SECTION 4

Design Considerations for Reducing Risk

4.1 General

Wastewater managers and designers have traditionally considered security to be an enhancement provided for a few facilities and limited to application of electronic access control systems and CCTV monitoring. Today, wastewater system managers, engineers, and architects must consider security as an integral design consideration for every building or site that may potentially be threatened by acts of violence, including vandalism, crime, sabotage, or terrorism. The objective of this section is to provide guidance that enables wastewater utility decisionmakers and designers to develop secure sites and facilities to protect people, information, property, and assets related to the mission of publicly owned treatment works (POTWs)—to provide quality services with effective collection and treatment of wastewater to protect public health and the environment.

4.1.1 Design Basis

The considerations presented in this section are applicable to designs of new wastewater infrastructure, upgrades to or expansions of existing infrastructure, and retrofitting of existing infrastructure for the purpose of increasing security and reducing risk.

Criteria for the design of security systems are based on identification of assets that may become potential targets, and the threat and vulnerability assessments related to those assets. The threat assessment determines which threats are credible and likely against a particular asset. The vulnerability assessment (VA) characterizes those assets that may be targeted, evaluates how they are currently protected and where they are vulnerable to attack, and considers the consequences of a successful attack.

Identification and characterization of assets are based on consideration of the mission and the functions that the assets are required to perform. For example, an administration building may house a number of different types of assets: people, records, money, tools, keys, computers, controls, and security or process monitoring systems. Once the assets have been identified, they can be characterized (i.e., their characteristics described with respect to their attractiveness to various types of crime or violent attacks). Each of the example assets may attract various types of attack—records, money, tools, and computers may be most attractive to criminals interested in theft; security and utility monitoring systems may be more attractive to saboteurs and terrorists interested in accomplishing significant compromise of the system.

Threats are described based on type of adversary and severity of attack; anticipated tactics (such as a theft or moving vehicle bomb); weapons, tools, explosives, and/or contaminant agents; and likelihood of attack. Protective measures that protect against higher severity-level threats may (or may not) provide sufficient protection against lower-level threats, but all types of threats must be included in the threat assessment because the protective measures may differ for each type of threat

regardless of severity level. The summation of this information is referred to as the Design Basis Threat (DBT). The DBT provides the information needed to design a physical protective system to delay and detect an attack.

This section addresses the delay and denial protective measures that should be coupled with detection and assessment technology described in Section 6. Attacks targeting command, communications, and control systems, referred to as cyber attacks, are addressed in the Cyber Security in Section 5, although the physical attacks generated by those adversaries to gain access to the systems should be protected using measures described in this section.

The VA considers the routes and means used to attack and to protect the asset from attack. A VA may consider features and effectiveness of a existing facilities or, if used as a design tool for new facilities, how access may be gained to an asset and how the asset may be compromised or destroyed. The consequences of a successful crime or attack must also be considered to provide an opportunity to weigh the cost and impact of implementing appropriate physical protective measures against the potential consequences of an attack. For example, if vandals using spray paint is the DBT, it may be costly to replace existing building finishes with materials that resist paint adhesion; if the likelihood of the attack is low and consequences minimal (i.e., no loss of life, mission disruption, or depletion of functionality anticipated after spray painting the building walls), the utility may determine that the consequences do not justify the investment to address that DBT. In another example, a successful theft may be disrupted after removal of the asset but before the thief successfully escapes the site. This allows the delay factor to include "getaway" time as long as the asset is still intact when the adversary is apprehended.

4.1.2 Utility Size and Resources

The basis for security system design is not a function of a utility's size. Rather, the determining factors as described above are the identification of assets that may be targets of malevolent attacks, the characterization of threats, and the assessment of the assets' vulnerabilities. Many small utilities, and some larger utilities, may not have the necessary resources to put into place many of the security systems that are presented in this section. Consequently, it is imperative that utilities go beyond the vulnerability assessment to evaluate associated risks and the costs necessary to reduce those risks before embarking on a program of physical protection system design and implementation. As discussed in earlier sections of this document, most utilities will achieve a significant reduction in risk at a relatively low cost through adoption and enforcement of security-related policies and operational procedures. Beyond that, the determination of what capital investments to make should be based upon the utility's analysis of risk reduction per unit cost.

4.2 Physical Protection System Concepts

In general, physical protection systems are focused upon reducing risks associated with outsider threats. Physical protection systems can be effective for insider threats only where security layers are employed to limit an insider's access to specific assets within a facility (see Section 4.2.2).

An important consideration when designing physical protection systems: Physical protection systems should NOT interfere with life safety, occupational safety, and fire protection provisions. Security systems must be balanced with and complementary to other design criteria and requirements.

4.2.1 Required Elements of a Physical Protection System

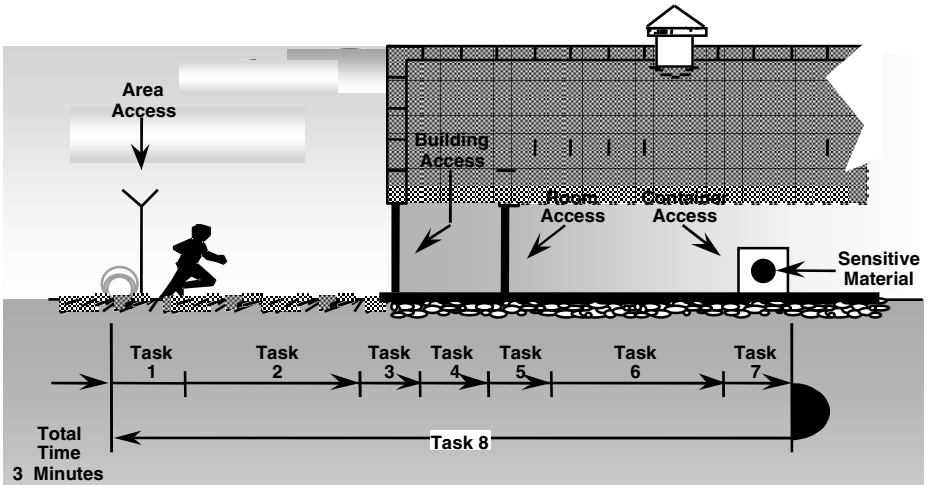
There are several elements required for an effective physical protection system design: detection, delay, and defense or response. Once a potential attack is detected, the physical protection system must delay an adversary from accomplishing his or her objectives until a response force can successfully prevent successful attack. Each of these elements is quantifiable in terms of timing. That is, detection is the point at which the clock starts with respect to an attack event; delay is the amount of time required to allow a response force to stop the attack. For example, local authorities may indicate to utilities that a team can be on site and disrupt an adversary within 15 minutes. That time dictates that the physical protective measures established must delay the adversary so that the response force may arrive in time. In this example, the delay times must add up to slightly more than 15 minutes to be effective.

Detection refers to the point at which a potential attack is discovered, assessed, and determined to be an attack in progress rather than a false alarm. Once an adversary has been detected, the delay timeline starts. To maximize delay, detection should be as far as possible from the targeted asset, with delay elements placed between the point of detection and the asset. Locating delay systems as near as possible to targeted assets also helps to reduce cost by minimizing the size of the security envelope surrounding the assets. The delay afforded by various building or perimeter protection systems can be (and for many systems, has been) measured (see Exhibit 4-1).

Deterrence is often a consideration in design as well, although deterrence cannot be quantified (if there is no attack, it is unknown whether these measures successfully prevented it). Therefore, deterrence typically is not considered part of an effective physical protection system. However, because deterrent measures can effectively prevent or reduce the opportunity or likelihood of attack and can often be cost-effectively integrated into a facility design through prudent application of appropriate strategies, deterrence measures are discussed in this section as well.

4.2.2 Protection in Depth

“Protection in depth” is a term used in the security industry referring to the recommended strategy of providing multiple layers of protective measures requiring an adversary to defeat a system, travel to the next protective layer and defeat that system, and so forth until reaching the target. An example of protection in depth is the application of layers of protective measures at the site boundary (perimeter fencing system), at the building envelope (exterior walls, doors, windows, grilles, and roof system), and at the target enclosure (the room in which the targeted asset is housed).



Time Estimate

Task	Mean Time (minutes)	Cumulative Time (minutes)	Task Description
1	0.1		Climb over fence
2	0.3	0.4	Run 76 m
3	0.8	1.2	Force door
4	0.4	1.6	Walk 45 m
5	0.2	1.8	Cut lock
6	0.1	1.9	Walk to container
7	0.2	2.1	Open container and gather material
8	0.9	3.0	Escape
	3.0		Total (approx. 3 minutes)

EXHIBIT 4-1
Concept of Delay Calculation

For example, as depicted in Exhibit 4-2, an effective security layering approach requires that an adversary penetrate multiple separate barriers to gain entry to a critical asset at a typical wastewater facility. Protection in depth can help to ensure that the security system remains effective in the event of a failure or an adversary bypassing a single layer of security.

Note that for each layer, the layer is only as effective as the weakest element within that layer. For example, investing in blast resistant doors to resist terrorist threats is unwarranted if the surrounding wall construction is inadequate to withstand the same loads. For specific DBTs, complete and consistent layers of protection in depth should be provided.

4.3 Physical Protection Systems Design

The approaches described in this section present a combination of two design principles:

- Crime Prevention Through Environmental Design (CPTED)
- Traditional target hardening

CPTED principles take advantage of integral features of site and facility design to enhance security by reducing the opportunity for crimes to occur. CPTED is essentially a crime prevention philosophy based on the theory that proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, as well as an improvement in quality of life. To accomplish this, designers use natural, mechanical, and procedural means.

