateral support system.

When the shockwave enters the building through an open window or breached curtain wall, it can exert an upward load on the bottom of the slab, causing the slab to fail. The loss of the slab can increase the unbraced length of the adjacent columns, potentially causing the columns to buckle. Failed columns can result in collapsed beams and the other consequences discussed above.

Columns

Columns typically carry axial gravity loads and are usually not designed to bend. When columns are part of the lateral resisting system, bending is taken into account. The strength of a column is limited by its length and by the size and shape of its cross section. If the unbraced length of a column (the distance along the column between horizontal members) increases due to the loss of a beam or slab, the strength of the column is reduced.

If an explosion destroys a perimeter column or columns, the girders and beams supported by those columns lose their support. This may increase the unbraced length of the adjacent columns due to the failures described above.

Blast Mitigation

The best methods of protecting a building from blast damage are effective access management techniques and appropriate standoff distances. Since no security system is foolproof; however structural engineers need to anticipate that buildings may be subjected to blast forces. Structures designed to resist catastrophic effects from blast forces are referred to as "hardened" buildings; these use a combination of structural design, architectural design, and mechanical design to minimize the consequences of a blast.

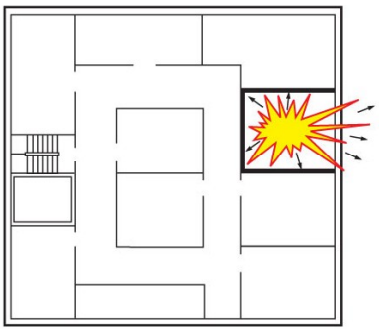
Constructing hardened structures can be expensive and time consuming, particularly when retrofitting an existing building. One possible alternative is to add redundant structural components to a building, although this approach can be just as expensive. Before hardening a structure, a transit agency should consider whether such an approach is necessary.

Avoiding Progressive Collapse

Agencies should consider designing buildings to sustain localized damage, including the total loss of multiple structural members, and still remain standing. Designs should take into account the stability of a structure if the structure loses a column or columns, a bearing wall, a beam or a combination of structural elements. Design techniques that help prevent progressive collapse include:

- Stiffening the perimeter frame by designing it as a rigid frame.
- Strengthening floor slab systems to distribute and sustain a load by catenary action to account for the loss of a column.
- Designing floor slabs to span in a direction in other than normal conditions (a lower factor of safety may be used for the secondary span condition).
- Designing load-bearing partitions to accept loading when slab spans change direction.
- Increasing the load capacity and ductility (ability to deform without breaking) of beam-to-column connections.
- Building returns (an angled section of wall at the free-standing end of a wall) on walls to increase their stability under suddenly increased loads.
- Reinforcing and tying walls and slabs together, allowing them to act respectively as the web and flanges of a beam to compensate for the loss of other structural members.

Underground parking presents an opportunity for a car bomb or other similar device to be placed under a building, and agencies should consider avoiding this design feature. When underground parking facilities are warranted, agencies can use structural design modifications. For example, columns in the garage can be designed for a greater unbraced length: double the unbraced length for one level of parking, triple it for two levels of parking, and so on.



Hardening vulnerable areas, such as a lobby, can protect other parts of the building from an attack.

Figure 6-4. Isolation of Vulnerable Areas

Agencies should consider structurally isolating sections of the building from each other, to prevent substantial damage in one area from causing a progressive collapse in other areas (see Figure 6-4). This compartmentalization serves two purposes. It can buffer high-risk areas (mailrooms, public lobbies, chemical storage areas, or other areas where an explosion is more likely to occur), from the rest of the building, so the destruction of such an area does not result in the total collapse of the building. It can also provide extra protection for critical rooms and equipment, such as control rooms, communications rooms, and staffed areas, so these remain structurally sound if a blast occurs elsewhere in the building.

6.2.3.2 Fire Management

While accidental fires may occur, fires resulting from an attack may have a different kind of impact. For example, an accidental fire usually starts at one location and often, but not always, spreads relatively slowly. On the other hand, a fire from arson is often strategically set in multiple locations to maximize the rate of spread and damage. An arsonist may also sabotage the fire protection system. An incendiary bomb that produces a fireball or intense heat (as opposed to a bomb that produces only a shock wave) ignites a large area and can cause substantial damage, including local damage to the fire suppression system.

Well-established design and construction practices for protecting structural members from fire are particularly important in case of an attack. Although not all structural materials will "burn," all structural members, regardless of their material composition, will lose a percentage of their original strength when subjected to intense heat. Excessive heat is the principal cause of a fire's detrimental effects on a structure. Therefore, upgrading or hardening the automatic sprinkler system is of tremendous benefit in mitigating the effects of fire on a structure. Additionally, many of the mitigation measures for blast impacts apply to fire management as well, such as isolating vulnerable areas to prevent the spread of fire and avoiding progressive collapse (see **Figure 6-4**).

This section discusses the effects of fire on four major structural construction materials: steel (structural steel), reinforced concrete, pre-stressed concrete, and timber.

Steel

At high temperatures, unprotected steel looses its strength. For this reason structural steel members used in building construction are protected (fireproofed). Fireproofing methods to protect steel members from heat insulate the steel from the fire. This increases the time required for heat to transfer from the fire to the steel.

There are several insulating methods for steel members:

- *Concrete encasement.* Encasing steel members in concrete provides excellent insulation to the steel. Lightweight concrete (see the About Concrete illustration on the next page) provides better insulation than standard concrete. The selection of concrete type depends on several design factors that are beyond the scope of this document. This method is well suited to insulating columns. It may also be used to insulate floor beams supporting a concrete floor slab. However this can be expensive due to complicated forming and increased dead load.
- *Sprayed on mineral fiber coatings.* Mineral fiber coatings are easy to apply, and they provide excellent protection when applied correctly. However, these coatings are easy to scrape off, and explosive blasts may damage portions of the insulation. Protection of the insulation is discussed at the end of this section.

- *Cementitious material coatings.* Cementitious coatings form a continuous coating around the steel. However, during a fire, they can spall (chip or flake on the surface), and there is a history of problems with lack of adhesion to the steel.
- *Intumescent paints and coatings.* Intumescent coatings swell when heated, thereby insulating the steel and retarding the effects of the flames and high temperatures. These coatings work well to protect the steel from heat. Exposure to flames can damage or destroy this type of coating and therefore should only be applied to components unlikely to be directly exposed to flames.

There are several concerns when selecting a method to fireproof steel, including method of building construction, and installation and maintenance costs. During a blast, it is likely that the fire proofing on the steel in the immediate vicinity of the blast will be damaged. However, the fire that may result (and spread) will have an effect similar to conventional fires. Assuming the progressive collapse considerations were used in design, protection of the remaining steel members will be effective.

About Concrete…

Concrete is a mixture of portland cement, coarse aggregate (stone), fine aggregate (sand) and water. Portland cement reacts with the water (hydrates) and hardens. The aggregate is basically used as filler (obviously the proportions determine the concrete's strength). The types of aggregate affect the properties of the mix. Lightweight aggregates such as vermiculite and perlite are used to create lightweight mixes as described above. Several other "admixtures" are available to modify the concrete's properties and even color. Admixtures include plasticizers to temporarily decrease the mix viscosity, agents to increase/decrease setting time, foaming agents and air entrainment.

Reinforced concrete is concrete embedded with steel rods to increase the member's strength (as distinguished from the material's strength). The steel reinforcement is usually placed were tensile stresses (tension) develop in the concrete member, although sometimes the steel is also used to reinforce compression zones.

Pre-stressed concrete is similar to reinforced concrete, except that the steel reinforcement are usually wire cables that are pre-tensioned *before* the members are loaded.

Reinforced Concrete

Concrete is often used as an insulating material. Although concrete structures rarely collapse from fire damage, the strength of concrete and reinforced concrete members is reduced by exposure to high temperatures. Type of aggregate and moisture content are the principal factors that determine concrete's sensitivity to heat.

Type of aggregate is the most significant factor. Lightweight aggregates such as vermiculite and perlite are used in lightweight concrete. Lightweight concrete, in addition to having better insulating characteristics, has better strength retention when exposed to intense heat.

The amount of moisture in a concrete affects the member's resistance to heat. The moisture is trapped in the small capillaries within the concrete. As heat energy is absorbed, the water in the concrete vaporizes, which locally helps maintain the concrete's strength until the moisture is burned

off. However, voids left by the vaporized moisture weakens the area. Structural engineers should consider this when fire is a concern for concrete members.

Pre-Stressed Concrete

The relevance of aggregates and moisture content for pre-stressed concrete are similar to those for reinforced concrete. The concrete used for pre-stressed concrete members is usually stronger than the concrete used for reinforced concrete members and has better fire resistance, but tends to spall and expose the reinforcement.

Pre-stressing steel is the principal concern when exposing pre-stressed members to intense heat. High carbon-cold drawn steel used in pre-stressing is more sensitive to intense heat than low carbon, hot rolled steel used in reinforced concrete. Also, the loss of strength in pre-stressing steel is permanent and not regained upon cooling. For example, the pre-stressing steel is initially under great tension. Over time this tension decreases, as the steel tends to creep (continually deform or lengthen). This is taken into account during the design process; however exposure to high temperatures, exacerbated by the spalling concrete, accelerates this "creeping" process. Engineers should consider this when considering fire effects on building hardening.

Timber

Unlike steel and concrete, wood will burn. The principal factors that determine how timber responds during a fire are the size of the timber member and its moisture content.

As wood burns, a charcoal layer forms on the wood's exterior. This char layer is an insulator and as the layer thickens, it slows down the rate of burning. The unburned interior wood retains its strength. Buildings constructed with large timber members can maintain their integrity for a long time during a fire, providing an opportunity for the fire to be extinguished before structural failure occurs. As is in all cases, but especially for timber construction, a hardened sprinkler system is important. Fire retardants can slow combustion and delay ignition of wooden members.

6.2.4 Architectural Features

The design of architectural features on a site can aid in surveillance, help deny an opportunity for an attack, and reduce injuries and property damage in case of an event.

This section describes the factors a transit agency might consider when designing security features into a site. These include:

- Façade
- Entrances
- Fenestration
- Small architectural features
- Utility openings

- Signage

6.2.4.1 Façade

A façade is the outside face of a building or wall. It can refer to just the outer surface, or more generally to all construction between the exposed surface and the structural frame. In some instances, the structural frame is visible as an integral part of the façade.

Materials

Façade design affects a building's resilience to terrorist attacks and other incidents. Designers can construct a building façade with materials that resist fire and produce little or no toxic fumes or minimal debris in an attack. Materials that ignite and spread fire quickly or produce toxic fumes, such as plastics, paints, and other finishes can trap building occupants and cause suffocation or other consequences.

Façade materials can be attached in a manner that will reduce the amount of secondary debris. Masonry or pre-cast concrete panels can be reinforced and securely fastened to the building frame. Bricks or other face materials that come loose in a blast may become projectiles and cause secondary damage. As with progressive structural collapse (refer to the subsection on progressive collapse in Section 6.2.3.1), façade design should prevent indirect damage that destroys the entire facade. On sides of the building that face likely directions of attack (such as public streets or nearby buildings), agencies should consider minimizing the use of weaker materials and/or openings. Overhanging design features should also be avoided where they could receive a blast load from underneath.

Façade features can also impact visibility; elements such as light color schemes, translucent canopy materials, and skylights provide more light in interior spaces. Transparent materials like glass may provide added opportunities for surveillance, allowing transit employees and passengers to see from one zone of a facility to another and to share light from one area to the next. Conversely, solid materials such as concrete block walls may prevent potential attackers from observing facility activity patterns at non-public locations such as maintenance facilities, compared to chain link fences, which allow unhindered observation.

Decontamination

Incident recovery may also be relevant to consider when choosing materials. Weapons of mass destruction, such as chemical or radiological agents, can be absorbed into materials such as concrete and plastics. Non-porous coatings may be able to minimize absorption of chemical contaminants when applied to porous materials like concrete or brick. Agencies should consider decontamination efforts—whether cleaning or removal—when choosing façade materials, and perhaps even consider comparing the extent of the decontamination effort required for the material options before settling on a selection.

In response to the anthrax attacks at the Hart Senate Office Building and Brentwood Post Office, gaseous chlorine dioxide gas was pumped through the buildings' heating and ventilation systems and

kept inside the buildings for 9 to 12 hours to ensure that all spores were killed. Liquid chlorine dioxide and other antibacterial gels were also used and potentially contaminated mail was irradiated before being sent to its destination. The Hart building was closed for three months while cleanup and testing was completed. The estimated costs for cleaning the 700,000 square foot Brentwood postal facility were $22 million.

6.2.4.2 Entrances

Agencies should consider locating entrances to the building, including main lobbies, service entrances, and loading docks, away from uncontrolled public spaces whenever possible. This reduces the opportunity for a direct attack on an entrance. Agencies should also consider locating exterior entrances where there is no direct access to key assets (such as OCCs) within a building.

The sizes of doorways and lobbies should be appropriate for the access management techniques used on-site. For example, at security checkpoints that span entryways it is extremely difficult to bypass them without detection, and in larger lobbies additional security staff may be required.

6.2.4.3 Fenestration

Fenestration is the design and arrangement of windows and other glass features on a building, including glass façade panels and openings. The location and construction of windows will likely vary, based on the location and contents of a building.

Designers may reduce the number of windows around sensitive or valuable assets, to make those assets less visible to the public and to minimize damage in the event of an attack. For facilities with large fenestrated areas, designers may compensate by incorporating standoff distances and orienting the windows away from unsecured areas. Where possible, agencies should consider locating windows out of convenient reach and use security screens or wire mesh to prevent unauthorized access through the opening.

