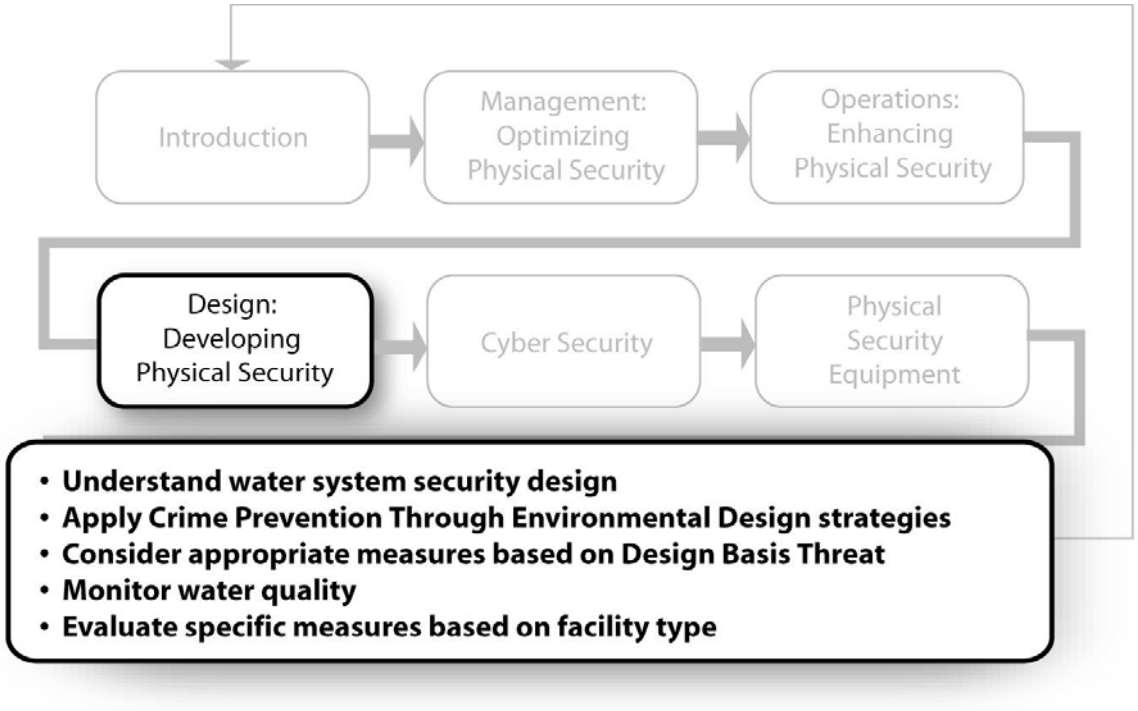
SECTION 4

Design Considerations for Developing Physical Security at New Facilities and Retrofits



4.1 Overview

The objective of this section is to provide guidance that enables water utility decision-makers and designers to develop secure sites and facilities. Because water systems cannot be made immune to all possible attacks, system design needs to address issues of critical asset redundancy, monitoring, response, and recovery to minimize risk to the utility. All public water supplies can identify and address security needs in the design and construction of new projects and retrofits of existing systems.

The considerations presented in this section are for the purpose of increasing security and reducing risk, and are applicable to designs of new facilities, water infrastructure upgrades, expansions of existing infrastructure, and retrofitting of existing infrastructure. This section addresses the delay and denial protective measures that should be coupled with detection and assessment technology.

Attacks targeting command, communications, and control systems, referred to as cyber attacks, are addressed in the Section 5, "Cyber Security Management, Operations, and Design Considerations," although physical attacks by those adversaries to gain access to the facilities housing cyber systems can be protected using measures described in this section.

The significant capabilities of an adversary pose challenges to any security system. Though complete protection against an attack may not be achievable, actions taken to lessen the effects of an attack can significantly reduce the damage caused by less capable adversaries.

4.2 Security System Design

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

Identification and characterization of assets is based on consideration of the mission and the resources required for performance. 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 adversaries) and prioritized based on their criticality. For example, 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 compromising the system to accomplish their objectives.

This section provides a number of key design considerations and criteria to be used when designing a security system for large, medium, and small water utilities. Design considerations are divided into Basic and Advanced Categories, with future considerations included where applicable. It includes information about the criteria used to evaluate designs as well as recommendations for the design team based on threat level and adversary.

4.2.1 Design Team Requirements

The utility should consider including design team members with demonstrated knowledge of, at a minimum, the following methods of protecting a facility:

- Securing the site perimeter.
- Regulating the avenues of approach to the building through the use of architectural design elements such as barriers and obstacles.
- Creating sufficient setback.
- Building hardening to mitigate potential blast damage.
- Using progressive collapse mitigation measures.
- Addressing envelope security appropriate openings, hardware, and site flow.
- Applying HVAC mitigation measures versus the risk associated with chemical, biological, and radiological threats.

- Protecting utility systems (indoor and outdoor) from intentional or unintentional damage, tampering, and accidents. This also includes safeguarding communications systems so they can be used in an emergency.
- Controlling building access by using barriers, keys, keypad systems, access cards, smart cards, or biometrics, as appropriate.
- Protecting high-risk spaces within the building, such as hazardous material storage rooms, loading docks, and laboratories.

4.2.2 Basic Design Considerations – "10 States Standards"

Utilities may want to consider applying the following water system security design guidance taken from the "Recommended Standards for Water Works" developed by the Great Lakes – Upper Mississippi River Board of State and Provincial Public Health and Environmental Managers. This document, which is also known as the "10 States Standards," may be considered an industry standard that utilities can implement to potentially limit liability.