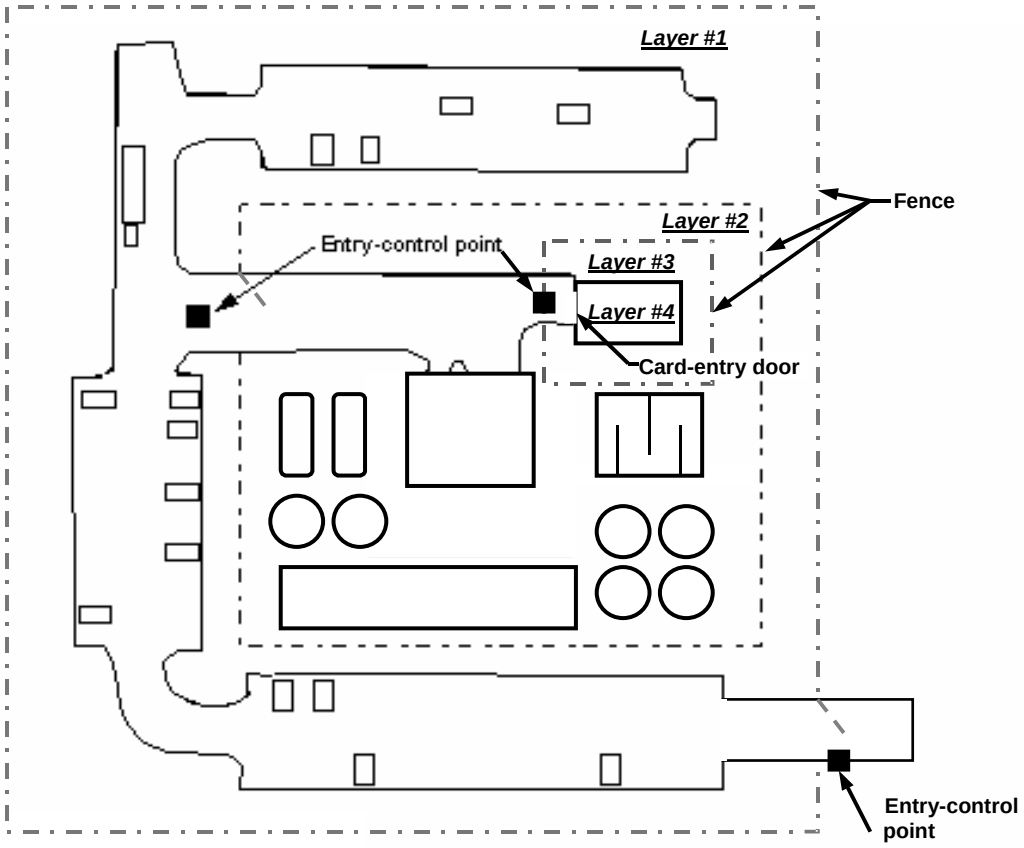


EXHIBIT 4-2
Example Layered Security Recommendations for a Facility

Target hardening refers to enhancement of physical construction systems to increase delay or deny access to the targeted asset. Hardening typically includes enhancements such as application of doors, locks, and window systems that have been tested and rated for specific levels of resistance to forced entry (rated in minutes delay time), ballistics (resistance to specific weapons and ballistic impacts), or blast (ability to withstand various blast loads at certain distances). The recommendations included in this section that are considered approaches to target hardening generally have measurable characteristics with respect to the DBT requirements for delay.

4.3.1 CPTED Strategies

CPTED strategies deter crime by reducing the opportunity to commit crimes, the likelihood that a crime will occur, and fear of crime generated by experience related to certain environmental conditions. The concepts embodied in CPTED strategies may be applied to all facilities, regardless of specific threats resulting in enhancing security as an integral part of design. Because CPTED strategies may be widely and cost-effectively implemented as prudent measures irrespective of specific threats, they should be among the basic design considerations for new, upgraded, and expanded wastewater facilities of any size. CPTED strategies can be considered within the following four categories:

- **Access control.** Physical guidance of vehicles and people going to and coming from a space through judicial placement of entrances, exits, landscaping, lighting, and controlling devices (e.g., guard stations, turnstiles, etc.)
- **Territorial reinforcement.** Physical attributes that express ownership, reinforce territoriality, and designate a gradient from public to restricted spaces. Examples include natural markers (landscaping, choke points), symbolic markers (signage, stickers), physical barriers (fences), and procedural barriers (receptionist, guard).
- **Surveillance.** The placement of physical features, activities, vehicles, and people in such a way as to maximize visibility by others during their normal activities. Surveillance may be natural or electronic, informal (office windows placed to facilitate surveillance of entry roads) or formal (continuous monitoring).
- **Image and maintenance.** Vigilant site and facility maintenance indicates that the space is being used and regularly attended to, and possibly occupied. Proper grounds maintenance also sustains surveillance. Image and maintenance activities are mostly related to management and operations rather than design.

The following are CPTED strategies that should be considered for the design of wastewater facilities.

4.3.1.1 Perimeter

- Provide access via no more than two designated and monitored entrances.
- Position all pedestrian entrances next to vehicle entrances.
- Control access with fences, gates, and/or attendants (guards).
- Provide sufficient lighting at all entrances (see Section 6).
- Create gateways or formal entrances delineated by plantings, different paving materials, fencing, and gates to separate public areas from controlled areas.
- Defining vehicle entrances by different paving materials and signage.
- Avoid opaque fencing, landscaping, and walls that might provide hiding places along the perimeter.

4.3.1.2 Site

- Provide a clear zone of 15 to 30 meters (50 to 100 feet) or more to enhance visual observation by personnel and to create a demarcation zone that makes unauthorized persons more noticeable.
- Thoroughly illuminate the clear zone (see Section 6) to make it easier for employees, guards, law enforcement, and others passing by to observe and identify intruders.
- Avoid dead-end driveways and pathways.
- Provide access to both the front and back of buildings to facilitate patrols.
- Provide close-in parking spaces for third-shift workers.
- Restrict access to roofs from adjacent buildings, dumpsters, loading docks, poles, and ladders.

- Place approach and parking as to be visible from building occupants, especially from a reception area if one is planned, and/or guard shacks.
- Use walls only where necessary; consider stretched aircraft cable as an alternative for maximum visibility.
- Prevent creation of hiding places (e.g., blind pathways, storage yards, etc.).
- Plan storage areas for visual and/or vehicular access by patrol cars, but limit access to personal vehicles.
- Use landscape plants that mature within the available space and do not obstruct light fixtures.
- Use plant materials that prevent easy passage as boundary delineators (e.g., crown of thorns and other thorned shrubs, hollies, Spanish bayonet).
- Include highly visible, appropriate signage, but do not describe asset or facility function on the signs. Use building numbers rather than names that could identify potential asset locations.

4.3.1.3 Buildings and Other Structures

- Design entrances to be well-lit, well-defined, and visible to public areas and patrol vehicles.
- Place elevators close to main entrances. The interior of the elevator should be in view from the entrance when the doors are open; in addition, the entire entrance should be visible from the interior of the elevator.
- Design stairways to be visible without solid walls.
- Position all employee entrances next to employee parking.
- Position restrooms to be observable from nearby offices or work areas.
- Design interior windows and doors to provide visibility into hallways.

4.3.2 Target Hardening to Address the Design Basis Threat

The measures discussed in this section provide specific and quantifiable results if implemented as part of a comprehensive physical protection system. As noted above, detection, delay, and defense/response are the basic elements of a physical protection system. This section addresses those physical security elements that support detection (such as fencing that delineates a boundary at which detection is provided) and delay or prevent the crime or attack event through application of target-hardening enhancements. The protective measures discussed below relate to the specific threats identified previously: vandal, criminal, saboteur, and terrorist.

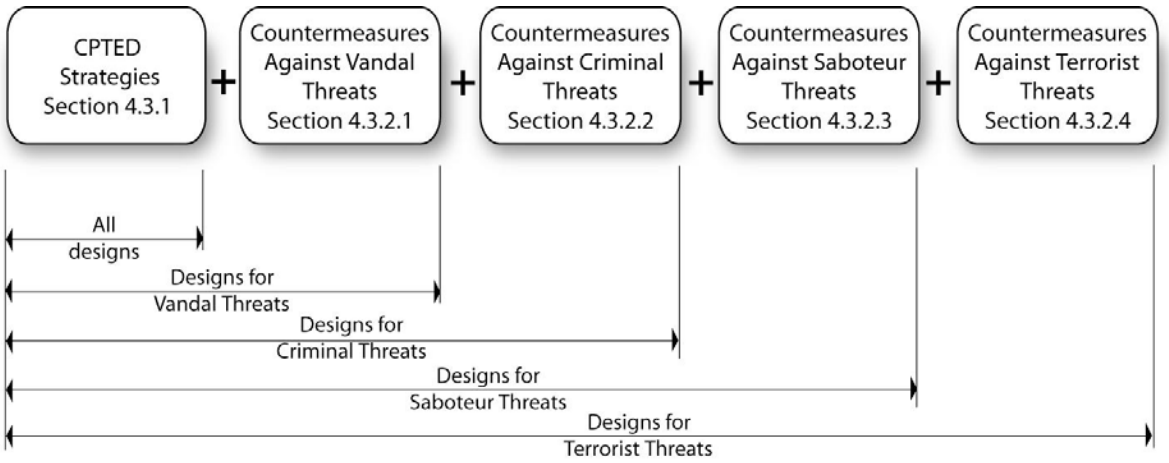
The measures indicated below were selected based on minimum measures being implemented for many federal facilities, including Department of Defense (DoD), Department of State (DoS), and General Services Administration (GSA) facilities. They relate to assumed threats such as stationary vehicle bombs carried in trucks parked near targeted facilities, various levels of forced entry, and ballistics threats.