Agencies should consider using windows and frames constructed of materials that resist tampering and easy destruction, and that prevent flying glass shards in an explosion. For example, tempered glass or polycarbonate composites that shatter cleanly (such as those found in automobile windows) may prove safer than conventional annealed glass that breaks into dangerous shards. Planners might also consider window treatments, including adhesive films, coatings, and blast curtains that limit the depth of in-room damage from shattering window glass.

6.2.4.4 Small Architectural Features

Agencies should incorporate small architectural features or amenities, such as planters, benches, and trashcans, in the facility design in such a way as to prevent them from causing damage in a blast. Anchoring objects made of blast resistant, reinforced materials to the ground will make them less likely to act as projectiles and cause secondary damage.

Agencies can also incorporate these design elements into access management techniques, such as barriers for vehicles, but should also be cognizant of not placing them in a location that could provide hiding spaces or shielding for potential attackers, especially near entrances or critical assets.

6.2.4.5 Utility Openings

Many buildings require numerous functional openings, such as utility tunnels, sewers, and HVAC vents, which provide the potential for unauthorized access or the introduction of harmful substances into a structure or tunnel.

Agencies should consider locating openings in inaccessible locations or where any suspicious activity would be easily observed to protect the openings. Security doors, hatches and grilles should resist tampering or damage and can be sized to prevent entry by a person or the introduction of harmful substances. In some cases, additional monitoring or surveillance equipment may be justified.

6.2.4.6 Signage

Signs are effective tools for access management and for assisting people unfamiliar with the building. They can direct public users to proper areas of the building, warn against unauthorized entry into nonpublic spaces, and indicate emergency evacuation routes.

Signs can also inform and instruct visitors on proper and improper activities within the building or facility. In some cases, transit agencies may consider reducing or eliminating signage for key assets, to hinder their discovery by potential aggressors. All signs should be legible and easily discernable to all passengers, including those with disabilities.[34] Emergency exit signs can also be designed with lighting elements, to make them visible in the dark. Agencies should consider designing signs in public areas to resist tampering or destruction, and, when placing signs on walls or other surfaces, should avoid adhering them in a way that allows items to be hidden on, in, or between the sign and the surface.

6.2.5 Systems and Services

Building services create a safe and comfortable environment for occupants and enhance a building's functionality. Individual systems have many similarities and may rely on shared or auxiliary systems for part of all of their service. In addition to having similar attributes, they also have many parallel vulnerabilities and countermeasures.

This section describes the principal systems and services in a transit building. These include:

- Public utilities

[34] All signs, emergency facilities, and any security measures should be compliant with the American with Disabilities Act (ADA).

- Electrical system
- Functional components[35]
- Heating, ventilation and air conditioning (HVAC)
- Lighting
- Communications
- Security systems
- Water and sewer
- Fire protection

Many of these services are vital to emergency response and may be targets of terrorism themselves. Consequences of building service disruptions can range from inconveniences to the public and the transit agency to a total shutdown of the system and potentially dangerous conditions. If the building services and utilities are required for emergency response, then willful disruption of these services may supplement the primary attack.

6.2.5.1 Public Utilities

Most transit systems receive electric power from public/private utility companies through the normal public transmission system. Transit agencies also rely on public gas and water supplies. The location of these utilities is public information that can be easily obtained by anyone.

Damage to power and gas lines can cause major disruptions at transit facilities. External utility lines for all services and systems need to be protected and monitored to prevent tampering. Natural gas lines are of particular concern because of the explosive nature of their contents.

Utility lines within transit buildings may also be targets of terrorists and agencies should consider their placement as part of the building design. Perimeters and parking garages are vulnerable to large explosions and vehicle ramming. Keeping utilities away from these areas reduces the risk of additional destruction or loss of critical emergency systems. Agencies should consider concealing and protecting all utilities to the greatest extent possible.

6.2.5.2 Electrical System

Agencies should consider facility backup power sources in case of a local or regional power failure, and identify those systems requiring emergency power in the event there is an outage.

Backup power can consist of a generator that uses fuel to create electricity or a battery that can store enough power to act as a supply in an emergency. Agencies should consider regular maintenance

[35] Building services use functional components such as wiring, mechanical equipment, switchgears and alarms that manipulate system inputs to produce the desired outputs. The only human interaction with functional components should be by maintenance or operational staff as these components are not part of the public interface.

checks to ensure backup power is operational. It is important to locate backup systems far away from the primary systems so that they are not damaged by incidents affecting the primary systems.

6.2.5.3 Functional Components

Control systems include electrical and mechanical equipment such as switchgears, alarms, sensors, meters, and other associated equipment used to coordinate other systems' functions and monitor their performance. Tampering with these controls can halt operations and compromise emergency response and evacuation.

Distributed control systems (DCS) are used to monitor whether the system is working properly, make system adjustments when necessary, and shut down the system if problems are identified. DCS can be integrated into ventilation, communication, and security systems, and located adjacent to other control components. They can be connected to an integrated facility communications system as an alarm system to notify system monitors of malfunctions or unusual activity.

Access to the control components is needed for maintenance but agencies should consider using appropriate access management controls to protect these components, and not leave them out in the open. They should also consider locating mechanical rooms away from the building perimeter, loading docks, and parking garages that are vulnerable to attack.

6.2.5.4 Heating, Ventilation and Air Conditioning (HVAC)

HVAC systems create a climactically comfortable environment and ensure air quality is adequate by regulating temperature and humidity, and filtering and replacing stale inside air with fresh outside air.

Miscellaneous Openings - refer to Section 5.3.9

While some buildings provide sufficient natural ventilation to remove carbon dioxide and other pollutants generated indoors, many buildings require mechanical ventilation systems to provide conditioned air by filtering, exchanging with outside air, and temperature and humidity control. Air vents collect air from outside; fans and ducts distribute it throughout the building and vent the "used" air out of the building.

Ventilation

Heating and cooling systems may be used in conjunction with ventilation systems to keep indoor temperatures comfortable. Transit buildings, such as open garages and above-grade stations, may not have mechanical HVAC systems since they have sufficient natural air transfer, while ventilation systems are a key component of tunnels and underground facilities.

Air vents may be used to gain access to the building if not properly located and secured. A terrorist could enter a facility through the vent shaft or use the opening to disperse weapons of mass destruction throughout the facility.

Agencies should consider designing HVAC systems to reduce the potential for break-in. Some techniques that can be used include:

- Designing vent shafts to have minimally sized openings.
- Securing doors and grates on ventilation systems accessed for maintenance.
- Locating vents away from areas with public access, such as sidewalks or medians, wherever possible. It is especially important they are not located on roadway gutters or other low spots, where oil spills or floodwaters could enter.
- Locating vent openings high up where they are out of reach.
- Installing actuated louvers over vent openings that open only while the fans are running.
- Monitoring vent openings with alarms and intrusion/tamper detectors to alert officials of the presence of humans or chemical substances.
- Installing sensors in vents to detect foreign substances in the ventilation systems.

Smoke and Fume Control

In addition to the vulnerabilities the HVAC system creates, it can also play an important role in smoke and toxic fume removal, especially for large or underground facilities. Agencies may use separate or auxiliary ventilation systems for smoke and fume control.

HVAC systems can create "safe zones" in buildings for occupants who cannot leave via emergency routes. Safe zones work by creating areas of higher pressure to keep fumes and smoke out until properly equipped rescue workers can assist the trapped occupants. It is important that these systems have backup power supply and can be manually controlled safely during emergency situations.

Fuel Oil/Propane

Some facilities, generally smaller ones and those in the northeastern United States, use fuel oil or propane for heating. Agencies should take into account that fuel storage locations and methods at these sites may cause security vulnerabilities.

6.2.5.5 Lighting

Lighting is an essential facility requirement, especially where buildings do not have adequate natural light or are used at night.

Surveillance

In addition to making buildings functional, lighting has a pivotal role in helping a facility prevent and recover from a terrorist attack. Appropriate lighting also creates a sense of security for people in the building. Without adequate light, surveillance, either human or mechanical, is limited in scope. Security and other personnel require light to clearly see what is going on around them and, more

importantly, beyond their immediate area. CCTV and motion detectors also require adequate levels of illumination in order to detect suspicious activity.

Lighting should provide illumination of pedestrian walkways and eliminate shadowed areas where attackers could hide. The selected type of exterior lighting should cast consistent color throughout the site, so the video surveillance quality is clear. The lighting intensity (foot-candles/square foot) should be greater around critical assets.[36] Lighting should be compatible with the particular camera systems in use, and should be designed to provide a bright, even distribution of light to eliminates hiding spots.

Lighting can also be faced outward away from a building entrance, to produce "glare" that reduces the visibility of anyone approaching a site or building checkpoint at night and providing an advantage to security personnel on duty. However, when selecting and positioning fixtures agencies should consider the possibility of concealed injurious devices within fixtures or between fixtures and the surface to which they are attached.

Evacuation

Lighting also plays a key role in the evacuation of a facility when an emergency occurs. Building occupants need sufficient light to safely exit the building without tripping or falling into others. Backup power is important for ensuring a safe evacuation if the main power source has been affected.

Security lighting installation - refer to Section 5.3.2

6.2.5.6 Communications

Communications systems interconnect various areas of transit facilities, connect to other transit facilities, and link to outside connections, such as emergency responders and the local phone network. In addition to facility and passenger communications systems, security systems and DCS should be connected to a central location to quickly identify and set in motion the response to emergency situations. Agencies should consider backups of vital communications systems, preferably through a secondary type of network. Wire-based communications should be backed up by radio or cellular systems and vice versa.

Agencies should consider all of the following communications systems when building a new facility or when updating existing communications systems.

Pubic Address Systems

Public address systems play a vital role in providing information to facility occupants in the event of an emergency, especially when on-going emergency egress training is impossible, such as at public

[36] Site lighting levels must satisfy the established minimum recommended levels outlined by the Illuminating Engineering Society of North America (IESNA) and other applicable codes.

facilities like transit stations. Where feasible, agencies should provide clear audio and visual directions in an emergency situation to direct patrons to safe locations. Agencies can also connect fire alarms to public address systems to alert all building occupants of an emergency situation.

Call Boxes

Call boxes provide a direct communication, linking isolated parts of a facility to either on-site personnel or a remote security service. They are commonly sited where they can be easily found at stations and stops on the platform, outside the station building and/or in parking lots. These systems allow citizens to report incidents quickly without leaving the site.

Agencies should keep public call boxes in working order, even if they are rarely used, and should design and locate call boxes that are accessible to persons with disabilities. They should also consider providing training for all staff responding to these calls so that emergency calls are responded to promptly and helpfully. It is important that the public is aware there are public call boxes available for reporting incidents and that they feel confident they will receive an appropriate response from the agency.

Emergency Response

Communications systems not only provide on-site communications, but also connect facilities to transit administrators and emergency response teams. Agencies should consider providing field employees with direct lines of communication between supervisors, control centers and/or emergency response personnel. Customer service booths and building reception desks can also be outfitted with silent emergency alarm buttons to inconspicuously activate an emergency response if required.

Agencies can also network monitors and alarms connected to building services, operations and surveillance equipment into the security system. Streamlining the communications networks can ensure they are all being monitored so that a response can be implemented rapidly when an incident occurs.

Communications technology overview - refer to Section 8.3

6.2.5.7 Security Systems

Security systems include CCTV, remote surveillance devices, video recorders, intrusion and motion detectors, tamper detectors, smoke or chemical detectors, and alarms.

Since constant surveillance by on-site personnel is often infeasible for most agencies, the practice must be supplement with other measures that can expand the ability of security staff to monitor large facilities. Surveillance equipment may be particularly appropriate in high-traffic and high-value areas since these systems can be integrated with other monitoring and communications systems to create a coordinated oversight and response center.

While remote surveillance and detection systems are important for identifying suspicious activity, an agency response plan should consider what actions to take once these activities have been identified. If possible, the systems should be designed so that a response team can prevent the threat from being carried out. In order for this to occur, there needs to be contact between those monitoring the alarms and local responders so that action can be taken quickly. Where possible, additional mechanisms, such as secondary locks or barriers, high-pitched alarms or pepper spray, should be used to thwart an attacker, to provide time for a response team to arrive and intercede.

Surveillance systems overview – refer to Section 5.2.5

Intrusion detection overview – refer to Section 5.2.6

Cameras can be either stationary or remotely/locally adjustable (pan/tilt/zoom) to make sure that they provide surveillance to the entire target area. A surveillance system that feeds video to a monitor for real-time observations is generally considered better for security, but is labor-intensive and requires constant diligence. As such, theses systems should be tempered with other measures: operationally, technically or both. Real-time observations can be supplemented if the surveillance system has integrated sensors and alarms. This "exception detection" method alerts security personnel when something abnormal occurs. Recorded feeds to be used for investigation are another option.

Sending feeds to a central, off-site location is preferable to on-site monitors. While some agencies prefer cameras and monitors to be available to on-site staff, remote monitoring can be more effective in the event of an evacuation. Agencies should consider how emergency responders can plug in locally to video feeds for on-site cameras.

When designing a remote surveillance system, it is important agencies consider potential obstacles to full surveillance, such as structural columns and sharp corners, when positioning cameras. Where a single camera cannot capture the entire area, multiple cameras can be set up to provide overlapping coverage areas. Agencies should consider motion detectors and other alarm systems as part of the security system design, to provide maximum coverage with a minimum of false alarm opportunities. These systems can be used in combination with other access management tools to provide an efficient and dependable security system.