- Security should be an integral part of drinking water system design. Facility layout should consider critical system assets and the physical security needs for these assets. Requirements for submitting, identifying, and disclosing security features of the design, and the confidentiality of the submission and regulatory review should be discussed with the reviewing authority.
- The design should identify and evaluate single points of failure that could render a system unable to meet its design basis. Redundancy (geographically separated) and enhanced security features should be incorporated into the design to eliminate single points of failure when possible, or to protect them when they cannot reasonably be eliminated.
- Critical components that comprise single points of failure (e.g., high volume pumps) that cannot be eliminated should be identified during design and given special consideration. Consideration should be made to ensure effective response and timely replacement of critical components that are damaged or destroyed. Design considerations should include component standardization, availability of replacements and key parts, re-procurement lead times, identification of suppliers, and secure retention of component specifications and fabrication drawings. Readily replaceable components should be used whenever possible and provisions should be made for maintaining an inventory of critical parts.
- Human access should be through controlled locations only. Per the 10 States Standards, intrusion deterrence measures (e.g., physical barriers such as fences, window grates, and security doors; traffic flow and check-in points; effective lighting; and lines of sight) should be incorporated into the facility design to protect critical assets and security sensitive areas. Effective intrusion detection should be included in the system design and operation to protect critical assets and security sensitive areas. All cameras and alarms installed for security purposes should include monitors at manned locations.

- Vehicle access should be through controlled locations only. Physical barriers such as moveable barriers or ramps should be included in designs to keep vehicles away from critical assets and sensitive areas. It should be very difficult for a vehicle to be driven either intentionally or accidentally into or adjacent to finished water storage or critical components without facility involvement. Designated vehicle areas such as parking lots and drives should be separated from critical assets with adequate standoff distances to eliminate or minimize impacts to these assets from possible explosions of material carried in vehicles.
- Sturdy, weatherproof, locking hardware should be included in the design of access for all tanks, vaults, wells, well houses, pump houses, buildings, power stations, transformers, chemical storage, delivery areas, chemical fill pipes, and similar facilities. Vents and overflows should be hardened through use of baffles or other means to prevent their use for the introduction of contaminants.
- Computer-based control technologies such as SCADA should be secured from unauthorized physical access and potential cyber attacks. Wireless and network-based communications should be encrypted as deterrence to hijacking by unauthorized personnel. Vigorous computer access and virus protection protocols should be built into computer control systems. Effective data recovery hardware and operating protocols should be employed and exercised on a regular basis. All automated control systems should be equipped with manual overrides to provide the option to operate manually. The procedures for manual operation include a regular schedule for exercising and ensuring an operator's competence with the manual override systems should be included in facility operation plans.
- Per the 10 States Standards, real-time water quality monitoring with continuous recording and alarms should be considered at key locations to provide early warning of possible intentional contamination events.
- Facilities and procedures for delivery, handling, and storage of chemicals should be designed to minimize the chance that chemicals delivered to and used at the facility can be intentionally released, introduced, or otherwise used to debilitate a water system, its personnel, or the public. Particular attention should be given to potentially harmful chemicals used in treatment processes (e.g., strong acids and bases, toxic gases, and incompatible chemicals) and on maintenance chemicals that may be stored onsite (e.g., fuels, herbicides, paints, and solvents).

In designing physical protection systems, it is important NOT to interfere with life safety, occupational safety, and fire protection provisions. Security systems can be balanced with and complementary to other design criteria and requirements as well as the overall operability and maintainability of the water system.

4.2.3 Balanced Approach to Security System Design

When developing a security design, it is important that a balance between hardware and procedural elements be adopted. A balanced approach would consider the following:

- To be effective, physical protection (doors, alarms, cameras, etc.) should also include policies and procedures designed to keep the physical protection systems functioning as intended. For example, an alarm system on doors does little good if the doors are routinely propped open.
- As discussed in Section 2, "Management Considerations for Enhancing Physical Security," and Section 3, "Operational Considerations for Enhancing Physical Security," security policies and procedures can be cost-effective in reducing risk.
- Without staff commitment to the security program, the program will not be effective.

4.2.4 Layers of Protection

Layered security systems are essential. They are built on the "protection in depth" principle, which requires that an adversary defeat several protective barriers or security layers to accomplish its goal. In addition, balanced protection implies that no matter how an adversary attempts to accomplish his goal, he will encounter effective elements of the physical protection system.

For example, as depicted in Figure 4-1, an effective security layering approach requires that an adversary penetrate multiple, separate barriers to gain entry to a critical asset at a water facility. Protection in depth helps to ensure that the security system remains effective in the event of a failure or an adversary bypassing a single layer of security. If funding is a limitation, utilities can add multiple layers as funds are available to increase security at each critical asset.

For each facility, multiple layers of security protection should be considered. To provide multiple layers, perimeter intrusion detection methods should be placed at the outer edges of the asset boundary, and delays should be located as close to the edge as possible. In this way, the security system can generate an early alarm in the event of intrusion of a facility, while delaying an adversary as it attempts to reach the intended target.

The layered approach starts with the outer perimeter of the facility and goes inward to the facility site, the buildings, structures, other individual assets, and finally to the contents of those buildings, structures, and assets. Approaching security in this manner allows utilities to incorporate additional layers of physical security to match the threat that may be associated with specific assets at the facility. For example, the perimeter of the facility typically includes the fence and access gates that surround the site. The perimeter is considered the first line of the physical security system that, through operational practices, can be sufficient for basic, low-level threats such as vandals.

The site is the area between the perimeter and the buildings, structures, and other individual assets. This open space provides a unique opportunity for early identification of an unauthorized intruder and initiation of early response. This space is used to calculate the standoff distance, that is, the distance between the outside perimeter (the public areas) to critical facilities or buildings inside the perimeter (the restricted access area).