These measures are listed as general guidelines. The specific DBT for each facility affects the implementation or selection of these measures, which in turn impacts implementation cost. For example, a minimum 45-meter (148-foot) standoff distance is included as a default distance where space allows. For extremely high threat levels (very large quantities of explosives), this may be insufficient; for extremely low quantities of explosives, such as what can be carried by a pedestrian or bicyclist, a lesser standoff distance is possible. Explosives threats require specific design to balance standoff distances (the least costly means of increasing survivability of structures against blast threats) with hardening of construction assemblies.

The following sections describe considerations to reduce risk through design of physical protective measures based on the specific threat categories described in Section 1.3.1.6. Protective measures are generally listed by site, building envelope, and specific building systems.

The following recommendations are in addition to those listed in the section above on CPTED strategies. These protective measures are considered design and construction enhancements that "harden" facilities to resist various types of attacks. Because the threats are listed in order of severity, protective measures listed for each lower-level threat are not repeated for the higher-level threats but assumed to be considerations for the higher levels as well. Exhibit 4-3 depicts the recommendation that the design of all wastewater facilities includes CPTED strategies and that, for increasing threats, additional considerations are recommended to be added to the design.

EXHIBIT 4-3
Recommendations for Design Progression



4.3.2.1 Countermeasures Against the Vandal Threat

Vandals typically use basic hand tools, such as pliers, wire cutters, hammers, crowbars, and baseball bats, to gain access to assets and may damage facilities using spray paint, fire crackers, fires, and improvised incendiary devices (IIDs). To prevent vandals from accomplishing their objectives, numerous materials, assemblies, and components have been developed for areas that attract significant vandalism and graffiti. These vandal-resistant items include:

- Composite plastics that resist graffiti, shattering, and scratches
- Lights with low-profile lenses or recessed lenses
- Security cameras and equipment
- Switches and controls
- Locks
- Valves
- Cages or other protective fittings

In addition to implementing vandal-resistant materials and components, the following physical protection measures are recommended:

Perimeter

- Establish a perimeter fence surrounding the facility at an appropriate standoff distance to provide a clear zone (see "Site" below). Standoff distance is the distance between the outside perimeter (the public areas) to critical facilities or buildings inside the perimeter (the restricted access area). See Exhibit 4-4.

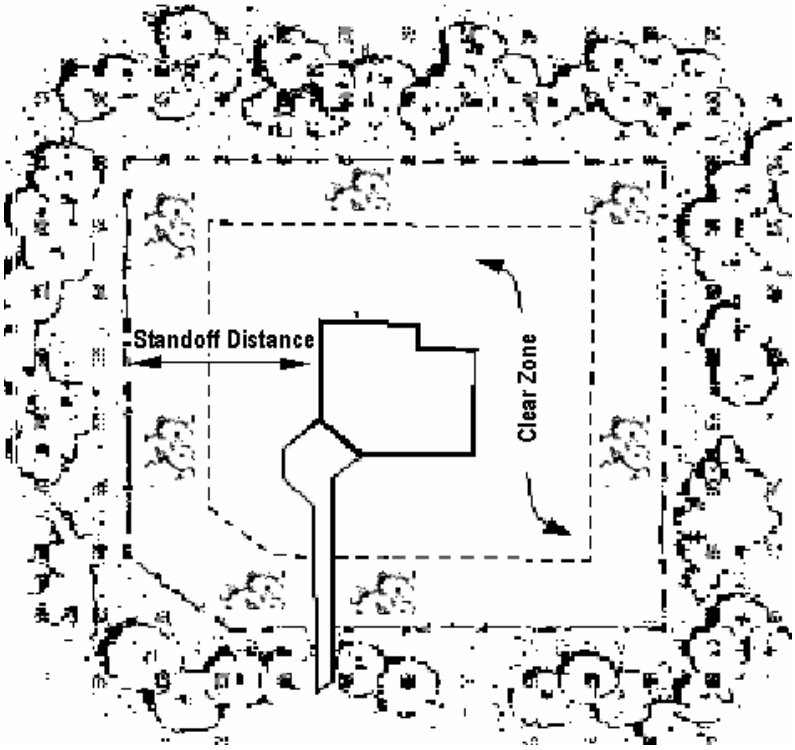


EXHIBIT 4-4
Example Standoff Distance and Clear Zone

- Use fencing that resists climbing. Examples of such fencing in order of increasing relative cost and climbing difficulty include chain-link fencing with small mesh openings, expanded metal mesh fencing, and climb-resistant security fencing, including ornamental iron fencing topped with curved pickets.
- Install fencing that is 2.5 meters (7 feet) or higher, with 9 gauge or thicker wire, and, as necessary, topped with one or two outriggers with barbed wire strands, razor tape, or concertina wire rolls. Fencing may also be curved at the top to prevent climbing over.
- Securely anchor fence posts in concrete footings to prevent the fence from being pushed over or pulled out of soft soils.

Site

- Designate a clear-zone area from the perimeter fence to building exterior. Within the clear-zone region, minimize landscaping and other features that provide concealment. Clear zones enhance visual observation by security personnel and create a demarcation zone that makes unauthorized persons more noticeable.
- Fence over the top of smaller site elements to completely enclose critical areas within the site.

Buildings and Other Structures

- Use non-removable bolts, hinges, screws, and other attachments to prevent removal of locks, fittings, and other items that are attached to surfaces
- For surfaces that may be subject to vandalism, use glazed concrete masonry units or glazed ceramic tiles. Special vandal-proof tiles that look attractive but will not readily mark or scratch are also available.
- Apply non-stick, non-mark polyurethane-based paints and coatings for internal or external surfaces.
- Rough-textured bricks, blocks, or rough concrete surfaces resist damage, and could present a challenge to vandals, although they are difficult to clean.
- Illuminate exterior areas surrounding assets and facilities.
- Use climb-resistant cages around exterior ladders.
- Locate luminaries beyond reach, placing them on high posts or locate high on building walls.
- Lighting equipment should not be located in hidden corners or behind buildings where it can easily be tampered with.
- Select lighting and other exposed equipment with scratch and vandal-resistant finishes that prevent corrosion, bending and deforming, and with locked and/or concealed fittings and controls.
- Instead of glass, use plastic materials such as polycarbonate.
- Select exterior furnishings of strong, vandal-resistant construction that is free of easily removed or uses projecting parts that are easily repaired. Anchor items to concrete if possible.
- Locate signs beyond reach where possible and feasible.

- Use vandal-resistant plastics in illuminated bollards, light fixtures, and traffic lights.
- Locate pipes, valves, and other appurtenances that may be damaged behind sturdy fencing or panels with tamperproof fastenings.
- Use materials that are nonflammable.
- Provide locked security cages around meters and exposed valves or fittings. Use vandal-resistant locks.

4.3.2.2 Countermeasures Against Criminal Threats

The criminal threat includes weapons such as knives and handguns, as well as hand and power tools. To accomplish the criminal's objective of using stealth, power tools are unlikely to be employed except by the highest severity level of criminal threats, which fall into the saboteur category. Criminals are generally assumed to be less interested in creating damage than they are in obtaining an asset and leaving the crime scene undetected. In addition to recommendations to resist vandalism, consider the following:

Site

- Provide emergency telephones throughout the site.
- Bury or otherwise conceal conduits and wires carrying electric supply, telecommunications, and alarm signals.

Buildings and Other Structures

- Minimize signage that may guide adversaries to specific asset locations. Refer to room numbers rather than asset locations.
- Provide warning signs to restrict access but avoid describing asset or reason.
- Provide a waiting area for visitors.
- Locate door locks minimum of 100 cm (40 in) from adjacent windows.
- Use single-cylinder dead bolt locks with minimum 1-inch throw on primary ground floor exits.
- Use locksets with removable cores to permit easy replacement should a keyed-alike system be compromised.
- Equip solid exterior doors with 180-degree door viewers.
- Minimize windows, including glazed entrance door windows.
- Use shatter-resistant glazing materials.
- Use two locking devices on all windows.
- If the DBT includes the potential to threaten people with handguns, provide bullet-resistant construction assemblies (walls, windows, doors) in those areas. For example, provide bullet-resistant prefabricated guard shelters, control rooms, or bill-paying booths for accounts receivables areas.

- Locate critical assets and functions to the interior of facilities to maximize layers of delay between access points and assets, and in within view of areas occupied 24 hours per day, if possible.
- Locate critical assets and functions in areas of buildings where they may be difficult to find. For example, locate control rooms or accounting areas away from lobby areas.
- Provide a facility access control system that employs:
  - Monitoring of all perimeter openings (personnel doors, rollup doors, and roof hatches) and locked interior doors for door ajar status.
  - Establishing a primary entrance door and adding access control, a visitor intercom, and video surveillance equipment.
  - Identifying critical exterior circulation doors, and adding access control to those doors. These doors should be designated as access-controlled doors and should only be accessible by employees. Access control methods could consist of adding key locks, keypads, or card readers with or without using personal identification numbers (PIN) for entry.
  - Designating remaining doors without exterior access control as exit-only. Remove exterior door hardware from exit-only doors. Ensure that on the interior side of the doors appropriate exit hardware remains, allowing free access under emergency egress conditions.
  - Establishing a secure lobby area, with hardened doors capable of being activated by security to go to "locked-down" mode.
  - Using hardened and protected hasp padlocks.
  - Providing CCTV camera surveillance of incoming personnel into the secure lobby area using a minimum of two cameras; one records body size and clothing characteristics and one records a close-up of facial characteristics. All CCTV surveillance should be recorded digitally. See Section 6.3.4 for available CCTV technology.
  - Establishing a secure area to house CCTV monitors, security computer equipment, radios, and so on.
  - Considering the addition of layered access control to high value areas within the facility (such as SCADA rooms).
  - Segmenting access control such that only employees requiring access to high-value areas are permitted access, rather than all employees having access to all areas.