Agencies can use these security measures as deterrents if they are designed to be obvious. Conspicuous surveillance measures provide a heightened sense of security, but they are also more vulnerable to vandalism. Vandal-proofing these systems is key to their proper functioning. Agencies should consider placing cameras, detection devices, and wiring beyond reach in secure enclosures. Surveillance cameras and other security technology can also be used to monitor an area covertly.

6.2.5.8 Water and Sewer

Transit facilities typically receive their water supply from the public network. This water supply is critical for fire suppression, but localized sections of the fire sprinkler system may be damaged in a blast or other violent event. Agencies should consider designing the on-site water distribution system with reinforcements and redundancies, to ensure there is a continuous supply of water throughout a facility and that damage to one section does not incapacitate the entire system. Agencies should consider providing access to water gates, manholes, and control valves only within a secured perimeter, to prevent someone from cutting off the water supply to the facility. Likewise, storm water culverts and other drainage facilities should be within a secure perimeter, to prevent them from being used to access the site.

6.2.5.9 Fire Protection

Fire protection systems are designed to minimize harm to people and the structure in the event of a fire. Fire detection systems include smoke detectors and alarms. Sprinkler systems, standpipes, and chemical fire extinguishers are used to minimize fire damage while emergency ventilation systems and emergency exit routes allow inhabitants to exit the building. Flammability of construction materials, furnishings, and other materials stored on-site are also regulated to minimize the risk of a major fire. A compartmentalized structure that allows fire or contaminants to be isolated can also minimize risk. Such compartmentalization might be accomplished through various measures, including movable barriers or partition walls, fire doors, etc.

This information is intended to supplement existing codes and considerations on fire protection, rather than to replace such information. States and municipalities regulate minimum fire protection for different types of structures and facilities. Many of these regulations are based on National Fire Protection Agency codes and standards, which can be viewed in NFPA 130, Standard for Fixed Guideway Transit and Passenger Rail System.

6.3 Security Approaches for Types of Transit Infrastructure

This section describes different types of transit infrastructure and facilities that agencies maintain and operate as part of the normal functions of a transit system, from the most obvious and visible to the most remote. They include:

- Transit stations
- **Transit stops**
- **Administrative buildings and OCCs**
- **Maintenance and storage facilities for transit vehicles**
- **Elevated structures**
- **Tunnels**

- Right of way, track, and signals
- Remote equipment and unmanned structures

For each type of transit infrastructure, where applicable there are subsections that describe: potential threats, site analysis, access management, emergency response and egress, protecting critical assets, protecting vulnerable assets, structural engineering, facility services, and systems and services

6.3.1 Transit Stations

Transit stations are facilities where passengers board and alight from transit vehicles. They vary greatly in size and design, both across systems and within a given system.

> A major security challenge at stations lies in **balancing the need for openness and convenience with the need to control the environment** in order to protect its users and system operations.

This section focuses on the more elaborate stations that typically include enclosed structures, full-time personnel, and separate paid waiting area, such as underground subway stations and off-street bus terminals. Since transit stations are prone to a different set of threats than less elaborate "transit stops," the two facility types are discussed separately. (See Section 6.3.2 for security approaches for transit stops.)

Stations may serve one or more modes of transit and differ in their levels of design complexity. All transit stations have some component that is at-grade, to connect with the surrounding pedestrian landscape. They may also have components that are underground or elevated, depending on the system. Since stations are designed for optimum passenger convenience and efficient traffic flow, they must be fully accessible and open as well as centrally located, often tightly integrated within a complex urban landscape.

Stations are typically divided into three types of areas, each of which has different security concerns and mitigation measures.

- Unpaid public areas are those locations within the site that passengers occupy before paying their fares (including entryways, lobbies, fare vending space, and concessions).
- Paid public areas are those locations that passengers occupy after paying their fares but before entering a vehicle (including additional passageways, platforms, and waiting areas).
- Non-public areas are intended only for authorized transit staff (including administrative offices, electrical and mechanical rooms, HVAC and maintenance areas, and vendor stalls).

Subsections describe:

- Potential threats
- Site analysis
- Access management

- Protecting critical assets
- Structural engineering
- Systems and services

6.3.1.1 Potential Threats

Stations are likely targets because they are high-profile facilities that serve large numbers of people in enclosed, relatively small spaces, are easily accessible, and are centrally located.

Arson

While stations are designed to be fire resistant, they are still vulnerable to an arson attack ignited either from an accelerant (flammable substance used to increase the spread of fire) brought to the station or from incidental materials such as garbage, vendor goods, and passenger baggage within the station. Any fire that does occur may damage the station and other property, as well as injure passengers and employees. Fires may be particularly dangerous in those stations that are enclosed or underground, where people may become trapped and exposed to fumes and heavy smoke.

Explosives

A vehicle carrying explosives that approaches the outside of a station or enters the station could generate a large explosion. The closer the detonation is to the station and its key components, the greater the potential for damage.

Stations are also vulnerable to people hand-carrying explosives into the facility. While the amount of explosives a person can carry produces a smaller blast, human carriers can penetrate deep within a station without detection and can choose a detonation point with the maximum destructive impact on people or structures. Explosives may be detonated on the carrier (a suicide attack) or be hidden in the station for future detonation.

Explosions can cause injuries and fatalities to the passengers and employees in a station, property damage or structural collapse of the station itself, and cause subsequent fire.

Weapons of Mass Destruction

Stations that are enclosed or underground may be particularly vulnerable to a WMD attack, and may serve as an access point for an attack on an entire underground network. As with explosives, someone could carry a WMD device into a station without detection and position it in a location for maximum destructive effect.

Substances may be released by hand or hidden for future dispersion, and may cause property damage as well as irritation, injuries, and fatalities among the patrons and employees exposed. Riders moving through the transit system can inadvertently spread a harmful substance to which they have been exposed, greatly increasing the consequences of such an attack.

Hostage or Violent Event

Stations may be seen as prime targets for a violent event because they are easily accessible, heavily populated by the public, and generally enclosed.

6.3.1.2 Site Analysis

Since stations are situated in areas where large numbers of people live, work, and travel, they are often adjacent to public space, dense development, and other facilities that might not otherwise be considered security threats. However, site planners may be able to make some choices that improve security without compromising nearby facilities.

Facilities located above, below, or adjacent to the station deserve special attention, especially roadways, loading areas, vehicle-service areas, offices, and parking lots, all of which may serve as access points for explosive-laden vehicles or as vantage points. Surveillance by transit personnel and the general public and the ability to identify and respond to an emergency situation are key components of safety within the station setting; open layouts with wide fields of vision support this goal.

6.3.1.3 Access Management

Transit stations are designed for convenient access, typically by large numbers of riders and agency staff. Stations may include access for a single, discrete transit line, or may feature transfers to other lines or services. For safety and security reasons, there are areas that must be inaccessible to the public and still other areas that must be inaccessible by vehicle.

The following sub-sections present an overview of access management at transit stations for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management*.

Admissions Control overview – refer to Section **5.3.3**

Perimeter Security

It is impractical to establish a strong perimeter around a transit station, even though it is often necessary to pay and pass through admissions-control barriers to enter the platform. Stations must be as accessible as possible to potential patrons arriving both by foot and in vehicles.

A transit station may have a range of other entrance types depending on the modes served, including tunnel portals for rail service or on-the-road throughways for buses to approach docking areas. Some of these entrance types may warrant additional security measures to prevent inappropriate vehicle access, which need not compromise passenger mobility. In addition, selecting a site where it is possible to maintain unobstructed sightlines around key access points or critical areas may also improve security without compromising the station's accessibility.

Perimeter Protection and Barriers overview – refer to Section 5.2.2

Vehicle Access

Agencies should consider how to minimize the potential for unauthorized vehicles to gain proximity to the station, crash into the station at a high speed, or enter the station through one of its entrances. Barriers to vehicle access need not be brick or concrete structures; natural elements such as trees and shrubs may also be appropriate depending on the location and configuration of the area.

Planners should consider locating key load-bearing structural components, as well as densely populated passenger waiting areas, away from areas that unauthorized vehicles can access. Design choices (the depth or height of the station, the dimensions of passageways between the street and the core of the station, and shielding passenger-waiting areas behind other structural elements) can mitigate the risk of a successful attack.

Transit vehicle entrances to the station can be limited to a small number of controllable access points. These entrances should be separate and clearly distinguishable from any public right-of-way or entrances, through the use of signs and/or channeling circulation. In addition, designers can use access controls, such as bollards, to limit the type of vehicle that may easily enter. Pedestrian entrances should be constructed in a manner that bars vehicles altogether or prevents access by vehicles other than maintenance or emergency responders.

In vehicle areas that must be close to the station, such as passenger drop-off areas, agencies should consider using traffic circulation tools to slow traffic, such as S-route curves, to minimize the opportunity for ramming (refer to Section 6.2.1).

Both passenger access and vehicular security are easier to manage when vehicle loading areas are segregated from passenger drop-off areas.

Vehicle Access Control and Parking overview - refer to Section 5.3.4

Human Access

While transit stations are generally designed to make human access as easy as possible, agencies should consider preventing after-hours access and access to non-public parts of the facility. When the facility is closed, the facility should be secured at its outermost perimeter, with locked gates or doors. Outdoor lighting can be used to illuminate station access points. Intrusion alarms and surveillance may also be helpful.

Since the non-public parts of a transit station may be located in publicly accessible spaces, a combination of access management measures may be necessary to consider. Locks, surveillance, credentialing technology, and highly visible locations may help secure the equipment from tampering. Designs can also cultivate an atmosphere of exposure, which is useful in both discouraging and detecting any unwanted activity. The combination of staff, surveillance technology, and unobstructed sightlines can help both transit personnel and the public to serve as watchdogs, helping to deny the opportunity for covert endeavors, and making any unusual activity easily detectable. In any areas of the station where direct surveillance by staff is difficult or impractical, call boxes can help connect patrons with authorities.

Credentialing overview: refer to Section 5.2.4

Surveillance Systems overview: refer to Section 5.2.5

Emergency Response and Egress

A station's emergency response plan should consider the capacity of the station and the fact that many users will not be familiar with the layout of the station and its emergency exits. Emergency systems can direct occupants to safe exit locations, especially if there are additional exits that are not commonly used for station access.

Agencies should consider including emergency communications systems, including blue-light phones and public address systems, in the plan, to allow rapid communications between remote areas of the station. Stations should be equipped with emergency lighting, sprinkler systems and safe rooms, especially if there are subway or elevated platforms.

6.3.1.4 Protecting Critical Assets

Agencies should consider locating critical assets in transit stations, such as building systems and operations equipment, in secure locations with adequate surveillance. For example, mechanical rooms should be within a secure perimeter, and, where feasible within sight of station attendants or monitored by surveillance systems. Agencies should also protect the assets from attack by explosives by locating them away from the site perimeter, where explosions are more likely to occur, and should protect station platforms against access by non-transit vehicles, using different types of barriers.

The location of entrance controls and station attendants is important in protecting the facility. Locating controls and attendants at the outer edge of a building may enhance security of the entire site if these attendants have views of the surroundings. This may mean there are other areas within the station that do not have constant surveillance. If the station attendant is located at platform level, they can observe activity in this area, although this may leave stairways and corridors leading to the platform vulnerable.

If bicycle lockers are on-site, agencies should try to locate them away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials.

Building materials are critical in minimizing the impact of an attack. Qualities such as fire resistance and resistance to absorption of toxic materials can greatly reduce the work needed to recover from an attack. For more information on building materials, see Section 6.2.3.

6.3.1.5 Structural Engineering

Structural considerations for the station depend on the station design: elevated stations will have very different concerns than underground stations. The primary consideration for agencies should be to protect the lives of staff and riders during an attack. A design that has redundant structural elements to prevent progressive collapse in the event of an explosive blast, vehicle ramming, or fire can greatly improve the security of people in the building. (See Section 6.2.3)

Table 6-2. Security-Oriented Design Strategies for Transit Stations

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Structures set back from roads and parking areas, if applicable	Deter/Minimize	
Physical barriers such as bollards, road spikes, and fencing to enforce setbacks and/or prevent ramming	Deter/Minimize	X
Minimum number of vehicle entrances	Deter/Detect	X
Unobstructed sightlines surrounding the station	Deter/Detect	X
Interior Layout		
Interior station layout provides unobstructed sightlines, minimizing hidden areas or remote passageways	Deter/Detect	
Kiosks, ads, and information positioned to not disrupt sightlines	Deter/Detect	X
Minimum use of columns and blind corners	Deter/Detect	
Security mirrors on columns and corners	Deter/Detect	X
Operator booth positioned for maximum presence and visibility within station	Deter/Detect	
Critical assets buffered from public or vulnerable areas	Deter	
Non-public facilities hidden and not identified	Deter	X
ADA-complaint emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Critical equipment secured with gates, locks, or other access control measures	Deter/Detect	X

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Dimensions of station entrances limit permissible vehicle size	Deter	X
"No Trespassing" signage	Deter	X
Posted or broadcasted instructions on how to report suspicious activity	Deter/Detect	X
Bright paint colors to increase ambient lighting	Deter/Detect	X
Vulnerable features designed to channel blasts	Minimize	
Shatter-proof glazing	Minimize	X
Façade materials that resist explosive blasts	Minimize	
Materials that do not absorb toxic substances when exposed	Minimize	Maybe
Fire-retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		
Appropriate surveillance at entrances, at access points to non-public areas, and throughout the station	Deter/Detect	X
Sufficient lighting for nighttime surveillance	Detect	X
Motion detectors or intrusion alarms on vehicle entrances	Detect	X
Intrusion alarms at access points to non-public areas	Detect	X
Communication links from remote station areas to station personnel (such as call boxes and a public address system)	Detect/Deter	X
Communication links to administrative and emergency response centers	Detect/Deter/ Minimize	X
Backup emergency lighting	Minimize	
Fire detection and suppression system	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

6.3.1.6 Systems and Services

Building systems play a critical role in transit stations because of the large numbers of people present, especially in enclosed facilities, such as underground stations. The continuous supply of electricity and ventilation after an attack can improve the ability of people to evacuate the facility. Signage is also critical during an emergency, because many users will be unfamiliar with the station layout and locations of emergency exits. Agencies should consider incorporating communications systems into the facility, both to direct occupants during an emergency and to enable riders to notify transit staff of any problems or threats they observe.