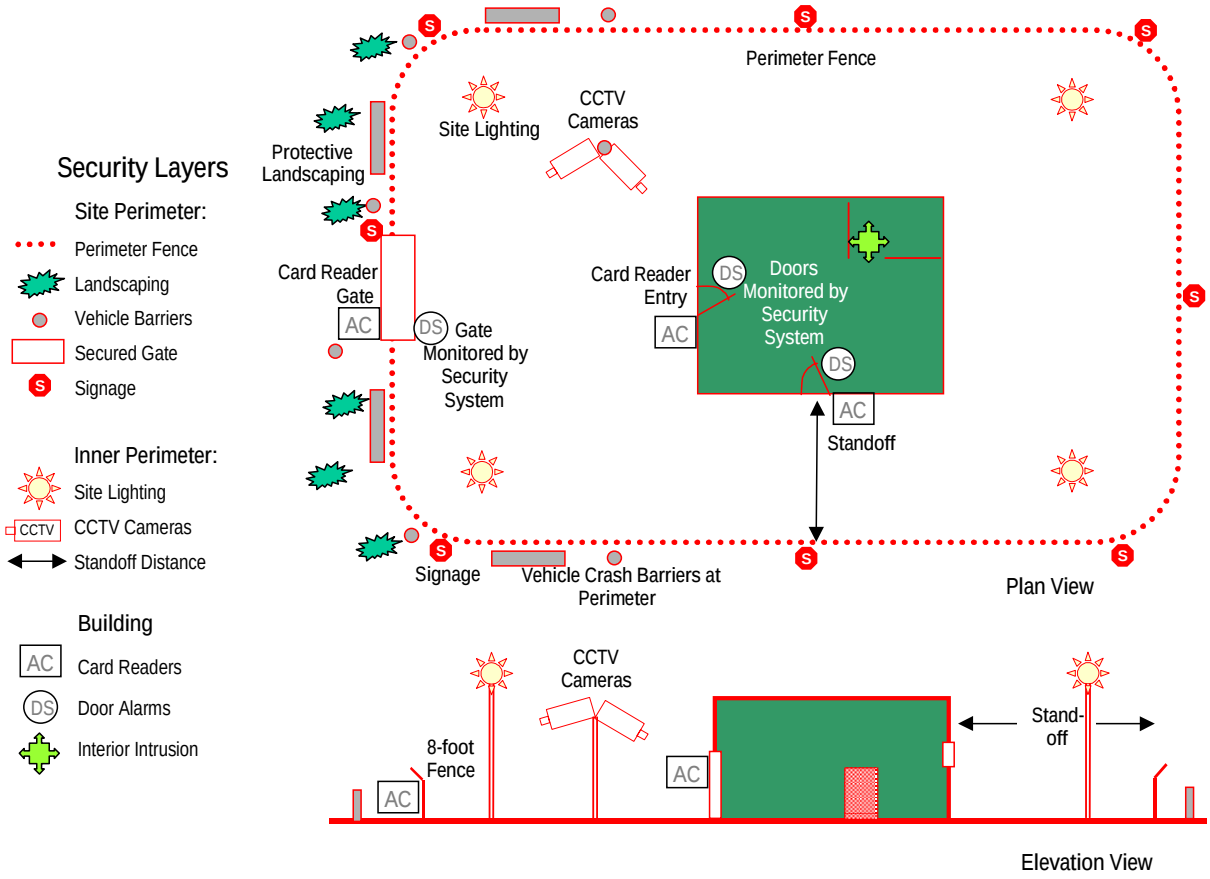


FIGURE 4-1
Sample Layered Security Recommendations for a Facility

The buildings and structures within a facility, such as an operations center, provide the next physical barrier for stopping intruders. The discussion of buildings and structures is limited to the external features, such as doors, windows, walls, materials, and skylights.

Building systems refer to the internal features of buildings and other structures that can provide physical security from intruders to protect critical assets or processes. Examples of these types of features include internal walls and doors, equipment cages, and redundant equipment.

Table 4-1 provides general considerations for operational practices for the different layers within a facility for the key threat levels.

TABLE 4-1
General Considerations for Physical Security at a Water Facility

Type Threat	Perimeter	Site	Building Envelope	Building Systems
Vandal	Fencing with barbed wire Locked gates No Trespassing signage	Clearzone Standoff distance Illuminated site areas with 6:1 light-to-dark ratio	Key-locked buildings 24/7 Illuminated building exterior Door ajar status alarm monitoring	Vandal-resistant materials, such as composite plastics, lights with low-profile lenses, locks, cages
Criminal	In addition to above: Well-lit parking areas	In addition to the above: Emergency telephones	In addition to the above: Signage that does not describe assets Visitor waiting area Facility access control CCTV at vehicle gate CCTV at building entrances	In addition to the above: Bars on windows Security deadbolts on door locks Shatter-resistant glazing on glass
Saboteur/ Terrorist	In addition to the above: Increased fence height Perimeter vehicle barriers Increased CCTV at site perimeter	In addition to the above: Increased standoff distance Secondary fencing around assets/facility Vehicle inspection entry with guard house and sally port CCTV at vehicle inspection entry Secured utility connections	In addition to the above: Turnstile personnel entry Motion-activated lighting Area presence sensors Increased CCTV at building perimeter CCTV at building interior	In addition to the above: Forced-entry resistant materials Bomb-resistant glazing and door materials Blast walls at large windows and entrances Protected HVAC intakes

4.2.5 Cost Implications

Utilities, like most organizations, are required to use their financial resources wisely. This section focuses on the considerations for effectively applying a utility's resources on security.

4.2.5.1 Threat Levels versus Cost

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 against high-level threats may (or may not) provide sufficient protection against low-level threats, but utilities may want to consider all types of threats during a 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 detect and delay an attack for the most probable adversary.

The vulnerability assessment considers the routes and means used to attack and to protect the asset from attack. A vulnerability assessment may consider features and effectiveness of a existing facilities or, as a design tool for new facilities, may consider how access can be gained to an asset, how the asset may be compromised or destroyed, and similar considerations. The consequences of a successful attack can also be considered when weighing the cost and impact of implementing appropriate physical protective measures. 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, no mission disruption, nor 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.

Identification of the DBT for a facility/asset/organization is an important management decision that requires the input of various operational and management level personnel. The DBT has a potentially significant impact on the cost and complexity of a security program that supports the utility's mission.

4.2.5.2 Ensuring Security Investments are Effective

Typically, developing a vulnerability assessment involves defining a list of vulnerabilities and potential improvements, ranked according to the potential risk. When presented with this list, utilities contemplate what level of protection is acceptable and how many of the recommendations to implement. In prioritizing security investments, utilities typically attempt to balance the external demand for security with the limited internal resources available to implement security measures. In addition to the legal considerations described in Section 1, "Introduction," there are other considerations that may be addressed in answering this question.