4.3.2.3 Countermeasures Against Saboteur Threats

Saboteurs intent on destruction, disruption, or contamination will avail themselves of an almost unlimited variety of hand, power, and thermal tools (including construction tools such as cutting torches), contaminant agents, IEDs and IIDs, as well as higher-level ballistic weapons. This represents a significant threat level and effective protection measures can be very costly. Consider the following recommendations in addition to those for the vandal and criminal threats:

Perimeter

- Locate entry control, perimeter detection and barriers as far as possible from facilities or assets to denote a standoff zone. If conventional building construction is used, the standoff zone should be

a minimum of 45 meters (148 feet)[16] from asset location to provide survivability against vehicle bombs. However, depending upon the DBT, the standoff distance necessary may be substantially greater. Refer to DoD's Unified Facilities Criteria[17] and the Army's IED Safe Standoff Distance Cheat Sheet[18] for further guidance.

EXHIBIT 4-5
Entry Control Point with Protected Guardhouse

- Control access to sites by unauthorized vehicles through use of an entry control point for vehicular and pedestrian traffic (Exhibit 4-5). An effective entry control point must provide a:
  - Means to associate vehicle with driver, such as validation of the drivers' identification prior to authorizing access,
  - Mechanism to turn away unauthorized vehicles or pedestrians
  - Location for inspection of vehicles and their contents including bomb detection equipment
  - Location to detain unauthorized persons and their vehicles
  - Bullet-resistant guardhouse with toilet facilities and weather protection
  - Turnstile for pedestrians that can entrap potential adversaries failing validation of identification
  - Barrier to prevent a vehicle from penetrating the gate or crashing into the guardhouse
  - Ram-resistant gate
  - A telephone or intercom
- Design entry control points to ensure unimpeded access by emergency vehicles (i.e., fire-rescue, police, and ambulance).
- Provide vehicle barriers surrounding perimeter of site.
  - Vehicle barriers to resist moving vehicles must be designed for the vehicle weight, including explosives carried, and the speed at which the vehicle may be traveling. The location of the barrier must consider the time to activate and fully deploy the barrier before the vehicle reaches the barrier, as well as the acceleration opportunity that distance allows for the vehicle.

---

16 *DoD Minimum Antiterrorism Standards for Buildings*, UFC 4-010-01, October 8, 2003

17 *Ibid.*

18 Improvised Explosive Device (IED) Safe Standoff Distance Cheat Sheet, U.S. Army

- Vehicle barriers to resist moving vehicles may be active or passive depending on the application requirements. If unrestricted access is generally required with deployable barriers available to stop unauthorized vehicles, active barriers should be used.
- Examples of active barriers are shown in Exhibit 4-6 and include:
  - Retractable bollards
  - Hydraulic ramp, drum, wedge, and plate barriers
  - Sliding gates
  - Cable-beam barriers
  - Manual plate barriers
  - Portable crash barriers

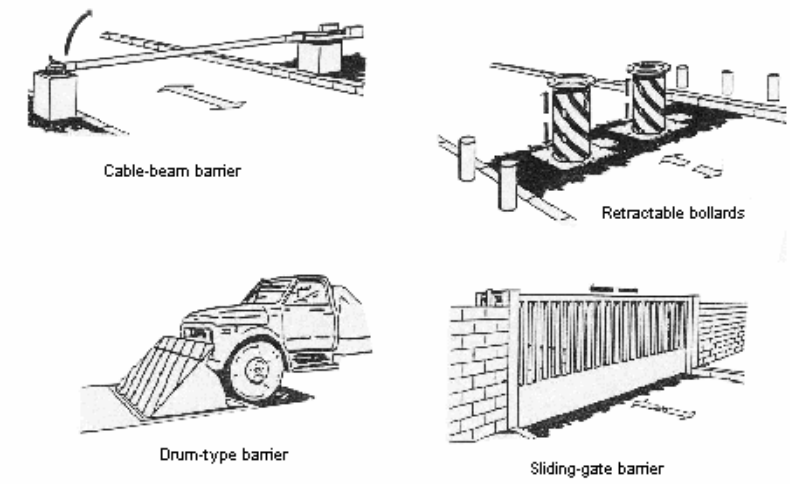


EXHIBIT 4-6
Examples of Active Barriers

- Passive barriers that resist ramming include:
  - Aircraft cable barriers that may be integrated into the perimeter fence. Aircraft cable must have anchorage and foundation systems designed to resist the forces of moving vehicles loaded with explosives (Exhibit 4-7).
  - Landforms and landscaping elements such as ditches, berms, heavy vegetation, boulders, bollards (designed to resist vehicle ramming), and concrete.

EXHIBIT 4-7
Perimeter Fence with Aircraft Cable Anchored to Concrete

- Provide remote meter reading devices or locate meters outside of the perimeter barrier to eliminate the need for electric, gas, and water meter readers to come onto the facility site.

Site

- Control the potential for vehicles to gain speed between the entry control point and assets by chicanes, speed bumps, or other traffic-calming devices.
- Select sites for critical assets that allow minimum 45 meter (148-foot) stand-off distance around occupied facilities and the critical assets subjected to attack.
  - Consider placing critical assets below grade or using earth-sheltered buildings to protect assets.
  - Provide redundant critical utility connections, such as power service, communications, water, and wastewater for high security assets.
- Secure exposed exterior valves, hydrants, manholes, and other appurtenances.
- Enclose exterior areas housing critical assets with expanded metal mesh enclosures, reinforced grouted concrete block, or reinforced concrete walls with roof grilles to prevent access to assets.
- Locate fuel tanks, natural gas lines, or fueling stations as far from critical assets as possible.

Buildings and Other Structures

- Use forced entry-resistant window and door assemblies. Assemblies must be rated for forced-entry resistance commensurate to the DBT level anticipated (rated assemblies are tested for minutes of resistance to attack using various combinations of hand, power, and thermal tools) and should include the entire assembly: window/door, frame, anchorage to wall, and lock and hinge hardware.
- Provide high security, forced entry-resistant hardware, including locks, lock bolts, hinges, etc.

4.3.2.4 Countermeasures Against Terrorist Threats

Unless the terrorist is intent on stealth, detection is relatively easy and of little importance to the terrorist. Depending on the specific DBT, the following tactics may be employed by terrorists: stationary vehicle bombs parked near targeted facilities; moving vehicle bombs; carried explosives and IEDs; RPGs and mortars; IIDs; any type of hand, power, or thermal tools; automatic assault-type weapons; and contaminant agents. Protective measures to resist blast threats are intended to prevent or minimize casualties; more costly systems may result in greater survivability and reusability of structures. Blast threats require specific blast engineering to develop appropriate resistance levels to various explosives threats. The greater the distance a blast can be kept from assets, the less likely the asset will be injured or damaged, so standoff distance is paramount where space allows. In addition to appropriate protective measures listed for the vandal, criminal and saboteur threats, consider the following recommendations:

Perimeter

- Provide a vehicle sally port where vehicles can be detained until the driver identity can be confirmed and the vehicle contents and undercarriage can be examined. A video surveillance system should be employed at the sally port.

Site

- Locate assets away from vantage points from where weapons such as RPGs may be fired.
- Provide pre-detonation screens (materials such as expanded metal or chain-link that serve to damage or detonate a RPG as the projectile passes through the material prior to reaching its target) at site perimeter between assets and vantage points. Pre-detonation points should be as far as possible from assets, including parking areas and occupied buildings.
- Consider circulation and access to site facilities, including service and mail deliveries. Provide sufficient standoff distance between receiving areas, occupied buildings, and critical assets in the event bombs are delivered in service or delivery vehicles.
- Prevent parking adjacent to and under/over facilities (such as rooftop parking or parking under occupied sections of buildings). Keep unrestricted parking areas as far from buildings as possible.
- Locate areas for dumpsters and trash barrels as far away from asset locations as practical. Explosive resistant trash receptacles are available, but diligent research must be done before purchasing since there is no standard for labeling receptacles as explosive resistant.

Buildings and Other Structures

- Locate blast walls behind entrances and large windows to prevent glass shards from penetrating building interiors.
- Design building systems to resist blast and contamination attacks included in DBT.
- Isolate areas where bombs could be received, including loading docks, mail rooms, storage areas, and lobbies. Isolation should be accommodated in both structural and mechanical systems. Provide vestibules at entries.
- Locate air intakes as high as possible, at a minimum of 3 meters (10 feet) above grade in building walls to prevent contaminants from being introduced. Ensure that equipment, loading docks, trash receptacles, ladders, and other building or site appurtenances do not allow access to air intakes. Note: air intakes for chlorine rooms must be near the floor.
- Protect openings to air intakes with sloped mesh screens to prevent objects from being tossed into intake openings.
- Install low-leakage dampers to minimize penetration of introduced contaminants after the HVAC system is shut down.
- Where chemical, biological, or radiological (CBR) release at some distance from a facility is part of the DBT, design facility for air tightness or ensure positive pressure is maintained within the structure to limit infiltration.
- Establish a protected clear zone around ground level or low air intake openings with entry restricted to authorized personnel only. The clear zone may be fenced or walled (provisions for air circulation required by air intake and HVAC equipment must be considered). Illuminate and monitor the clear zone (guard patrols or CCTV).