6.3.2 Transit Stops

For the purposes of this report, transit stops are considered separately from transit stations and more elaborate transit facilities. (See Section 6.3.1 for security approaches at transit stations).

Transit stops are facilities where riders board and alight from buses or light rail transit vehicles. These sites range from a simple signpost in the sidewalk indicating where a vehicle stops, to an elaborate transit plaza with sheltered waiting areas serving multiple bus routes or light rail lines. They are almost always at-grade, and may be located either right at the street curb or, in the case of larger sites, set back from the street on a dedicated parcel of property. Transit stops are often on public land, and have minimal facilities: signage, open shelters, lighting, and occasionally heating elements in colder locales. Although some transit stops have staffed information or fare-collection kiosks, most have no consistent on-site personnel.

The public nature of transit stops makes such sites easy targets for terrorist attacks. Worldwide, buses are the most frequently attacked transit vehicles,[37] and the sites that serve them are at risk by association. Although their high level of accessibility and lack of opportunities for security elements mean many of the techniques in this report cannot be implemented at transit stops, certain measures can be used to increase their level of security. These include improving visibility in and around transit stops, and using construction materials that resist damage in an explosion or collision.

There are three categories of transit stops referenced in this section:

- Curbside stops are waiting sites located on public streets. These typically have a signpost indicating the transit route, and may have some combination of lighting, a bench, or a partially enclosed shelter on the sidewalk.
- Transit plazas are separate parcels of land typically dedicated to light transit service, although transit vehicles access these sites from public roadways. These include off-street bus plazas and light rail stops serving one or multiple routes.
- Light rail stops reached by dedicated rights-of-way are typically at-grade. They may or may not be isolated from public roadways, and are therefore less accessible to public vehicles. Transit plazas and light rail stations often have basic amenities, such as shelters, a small concession stand, or a fare collection/information booth—staffed or unstaffed.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets

[37] "Protecting Surface Transportation Systems and Patrons from Terrorist Activities," Brian Michael Jenkins, International Institute for Surface Transportation Policy Studies (December 1997): p. 106.

- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.2.1 Potential Threats

Since most transit stops have limited staff or facilities, transit riders are the primary targets at these sites since the death or injury of riders would receive substantial media attention and provide a strong opportunity for a political terrorist statement. Attacks on light transit vehicles, especially buses, are the most common transit-related terrorism events, and the stops that serve these vehicles should take this into account in their design.

The following principal threats to a transit stop are intended primarily to harm the greatest number of transit riders as possible, but also to cause damage to the facility.

Explosives/Fire

Transit stops are easy, high profile targets for an explosive device. Since people tend to congregate at stops, they are attractive targets for prospective terrorists. The small size and lightweight construction of most shelters would require a small amount of explosives to achieve a high level of damage, and few if any measures are in place to prevent a bomb from being detonated at a transit stop. Such facilities are typically in public places, so there is also the potential to spread the collateral damage from a blast to adjacent properties.

Vehicle Ramming

The small size of most transit stop facilities means they could be severely damaged or destroyed by a vehicle collision. This threat is exacerbated by their open layout and close proximity to public roadways. Transit riders and staff need to be protected against the possibility of a non-transit vehicle intentionally colliding with people or structures on the site.

Weapons of Mass Destruction

Transit stops present an opportunity to use biological or radiological agents to harm not only transit riders, but an entire region as well. Since riders have a wide geographic range of destinations, a toxic substance with delayed effects can be released at a transit stop and inadvertently carried by riders to different areas of a city. This dispersal would help to maximize the harmful effects of the attack on the region as a whole, rather than concentrating the effects in a small area that could be contained and treated. Transit stops are less likely to be a target for this type of weapon than subway stations, since the latter have higher numbers of riders and present a more attractive target to terrorists.

6.3.2.2 Site Analysis

Agencies should consider several aspects of a site when determining appropriate security precautions. Most important is the site's relationship to the road, since this is the most likely direction of an attack. Agencies should consider designing and orienting on-site facilities both to provide clear views of the road(s) and to shield occupants from attacks. In most cases, views of approaching traffic are already incorporated into the site design (so riders can see arriving transit vehicles), but views of opposing traffic and adjacent land should also be considered. Adjoining properties and nearby buildings may be evaluated for their potential as hazards or protective buffers in an attack, and factored into layout and design considerations.

6.3.2.3 Access Management

The following sub-sections present an overview of access management at transit stops for perimeter security, vehicle access, human access, and emergency response and egress. Cross-references provide more specific information in *Chapter 5: Access Management*.

Perimeter Security

Perimeter security is largely impractical at transit stops. The public function of these sites means that people should be able to access them easily; any features that hinder approach will ultimately be seen as counterproductive to the site's primary function.

A transit agency may choose to establish a perimeter with limited access points around a stop, especially at transit plazas and light rail stops. This not only limits people to moving through entry points that are under surveillance, but can serve a safety function by separating pedestrian and vehicle traffic. Some larger facilities may have non-public areas to be secured against unauthorized access; these can have barriers around them to establish a small-scale perimeter.

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access Control and Parking overview: refer to Section 5.3.4

Vehicle Access

Vehicle access issues vary for each type of transit stop. At curbside stops, the transit vehicles share the roadway with public vehicles, and all vehicles (transit and private) must be able to access the site. Design features such as bollards can prevent a vehicle from ramming benches or a shelter, but any vehicle can get close enough to a curbside stop to inflict extensive damage with explosives. Agencies may consider using blast-reducing measures, as described in Section 6.2.3.1.

For bus lanes and transit plazas, where private vehicles are not allowed in the lanes intended for transit vehicles, the challenge is providing easy access for transit vehicles from public roadways, while preventing access by unauthorized vehicles. It is possible to equip exclusive bus lanes with automated gates triggered by a transmitter in each transit vehicle as it approaches, but this

technology may be cost-prohibitive for many agencies and reduces the overall operating speed of the transit vehicles.

Light rail stations, especially those with dedicated rights-of-way, are typically more isolated from roadways than other transit stops. Where possible, barriers can be installed to prevent vehicle access from public roads and parking lots to the transit stop and right-of-way. These barriers can be designed to withstand impacts from vehicles while still enabling pedestrians to pass through.

Human Access

Transit stops are meant to be accessible to all people, so it is virtually impossible to prevent specific people from gaining access. These considerations are intended to increase the security of riders and staff in the facilities by increasing their ability to detect potential threats, rather than through access management.

When constructing staff booths used for fare collection or providing information, agencies should consider using mechanical locks, pass codes or key cards, and other access controls to resist tampering and forced entry. Booth orientation and design should provide staff with clear views of as much of the site as possible, for both surveillance purposes and staff safety.

Agencies should consider situating shelters for waiting riders so the interiors are visible to either an electronic surveillance system or to transit staff, including the drivers of approaching vehicles. The shelter design should eliminate potential hiding spots for bombs or other devices. Windows and cutouts should be located to allow users to view approaching traffic (both transit vehicles and others), and reduce the possibility of anyone approaching the shelters undetected; this may affect an agency's policy regarding billboards and other forms of advertising incorporated into shelters. Some transit systems (such as BRT systems) have paid fare areas to secure, but access management in these situations addresses scofflaws more than it addresses security risks.

Emergency Response and Egress

Every transit facility design must enable easy evacuation and response by emergency personnel in the event of an attack.

Agencies should consider a facility layout that facilitates the detection of a serious problem, with traffic lanes that are wide enough to permit access by responding personnel and vehicles. However, agencies must balance these needs against the goal of preventing access by unauthorized vehicles.

The design of any on-site enclosed structures (attendant booth, paid fare secure area, etc.) should ensure easy evacuation by riders and staff. Emergency exits must be appropriately located and well marked. Agencies should consider installing an integrated emergency call box to the transit agency or local police, with the transit stop name/facility number clearly displayed to enable quick identification.

6.3.2.4 Protecting Critical Assets

The principal assets at transit stops are riders and on-site agency staff. Facility layout can contribute to their protection by providing a high degree of visibility from the site into the surrounding area, sufficient lighting to detect any potential threats, and structural elements (such as reinforced shelters or traffic bollards) that shield occupants from likely directions of attack. Where possible, waiting areas, staff facilities, and any other assets should be set back from public roadways as far as possible.

If bicycle lockers are on-site, they should be situated away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials.

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.2.5 Structural Engineering

Agencies should design all structures at transit stops to resist damage or destruction. Passenger shelters, staff kiosks, and utility housings can be reinforced against accidental or intentional ramming by a vehicle and construction materials selected that minimize the amount of flying debris in an explosion (especially window material, which is more easily dispersed). Any street furniture such as benches or trash cans can be anchored to prevent them from becoming projectiles in a blast, and designed to redirect blast force in a safe manner, whenever possible.

6.3.2.6 Facility Services

Mechanical Systems

Most transit stops are too small to have substantial mechanical systems. The main exceptions are facilities with fare machines or on-site staff, normally in small booths. Agencies should consider installing communications equipment and basic HVAC capability in booths. Most mechanical systems will be relatively easy to access, but since they serve more of an accessory function within the transit system, their vulnerability merits less concern than other elements of the infrastructure. Agencies should consider housings for any on-site equipment that are durable and tamper-resistant and locate equipment, where possible, in view of riders or on-site staff to assist the detection of tampering attempts.

Electrical Systems

Some transit stops have basic electrical systems for lighting and, in colder locales, heating elements in shelters for waiting riders. At curbside stops, the city power lines serving streetlights often supply the electricity, meaning they are not under the direct control of the transit agency. In most cases, the size and open layout of transit stops make on-site backup electrical systems unnecessary.

Agencies should consider installing emergency communication equipment in as many transit stops as possible. This enables transit staff and riders to notify the agency of any emergency as soon as it occurs, increasing both the safety and security of the site. Call boxes can be located in rider waiting areas and on-site staff booths can have direct communication capabilities with the transit OCC.

Table 6-3. Security-Oriented Design Strategies for Transit Stops

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Unobstructed sightlines surrounding the stop	Deter/Detect	X
Physical barriers such as bollards and fencing to prevent ramming, or to prevent unauthorized access if the stop has a segregated transitway	Deter/Minimize	X
Interior Layout		
Kiosks, ads, and information positioned to not disrupt sightlines	Deter/Detect	X
Architectural Features		
Signage to deter non-transit vehicles from the stop area	Deter	X
Structural Engineering		
Structures and street furniture anchored to prevent being dislodged	Minimize	
Materials chosen to minimize flying glass and debris	Minimize	
Systems and Services		
Emergency call boxes to report incidents	Minimize	X
Adequate lighting for surveillance	Detect	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

6.3.3 Administrative Buildings and Operations Control Centers

Administrative offices and operations control centers (OCCs) are the facilities from which transit systems are managed. Administrative functions at these sites include strategic planning, engineering and construction, revenue processing, real estate and community development, and customer service. Operations activities include ongoing supervision of tracks and signals, vehicle tracking, communications with all fleet vehicles, and emergency response. Facilities are typically not open to the public, although administrative offices generate some business-related visitor traffic.

These functions and activities may or may not be integrated into a single, centralized facility. A larger transit system may conduct administrative functions in a conventional office building (either entirely dedicated to the transit agency or shared with other office tenants), while operations control occurs at a specialized facility in a

Administrative buildings and operations control centers might be strategic targets because of their important role in system operations.

separate site. For smaller transit systems, all the activities are often integrated into a single facility, and may be co-located with another facility such as a maintenance yard.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.3.1 Potential Threats

OCCs and administrative buildings are potential targets for attack because they are necessary for transit operations and are often linked to the entire system. Terrorists may target a centralized facility as a means of halting service, or of obtaining documents and sensitive information about the system. These facilities are not likely targets for attacks meant to inflict civilian injuries, since they are not usually open to the public and typically contain fewer people than other types of facilities.

Explosives

A vehicle could deliver a large explosive device to the exterior of a facility, or a human carrier could carry a smaller device into an OCC or other administrative building. In addition to injuries, potential property damage, and structural collapse; an explosive blast and any ensuing fire may damage equipment that is necessary for system operations or emergency response, potentially disrupting service or disabling the entire system.

Arson

A fire, especially one deliberately set in a critical area of an OCC or administrative facility, could have the same effect as an explosive blast: injuries, property damage, and destruction of critical equipment that results in the disruption of transit service.

Tampering

Critical operations control and computer systems at administrative buildings and OCCs are at risk of being tampered with because of their importance throughout the transit agency's network. An attacker may tamper with systems to gain control of the system, to inhibit emergency response capabilities, or to obtain information about the system to use in a later attack; all of which potentially

endanger transit users and assets throughout the network. Documents that reveal information such as confidential operating procedures or details of the system's design may also be vulnerable to tampering or theft in support of a later attack. Attacks on information systems and documents may be particularly easy for an insider to carry out.

Hostage Situation or Violent Incident

An attacker may use a hostage situation or violent incident in an attempt to gain control of systems operations. Staff could be violently coerced to manipulate the system in a manner that endangers staff, riders, and equipment.