A cost-benefit analysis can be performed for security improvements, as is commonly done for other engineering alternative evaluations. A cost-benefit evaluation is most robust if benefits can be readily quantified, and it is less effective when benefits are not easily converted to monetary terms. For example, the cost of improvements in physical security (such as improved locks, alarms, and fencing) can be compared to the value of avoided vandalism damages, yet it is difficult to quantify the value of lives saved.

Security improvements can also be prioritized by comparing the cost to implement a security measure against the degree of risk reduction that the measure would provide. For risk assessment methodologies such as RAM-W™, the amount of risk reduction can be expressed numerically by determining the risk score for an asset before and after the proposed security improvement. A cost-to-risk-reduction curve can be generated (as shown in Figure 1-5), and a determination can be made as to the measures that should be implemented by identifying the "knee of the curve," or the point at which the risk reduction associated with implementing additional costly security measures becomes marginal.

Reducing all components of a water system's risk in the case of a terrorist attack to low is, therefore, not practical. Rather than attempt to reduce all risks to low, the utility would be better served by implementing improvements that reduce risk to all critical facilities to medium. The resources saved could be used to improve response in the case of an event. Thus, protection of the water system mission could be strengthened by a combination of physical protection improvements to prevent an attack and improved response, helping to ensure continued delivery of quality water in the event of an attack.

A utility may choose to implement a security plan over multiple years, depending on funding demands and current revenues. Utility management teams need to develop an implementation plan that fits the projected financial conditions relative to the timeframe chosen for implementation. Implementing security policies and procedures such as background checks, key control, and alarm response procedures are usually relatively low in cost and often implemented first as part of a holistic approach. When designing physical security for a new facility or a facility retrofit, improvements can be prioritized in the following order, working from the outside perimeter to critical assets: perimeter (e.g., fence, signs), site (e.g., additional lighting, video surveillance for alarm assessment), facility (e.g., buildings and valve vaults with locks, alarms, and motion sensors), video surveillance for alarm assessment, and building systems (e.g., to fix glass doors and windows, install tamper-resistant door hardware).

4.3 Crime Prevention Through Environmental Design

Crime Prevention Through Environmental Design (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. Deterrence is typically not considered in vulnerability assessment methodologies such as RAM-W™, but deterrence can be a method to reduce risk. The concepts embodied in CPTED strategies may be applied to all facilities, regardless of specific threats, resulting in enhanced security as an integral part of design. Because CPTED strategies may be widely and cost-effectively implemented as prudent measures regardless of specific threats, they should be considered among the basic design considerations for new, upgraded, and expanded water 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 judicious placement of entrances, exits, landscaping, lighting, and control devices (e.g., guard stations and turnstiles).
- **Territorial reinforcement.** Physical attributes that express ownership, reinforce territoriality, designating 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 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 ground maintenance also sustains surveillance. Image and maintenance activities are most often related to management and operations rather than design.

The following CPTED strategies should be considered for the design of water system facilities. As with the other strategies in this document, each should be evaluated for its specific applicability to a utility's needs before implementation.

4.3.1 Perimeter CPTED Strategies

- Provide outside 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.
- Create gateways or formal entrances delineated by plantings, different paving materials, fencing, and gates to separate public areas from controlled areas.
- Define vehicle entrances by different paving materials and signage.
- Avoid opaque fencing, landscaping, and walls that might provide hiding places along the perimeter.

4.3.2 Site CPTED Strategies

- Avoid dead-end driveways and pathways.
- Provide outside 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 by building occupants, especially from a reception area (if one is planned), operations center, 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 or storage yards).
- Plan storage yards for visual and/or vehicular access by patrol cars and/or facilities staff, 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, and Spanish bayonet).
- Include highly visible, appropriate signage, but do not describe the asset or facility function on the signs. Use building numbers rather than names that could identify potential asset locations.

4.3.3 CPTED Strategies for Building Envelope and Other Structures

- Design entrances to be well-lit, well-defined, and visible to public areas, facilities staff, and/or patrol vehicles.
- Place elevators close to main entrances. The entire 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.

4.4 Recommendations by Threat Level

The measures discussed in this section can provide specific and measurable results if implemented as part of a comprehensive physical protection system. As noted, detection, delay, and 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 attack through application of target-hardening enhancements. This section recommends protective measures that may be most appropriate for the specific threats identified in Section 1: vandal, criminal, saboteur, and terrorist.

The measures indicated within this section 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. In addition, some recommended measures were developed from the following: The Design and Evaluation of Physical Protection Systems by Mary Lynn Garcia and course materials presented in the "Physical Protections Systems Training Course," offered by CH2M HILL.

These measures are listed as general guidelines. The specific DBT for a facility affects the implementation or selection of these measures, which in turn impacts implementation cost. For example, a minimum 25- or 50-foot standoff distance from an asset is included as a default distance where space allows. For high threat levels (very large quantities of explosives), this distance 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. Explosive 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 considerations 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 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. Figure 4-2 depicts the recommendation that the design of all water facilities include CPTED strategies, and that for increasing threats additional considerations are recommended to be added to the design.