- Provide grilles with openings no larger than 6 inches in diameter in all openings (both intake and return air). Grilles should be resistant to forced entry and anchored firmly into building structure to prevent penetration through ductwork or openings.
- Prevent unrestricted or public access to rooftop areas where mechanical equipment is located. Other roof openings, including skylights and roof scuttles, should be locked and replaced with forced entry-resistant assemblies.
- Restrict access to mechanical equipment yards and rooms to authorized personnel only. Illuminate and monitor entrances to these areas.
- Evaluate building control programs to consider isolation and zoning of various areas of facilities that house critical assets that may be targeted by contamination tactics, automatic shut-off switches to zones or facilities, and pressurization and airflow control especially with respect to egress areas. "Shelter in Place" concepts require a single point of control to immediately shut down all HVAC systems when a contamination event has been detected or is anticipated (i.e., if a cloud is moving toward a facility). This switch must also be readily accessible to building personnel or facility manager.
- Install back-draft dampers on exhaust fans.
- Provide safe rooms with separate, dedicated HVAC systems to provide secure areas for personnel to move to when the facility may be exposed to contaminants. Safe rooms should include indoor air purifiers.
- Use ducted returns to limit access points from which CBR contaminant agents may be introduced.
- Minimize mixing between HVAC zones.
- Evaluate adsorbent filtration options with respect to specific DBT contaminants. Higher efficiency filtration may be beneficial for certain exposures, but not effective against chemical vapors or gases used in chemical attacks, and will likely be extremely costly, require extensive area to accommodate the filters, and reduce airflow. Refer to National Institute of Occupational Safety and Health (NIOSH) guidelines for more considerations and information.

4.3.3 Additional Design Considerations for Wastewater Treatment Facilities

The heart of any wastewater treatment facility, and a prime target for malevolent acts, is the series of physical, chemical, and biological processes used to treat the wastewater. Each unit operation and process is generally designed for a specific function, with the quality of the plant's final effluent dependent on the symbiotic and coordinated performances of all the processes. Although generally robust, an individual treatment process could be disabled or destroyed by a malevolent act resulting in excessive or incompatible pollutant loadings to subsequent processes and, eventually, upset conditions throughout the treatment plant. A treatment plant in an upset condition will not be able to adequately provide the degree or capacity of treatment for which it was designed and could impact

the quality of the receiving water resulting in detrimental impacts to the environment and downstream users.

Design considerations for securing sites and facilities in general were covered in previous sections of this section. What follows are specific design considerations for the impacts of malevolent acts conducted by individuals once access to the treatment processes has been gained, or the raw wastewater has been contaminated through the collection system. These design considerations are not meant to replace what is required by good engineering practice, wastewater industry design manuals, and regulatory requirements. Rather what follow are additional design considerations to mitigate risks associated with malevolent threats of sabotage and terrorism.

For guidance in designing wastewater treatment facilities and individual unit processes, refer to the numerous publications that are available, including the following:

- *Design of Municipal Wastewater Treatment Plants – MOP 8,* WEF, 1998
- *Wastewater Treatment Plant Design,* WEF and International Water Association (IWA), 2003
- *Recommended Standards for Wastewater Facilities - 10 States Standards,* Health Education Services, 2004
- *Wastewater Engineering: Treatment and Reuse,* McGraw-Hill, 2002
- Several other Manuals of Practice published by WEF that address specific systems and processes

4.3.3.1 Treatment Facility-wide

Redundancy

Redundancy in design provides multiple tanks, basins, treatment units, pumps, and conveyance piping and channels to minimize the potential for single points of failure, which are likely to be key targets for knowledgeable threats. For more information on redundancy refer to WERF's publication, *Efficient Redundancy Design Practices*.[19]

- To minimize risk to the greatest extent, redundancy should be extended to entire treatment facility so the treatment process consists of multiple parallel trains that are separated by a distance that would maintain at least one treatment train operational if another was damaged. Interconnected all treatment trains for maximum operational flexibility.
- Each unit process should consist of two or more process units operating in parallel.
- Equipment such as pumps, motors, blowers, and chemical feed equipment should also be designed in multiples, with sufficient capacity to handle peak flows if the largest piece of equipment fails or is taken out of service.
- Twin power feeds to motor control centers and an individual motor control center for each train should be considered.
- At a minimum, the design for individual processes should be conservative and at peak loadings with one unit out of service.

[19] *Efficient Redundancy Design Practices*, Water Environment Research Foundation, 2003

- For treatment plants with multiple trains, consider peak loadings with one train out of service.
- Higher redundancies should be considered for critical processes, such as biological processes or disinfection systems, where redundancies should be 100 percent of design capacity.
- On-the-shelf spares of process pumps, motors, valves, meters, controllers, etc. provide redundant critical components.

Flexibility

- Provide each unit process with bypass channels, pipes, and pumps to enable an individual unit to be removed from service while providing sufficient treatment at peak flow conditions.
- Provide channels, gates, pumps, valves, and piping to enable unit processes to be used for additional purposes, such as using a secondary clarifier as a temporary chlorine contact chamber.
- Critical valves, gates, and transfer pumps should be automated to allow for quick shutdown or diversion of flows. However, all automated equipment should have manual overrides should automated controls or SCADA systems be compromised or offline.

Back-up Power

- Two independent main power supplies are not sufficient for protecting against saboteur and terrorist threat categories. Wastewater treatment facilities should have an onsite backup power generation capacity to provide sufficient power during a power outage or blackout to maintain, at a minimum:
  - Processes that are critical to maintaining adequate treatment to meet effluent or reclaimed water quality criteria
  - A reduced level of lighting throughout the plant
  - Lighting of warning signs, hazardous areas, stairways, and emergency exits
  - Proper ventilation in confined areas and other locations (e.g., laboratories) that require a controlled atmosphere
  - Power to outlets throughout the facility to permit electric power tools to be used for repairs

Small Utility Tip

When designing smaller treatment plants, consider having a receptacle for attaching a portable stand-by generator rather than an onsite generator

- Provide an automatic transfer switch for rapid transition to backup power when primary power fails.
- Recent events such as the August 2003 Northeast Blackout suggest that backup power supplies and fuel storage should able to provide at least 48 hours of service.
- Locate a supplier of skid-mounted or modular housed generator sets that could be rented if needed. Consider establishing a contract for preferred-customer status.
- Treatment facilities should consider looped power distribution networks within the treatment plant to enable rapid isolation and removal of a damaged power feed or electrical equipment from the power net.
- Provide uninterruptible power supply (UPS) systems for process controls, SCADA systems, alarms, computer networks, and communication systems. See Section 6 for further information.

Access Control

- Whenever and wherever feasible, tanks and open channels should be covered, and the access doors and hatches should be secured.
- Critical components such as blowers, pumps, motors, motor control centers, and SCADA components should be secured within enclosures and hidden from the view of anyone outside the perimeter of the facility.
- Piping and blower ducts should be installed below ground or within secured structures. Utilities should be installed underground.
- Locking mechanisms should be provided for valves and gate operators.
- Designers should assure that limiting access to process components does not significantly impact O&M activities. For example:
  - Adequate access and room for maintenance and repair must be considered in the layout of individual unit processes and equipment.
  - The ability to remove enclosures maybe necessary to replace or repair equipment.
  - Sufficient ventilation must be provided within enclosures and structures to remove noxious and toxic gases and fumes and ensure a healthy work environment for O&M staff.

4.3.3.2 Influent Pump Station, Preliminary and Primary Treatment

Pretreatment and primary treatment generally consists of influent structures, pump stations, bar screens, grit chambers, septage receiving stations, primary clarifiers, and associated support processes such as chemical feed systems, grit and screenings removal, and odor control.

4.3.3.3 Influent Pump Stations and Influent Structures

- Influent pump stations should be designed to handle peak flows with the largest pump out-of-service.
- Influent pump stations should designed to enable removal of pumps and motors for repair while maintaining the operability of the facility at full capacity.
- Oversizing the influent pump station wet well or having redundant wet wells should be considered.
- Where feasible, provisions should be made for temporary bypass of the raw wastewater around the influent pump station to wet-weather or similar storage facilities to provide additional downtime capability for repair of the pump station.
- Real-time monitoring for the presence of toxic or explosive chemicals in the influent wastewater stream should be provided. At a minimum, pH and lower explosive limit (LEL) monitors should be installed, with consideration given to automatic diversion of suspicious influent into holding basins. Biotoxin-specific and similar monitors are currently under development for potable water systems and may be available for wastewater systems in the near future.[20]

[20] ASCE Water and Wastewater Security White Papers, 2004

- Provisions for emergency pretreatment of the influent wastewater may also be considered if real-time monitoring indicates abnormal conditions and the presence of a toxicant is suspected. Pretreatment approaches include the addition of powdered activated carbon, a strong oxidant such as chlorine or potassium permanganate, and the addition of a caustic to neutralize or precipitate the toxic chemical.

4.3.3.4 Preliminary Treatment

- Manual backup processes can provide the redundancy desired, especially for smaller wastewater treatment plants. Examples include manual bar screens and grit removal.
- A minimum of two screens in separate channels should be provided. One screen should be designed to permit manual cleaning.
- Grit chambers should be provided that have adequate capacities under peak flow and load conditions with at least one unit of service.

Small Utility Tip

Designs for smaller treatment plants may consider redundancy at 50 percent of peak load conditions, or disregard redundancy of primary clarifiers altogether.

- Individual unit bypasses and multiple full-capacity feed channels should be considered.
- Redundant support systems such as multiple blowers and ductwork for aerated grit chambers and chemical feed systems should be considered.
- Septage receiving stations should be located in a sally port at least 45 meters (148 feet) away from occupied buildings. Discharges from these stations should be upstream of the screens to maximize the ability of the treatment plant to treat these wastes.
- Visual inspection of discharges into the septage receiving station should be performed, along with monitoring using sampling equipment.
- Offline flow equalization/storage basins should be considered to allow any influent that is suspected of being contaminated to be diverted from the treatment processes. If possible, at least 8 hours of storage at the average daily flow rate should be provided. Basins should be located to take flow after preliminary treatment but before primary treatment.
- Odor control processes such as chemical scrubbers that utilize fans or blowers should be secured within a higher security layer to lessen the risk of a toxic agent being added that could be aerosolized.