Weapons of Mass Destruction

WMD may be used to contaminate the facility, putting transit employees at risk of illness, injury, and fatality. If the site is contaminated, evacuation of the site may disrupt systems operations. Any substance that proves difficult or impossible to eradicate from the facility could extensively disrupt operations and cause property damage.

6.3.3.2 Site Analysis

These sites differ from most other types of transit infrastructure in that they do not need to be located for public convenience and are best sited in out-of-the-way, inconspicuous locations. For activities that are critical to system operation, such as operations control, redundant facilities in separate locations may help ensure full or partial operations in the event of an attack on a primary facility. Because hardened facilities may be expensive to establish and maintain, a transit agency may consider co-locating some of their facilities with other agencies that have similar security goals.

Most importantly, planners should consider a site with a securable perimeter, setting the building back from any public roadways. Within the site perimeter, on-site parking can also be setback from the building, potentially with separate areas for visitor and employee parking, and entrances located so they do not face the street directly. Agencies should consider planning a buffer zone that separates the facility from neighboring land uses with unobstructed sightlines. Designers may use lighting to improve visibility from the structure at night as well as to produce glare that may hinder any approaching attackers. Although sensitive sites should generally be inconspicuous and vaguely labeled, "keep out" signs may help protect nonpublic areas.

6.3.3.3 Access Management

The following sub-sections present an overview of access management at administrative buildings and OCCs for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management*.

Perimeter Security

OCCs and other administrative buildings are not typically open to the public, so stringent perimeter security can be implemented without compromising the facilities' intended uses. When planning access to the facilities, designers need to accommodate employees, job applicants, deliveries, visitors seeking tours, public officials, and contractors or others doing business with the transit agency. Agencies should consider consolidating entrances to the site to a minimal number of access points and monitoring them for access control, in addition to developing a means for screening visitors in vehicles, pedestrians, or bicyclists.

Perimeter Protection and Barriers: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access Control and Parking overview: refer to Section 5.3.4

Vehicle Access

Within the site perimeter, designers should consider traffic circulation and parking areas that minimize the opportunity for vehicles to drive close to site structures, to crash into a structure at a high speed, or to enter a structure through one of its entrances.

Human Access

Within the facility, access management techniques can be used to differentiate between employees and visitors and to enforce different levels of security clearance for different types of employees. For example, employees who are not responsible for operations control may not be allowed access to those systems or to the areas of the building where the systems are located. Locks, card-key access, biometrics, and pass code protection can all help enforce appropriate access among employees, as well as make it more difficult for outsiders to break in.

In addition, surveillance and intrusion-detection techniques can be used for early discovery of an intruder. The interior building design can minimize hidden spaces such as niches, blind corners, or isolated passageways in order to facilitate surveillance. Wherever possible, designers should consider clear fields of vision so that all areas of the building are in plain view of security personnel and other employees. Cameras can help expand the surveillance area of live personnel, while intrusion alarms such as motion detectors and alarmed doors can help alert personnel to points of intrusion.

Admissions Control overview: refer to Section 5.3.3

Credentials and Credentialing overview: refer to Section 5.2.4

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.3.4 Emergency Response and Egress

To protect the people inside an administrative or OCC facility, agencies should consider incorporating emergency-detection systems and egress routes. One consideration unique to this type of facility is how to maintain maximum operability, even during an emergency. Designers may consider ways to seal off certain areas of the building from other areas, for example to prevent a fire from spreading to important operations equipment areas.

6.3.3.5 Protecting Critical Assets

Not all assets in a facility share the same vulnerabilities, and therefore may require different security measures. One way to address this is to create areas of varying security, or "layers of security," within a facility. This can be particularly effective in administration buildings and OCCs because it locates critical or vulnerable assets behind tight security, while minimizing the impact on daily operations that require less security. For example, entry lobbies and conference rooms are less critical targets than control rooms and document vaults. Planners can locate control rooms and document storage at the core of several "rings of protection" within the building, so that any attacker would have to cross increasingly stringent controlled-access areas in order to reach a critical target. For more information refer to Section 5.1.5.4.

If bicycle lockers are on-site, agencies should try to locate them away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials.

6.3.3.6 Structural Engineering

Planners should consider the full effects of various blast loads, fire, and ramming when designing the building to protect employees, as well as the areas that are critical to operations. Critical facilities can be "hardened" (see Section 6.2.3) to resist these types of threats. Glazing materials are a particular concern, since an administrative office building may face adjacent unsecured buildings on multiple sides.

6.3.3.7 Facility Services

Administrative and OCC facilities provide a variety of services to make the building a comfortable workplace. While all of these services impact security, some services warrant special treatment because of the function of the facility and the associated security concerns.

Certain areas of a building may call for heightened fire protection measures, such as erecting fire doors to seal off an area or installing sophisticated detection and extinguishing systems. The ability to provide uninterrupted power to the facility after an attack is of critical importance. Power lines into the building should be secured and planners may consider redundant power sources as well as

on-site generators. Communication equipment may also deserve special attention on OCC sites. Communication systems may be critical for security and for operability throughout the transit agency's network, and agencies should consider protecting any critical communication conduits or receivers from attack and incorporating redundancy.

Table 6-4. Security-Oriented Design Strategies for Administrative Buildings and OCCs

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Inconspicuous facility location	Deter	
Co-location with facilities having similar security needs	Deter	
Securable perimeter	Deter	
Structures set back from roads and parking areas	Deter/Minimize	
Physical barriers such as bollards, road spikes, and fencing to enforce setbacks and prevent ramming	Deter/Minimize	X
Minimum number of access points necessary	Deter	X
Building entrances facing away from unsecured areas	Deter/Minimize	
Unobstructed sightlines surrounding the building	Detect	X
Interior Layout		
Building layout provides unobstructed sightlines, minimizing hidden areas and blind corners	Deter/Detect	
Critical assets buffered from public or vulnerable areas	Deter	
Zones of activity segregate building uses	Deter/Detect	maybe
Ability to isolate critical areas and maintain operations	Minimize	maybe
ADA-compliant emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Critical equipment secured with gates, locks, or other access control measures	Deter/Detect	X
"No Trespassing" signage	Deter	X
Vulnerable features designed to channel blasts	Minimize	
Shatter-proof glazing	Minimize	X
Façade materials that resist explosive blasts	Minimize	
Fire retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Redundant OCC off-site	Minimize	X
Sufficient lighting for nighttime surveillance	Detect	X
Appropriate surveillance and access management system at entrances and throughout the facility	Detect/Detect	X
Backup power supply	Minimize	X
Backup communications system	Minimize	X
Backup emergency lighting	Minimize	X
Fire detection and suppression system	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

6.3.4 Maintenance and Storage Facilities for Transit Vehicles

Thoughtful design of vehicle maintenance and storage facilities can help prevent unauthorized site access.

At transit maintenance yards and storage facilities transit vehicles are serviced for cleaning, fueling, maintenance, and repair; and vehicles are stored when not in use. The site may include fleet vehicle parking areas; garages where vehicles receive regular inspections and service; maintenance yards where substantial vehicle repairs occur, and where partially assembled vehicles are housed; fuel-storage facilities (either underground or above-ground tanks); and administrative offices. There may be lounges for off-duty drivers and offices for supervisors whose work is based out of the maintenance yard rather than the transit system's operations and control center. Some sites may also house a secure fare-processing facility, as well as training facilities for operators and other field workers. Maintenance yard and storage facilities may be co-located with a station or operation and control center.

This section focuses on-site security for these facilities, including access to stored vehicles on the site, but does not address vehicle design. Refer to Section 7.4 for rail and bus vehicles security-oriented design considerations.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.4.1 Potential Threats

Maintenance and storage yards typically have few on-site staff, but house numerous vehicles, equipment, and stored fuel. Vehicles and fuel are the most likely targets for terrorist attack. Agencies should consider focusing security precautions on preventing unauthorized access to parked vehicles and fuel-storage areas to protect transit staff, riders as well as the transit vehicles.

These facilities are more vulnerable to attack by individuals with knowledge or expertise in yard operations. Agencies should consider a site layout and design that facilitates the detection of any improper behavior, regardless of whether the perpetrator is authorized to be in the facility.

Explosion/Fire

Fuel-storage sites are especially attractive targets at bus yards, where fuel tanks hold as much as 50,000 gallons—enough fuel to cause a major fire that could destroy the facility and the vehicle fleet stored there. Liquid fuel is more likely to spread out into a pool and burn for an extended period of time, while gaseous fuel can release under high pressure and cause an explosion. Fuels that ignite more readily than others must be kept farther away from potential ignition sources. Facilities with compressed natural gas, or other fuels stored under pressure, are at a particular risk for a major incident.

Maintenance facilities are also potential targets for attacks using explosives or arson, although other transit infrastructure assets might be more likely targets for this type of terrorist attack.

Tampering

Maintenance facilities provide the opportunity for terrorists to sabotage vehicles by tampering with the electrical and mechanical systems in a manner that would cause an accident when the vehicle is in service. Such an incident could result in as much damage as a direct attack on a vehicle or transit station. In addition, although maintenance sites might be unlikely targets for an attack with explosives or WMD, a terrorist could try to place a device on a stored vehicle for subsequent

detonation or release while the vehicle is in service. For this reason, access to the vehicles should be a key concern at maintenance and storage facilities.

6.3.4.2 Site Analysis

When locating a new maintenance or storage facility, agencies should consider the ability to secure and isolate the site. Maintenance and storage facility sites can have a clear perimeter equipped with strict access control measures. Other important considerations might include the location of vulnerable assets such as fuel-storage tanks and maintaining divisions between any adjoining transit facilities that have different security goals.

6.3.4.3 Access Management

The following sub-sections present an overview of access management at transit vehicle maintenance and storage facilities for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management.*

Maintenance and storage facilities can be contained within a secured perimeter.

Perimeter Security

Because these sites are not public facilities, agencies can maintain a fairly strict perimeter without interfering with normal operations of the facility. Transit vehicles, transit employees, and employee vehicles need to cross the perimeter on a regular basis, and the site may also need to accommodate occasional visitors and their vehicles. Access control measures can help distinguish those authorized to access the site through its entrances and prevent and detect covert access elsewhere along the perimeter.

Agencies may need to consider additional access control measures if adjoining transit uses require public accessibility. For example, rail facilities need to be adjacent or connected to the rest of the rail system. This means that storage and maintenance facilities may be adjacent to stations, which have widespread public access. Planners may consider ways to monitor the division between the public and nonpublic zones of the site.

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access Control and Parking overview: refer to Section 5.3.4

Vehicle Access

Maintenance and storage vehicles require regular transit-vehicle access. Creating a limited number of carefully controlled access points reduces the opportunity for unauthorized vehicles to enter the site. Access control measures might be particularly important at bus yards, where transit vehicles enter directly from public streets into the yard.

Agencies should consider dedicated entrances for transit vehicles that can be monitored, either electronically or by on-site security staff, to ensure no unauthorized vehicles gain access. Placing tracks and driveways for transit vehicles adjacent to one another instead of intermittently around the site, can also provide more streamlined site control. Non-transit vehicles, including staff cars, visitors' cars, and delivery trucks can be directed to parking areas that are separate from the parking and maintenance areas for transit vehicles. This can make it more difficult for perpetrators to gain access to transit vehicles and equipment.

Human Access

A secure perimeter and access control measures at the entrance to the site can help prevent unauthorized access onto the site. Additional access control measures can further protect critical areas such as vehicle garages and repair buildings, where open vehicles might be found. Keys, locks, and credentialing, as well as surveillance using security guards or CCTV may help deter and detect an attacker from accessing the buildings on a site. Technology such as cameras and intrusion alarms can extend the reach of surveillance in those areas with a limited staff presence.

Admissions Control overview: refer to Section 5.3.3

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.4.4 Emergency Response and Egress

Agencies should consider the location of hazardous substances and equipment, such as fuel-storage tanks, when planning emergency routes and response equipment.

6.3.4.5 Protecting Critical Assets

Transit Vehicles

Vehicles in the maintenance barn may be in various stages of repair, with parts removed or components exposed, presenting an opportunity for tampering and sabotage. Agencies should consider a location out of public view, within secured buildings.

The exposed underbelly of a transit vehicle may be at risk for a tampering attack while undergoing repairs.

Sunken inspection bays or reflective mirrors can facilitate under-vehicle inspections, which ideally should be completed prior to returning a vehicle to service. Transit agencies might also utilize technologies such as sensor systems to evaluate whether a vehicle underbelly deviates from its expected design, triggering an alarm if anything unusual is detected.

Vehicle parking areas can be designed to provide clear sightlines between rows of vehicles to allow for easy surveillance and minimize places where a person might hide. For example, parking buses in either a parallel, perpendicular, or angled formation, rather than a chevron formation, allows a security guard to see between multiple vehicles at a time instead of having to walk by each vehicle to have a clear view. If space and maneuverability constraints require a chevron formation, stricter access controls may be required for the vehicle parking areas.

Fuel-Storage Tanks

Agencies should consider storing fuel tanks far enough away from structures to minimize damage to buildings in the event of an explosion or fire. Additional fencing and access controls can help limit access to authorized personnel. CCTV or other surveillance devices can be used to monitor the tank enclosure and a well-lit area can provide adequate surveillance.

6.3.4.6 Structural Engineering

Buildings should follow standard physical, mechanical, electrical and emergency requirements of other buildings, and agencies should consider designing them to maintain their structural integrity in fuel fires as described in Section 6.2.3. Facilities can also be locked when not in use.