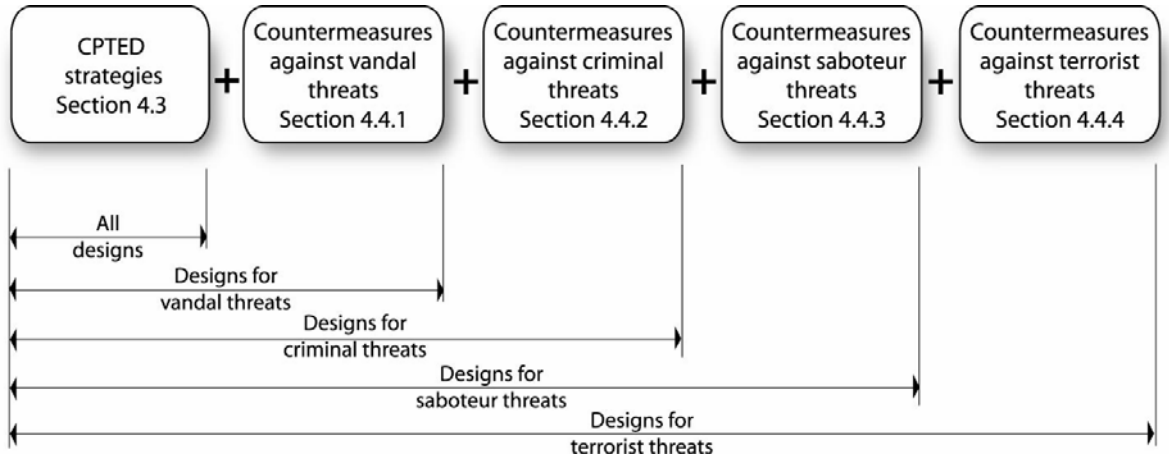


FIGURE 4-2
Recommendations for Progressive Design Consideration

4.4.1 Countermeasures Against Vandal Threats

Vandals typically use basic hand tools, such as pliers, wire cutters, hammers, crowbars, and baseball bats, to gain access to assets. They may also damage facilities using fire crackers, fuel to start fires, improvised incendiary devices (IIDs), and spray paint. 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 can be considered.

4.4.1.1 Perimeter Zone

- Provide 6-foot perimeter fencing with three-strand barbed wire and break-away stanchions. Consider high-quality fencing, but it does not have to be specifically rated for vehicle crash-resistance.
- Establish a 25-foot minimum (preferably 50-foot or greater) standoff distance from perimeter fencing to the facility structure.
- Establish an 8-foot clearzone region on either side of fence. This should be an important consideration of the landscaping design.
- Within the clearzone region adjacent to the fence, there should be no planted material or landscape feature that is taller than 24 inches or wider than 15 inches at full maturity.

Tips for Small Utilities

If a particular facility experiences frequent acts of vandalism, consider renting and temporarily mounting a small CCTV system. The camera images may then be shown to police and parents in the area. In many cases, the troublemakers live nearby and will stop if the police confront them with camera evidence. When the vandalism stops, the system may be removed and returned or used at another site.

- If visual screening of the facility is desired outside the fenced perimeter, provide appropriate landscaping no closer than 10 feet from fence. Verify that vegetation at full maturity will not provide climbing advantage to an adversary attempting to enter site property.
- Provide 12-foot double swing gates for vehicle access, manually opened (non-electric).
- Close entrance gates and lock with a shackle-protected padlock (as shown in Figure 4-3).
- Provide exterior shackle-protected padlocks that are weather resistant, with 4,500 lbs. of resistance against pulling shackle attacks and resistant to 10,000 lbs. minimum pressure from bolt cutter attacks.

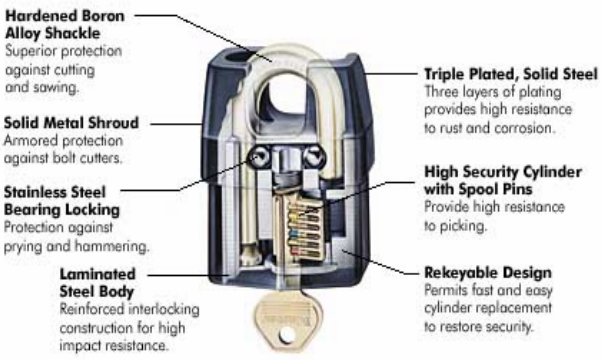


FIGURE 4-3
Example of a Tamper-proof, Shackle-protected Lock

- Post "No Trespassing" signage at appropriate intervals (a minimum of every 50 feet) on perimeter fencing. Install signs that read "Trespassers Will Be Prosecuted" and "Video Surveillance." Follow local municipal ordinances, and state and federal regulations in installing signs. Depending on the diversity of the population, multi-lingual signs may be required. (Signs mainly serve as deterrence to low-level threats such as vandalism.)

4.4.1.2 Site Zone

- For the standoff region between facility exterior and perimeter fence, use appropriate landscaping vegetation, i.e., no taller than 24 inches or wider than 15 inches, with a density of less than 15 percent of landscaped region at full maturity.
- No specific vehicle control measures are recommended because a locked main gate prevents public vehicles from accessing site.
- Provide lighting in the site yard area between the facility and the fenced perimeter that is 1 foot-candle, minimum.
- Provide lighting at entrance gates, roadway, and perimeter door entrances that is 2 foot-candles, minimum.
- Provide a minimum light-to-dark illumination ratio of no greater than 6:1, and preferably 4:1, for all lighting.

4.4.1.3 Building Envelope and Other Structures

- Lock exterior doors with a deadbolt cylinder keylock during business and after hours.
- Use hardened steel inserts on keylocks to protect plug face, shell, and sidebar, and for drilling attack resistance.
- Provide facility exterior lighting that is 1 foot-candle, minimum.
- Locate door status switches at perimeter doors to monitor for door ajar and door forced-open conditions. Use a high-security, balanced magnetic switch.

4.4.1.4 Building Systems

- 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 that are subject to graffiti.
- Use solvents specially designed to remove graffiti made using paint, lipstick, felt-tip pens, and oil; solvents are available for easy-to-clean or untreated surfaces.
- Use rough-textured bricks, blocks, or rough concrete surfaces to resist damage. These could present a challenge to vandals, although they are difficult to clean.
- Use climb-resistant cages around exterior ladders.
- Locate luminaries beyond reach, placing them on high posts or high on building walls.
- Locate lighting equipment away from hidden corners or behind buildings to discourage tampering.

- 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.
- Consider shatter-resistant plastic materials such as polycarbonate instead of glass.
- Select exterior furnishings of strong, vandal-resistant construction that are free of easily removed or projecting parts and 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 tamper-proof fastenings.
- Use materials that are nonflammable.

4.4.1.5 Critical Assets

- Provide locked security cages around meters and exposed valves or fittings. Use vandal-resistant locks.
- Fence the top of smaller site elements to completely enclose critical areas within the site.
- Provide status switch alarms on all hatches or vault covers to monitor for forced-open conditions.

4.4.2 Countermeasures Against Criminal Threats

The criminal threat includes weapons such as knives and handguns, as well as hand and power tools. To accomplish criminals' objective of using stealth, power tools are unlikely to be employed except by criminal threats that 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 security systems considered to deter vandalism, consider the following.