4.3.3.5 Primary Clarifiers

- Redundant unit processes and adequate capacities under peak flow and load conditions with at least one unit of service should be considered.
- Treatment plant designs should incorporate the flexibility to use primary clarifiers as short-term backups for more critical unit processes, either with permanent or temporary piping and pumps. Examples include using these units as secondary clarifiers, gravity thickeners, aerobic digesters (with floating aerators), waste-activated sludge storage, and digested sludge storage.

4.3.3.6 Secondary Treatment

The vast majority of secondary treatment processes include some type of biological process for treatment of organic wastes followed by clarification to remove the biological growth from the waste stream. Although biological processes are fairly robust with regard to normal organic wastes, these wastes are susceptible to a broad array of organic and inorganic toxins. These toxins can inhibit the growth, and thus the effectiveness, of the biological system or kill the biomass. Operational flexibility is a key factor in the design of biological systems to minimize the impacts of toxins.

Biological Treatment

- The most stable biological process should be employed to reduce the biomass upset from shock loads.
- A sufficient number of blowers or mechanical aerators should be provided to enable the design oxygen transfer to be maintained with the largest-capacity unit out of service.
- Installing blowers in two separate blower buildings should be considered, with the buildings located on either side of the aeration basins with interconnected, but isolatable, air supply piping.
- Air diffuser systems for each aeration tank should be designed so that the largest section of diffusers can be out-of-service without measurably impairing the oxygen transfer capability of the system.
- The overall capacity of air supply system should include at least 50 percent more capacity than estimated peak demand conditions. It may be feasible to backup the aeration system with floating aerators that can be installed relatively quickly.
- At least one backup aeration tank should be provided that is equal to or greater than the capacity of the largest of the other tanks. This tank can be used as part of the activated sludge process or for storing diverted mixed liquor in the event of contamination.
- In addition to multiple process units and bypass channels, the biological process should be designed with as much flexibility as possible to minimize impacts to the biological organisms in the units. Examples include designing an activated sludge plant to be able to operate in a variety of process modes, including complete mix, contact stabilization, step feed, or extended aeration. This flexibility provides the operators with tools to either dilute the toxins to manageable concentrations or to maintain a significant quantity of biomass out of harm's way to reseed and stabilize the process.
- For fixed film processes, a sufficient number of units should be provided so that the peak flows can still be processed with the largest unit out-of-service.
- Provide sufficient recycle system capacity and flexibility to maintain a viable biomass should the flow be affected by a toxin.

Secondary Clarifiers

- The number and size of secondary (final) clarifiers should allow for effective treatment at peak flow rates with at least one unit out of service.

- Design the secondary clarifiers, piping, and pumps with the ability and flexibility to serve as temporary backup units for other processes.

4.3.3.7 Effluent Filtration

- Multiple filter units should be provided so that adequate filtration is achieved with the largest unit out of service at peak flow conditions.
- Interconnected, dual backwash systems, each with a capacity for 100 percent of the peak flow, should be provided.
- Backwash systems should be designed to permit manual backwashing if the automatic system fails.
- Chemical systems used to enhance filtration should also include a measure of redundancy.
- Replacement media should be stored in a secured storage building away from the filters.

4.3.3.8 Disinfection

General

- Ultraviolet (UV) light should be the disinfection method of choice for new, upgraded, and expanded wastewater treatment facilities. Should the utility be required to maintain a chlorine residual (e.g., for reclaimed water distribution), sodium hypochlorite should be added after the UV process. This will reduce the chlorine demand of the effluent and minimize the amount of chlorine required.
- Disinfection with gaseous chlorine should be avoided due to its toxicity to the environment and the extreme hazard to human health should the gas be released to the atmosphere.
- A location for manual feeding of calcium hypochlorite should be provided as a fail-safe method of disinfection should other disinfection processes fail.
- Where disinfected effluent is to be reused as reclaimed water, disinfection contact tanks and outlet channels should be covered.

Ultraviolet Light

- Provide multiple UV modules in multiple channels designed so that there is adequate disinfection at peak flow rates with the largest module and largest channel being out of service.
- A standby sodium hypochlorite feed system should be considered to provide a backup means of disinfection should the UV system become inoperable.
- Provide secure storage area for UV replacement lamps and modules away from the UV channels.

Chlorination

The design of chlorination facilities involves a wide range of safety considerations and compliance with a variety of federal, state, and local regulations. The recommendations below are to be considered in addition to all other design criteria, safety requirements, and regulatory issues associated with the use of chlorine as disinfectant.

- Chlorination facilities, whether using gas cylinders, chlorine dioxide generators, or liquid sodium hypochlorite, should be housed within a building and located within an enclosed higher security layer (see Section 4.2.2) that is a minimum of 45 meters (148 feet) from the treatment plant's secured perimeter.
- Onsite generation of sodium hypochlorite should be considered to reduce the quantity of chlorine required to be kept onsite.
- All chlorination equipment, including chlorinators, evaporators, scales, chlorine dioxide generators, storage tanks, and feed pumps, should be designed in multiple units with adequate disinfecting capacity at peak flow with the largest unit being out of service.
- All chlorine cylinders or tankers should be screened from the view of anyone outside of the treatment plant's secured perimeter view by an opaque partition.
- See Section 4.3.3.11, "Chemical Systems," for additional information.

Dechlorination

- Dechlorination facilities, whether using sulfur dioxide, sodium bisulfate, or sodium metabisulfite, should be housed within a building and located within an enclosed higher security layer (see Section 4.2.2), and a minimum of 45 meters (148 feet) from the treatment plant's secured perimeter.
- All dechlorination equipment, including storage tanks and feed pumps, should be designed in multiple units with adequate capacity at peak flow with the largest unit being out of service.
- See Section 4.3.3.11, "Chemical Systems," for additional information.

4.3.3.9 Effluent Disposal and Reclaimed Water Production

At the end of the treatment system, flexibility in the design should allow diversion and holding of effluent that may not be suitable for disposal or as reuse as reclaimed water.

Surface Water Disposal

- Equalization storage and holding capacity for diversion of effluent should be provided in the event that contamination be suspected.
- A redundant outfall at a different location than the primary outfall should be considered.
- Outfall areas, including effluent sampling equipment and monitoring instrumentation, should be secured within a higher security layer.
- If the outfall pipe does is not permanently capped, a bar should be installed to prevent persons from using the outfall as a conduit to the treatment facility or combined sewer system.

Reclaimed Water Production

Reclaimed water may include, but is not limited to, highly treated wastewater effluent that is used for irrigation, cooling water, lake or stream augmentation, groundwater recharge, and other non-potable uses. Most reclaimed water systems are characteristic of drinking water systems in that they provide

water (albeit non-potable) to the public under a pressurized system. Therefore, utilities that process reclaimed water are recommended to also refer to the *Security Guidance for Water Utilities*.[21]

- Multiple, covered tanks for storage of reclaimed water prior to distribution should be provided to allow operators sufficient time flexibility to test and appropriately manage the produced water. A minimum of one-day storage is recommended.
- In-line continuous water quality monitors for general water quality parameters such as pH, turbidity, conductivity, and disinfectant residual should be installed to measure the quality of the water immediately prior to distribution.
- More sophisticated instrumentation that can detect contaminants should be installed as it becomes available (refer to *Guidelines for Designing an Online Contaminant Monitoring System* [ASCE 2004]).
- Pumps, piping, valves, and related facilities should be provided to enable the system operators to either discharge or return the water to the treatment plant's influent rather than distribute water that does not meet water quality requirements.
- An additional disinfection system should be included to enable operators to provide supplemental disinfection immediately prior to distribution.
- Subject to regulatory approval, provide a means to divert reclaimed water to an alternative disposal system such as a surface water outfall if the water cannot meet reclaimed water quality but will not adversely affect surface waters, or to infiltration ponds if groundwater will not be adversely affected.
- Alarms should be provided to alert operators to reclaimed water quality problems and automatically actuated devices installed to divert reclaimed water to emergency storage areas instead of the distribution system.
- All reclaimed water facilities should be enclosed within a higher security layer.

4.3.3.10 Solids Handling

- Solids concentration process systems such as thickeners, centrifuges, and belt filter presses should be designed in multiple units with the design capacity adequate to provide necessary thickening with the largest unit out of service.
- Aerobic digesters and anaerobic digesters should be designed in multiple units with the design capacity adequate to provide necessary thickening with the largest unit out of service.
- Anaerobic digesters and related equipment, including mixing, heating system, gas collection, and gas storage, should be enclosed in a higher security layer (see Section 4.2.2), and located a minimum of 45 meters (148 feet) from occupied buildings.
- Waste gas burners should be located a minimum of 15 meters (50 feet) from any other structures.

---

[21] *Security Guidance for Water Utilities*, American Water Works Association, 2004

- Gas piping and storage facilities should be screened so that they are not visible from outside of the treatment plant perimeter.
- Provide methane gas sensors and alarms where anaerobic digestion is employed.
- Provide automatic shutdown of gas systems at preset pressures.
- Heat dryers and pelletizing processes should be located a sufficient distance away from other structures to minimize the risk of spreading fire should the heating fuel ignite. This standoff distance will be dependent upon the type of fuel and fuel storage quantities used.
- Stand-by drying beds should be provided to serve as a backup should other solids handling processes fail, or provide storage lagoons or tanks for temporary storage of untreated or partially treated solids.
- Stockpile areas for treated sludge should be provided if transportation to disposal sites becomes unavailable, or if contaminants in the wastewater have made the solids unsuitable for there normal disposal or application site. Stockpile areas should be enclosed within a higher security layer.
- Solids loading and transfer areas should be located within a sally port if non-utility staff and non-utility vehicles may load or transport the solids. The sally port should be a minimum of 45 meters (148 feet) from occupied buildings.