6.3.4.7 Facility Services

Appropriate equipment must be on-site to handle fuel fires and any other hazardous materials stored on-site. Agencies should consider having backup systems in place to provide continuous power and communications in the event of an attack.

Table 6-5. Security-Oriented Design Strategies for Maintenance and Storage Facilities

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site layout		
Securable perimeter	Deter	X
Structures and vehicle-storage areas set back from roads and public parking areas	Deter/Minimize	
Physical barriers such as bollards, fencing, and grade changes to enforce setbacks and secure perimeter	Deter	X
Minimum number of access points necessary	Deter/Detect	X
Staffed security checkpoints at site access points	Deter/Detect	X
Unobstructed sightlines throughout site	Detect/Deter	X
Fuel storage site isolated from rest of facility with appropriate standoff distance	Minimize	Maybe
Parking areas segregated from transit vehicles and fuel storage	Deter/Minimize	X
Interior Layout		
Building layout provides unobstructed sightlines, minimizing hidden areas and blind corners	Detect	
Access management and layout used to segregate facility uses with different time-of-day and security needs	Deter/Detect	
Architectural Features		
Rolling doors to restrict view or access into maintenance barns	Deter	X
Critical equipment secured with gates, locks, or other access control measures	Deter	X
Underground fuel tanks (instead of aboveground)	Deter	
Fire-retardant construction materials	Minimize	
Structural Engineering		
Multi-hull fuel storage containers with secure openings	Deter	
Resistance to progressive collapse	Minimize	
Systems and services		
Remote surveillance and alarm systems	Detect	X
Sufficient lighting for nighttime surveillance	Detect	X
Backup emergency lighting	Minimize	
Fire detection and suppression system	Minimize	

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances

6.3.5 Elevated Structures

Bridges and other elevated structures provide a throughway for transit vehicles and their passengers over barriers such as waterways and sites that might otherwise obstruct the right-of-way. A bridge might serve multiple types of transit vehicles, and may also incorporate non-transit utility conduits. Example facility types include an elevated railway or a bus overpass.

Elevated structures provide valuable connections, linking key pieces of infrastructure that enable the movement of people and goods. However, as connectors rather than hubs, these structures do not necessarily host large numbers of people at one time.

Security challenges lie primarily in protecting the integrity of the structure, preserving its usability, and ensuring the safety of its users. Loss of elevated track or bridges can be a major obstacle to continued service, especially for rail-based systems that may be impossible to reroute, and for bridges spanning bodies of water. Rebuilding a damaged elevated structure takes considerable time and expense.

Elevated structures might span unusual natural features or navigate dense development.

This section focuses only on the elevated structure itself, and is limited to transit-only infrastructure. Multi-modal bridges and overpasses that serve the public right-of-way are beyond the scope of this report.

Rights-of-Way overview: refer to Section 6.3.7

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering

- Facility services
- Systems and services

6.3.5.1 Potential Threats

Bridges and other elevated structures can impose a major disruption of service because of their role as unique connections within a transit system. Attacks will most likely be designed to cause structural damage that destroys them or renders them unusable, possibly while a transit vehicle is on the structure. Agencies should consider focusing security strategies on protecting components that are critical for structural integrity.

Explosives/Fire

An explosive blast may disrupt services, hurt people, and damage or destroy an elevated structure. Explosives can be delivered to a bridge by several means: a car, truck, or other vehicle driven over, under, or near the elevated structure; a boat or barge positioned under or near the structure; or carried onto the bridge by hand, or positioned by hand on the structure itself. The greater the opportunity to position a large amount of explosives near important structural members of the bridge, the more extensive the damage that can result. Resulting fires may cause damage or collapse to an elevated structure or to nearby assets such as any vehicles on the deck. It may also imperil any passengers or personnel using the elevated structure at the time.

Ramming

A collision of sufficient magnitude may impose a shock to the structure comparable to that of an explosive event. Any vehicle such as a boat, car, truck, bus, or airplane with the opportunity to approach important structural components at great speed may endanger the facility.

6.3.5.2 Site Analysis

The most important consideration for the location of elevated structures is an evaluation of adjoining land uses as points of access to structural elements of the bridge, particularly load-bearing columns or the deck itself. For elevated structures that do not inherently straddle a public roadway, agencies may consider avoiding placing the structure directly above a public roadway, parking area, or other land uses that cannot be secured by the transit agency. Given the amount of land required for elevated rights-of-way, it may be impossible to entirely prevent access to the bridge from nearby uses. In these cases, the agency should consider focusing on isolating crucial elements of the structure (such as foundations), and situating these vulnerable areas at a safe distance from uses that the agency cannot control. For existing structures, the agency may consider eliminating nearby uses that are incompatible, such as eliminating public parking from under the structure.

Planners should consider providing clear areas with adequate lighting around secured areas and avoid providing places that might conceal someone attempting to access or tamper with the facility.

They can also identify unusual topography that could provide a niche or concealed approach, as well as dense foliage or other landscaping that obstructs sightlines.

6.3.5.3 Access Management

The following sub-sections present an overview of access management at elevated structures for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management.*

Perimeter Security

Although the footprint of an elevated structure may overlap roadways, waterways and buildings, the structures themselves do not require frequent access, except by transit vehicles. Perimeter security might focus on reducing the risk of terrorists gaining access to the deck and the structural support columns. The ability to fully protect the structure will depend on the need for movement on adjacent public ways. One aspect of perimeter security that may be difficult to control, especially for bridges spanning water, is the risk of ramming by an aircraft, since there is likely to be minimal surrounding infrastructure that could act as a buffer.

A vehicle could gain close proximity to this column or could ram it at high speed. However, the design may help inhibit an individual from attempting to climb the structure.

Vehicle Access

Agencies should consider designing the site to prevent unauthorized vehicles from accessing the deck of the structure, gaining proximity, and being able to ram structural columns.

If possible, designers may attempt to seal the entire area around the structure from public access. However, for elevated structures that span areas with public access, such as roadways, parking lots, non-transit buildings, and waterways, designers should consider enforcing buffer zones around key structural elements using physical barriers, such as bollards, fenders, pile piers, abutments, fencing, landscaping, and deep shoulder widths. In addition, slowing the permissible speed of passing vehicles using speed limits and curved routes may help diminish the risk of damage by ramming. Appropriate controls can be implemented to keep unauthorized vehicles from accessing the structure's deck. Fencing and bollards may be used where they do not impede transit vehicles' access while monitoring systems should be use in locations that cannot be blocked off.

Perimeter Protection and Barriers overview: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Human Access

Since individuals on foot may also pose a threat by positioning explosives directly on the structure, agencies should consider a design that denies unauthorized pedestrian access onto or beneath the structure using physical barriers, monitoring, intrusion alarms, and surveillance.

If an essential pedestrian throughway is necessary in the vicinity of the structure, the focus can be on denying access to critical structural components. Buffer measures designed for vehicles can be difficult for people to climb. They can be secured with features such as signage, fencing, barbed wire, and intrusion alarms. Agencies should consider not including accessible ladders or other features that facilitate climbing the base of the structure and should lock and secure any access points intended for maintenance personnel.

6.3.5.4 Emergency Response and Egress

Placement and types of any physical barriers designed to keep people at a distance from the structure should be chosen so that they do not compromise needs for emergency egress from the structure and access to the site by emergency responders. Agencies should consider including space for maintenance and emergency evacuation that does not compromise the ability to keep human carriers (on foot) from accessing the structure.

6.3.5.5 Protecting Critical Assets

Elevated structures are themselves critical infrastructure links. Maintaining structural integrity is a primary concern. Designers might focus on hardening the structural engineering of the asset.

Though this may be a convenient location for bicycle parking, agencies should try to locate bicycle lockers away from critical structures and dense areas, or designed so that the interiors are visible. While bicycle racks are less problematic, bicycle lockers may provide hiding spaces for bombs, weapons, etc. unless constructed of transparent or translucent materials. However, this goal should be balanced with concerns for safety of cyclists and the overall number and type of parking locations provided on-site.

6.3.5.6 Structural Engineering

Since it can be difficult to prevent access to the load-bearing columns of a bridge or elevated track, designers might consider engineering the structure to withstand additional forces. Load-bearing columns can be reinforced and hardened with appropriate construction techniques to withstand attacks. Redundancy can help minimize failure and prevent progressive collapse. Refer to Section 6.2.3.1.

6.3.5.7 Systems and Services

Elevated structures have minimal building systems although conduits for transit and other services may share the right-of-way. Agencies should consider locating transit utilities in such a way as to allow adequate maintenance and provide as much protection from impacts and tampering as possible. Other utilities such as water and gas pipelines that are co-located with elevated structures can be placed to minimize interruptions and damage to the transit system if they are compromised.

Table 6-6. Security-Oriented Design Strategies for Elevated Structures

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site layout		
Restricted access to land below structure, where possible	Deter/Minimize	Maybe
Structure setback from roads, parking areas, and other buildings, if possible	Deter	
Physical barriers such as fences, bollards, and fenders enforce setbacks and prevent ramming	Deter/Minimize	X
Adjacent roadways designed to inhibit high-velocity ramming of columns	Minimize	
Clear sightlines under and around structure	Detect	X
Interior Layout		
Emergency and maintenance access points limited	Deter	
Protected locations provided for limited-mobility occupants to wait for emergency personnel	Minimize	
Architectural features		
Emergency and maintenance access points secured with gates, locks, or other access control measures	Deter	X
“No Trespassing” signage	Deter	X
Columns made difficult to climb (by choice of materials or dimensions, or by barriers such as fences)	Deter	X
Fire retardant construction materials	Minimize	
Structural engineering		
Columns and piers able to withstand the impact of ramming by a truck, boat, or other vehicle	Minimize	
Resistance to progressive collapse	Minimize	
Systems and Services		
Motion detectors or intrusion alarms at vehicle entrances and other restricted-access areas around the structure	Detect	X
Electrical conduits and utilities built into structure to reduce exposure to vandals and fire	Deter	

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances

6.3.6 Tunnels

Transit vehicles use rail and bus tunnels to move passengers from station to station underground or underwater. This section addresses design issues relating to the tunnel structure itself and assumes that private vehicles do not share the tunnel with transit vehicles. For information on transit stations, refer to Section 6.3.1 and for rights-of-way, refer to Section 6.3.7.

Tunnels are long underground or underwater structures that typically have few access points. Although public access to tunnels should be prevented, tunnels cannot be altogether closed systems, as authorized transit vehicles need regular access and ventilation shafts must be open to fresh air. Tunnel design must also accommodate maintenance and emergency personnel access. Designing a tunnel to minimize access by unauthorized persons is the best way to keep tunnels safe from many potential terror threats.

Tunnel access points may include:

- Portals, where transit vehicles enter and exit the tunnel, usually at the point where the right-of-way submerges below grade.
- Station platforms, where passengers in an underground station board a transit vehicle.
- Maintenance entrances, which may be separate access points or adjoined to a station platform or portal.
- Ventilation openings that connect tunnels to the surface for air exchange via a network of ducts.
- Emergency evacuation routes and access points for emergency responders.

Fencing and a grade change help segregate this portal from nearby public areas.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering

- Facility services
- Systems and services

6.3.6.1 Potential Threats

Because tunnels are enclosed spaces that have few access points and depend on ventilation systems, they are particularly vulnerable to attacks on their ventilation systems, and to attacks that might trap people in the tunnel while exposed to fire, smoke, chemicals, flooding, or air deprivation.

Explosives/Fire

Depending on the magnitude of the blast and materials surrounding the tunnel, consequences of a blast will vary. Tunnels in bedrock have additional support provided by the surrounding rock, while those built in soils or water bear the load of the surrounding material and are likely to have more catastrophic structural failures.

Fires resulting from explosions pose a particular threat in tunnels because there are few exits, and smoke and toxic fumes can build up quickly in the enclosed spaces. Smoke has a tendency to rise, making emergency exits to the surface excellent conduits for smoke to escape from tunnels, and making exit use potentially difficult.

Weapons of Mass Destruction

WMD such as chemical, biological, or radiological agents that are released into a transit tunnel could make them permanently unusable if the materials are able to be absorbed into the tunnel structure or façade. Tunnels can be good conduits for WMD because they can be delivered through the ventilation system and spread throughout the system and into stations. Depending on the vehicle design, passengers within transit vehicles will have different levels of exposure to these agents.

6.3.6.2 Site Analysis

In choosing where to situate tunnels, agencies should consider avoiding certain geographic peculiarities and land uses, such as sites adjacent to gas or chemical tanks or to major public works pipes. While it may seem advantageous to allow external utilities to use tunnel facilities, their need for access and consequences of their systems' failures need to be considered when making agreements.

From a security standpoint, carefully choosing the location of tunnel access points may be even more important than the location of the tunnel itself. Access- point locations can be chosen based on how easily they may be secured and made inconspicuous. Planners should consider how nearby roads, topography, and land uses impact these factors.

6.3.6.3 Access Management

The following sub-sections present an overview of access management in tunnels for perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in *Chapter 5: Access Management.*

Perimeter Security

The "perimeter" of a tunnel may be thought of as the perimeter areas around each of its access points (such as portals and vents). Because tunnels must not be accessible to the public, this perimeter can be strictly protected without compromising the tunnel's intended use.

The types of tunnel access (when the perimeter must be crossed) include: use of the tunnel by transit vehicles, occasional access to the tunnel by maintenance personnel, and emergency access and egress routes. Planners should consider how to selectively allow appropriate access and prevent inappropriate access at these points.