4.4.2.1 Perimeter Zone

The measures that can be applied to the perimeter zone for a criminal threat are the same as those that can be applied for a vandal threat (see Section 4.4.1.1, "Perimeter Zone").

4.4.2.1 Site Zone

- Provide emergency telephones throughout site, enabling staff to summon emergency help. Another option would be to provide operations staff with panic buttons that immediately summon emergency help when activated.
- Bury or otherwise protect conduits and wires carrying electric supply, telecommunications, and alarm signals.

4.4.2.2 Building Envelope 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 the asset or reason for the restriction.
- Provide a waiting area for visitors.
- Provide a facility access control system that:
  - Monitors perimeter openings (personnel doors, rollup doors, and roof hatches) and locked interior doors for door ajar status.
  - Establishes a primary entrance door and adds access control, a visitor intercom, and video surveillance equipment.
  - Identifies critical exterior circulation doors. These doors should be designated as access-controlled doors and should be accessible only by employees. Access-control methods could consist of adding key locks, keypads, or card readers with or without entering a personal identification number (PIN) for entry.
  - Designates remaining doors without exterior access control as exit-only. Exterior door hardware from exit-only doors is removed. Appropriate exit hardware remains on the interior side of the doors, allowing free egress under emergency conditions.
  - Establishes a secure lobby area, with hardened doors capable of being activated by security to go to "lock-down" mode.
- Consider adding layered access control to high-value areas within the facility (such as SCADA rooms).
- Segment access control such that only employees requiring access to high-value areas are permitted access, rather than all employees having access to all areas.

4.4.2.3 Building Systems

- Locate door locks minimum of 40 inches from adjacent windows.
- Use single-cylinder dead bolt locks with minimum 1-inch throw on primary ground floor exits.
- Equip solid exterior doors with 180-degree door viewers.
- Minimize windows, including those in glazed entrance doors.
- Use shatter-resistant glazing materials.
- Use two locking devices on all windows.
- Consider installing bars or grilles inside windows.
- If DBT includes the potential to threaten people with handguns, provide bullet-resistant construction assemblies (e.g., walls, windows, and doors) in those areas. For example, provide bullet-resistant prefabricated guard shelters, control rooms, or bill-paying booths for accounts receivables areas.

4.4.2.4 CCTV Surveillance

- Provide CCTV camera system, with integration to security access control system. In an ideal setup, CCTV video images would be viewed directly on the access control computer workstation monitors, with alarm images called up and displayed automatically during security events using a single program.
- Suggested Camera Locations:
  - Vehicle Gate: Provide a minimum of one color, fixed-position camera viewing each vehicle entrance gate. Position camera to view car, driver, and vehicle license plate. Image target (incoming vehicle) typically occupies a minimum of 25 percent of image scene.
  - Building Entrances: Provide a minimum of one color, fixed-position camera at each exterior door viewing incoming personnel entering facility. Image target (entering personnel) to occupy minimum of 25 percent of image scene.

Tips for Small Utilities

When contemplating a small CCTV camera system at a remote site, consider cameras having integral hard disks which can store images locally at the site, reducing the need for costly cabling and communications back to the security headquarters. During an alarm condition, these cameras can signal the security or SCADA system that a security alarm event is occurring, and responders can view and retrieve video onsite.

4.4.2.5 Critical Assets

- Locate critical assets and functions to the interior of facilities to maximize layers of delay between access points and assets. The assets should be in 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.

4.4.3 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 security systems in addition to those for the vandal and criminal threats.

4.4.3.1 Perimeter Zone

- Increase fencing height to 8 feet, with 3-strand barbed wire and helical razor wire as top dressing with break-away stanchions.
- Provide secondary secure fencing (anti-climb) around critical assets or primary facilities.

- Increase standoff distance. If conventional building construction is used, the standoff zone is generally a minimum of 45 meters (148 feet)[5] 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[6] and the Army's IED Safe Standoff Distance Cheat Sheet[7] for further guidance.
- Control access to sites by unauthorized vehicles through use of an entry control point for vehicular and pedestrian traffic (Figure 4-4). An effective entry control point provides these features:
  - 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, including bomb detection equipment, for inspection of vehicles and their contents
  - 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
  - Crash-resistant gate
  - A telephone or intercom
  - Dual-vehicle entrance gate to eliminate tailgating (where a second vehicle, bicycle, or person on foot enters after the first vehicle)

FIGURE 4-4
Entry Control Point with Protected Guardhouse

- Design entry control points to provide unimpeded access by emergency vehicles (e.g., fire-rescue, police, ambulance).
- Provide vehicle barriers surrounding perimeter of site, capable of stopping a 4,000-pound vehicle traveling at 30 miles per hour within 5 feet or less.
  - Vehicle barriers to resist moving vehicles can be designed for the vehicle weight, including explosives carried, and the speed at which the vehicle may be traveling. The location of the barrier can 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.

---

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

6 *Ibid.*

7 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 can be used.

Active barriers that resist ramming include:

- "Pop-up" bollards
- Hydraulic ramp, wedge, and plate barriers
- Manual plate barriers
- Portable crash barriers

Tips for Small Utilities

Installing landscaping boulders around perimeter areas can serve as a cost-effective and attractive yet practical vehicle barrier.

Passive barriers that resist ramming include:

- Aircraft cable barriers that may be integrated into the perimeter fence. Aircraft cable should have anchorage and foundation systems designed to resist the forces of moving vehicles loaded with explosives (Figure 4-5).
- Landforms and landscaping elements such as ditches, berms, heavy vegetation, boulders, bollards (designed to resist vehicle ramming), and 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.

FIGURE 4-5
Perimeter Fence with Aircraft Cable Anchored to Concrete

4.4.3.2 Site Zone

- 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 100 feet stand-off distance around occupied facilities and the critical assets that may be 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, pipes, or 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.