4.3.3.11 Chemical Systems

- Local, state, and federal laws and regulations, such as fire codes, occupational and health requirements, must be followed when designing proper and safe storage of chemicals and locating mixing and chemical feed equipment.
- Sufficient quantities of chemicals should be kept available on utility property to provide a 30-day supply without additional shipments.
- Chemicals should be stored in unopened shipping containers, or be transferred into a covered storage tank. Hazardous chemicals should be stored within an enclosed area of a higher security layer.
- At least two storage tanks per liquid chemical are required to provide adequate redundancy.
- Adequate spill containment and control is required for all storage tanks, and separate containment structures are required for each chemical. The containment should be designed to hold the volume of the largest tank within the containment, plus an additional volume for fire flow or wet weather (if located outside of a building).
- Spill detection systems should be included in the design of storage and feed areas to assist in detecting theft or release of the chemical. Typical systems include vapor monitors for specific chemicals or liquid levels in containment sumps.
- Chemical tanks should have a high liquid alarm and the containment areas should contain a leak-detection and alarm system.
- Chemical piping should be installed below ground if possible.

4.3.4 Laboratories

- If the laboratory is located within the perimeter of a treatment facility, consideration should be given to enclosing the laboratory within a higher security layer.
- Local, state, and federal laws and regulations, such as fire codes, building codes and occupational and health requirements, must be followed when designing laboratories.
- Laboratories may become a target all four threat categories: vandal, criminal, saboteur or terrorist. Provide appropriate physical protection systems to secure analytical equipment, instrumentation, computer hardware, software and chemicals from the identified DBT (refer to Sections 4.2 and 4.3).
- Consider installing tamper- and chemical-resistant locking cabinets in which to store reagents.
- Gas cylinders that are used for laboratory analysis should be stored within the higher security layer of the laboratory and be screened from the view of persons outside of the laboratory.

4.3.5 Maintenance Shops, Warehouses, and Storage Areas

- If the building or area is located within the perimeter of a treatment facility, consideration should be given to enclosing it within a higher security layer.
- Local, state, and federal laws and regulations, such as fire codes, building codes and occupational and health requirements, must be followed when designing these support facilities.
- Consider locating these support facilities offsite of the treatment facility so that spare parts and materials, and replacement equipment are available for response and recovery from an incident at the treatment plant.
- Maintenance shops, warehouses, and storage areas may become a target in all four threat categories: vandal, criminal, saboteur or terrorist. Provide appropriate physical protection systems to secure equipment, materials, instruments, chemicals and fuels from the identified DBT (refer to Sections 4.2 and 4.3).
- Delivery areas for equipment and supplies, as well as for chemicals and fuel, should consist of a sally port to allow for inspection of the delivery vehicles and contents of the delivery. The inspection area should be designed to allow multiple inspections should more than one delivery vehicle be detained for inspection. The inspection areas should include appropriate equipment to allow for the sampling of chemical and fuel deliveries so that a chemical assay can be done prior to accepting the delivery.
- Vehicle fueling stations should be located at a sufficient standoff distance from treatment process units and inhabited buildings. The standoff distance should be based upon the DBT of both the fuel station itself to avoid damage to other parts of the treatment facility and the structures within its proximity to avoid damage to the fuel station.
- Gasoline and diesel fuel tanks should be installed underground in approved vessels.

- Automatic fuel dispensing systems requiring key cards that identifies the person using the fuel pump (and the vehicle if practical) should be installed at all fueling stations.
- Consider installing active barriers as described in Section 4.3.2.3.

4.3.6 Administrative Offices

- Provide space for gatekeepers, such as receptionists or guards, at the entrance to the buildings and possibly at key locations on other floors.
- Silent panic alarm buttons should be available to alert local law enforcement of malevolent incidents and provide notice to facility employees to take action as provided in the utility's emergency response plan.
- Consider creating sufficient space for sleeping, eating, and personal hygiene to accommodate staff members who may have spend long periods of time in the building during emergency conditions.

4.4 Additional Design Considerations for Remote Facilities

In the design of remote facilities such as pump stations (lift stations), CSO facilities, and stormwater retention ponds, all of the concepts discussed earlier in this section should be taken into consideration and selected for inclusion depending upon the DBT. In addition, to the extent that the remote facilities have pumps, motors, chemical storage, and other processes, the specific considerations presented for wastewater collection facilities in Section 4.5 should also be examined for applicability.

Remote facilities may have different risks based upon their location. For example, pump stations serving military installations, government buildings, financial institutions, and major industrial sites may be identified as facing a saboteur or terrorist category threat, while pump stations serving residential areas may be determined to have only a vandal category threat.

4.4.1 Pump Stations

Many wastewater utilities find that their pump stations are frequently targets of vandals because they are typically unattended and may be located away from populated areas. Designers of wastewater systems should strive to keep the number of pump stations to a minimum, although it is recognized that this is may not possible when new developments connect to an existing collection system, or when other factors such as a high groundwater table or rock near the surface makes construction of deep gravity sewers unrealistic or cost-prohibitive.

If possible, remote pump stations should be located in areas that have residences or commercial establishments where people can easily witness any malevolent actions that may be taken on the stations. Where possible, pump stations should be designed as submersible facilities with a minimal amount of equipment visible aboveground. Equipment, such as motor control panels, standby generators, or chemical feed systems, should be enclosed in a building. For non-submersible stations, consideration should be given to designing a structure that blends into the surrounding area (e.g., a

pump station that looks like a single-family home in a residential area) so that it becomes a less likely target at all threat levels.

Other considerations for pump stations include:

- Limiting number of pump stations through deeper and longer gravity sewers.
- Conversely, increasing the number of pump stations to provide redundancy and limit impact of failure of any given facility.

Pump stations should be designed with:

- At least one redundant pump that matches the largest pump so that the pump station can handle peak design flows with one of the largest pumps out of service.
- Each pump should have a separate electrical supply, motor starter, motor sensor and alarm, electrical components, and instrumentation and control components.
- A permanent standby power generator with automatic transfer for master pump stations and critical smaller pump stations should be provided; a receptacle for a portable generator is acceptable for smaller, less critical pump stations.
- Permanent generators should be located inside a building or other weather-tight enclosure to ensure startup in cold weather.
- Fuel for generators should be stored in underground tanks with a volume sufficient for a minimum of 24 continuous hours of operation without refueling.
- Sufficient excess wet well capacity, or redundant wet wells, should be available to retain a minimum of 2 hours at peak flow during an outage for all pump stations not having permanent standby generation onsite.
- Pump-out and pump-around capabilities.
- Central monitoring of intrusion, flows, pump status, wet well levels, fuel level via a SCADA system.

4.4.2 CSO Facilities

CSO near surface storage and treatment facility locations are often highly constrained by the location of existing CSO outfalls. As with remote pump stations, designs should limit amount of aboveground equipment, striving to make the facility invisible to the public. For underground storage facilities without chemical systems, restricted access may not be necessary if accessways and equipment are hidden and secured. Any aboveground equipment should be enclosed in a building designed using CPTED strategies discussed in Section 4.3.1.

A unique aspect of CSO facilities is that large-volume tanks are located in areas that are unattended by utility staff. Thus, at a terrorist threat level, the facility is vulnerable to being filled with a flammable or explosive substance that could cause damage to surrounding properties and result in fatalities. Consequently, at this threat level, CSO facilities should be located away from populated areas, or the applicable target hardening methods discussed in Section 4.3.2 should be employed.

Further, because CSO facilities include many of the mechanical and electrical components included in wastewater treatment facilities, the designer should consider all of the recommendations included in Section 4.3.3.

4.4.3 Stormwater Retention Ponds

Stormwater retention ponds have become increasingly prevalent in newer residential, commercial, and industrial developments, as well as along newly widened roadways. They are designed to retain at least the initial runoff from a storm to reduce the amount of pollutants entering surface waters and to mitigate flooding. Some may be designed as dry-bottom ponds, meaning that they have water in them only during wet periods. Others may be designed as wet-bottom ponds where the pond always has some water. Wet-bottom ponds are frequently used as amenities (artificial lakes) in communities.

Typically, the only structures associated with a retention pond are its inlet headwall and its outlet overflow weir. While damage to these structures or a breach of the pond sidewall may result in flooding, retention ponds may not pose much of an attractive target for malevolent actions. Should a vulnerability assessment identify a DBT that should be addressed, the CPTED strategies and target hardening methods described earlier in this section should be implemented as appropriate.

4.5 Special Design Considerations for Collection Systems

As with any utility network, sanitary sewer systems, combined sewer systems, and stormwater conveyance systems cover large areas, traveling through remote and unmonitored locations with numerous access points along its routes. But unlike other utility networks, gravity collection systems are not only targets of malevolent acts themselves, these systems can also serve as conduits for saboteurs and terrorists to inflict damage on other infrastructure and private property, as well as to harm or kill persons not associated with the wastewater utility. Consequently, designers must consider protecting a collection system from direct attacks as well as from its use as a conduit for other malevolent acts.

Different portions of the collection system may have different risks based upon their location and size. For example, the section of the collection system serving military installations, government buildings, financial institutions, and major industrial sites may be identified as facing a saboteur or terrorist category threat, while a section of the collection system serving residential areas may be determined to have only a vandal category threat. Likewise, because large diameter gravity sewers can provide access to other sensitive infrastructure and targets, sewers above a certain size may be considered to face saboteur or terrorist level threats.