Perimeter Protection and Barriers overview: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access

Site layout can be used to minimize how close a vehicle can be near a tunnel (above or below ground), its portal, or its affiliated network of air ducts. Wherever possible, agencies should consider positioning tunnel portals at a distance from public roadways, and oriented so that driving an unauthorized vehicle into the portal is difficult or impossible. In rail tunnels, the track and third rail may make the tunnel difficult to access for other vehicles. Designers can consider other ways to manipulate the size and design of openings to limit access by non-transit vehicles, or at least prevent the largest trucks from entering. In addition, ditches, bollards, and road-spikes can be used as additional protection against unauthorized vehicles. Air vents can be housed in secure structures and concealed. Although vents can be positioned off roadways and elevated to prevent accidental spillage from the street into the vent, designers might position vents even farther from roadways and elevated a number of feet above grade, making intentional spillage more difficult to perform.

Human Access

Agencies should consider keeping at-grade tunnel access points (portals, maintenance entrances, vents, and emergency exits) as inconspicuous as possible, but oriented for easy surveillance. Clearing brush and other visual obstructions, as well as supplying adequate lighting, can provide more effective surveillance. A transit agency may encourage passive surveillance by notifying neighboring property owners or local authorities about what to do if they observe suspicious activity in the vicinity of the access point.

Grates, manholes, and other entrances can be secured with locks, electronic keys, or biometrics, and those used for air intake elevated to prevent materials from easily pouring in. Fencing and warning signs may also play a role in deterring individuals. Remote monitoring techniques such as intrusion alarms, chemical sensors, and CCTV can be used to monitor access points.

Station platforms require particular attention as access points into tunnels. Tunnel walkways are of particular concern because they are often built adjacent to the platform. The tunnel-platform interface can be designed to discourage unauthorized passage. Uneven surfaces, electrified rails, and oncoming vehicles can act as deterrents for access via the road/rail bed. Vertical grade separation between the platform and the road/rail bed does not provide an actual barrier, but does create a psychological barrier that may make bystanders more responsive to a breach.

Physical barriers separating the platform from the tunnel can be used to prevent passengers from accessing the tunnel. Platform screen doors, which open on the platform simultaneously with those of the train car, can allow passengers to board and alight without providing continual access to the track and also increase passenger safety. Station walls can be extended to be flush with the platform edge. Locked doors or barrier gates can be used to provide access from the station to the walkway as long as they do not interfere with emergency evacuation routes. Personnel, remote surveillance, and intrusion alarms can also be used to observe activity at platform periphery/tunnel entrances to detect unauthorized passage or suspicious behavior. Appropriate lighting and clear sightlines to the platform edges may also help deter and expose attackers.

Agencies should provide passengers with general instructions on what to do if they see suspicious activity, such as a person walking into the tunnel. Providing on-platform emergency phones may result in faster response times than reported.

6.3.6.4 Emergency Response and Egress

Emergency exits must be provided to allow safe egress in case of an emergency. NFPA 130, 3-2.4 prescribes emergency exits every 1,250 feet.[38] Planners should also consider providing passages for emergency responders and invite them to participate in the tunnel design and emergency planning process. Since these passageways may double as access points for maintenance personnel, they must be secured at the street level to ensure only authorized entry, while allowing easy opening from the inside for emergency egress. Agencies should consider clearly labeling emergency passageways and not rely on power or other systems to display the labels, since these may fail in an emergency or should be served by systems with redundancy.

6.3.6.5 Protecting Critical Assets

Tunnels may contain assets such as power and communications lines that may be critical for operations and for emergency systems, and may also be dangerous if tampered with. Agencies

[38] See Appendix F for more information on codes and standards.

should consider embedding power and communications wiring into the tunnel, not attached to the surface, to help protect these systems from damage in case of an incident.

In addition, the tunnel itself may be considered a critical asset for the operation of the transit agency and for the safety of transit users. Planners may treat tunnel access points as critical and choose to implement heightened access control measures.

6.3.6.6 Structural Engineering

The primary structural purpose of a tunnel is to support the tunnel against pressures from the surrounding soil, water and other loads. Cut and cover and boring are the two main techniques used to build tunnels.

Bored tunnels are generally deeper underground and are not usually threatened by explosions at ground level. Cut and cover tunnels just below grade, may need to consider the effect of a major explosion at-grade. If the tunnel is designed to prevent unauthorized vehicle entrance through the portals, explosives are most likely to be brought in by hand.

6.3.6.7 Systems and Services

Heating, Ventilation, and Air Conditioning

Ventilation is crucial to people working and traveling through tunnels in transit vehicles. Ventilation in underground, electrified rail systems usually relies on the natural piston action of vehicles to draw air in and push air out of tunnels. Fans are required for emergency situations, such as fires and stalled trains. High-speed transit systems require air relief vents to minimize the blast effects of air ahead of the train entering a station. Ventilation shafts can also provide blast over-pressure relief in the case of an explosion.

While fans and vents play an important role in minimizing harm from explosions and fires, they can have unintentional consequences in a situation involving a WMD or other contaminant. The ventilation system should not be used to remove harmful substances from a station or tunnel; this would only spread the contaminants more. Instead, the ventilation system can be used to help limit the contamination by shutting down and sealing off openings. Other isolation techniques include inflatable dams in tunnels and reducing train speeds to 5 mph or less. Agencies should consider making available additional manual controls for the ventilation system at the tunnel opening for use by emergency responders.

NFPA 130, Chapter 4 mandates the performance standards for transit tunnel ventilation. FTA has developed the *Subway Environmental Simulation* software to accompany the *Subway Environmental Design Handbook* to provide guidance in determining ventilation needs.[39]

[39] *Subway Environmental Design Handbook*. FTA. [need complete reference]

Water Management

For tunnels located below the water table, portals and cracks produced by an attack may allow minor leaks through percolation or major leaks that lead to flooding. Water used in fire suppression may also flood a tunnel. Planners may consider installing water-monitoring devices, floodgates, water pumps, and drainage systems. These water management devices may be alarmed and connected to Central Control.

Fire Protection

Tunnels can be equipped with fire alarm and suppression systems connected to a central control panel. Planners may consider installing dry fire standpipes systems, and deluge systems that release large volumes of water at track level to quench fires beneath rail vehicles. This information is not exhaustive, however, and should only supplement existing guidelines and regulations, such as those contained in NFPA 130.

Lighting Systems

Since tunnels are naturally dark, tunnel lighting is important both for the operation of vehicles as well as the detection of unusual activity in the tunnel. Emergency lighting may be essential in a tunnel emergency when people may need to move around in unfamiliar and potentially hazardous conditions. Planners should consider supplying emergency exits and pathways with independent and/or redundant power sources.

Security Systems

Security systems such as door alarms, motion detectors, and surveillance cameras may be used to protect tunnels and their remote access points. Because many parts of a tunnel network are dispersed and remote, tunnel security systems may be particularly apt to link to Central Control.

Table 6-7. Security-Oriented Design Strategies for Tunnels

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
Access points isolated from public roadways and parking areas	Deter	
Physical barriers such as ditches, bollards, road spikes, and fencing around portals and other access points	Deter	X
Unobstructed sightlines around access points	Deter/Detect	X
Vent ducts situated in self-contained secure buildings, locked, elevated, and hidden	Deter	
Interior Layout		
Tunnel-level enclosed areas for rescue assistance (AORA) with pressurized fresh air	Minimize	

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
No unnecessary niches in the tunnel that may conceal people or explosives	Deter/Detect	X
Physical barriers that shield tunnel walkway from platform or portal access	Deter	X
Emergency exit doors that lock from the outside but allow unimpeded egress during emergencies	Deter/Minimize	X
ADA-compliant emergency evacuation routes/safe areas	Minimize	X
Architectural Features		
Portal entrance that limits permissible vehicle dimensions, if possible	Deter	
Screen doors that seal platform from tunnel, only opening during vehicle boarding	Deter	X
Solid access doors to ventilation shafts whenever grating is unnecessary	Deter	X
"No Trespassing" signage	Deter	X
Ample freeboard that helps protect tunnel from flooding	Minimize	
Materials that do not absorb toxic substances when exposed	Minimize	Maybe
Fire-retardant construction materials	Minimize	
Structural Engineering		
Resistance to progressive collapse	Minimize	
Hardened emergency access routes	Minimize	
Systems and Services		
Electrical conduits built into structure to reduce exposure to vandals and fire	Deter	
Remote surveillance of portal entrances and other access points	Detect	X
Automated central control of ventilation system, with manual override available to emergency professionals	Minimize	X
Blast- and fire-resistant, rapid-startup ventilation system	Minimize	X
Backup communications system	Minimize	X
Backup emergency lighting	Minimize	X
Water detection system and pumps capable of removing accumulating water	Detect/Minimize	X
Fire detection and suppression system	Minimize	X
Actuated vent louvers that open only when fans are running	Minimize	X
Inflatable dam to seal tunnel, to prevent spread of contaminants	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances

6.3.7 Right-of-Way, Track, and Signals

A right-of-way (ROW) is the continuous stretch of land dedicated to transit vehicle movement. Although some bus systems (notably Bus Rapid Transit systems) use exclusive rights-of-way, this type of infrastructure is typically relevant only to rail vehicles. The focus of this subsection is rail alignments and equipment, even though many of the principles are transferable to bus rights-of-way. The transit agency may own, lease, or have a use easement for the land comprising the right-of-way, and may share use of the right-of-way with other agencies or companies. Elevated structures and tunnels, while typically considered elements of a right-of-way, due to their particular security concerns are covered separately in Sections **6.3.5 (Elevated Structures)** and **6.3.6 (Tunnels)**.)

Switch and signal equipment provide essential functions for a rail line.

Assets within the right-of-way include track, signaling equipment, power conductors and ancillary assets. Track hardware supports and guides vehicles, and consists of rails, switches (used to guide vehicles at junction points), and ties, all resting on the "ballast," the base material (usually crushed stone) that holds the ties in place.

Signaling equipment is a system of visual indicators along the right-of-way informing vehicle operators of transit system conditions and when to stop, slow down, or proceed at full speed. Historically, signals regulate the spacing of trains on a section of track (a "block") to prevent collision between trains, advise of switch conditions, and coordinate railroad-crossing controls (automatically or manually) to avoid collisions of trains with roadway vehicles and pedestrians. Newer technology now enables some of these functions to be incorporated into alternate communication methods, including wireless systems and data transmission through third rails.

Power is supplied to vehicles via either an electrified third rail or through an overhead catenary wire, depending on vehicle type and right-of-way location. Auxiliary equipment along rights-of-way includes such items as fencing, signage, and barriers.

These assets typically do not receive as much public attention as other infrastructure assets such as stations or vehicles, but they are essential for the operation of the transit system. This section focuses on the vehicle support, collision avoidance and switching application of right-of-way assets, and how best to maintain their operation during attacks.

Subsections describe:

- Potential threats

- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.7.1 Potential Threats

Damage or destruction of the track, signaling system, or power conductor along a right-of-way can have significant consequences. These could cause a derailment involving a high number of casualties, damage to vehicles and equipment, or a prolonged disruption of service.

Right-of-way assets also have strategic value to terrorists. With the increased awareness of vulnerability to terrorist attacks, communities are creating Emergency Response Plans, which often rely on transit systems as a means of carrying out mass evacuation and/or delivery of law enforcement and medical services to the affected area. Disabling the transit system by damaging the right-of-way prevents its use as part of such a plan.

Rights-of-way are vulnerable to attacks because of their extensive size and insecure nature. They may pass through locations that are remote, infrequently observed and difficult to secure.

Explosives

The detonation of an explosive device is an effective method of attack within a right-of-way. The device could be set to explode anywhere along the alignment, or when a train passes over the track, inflicting mass casualties and temporarily closing down the line. Explosions can also destroy switches and signaling equipment with the same interruptions of service. The nature of transit rail networks would make it difficult to reroute service around the damage, further disrupting the transit service.

Tampering/Disabling

Sabotage carried out against the track, especially signaling equipment, can cause collisions and derailment. Perpetrators with technical knowledge of track and signal operations could tamper with the signaling and switching equipment in a manner that incapacitates the line, or causes casualties.

Cyber Attacks

As signaling and communications systems merge, they become more centrally controlled by computers. This makes them vulnerable to cyber attacks by computer hackers. Such an attack, and the measures to defend against it, is beyond the scope of this report.

6.3.7.2 Site Analysis

Rights-of-way may pass through areas that make them difficult or even impossible to secure. In addition, their contiguous layouts mean that any access point compromises access management for the entire right-of-way.

Given their size, rights-of-way typically have a variety of surroundings. A single alignment may pass through dense urban development, natural environments, and a range of land uses. The right-of-way may have a substantial buffer space between it and adjacent property (with or without a fence or wall separating the two), or vehicles may travel within a few feet of adjacent, non-transit buildings. The type of border separating a right-of-way from adjacent property affects its accessibility: for a below-grade, open-cut right-of-way, a vertical 10-foot retaining wall is a much more effective barrier than a gradual slope covering the same grade change.

Likely entrance points to a right-of-way can be identified, and their locations factored into the placement of access management measures, critical system hardware, and remote surveillance equipment. Abutting structures, adjacent public space, and at-grade intersections all constitute potential entry points for attackers. Agencies should consider locating critical equipment, like signals and electronic relays, away from such sites, preferably at points along the right-of-way that are visible from farther along the alignment or from adjoining facilities; this makes them more difficult for terrorists to access, while increasing the odds of inappropriate activity being seen and reported.

6.3.7.3 Access Management

The following sub-sections present an overview of access management for right of way, track, and signals, relating to perimeter security, vehicle access, and human access. Cross-references are provided to more specific details in **Chapter 5: Access Management**.