4.4.3.3 Building Envelope and Other Structures

- Use forced entry-resistant window and door assemblies. Assemblies can 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, and hinges.
- If a magnetic lock is installed at a facility door, the 2000 edition of National Fire Protection Association (NFPA) 101, Life Safety Code, Section 7.2.1.8.2 requires a request-to-exit motion sensor and a push-to-exit button at the door. The security panel should have a connection to the facility's fire alarm panel (if there is one onsite).

4.4.3.4 CCTV Surveillance

No cameras are provided for general site surveillance. However, if general surveillance capabilities are desired, provide one pan/tilt/zoom color camera with a minimum of three presets for viewing site conditions from a remote location.

Suggested camera locations for vehicle gates and building entrances are the same as those that can be applied for a criminal threat (see Section 4.4.2.4, "CCTV Surveillance").

4.4.4 Countermeasures Against Terrorist Threats

Unless a 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; rocket propelled grenades (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 improvements relative to the utility's DBT.

4.4.4.1 Perimeter Zone

- Establish a "no stopping" zone along the roadway serving the facility, with appropriate signage. Security personnel or local law enforcement can monitor and patrol the roadway and have stopped or parked vehicles towed.
- Provide a security checkpoint with guards and electronic access control equipment to search vehicles travelling within the standoff zone.

  - The security checkpoint can consist of a guardhouse adjacent to 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.
  - Provide bullet-resistant guardhouses with toilet facilities and weather protection. Barriers can prevent a vehicle from penetrating the gate or crashing into the guardhouse.
  - Install a video surveillance system at the sally port.
- To reduce search requirements, exempt authorized personnel with appropriate credentials (personal and vehicle IDs that are linked in databases for validation) and who have had background checks.
- Require pedestrians to pass through a high-security turnstile (which may be used to entrap potential adversaries failing validation of identification). Other options include providing a location to detain unauthorized persons and their vehicles.
- During unmanned periods, crash-resistant gates can be used. A telephone can be provided for use by on-call personnel for entry, if required.

4.4.4.2 Site Zone

- Locate assets away from vantage points from where weapons such as RPGs may be fired.
- Provide pre-detonation screens at site perimeter between assets and vantage points. If provided, 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 area to allow location of receiving areas to be a minimum of 100 feet away from occupied facilities or 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.
- Park vehicles in publicly accessible spaces at least 100 feet from the structure.
- Locate areas for dumpsters and trash barrels as far away from asset locations as practical.
- Provide motion-activated lighting at the building perimeter and site yard for “instant-on“ from nominal 1.0 foot-candle illumination to 5 foot-candle illumination under motion activity.
- For alarm assessment, provide a minimum of one color, fixed-position camera viewing each alarmed site element (hatch, substation, etc.). Position camera to view protected asset and attacker. Image target (attacker) to occupy 30 percent of image scene.
- For parking lot surveillance, provide a minimum of two color, low-light capable, fixed-position cameras for viewing parking areas. Position camera to serve an approximately 200-foot by 100-foot field of view. Provide sufficient cameras to monitor entire parking lot areas.

- For site surveillance, provide a minimum of one color, low-light capable, pan/tilt/zoom camera with a minimum of three presets for viewing site conditions from a remote location. Camera to serve approximately 200-foot by 200-foot region. Add cameras as necessary to serve entire site.
- Provide site intrusion detection system, using one of three sensor technologies as applicable to site conditions: microwave, buried cable, or fence-mounted.

4.4.4.3 Building Envelope and Other Structures

- Provide area presence sensors within the interior spaces to monitor for unauthorized presence of personnel within the building. Presence sensors to be dual technology (passive infrared and microwave) high-security sensors.
- Install area presence sensors approximately every 75 feet within the building interior and at critical corridor intersections.
- Install interior detector sensors that meet Underwriters Laboratory (UL) Standard UL639, Intrusion Detection Units (http://ulstandardsinfonet.ul.com/scopes/0639.html).
- Provide push-button duress system for signaling operator assistance. When an operator who is threatened or under attack presses the duress button, the security system is notified that there is a security condition alert, and response personnel are dispatched to the scene to investigate.

4.4.4.4 Building Systems

- Locate blast walls behind entrances and large windows to prevent glass shards from penetrating building interiors.
- Design building systems to resist blast and aerosol contamination attacks that may be included in the DBT.
- Isolate areas where bombs could be received, including loading docks, mail rooms, storage areas, and lobbies. If provided, isolation should be accommodated in both structural and mechanical systems. Provide vestibules at entries.
- Locate air intakes high (a minimum of 10 feet above grade) in building walls to prevent contaminants from being introduced. Verify that equipment, loading docks, trash receptacles, ladders, and other building or site appurtenances do not allow access to air intakes. Where locating air intakes away from these items is not feasible, move air intakes to higher elevations.
- Provide breathing mask dispensers in convenient locations.
- 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 HVAC system is shut down.
- Where a chemical, biological, or radiological (CBR) release at some distance from a facility is part of the DBT, design facility for air tightness or pressurize facility to limit infiltration.

- Establish a protected clearzone around ground-level or low air intake openings with entry restricted to authorized personnel only. Clearzone may be fenced or walled (provisions for air circulation required by air intake and HVAC equipment should be considered). Illuminate and monitor the clearzone (guard patrols or CCTV).
- Provide grilles with openings no larger than 6 inches in diameter (both intake and return air). Grilles should be forced-entry resistant and anchored firmly into the 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, especially with respect to egress areas, and that may be targeted by contamination tactics, automatic shut-off switches to zones or facilities, and pressurization and airflow control. "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 should 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 filters, and reduce airflow. Refer to National Institute of Occupational Safety and Health (NIOSH) guidelines for more considerations and information.

4.5 Water Quality Monitoring

The use of water quality monitoring systems for security purposes is a relatively new and, currently, relatively rare application among water utilities. Thus, guidance for the design of water quality monitoring systems, that is, early warning systems (EWSs), is rather limited. Despite the extent of information gaps in the design of EWSs, some utilities are proceeding in installing EWSs in their

utilities. These can be considered best-in-class utilities and their experiences are helping the development of industry-standard practices and guidance for other utilities.

As mentioned in Section 3, "Operational Considerations for Enhancing Physical Security," there are three key documents that provide information on the subject. They are Grayman, et al. (2001) for source water, Pikus (in press) for distribution systems, and Hergesheimer, et al. (2002) for both. These documents provided information for the guidance provided here.