4.5.1 Alternative Approaches for Designing Collection Systems

When planning new collection systems, certain legacy design principles may need to be reconsidered. Mitigating the risks from a malevolent attack on a collection system may be better addressed through alternatives to large service areas with single backbone interceptors.

4.5.1.1 Decentralization

Since the 1970s, with the beginning of federal funding for wastewater infrastructure, the municipal wastewater sector has been focused on centralizing wastewater treatment. During this time, hundreds of individual treatment facilities have been phased-out and replaced by extensive collection systems designed to carry wastewater to large regional treatment facilities for appropriate treatment. This trend increased the vulnerability of wastewater systems to threats from saboteurs and terrorists that may wish to use large-diameter gravity sewers as access ways to commit malevolent acts. Centralized systems also have the additional vulnerability of providing a single-point of failure for the wastewater utility.

Recently, there has been discussion among wastewater professionals about the benefits of decentralized wastewater systems.[22] Much of the impetus for this approach has been to provide more local sources of reclaimed water for reuse without incurring the cost of constructing large collection systems and large reclaimed water distribution systems to bring the reuse water back to communities for disposal. Now, with the increasing concerns for wastewater infrastructure security, decentralization of wastewater facilities also mitigates risks by incorporating smaller-diameter sewers that travel shorter distances, as well as redundant facilities that eliminate the single point-of-failure vulnerability. This trend has already taken hold for many new stormwater systems where runoff is contained within a development and routed to an onsite retention pond.

While decentralization is not a viable option for existing wastewater infrastructure, it may warrant consideration for new development that would otherwise be served by expansion of the collection system. Decentralization may be an approach to mitigate future terrorist threats and assure that portions of the utility's service area remain in service when other portions have service interrupted.

4.5.1.2 Redundancy

When addressing terrorist threats for new collection systems or extensions of existing collection systems, provide redundancy for interceptors and other critical trunk sewers. One alternative is to provide smaller parallel pipes along parallel roads rather than one large gravity sewer that could serve as a single point of failure and also provide easier access through the pipe.

4.5.1.3 Standardization

A utility should develop a standard for sizes and materials used in its collection systems to minimize the need to stock numerous replacement parts and materials and to facilitate replacement of damaged infrastructure. Uncommon pipe sizes and unique pipe materials should be avoided, as should non-standard manholes, catch basins, and force main valves.

---

22 The Water Environment Federation is funding a project titled, "Incorporating Decentralized Wastewater Technologies and Management Into the Practice of Water Resources Planning and Engineering.

4.5.1.4 Other Recommendations

As apparent from the discussions about decentralization and redundancy, mitigating risks to a collection system is expensive, resource intensive, and sometimes counterintuitive. Consequently, the following suggestions are offered for consideration in addressing threats of saboteur and terrorist, and only for new collection systems, replacement of portions of collection systems, or extensions of collection systems.

- Swales and open channels rather than pipes should be used for stormwater conveyance.
- Large-diameter pipe gravity sewers should be replaced with smaller-diameter parallel pipes to discourage persons from crawling through.
- Deeper gravity sewers should be used in the vicinity of other sensitive infrastructure and potential civilian, commercial, and government targets to prevent damage from explosions in sewers and, conversely, to prevent damage to sewers from explosions on the surface.
- The number of manholes, especially in remote areas, should be reduced by increasing the conventional distance between manholes. Traditional design standards of 90 to 120 meters (300 to 400) feet may no longer be necessary with newer maintenance equipment.
- Buried force mains or inverted siphons rather than exposed pipe crossings should be used.

One Sewer Cover per Day Gets Stolen in Budapest

"In the Hungarian capital 120 thousand sewer covers of cast steel and 80 thousand drain-tap gratings are registered by FCSM out of which 105 sewer covers and 267 drain-trap gratings disappeared last year. In addition to the significant financial damage, the uncovered manholes constitute grave risks for accidents: e.g. recently a car has been completely destroyed because it ran into an open man-hole - the driver was lucky to get away with minor injuries."

Source: Aquamedia, Vienna, Austria

4.5.2 Preventing Access into Collection Systems

Misuse of sanitary sewer systems has been a recurring problem for wastewater utilities. Purposeful and unintentional disposal of substances such as oils, pesticides, and herbicides into residential and non-residential sink drains, water closets, and floor drains has caused treatment plant upsets and threatened the health of utility workers. More dramatic, however, has been the dumping of chemical wastes from industrial sources into sewage collection systems, resulting in loss of treatment capabilities and destruction of infrastructure and surrounding properties, such as in Louisville, Kentucky in 1981. Unfortunately, with every wastewater customer being a potential source of dangerous substance entering the collection system, no physical means of preventing such incidents are available. Instead, wastewater utilities have depended upon pretreatment programs, along with sewer ordinances and inspections of non-domestic dischargers' premises and operations and public education programs, to reduce the number of incidents and quantity of non-sanitary sewage that enters the system.

Another misuse of collection systems has been the dumping of wastes from chemical toilets, septic tanks, and grease traps into the sewer via manholes. This type of vandalism or theft, assuming the

reason for the dumping into the manhole is to avoid payment of disposal fees at the treatment plant, can be controlled if not eliminated by securing manhole covers. Securing manhole covers also prevents vandals from removing covers causing hazardous conditions for motorists and pedestrians and discourages thefts of manhole covers by collectors. A few alternatives are available for securing manhole covers to their frames, thereby providing security to the manhole and collection system: tack welds, bolt-type locks, and pan locks.

- Tack welding provides a rapid security measure that can be used where no other means, such as bolting, is available. Utilities have used tack welding to secure manholes prior to visits of dignitaries to prevent IEDs from being placed under the street or to prevent persons hiding in the manholes. Tack welding has also been used in areas of the collection system known for illegal dumping into manholes and areas that are prone to theft of manhole covers. While tack welding requires no excavation or replacement materials, it does make maintenance difficult because welds need to be broken before utility staff can enter the manhole.
- Bolt-type locking devices consist of bolts that anchor the manhole cover to the frame. Bolts are available with various-shaped heads that require specialized wrenches or keys that are restricted for distribution to utilities. Specially manufactured head shapes are also available to assure that the wastewater utility has a unique locking device. The bolt-type devices prevent the cover from being removed, as well as preventing access into the manhole.
- Pan locks prevent access into the manhole as well as preventing dumping into the collection system. However, it does not prevent the manhole cover from being removed. The pan is installed with its rim resting on the manhole cover frame and locked into place with either a padlock or specialized lock. The manhole cover is placed on top of the pan.

Multiple Benefits

Pan-type manhole locks also restrict inflow into the sewer thereby lowering inflow/infiltration.

The DBT should lead to the decision as to whether manholes will be secured and, if so, what method will be used. Welding, bolt-type locks, and pan locks will prevent a vandal, criminal, saboteur, or terrorist from dumping substances into the collection system, as well as restrict personal entry into the manhole. However, pan locks will not protect the manhole cover from being removed by a vandal or stolen by a criminal.

Combined sewer and separate stormwater systems present the additional challenge in that storm drain catch basins and curb inlets are always vulnerable to having liquid substances dumped into them. Persons, however, can be prevented from entering through a catch basin or curb inlet by tack welding grates to frames or securing the grates to the frames with the bolt-type locking devices discussed above. Additionally, choosing grates with smaller openings may discourage saboteurs and terrorists from trying to place IIDs or IEDs into the system.

4.5.3 Force Mains

Sewage force mains present two additional vulnerabilities to the collection system—valves and aboveground crossings. The following recommendations are offered depending upon the DBT.

- Buried force main valves can be secured through the use of bolt-type locks on the valve box cover should the DBT be based upon a saboteur or terrorist threat category.
- Exposed valves, such as air-release valves on bridge crossings, may be subject to vandals as well and can be secured by a perimeter fence or other metal enclosure.
- Exposed force mains on bridges should be placed so that the mains are not easily accessible from the roadway, and access along the pipe can be restricted through a fan-shaped fence with or without barbed or razor wire where the pipeline begins its crossing.
- For a DBT at a saboteur or terrorist category, consider installing exposed force mains in a casing pipe.
- Where possible, boring or tunneling should be employed to eliminate the need for hanging force mains from bridges or otherwise exposing the pipe in a separate crossing.

4.5.4 Culverts

Large diameter culverts and large box culverts that carry stormwater under major roads can provide a hidden location for an explosive and a haven for saboteurs or terrorists. For saboteur and terrorist threat categories, the following design modifications to culverts should be considered.

- Horizontal bars can be positioned across the inlet and outlet openings of the culvert. The horizontal bars can be secured using vertical bars if the length of the horizontal bars results in insufficient strength.
- A 6-inch clear opening should be provided at the bottom of the inlet and outlet to facilitate flow and avoid a buildup of debris.
- Both inlets and outlets should be designed for easy access for frequent maintenance and clearing away of debris.

4.5.5 Deep Tunnels

By their very nature, deep tunnels are typically 100 meters (328 feet), more or less, underground and bored through rock. Thus, they do not provide a preferable location for an adversary to place an explosive device to damage or destroy buildings or other infrastructure on the surface, or even create significant damage to the tunnel itself. Deep tunnels, which may be more than 10 meters (33 feet) in diameter do, however, provide a virtual freeway for adversaries to gain underground access throughout a large portion of a city because the water level is usually shallow except during rain events. Under all threat categories, entry to access shafts should be locked and intrusion control monitored. For saboteur and terrorist threat categories, the following countermeasures should be considered:

- Adequate lighting and ventilation should be provided in access shafts to facilitate inspections.
- Installation of motion detectors in access shafts should be considered.
- Installation of video motion detection systems or thermal imaging devices (see Section 6.3.4) in access shafts and tunnels should be considered. Cameras and other equipment can be mounted in corrosion-resistant enclosures.

.