Perimeter Security

It is effectively impossible to establish an effective perimeter around an entire right-of-way; it passes through too many types of areas and has insufficient staff presence to secure it.

In many places, the perimeter is simply a fence, wall, or building. Fences, walls, and other barriers can be designed to prevent people from climbing over them (or, in the case of chain link fences, cutting through them), and be able to resist vehicle impacts where appropriate.

Typically a fence or barrier is placed on or close to the legal boundary of the right-of-way. Rights-of-way by their nature present a clear unobstructed space. However, a clear area along the outside of the fence line should be established when practical, by installing a double row barrier (an inner row of fencing enclosing the assets and an outer row along the property line) or by obtaining clearance easements along the right-of-way. Where possible, remote surveillance and/or intrusion detection systems can be installed to enable the transit agency to monitor the right-of-way.

In some areas, non-transit buildings may form the boundary of the right-of-way. This situation is common in older urban areas where buildings were constructed on lots with a "zero setback" that allows buildings to stand on the property line. Transit agencies typically do not have control over access to these buildings, and tenants have an expectation of privacy. In these situations, right-of-way equipment and passing trains are vulnerable to threats from people with easy access to the right-of-way. Security options available to a transit agency include taking ownership of the building, or leasing space adjacent to the track. Increased surveillance of these areas is another option. These situations should be handled by the transit agency on a case-by-case basis.

Perimeter Protection and Barriers overview: refer to Section 5.2.2

Vehicle Barriers overview: refer to Section 5.3.5

Vehicle Access

Rights-of-way should allow transit vehicles to move easily, while discouraging access by unauthorized vehicles. Wherever possible, agencies should consider not locating rights-of-way adjacent to public roadways, especially not without barriers separating the two. Grade changes, fences and walls, and dense vegetation are all options for effective barriers. At-grade crossings with roads are a common vulnerability for rights-of-way. These can be monitored with surveillance equipment where possible to ensure rapid detection of trespassing. Rights-of-way may also have service roads and gates to provide access for transit agency maintenance vehicles. These points can be controlled with locked gates and other barriers where appropriate.

Human Access

As discussed in the subsections on **Site Analysis** and **Perimeter Security**, it is effectively impossible to control all human access to a right-of-way. For this reason, it is probably more cost efficient to focus on intruder detection methods that will initiate a security response, rather than on efforts at total access management.

A right-of-way protected with fencing and a grade change (below) is more difficult to access (than above).

6.3.7.4 Emergency Response

Some rights-of-way are wide enough to provide a drivable or navigable area along side the track. Others sections through remote locations or those flanked by building are less accessible. In this case the only access is along the right-of-way itself. Agencies should consider developing emergency evacuation and access routes for all segments within the rights-of-way as part of an emergency response plan. They should also consider factoring the presence of a live "third rail" into any plans involving the evacuation of passengers by responding emergency personnel.

6.3.7.5 Protecting Critical Assets

Since most of a right-of-way has no ongoing staff presence, security measures must rely on remote surveillance and tamper detection to safeguard on-site equipment in addition to the access management measures already mentioned. Asset protection can include the following:

- Tamper-resistant housings and locks
- Remote tamper detection
- Remote Intrusion detection
- Audible/lighted local alarm systems
- Remote surveillance
- Redundant systems
- Regular inspections of assets

If assets are successfully destroyed or compromised, measures should be in place to detect and respond to the fault and reroute services as appropriate.

Tracks and Switches

Diligent remote surveillance and tamper detection are the best protection against the intentional destruction of tracks and switches. Derailments can be caused by explosives and by tampering with the installation of track rails and switches, such as loosening the track connectors (spikes and clips) along a continuous length of track. The first train over the damaged or altered track may not be derailed, but as subsequent trains pass by, the misalignment of the rail worsens. The rails in switches have similar vulnerabilities; switches are also vulnerable through their mechanical components and the integrated signaling hardware.

Transit agencies can use advanced telemetry systems that remotely monitor the conditions of track and the operations and setting of switches, and report this information to an operations center. These systems can be programmed to alert transit staff if tampering or incorrect settings are detected. Frequent human inspection of track, switches and associated equipment is an alternative.

Signaling Equipment

Signaling equipment provides collision avoidance by maintaining safe spacing between trains along the rail line. Rail lines are divided into electrically separated linear segments called "blocks." Each block is part of a circuit that controls a signal placed at the entrance to the block or blocks behind a train. These signals tell operators of other trains approaching the block either to stop or to proceed at a predetermined slower speed. As a train enters a block, the train becomes part of the circuit, causing the signal at the block entrance to indicate that a train is in the block.

Table 6-8. Security-Oriented Design Strategies for Rights-of-way, Tracks, & Signals

Design Feature	Goal (Detect/ Deter/Minimize)	Able to Retrofit
Site Layout		
ROW set back from roads and parking areas	Deter/Detect	
Physical barriers such as bollards, fencing, and grade changes to enforce setbacks	Deter/Detect	X
Unobstructed sightlines along ROW	Deter/Detect	X
Appropriate treatment of likely entrance points to ROW	Detect/Deter	X
Interior Layout		
None		
Architectural Features		
Enclosed control signal boxes secured with locks or other access control measures	Deter	X
Tamper-resistant equipment	Deter	X
Structural Engineering		
None		
Systems and services		
Motion detectors or intrusion alarms on critical equipment	Detect	X
Redundant power/communication supply systems/routings	Minimize	X
Remote surveillance systems	Detect	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.

Tampering with these systems is remarkably simple. Shorting the signaling system could cause the signal for that block to show red. At a minimum this would be an inconvenience, but this would also leave the sitting train vulnerable to attack. A coordinated effort could also use shorting to stop several trains simultaneously; transit staff could interpret this as a serious malfunction of network or control center equipment, triggering a system-wide shutdown while the problem is diagnosed.

A more sophisticated and serious sabotage method is modifying the circuitry so a signal shows green to an approaching train, even when a preceding train is in the block. This has the potential for causing a collision between trains.

Tamper-resistant housings for signaling equipment and telemetric systems to remotely monitor the conditions of track and switch signals are the best defense against deliberate attack. Where possible, signaling equipment can be located in a high visibility area (near a well-traveled intersection or adjacent to a transit station, for example) to increase the likelihood that tampering attempts will be seen and reported.

6.3.8 Remote Equipment and Unmanned Structures

Unmanned and remote structures include all of the support structures owned, managed or maintained by a transit agency: electrical substations, communications relay towers, and the like. Though less visible, they are vital to the daily operation, maintenance and management of transit systems.

Remote or unmanned equipment plays a less visible, but critical, role in the transit. Ownership and responsibility for these structures vary among systems. They are not always owned and operated by the transit agency; a separate utility company or other organization may operate them instead. Since they are not high-profile sites and typically have no ongoing staff presence, their value as a terrorist target is exclusively a strategic one: the destruction of a substation or communications tower could prevent effective management of the system or disrupt transit operations. The isolated locations and open design of these facilities make them vulnerable to attack. The most effective strategies for mitigating attacks on these facilities are physical hardening and providing redundancies within the transit system's power or communications network, along with access management for particularly critical structures or those located in notably vulnerable locations.

Subsections describe:

- Potential threats
- Site analysis
- Access management
- Emergency response and egress
- Protecting critical assets
- Protecting vulnerable assets
- Structural engineering
- Facility services
- Systems and services

6.3.8.1 Potential Threats

The probable objective of any attack on a substation is to incapacitate it through damage or destruction, and prevent it from providing power to the transit system. The same can be said of communications towers and relays, which allow communication between operations control, emergency response personnel, and vehicle operators or field staff. This would cause a disruption in the control, coordination and/or operation of the transit system. The same result can be achieved by destroying the power lines or tampering with the networking cables leading to or from the facility. This is extremely difficult to prevent. Refer to Section 6.3.8.5 for more information.

Explosion/Fire

The detonation of an explosive device is a potential method of attack on an unmanned structure. It would not only incapacitate the facility, but would also create a noticeable event and possibly spread environmentally harmful, flammable on-site substances (coolant in transformers, etc). An attack of this kind would not require direct access to equipment controls or technical knowledge of operations.

Collision

Ramming with a vehicle could incapacitate a substation or tower by destroying key components such as the power poles serving the site. Communications arrays can be somewhat more fragile, and are more endangered by heavy objects that can be thrown or hurled at the structure, damaging its antennae or other critical components.

Tampering

A more sophisticated attack on an unmanned structure is sabotage. Terrorists with technical knowledge of facility operations could activate or modify components of the facility in a manner that not only incapacitates the equipment, but causes damage to other system components as well. This method requires direct access to on-site components.

6.3.8.2 Site Analysis

Most substation sites are small areas with no on-site personnel. Typically, the only equipment on-site are transformers and associated equipment; there may also be a small utility building. Since transit agencies generally obtain their power through the public grid system, agencies might have little or no control over the siting, design, and construction of these substations. When the agency does own the substation, they can use the principles of hindering accelerated approaches, access control, and remote surveillance as appropriate. Many of these same attributes apply to other remote or unmanned structures, including communications towers, etc.

Current practice and applicable codes require clearances around substation transformers and other structures, along with other requirements, based on fire protection concerns rather than blast-related

stand-off distances. These standards also dictate that access be limited to qualified personnel. See Appendix F1, "Codes, Standards, Regulations: Infrastructure", for more information on codes and standards.

Agencies should consider addressing security concerns relating to site layout for remote facilities and unmanned structures, and focus on preventing unauthorized access to the equipment, protecting the equipment from attack or tampering, and protecting the transmission lines to and from the transformer, tower or array.

6.3.8.3 Access Management

The following sub-sections present an overview of access management for remote equipment and unmanned structures, relating to perimeter security and human access. Cross-references are provided to more specific details in **Chapter 5: Access Management**.

Perimeter Security

Because substations and other remote structures should not be accessible to the public and because agency staff accesses them only periodically, the site's perimeter can be strictly secured. Since most of these facilities do not have an ongoing staff presence, perimeter security measures should be robust enough to prevent access attempts without direct human involvement. Most existing facilities, regardless of ownership, have security protection such as fences, walls, and other barriers to ensure safety of accidental or curious trespassers and to prevent vandalism. These measures may include alarms to local police and fire.

Agencies should consider designing perimeter security to prevent people from climbing over or cutting through existing barriers, and to establish a standoff distance sufficient to prevent an attacker from placing or throwing an explosive device next to key on-site equipment.

Perimeter Protection and Barriers overview: refer to Section **5.2.2**

Vehicle Barriers overview: refer to Section **5.3.5**

Vehicle Access

Bollards are used frequently to surround the limits of the structure or facility to protect the facility from "bumping" by vehicles. These are typically passive barriers, such as concrete-filled bollards, designed to stop accidental collisions. However, a determined terrorist with a large enough vehicle may be able to overcome these types of passive barriers. Agencies should consider using walls or more substantial barriers, especially if a high-speed approach is possible.

Human Access

Agencies should consider designing the site, equipment, and individual structures, if any, to discourage unauthorized access. The principal enhancements to existing perimeter security systems

include increased remote surveillance and intrusion detection. Planners can consider passive access control methods (no on-site personnel required) for remote or unmanned areas. Techniques such as cipher locks and biometrics can also be used.

Critical and Restricted Area Access overview: refer to Section 5.3.6

6.3.8.4 Emergency Response and Egress

Regardless of whether a remote structure is staffed, the site and all structures should have predetermined evacuation routes and procedures. The presence of high-voltage equipment and volatile substances pose serious threats to on-site staff and the surrounding area, and emergency routes and procedures should reflect their nature and locations. Agencies should consider incorporating rapid shutdown mechanisms incorporated into their equipment at high-risk facilities, to minimize the damage resulting from an attack.

6.3.8.5 Protecting Vulnerable Assets

Although there are certain pieces of equipment at a remote facility or unmanned structure that may be more critical to operations or more vulnerable to damage, agencies should consider treating the entire facility as a single asset. Since these facilities are often isolated and have little, if any, staff presence, it is extremely difficult to prevent attacks. For this reason, a security plan must focus on making the system more resilient to attacks. There are two protection strategies that agencies can consider: physical reinforcement and redundant systems.

Physical reinforcement focuses on strengthening the facility to resist attack. This includes many of the normal measures discussed throughout this document: access management, appropriate standoff distances, and reinforced structures that resist fire and explosion.

Redundant systems are a more effective strategy for minimizing the consequences of an attack on a substation or communications relay, in which redundant power-transmission or relay sources are established within the transit system, so that if a particular facility is incapacitated, an alternate means of power or communications delivery exists. This strategy increases the resiliency of the system as a whole. The same strategy applies to power lines; multiple possible routings decrease dependency on particular power lines and minimize the disruption of service that results from an attack. The power companies that operate the grid are generally responsible for and provide redundancy.

Table 6-9. Security-Oriented Design Strategies for Unmanned Structures

Design Feature	Goal	Able to Retrofit
Site Layout		
Structure set back from roads and parking areas	Deter	
Minimum number of entrances	Deter	X
Key equipment located toward center of site	Deter	
Entrance dimensions minimized	Deter	X
Interior Layout		
None		
Structural Engineering		
Reinforced structures	Deter/Minimize	X
Architectural Features		
Full enclosures (but must provide ventilation per local electrical / fire requirements)	Deter	X
Access doors secured with multiple locks or other access control measures	Deter	X
Systems and Services		
Emergency shutdown mechanism	Minimize	X
Remote surveillance and intrusion alarms	Detect	X
Redundant power supply systems and routings	Minimize	X

The design features are suggested approaches. Since every transit agency faces a unique set of threats and needs, it is up to each agency to determine which security strategies are appropriate for its particular circumstances.