The reasons for installing EWSs can be summarized as follows:

- They should detect accidental or intentional contamination of the water supply by chemical (including biotoxins), biological, and radiological contaminants early enough to take countermeasures, if possible.
- The consequences of contamination would put public and employee health, public confidence, and regulatory compliance at risk.
- There should be as few false positives and false negatives as possible.
- They should be affordable and cover as many customers as possible.

To meet these objectives, the factors discussed below need to be considered in the design of EWSs.

4.5.1 Contaminants of Concern and Their Concentrations

A comprehensive list of potential contaminants that include chemical (including biotoxins), biological, and radiological contaminants would be large and unrealistic to tackle. Lists of potential contaminants have been developed (Pikus 2004). Utilities should not take any general list as definitive for the specific purposes of its use. Contaminants that are more readily available in a specific region or that seem for any other reason to be more appropriate for the utility in question to consider should be added. Utilities, using their DBTs, are responsible for identifying the contaminants for which they should design their EWSs.

Although there is no consensus on the concentrations that need to be detected, it appears that concentrations above NOAEL should be considered. NOAEL is defined as "the greatest concentration or amount of a substance, found by experiment or observation, which causes no detectable adverse alteration of morphology, functional capacity, growth, development, or life span of the target organism under defined conditions of exposure." (Pikus 2004).

4.5.2 Fate and Transport Models for Contaminants

In the selection of the instruments and their locations, utilities need to understand where the contaminants travel and what kinds of changes occur during their transport. For surface waters spill models are typically used to estimate the fate and transport of contaminants, while distribution system network models are used for distribution systems. Water utilities need to have access to appropriate models to apply to their water supply systems.

4.5.3 Sampling Frequency and Integration with Existing Water Quality Monitoring Programs

Water systems monitor water quality for both regulatory and operational performance purposes. Water samples are collected at specific locations and, depending on the parameters, are either tested at the field or in the laboratory. These grab samples are collected periodically from a relatively small number of locations. Because a contamination event may last a relatively short period of time, grab sampling may miss contamination events of concern. Furthermore, regulatory samples are typically sent to laboratories, adding more lag time to the detection of a contaminant.

As such, continuous or near continuous monitoring (in-line or on-line) is recommended for EWSs. Most utilities already collect continuous samples at their plants, monitoring parameters such as flow, pH, turbidity, and chlorine residual, so there is already a foundation for continuous monitoring in water systems. The challenge is selecting meaningful parameters, instruments, and locations for sampling. At this time, due to technological limitations, the presence and properties of contamination are inferred from changes in surrogate parameters. Unfortunately, the sensitivity and accuracy of these parameters by which the contamination event can be detected is still questionable.

In designing an EWS, a utility should integrate it with its existing monitoring program by using staff already knowledgeable in sample collection, analysis, and instrumentation.

4.5.4 Selection of Instruments

Until further advances occur in instrumentation, the emerging practice is the use of Tier 1 instruments for detecting contamination and its location. Tier 1 instruments typically measure changes in some of the basic properties of water, such as pH, oxidation reduction potential, chlorine residual, TOC, and adsorption of light. These measurements should be followed by Tier 2 instruments for identifying the contaminant and its concentration (including the use of laboratory analysis).

In the selection of instruments, consider the following:

- parameters measured, sensitivity, accuracy, reliability, ruggedness, cost
- characteristics of the instrument location (see Section 4.5.3, “Sampling Frequency and Integration with Existing Water Quality Monitoring Programs”)
- O&M characteristics such as maintenance requirements, down time, calibration and testing requirements, housekeeping, and data reporting capabilities

4.5.5 Siting of Instruments

Identifying where to place an instrument is relatively easy for source water, but very complex in distribution systems. In source waters the pathway of water is known, so the instruments are typically placed upstream of the intakes with the distance and location somewhat determined by the use of surface water spill models. In the case of distribution systems, as the intrusion point and time of the contaminant are not known, there is an infinite number of potential locations that the

instrument could be placed. A utility needs to identify the best locations and number of instruments that will cover the largest number of consumers within its budget. Depending on the technical and financial resources of a utility, these locations could be identified either by using staff intuition, or distribution system network simulation models, or distribution system network optimization models. Because optimization models are too complex for routine utility use, the other options should be considered. While simulation methods are better than intuitive methods (because they incorporate some of the intuitive factors), there is no implication that sensors located there will 1) detect the contaminants 2) in a timely fashion. EPA's PipelineNet model can be used for this purpose. Regardless of the method used, both local and system-wide factors need to be considered in the selection of candidate sites (Pikus 2004).

4.5.5.1 Local Factors

- Easy access to the instrument site by authorized personnel
- Available space for the instruments and auxiliary equipment
- Suitability of candidate instruments or sample collection method for the sampling site
- Physical security of the instrument site
- Hydraulic conditions at sampling sites
- Existing water quality sampling sites

4.5.5.2 System-wide Factors

- Potential areas or entry points of contamination
- Likely contaminants
- Contaminant transport time and concentration
- Vulnerable populations (such as children, elderly, sick) at different parts of the network
- Relative water demand and associated flow characteristics
- Frequency of sampling, i.e., periodic vs. continuous sampling,

4.5.6 Data Analysis and Interpretation

Pikus lists the following objectives for analyzing the data from EWS instruments:

- To identify the presence and location of significant contamination in the system (essential)
- To identify the contaminant or its class with sufficient specificity to allow appropriate responses (desirable)
- To characterize the contaminant concentration profile (pulse morphology) (desirable)
- To determine time to consumer (essential)
- To eliminate false negatives and minimize false positives (essential)

- To assess public health risk (highly desirable)
- To provide timely information to decision maker (essential)

To properly interpret the data from instruments, reasons for water quality parameter variations need to be well understood. The sources of variation include:

- noise in the instrument
- variations in the actual properties of the water
- variations in the measured parameters from changes in operating conditions

To determine whether a set of readings is an indication of contamination, a utility needs to distinguish between a contamination event and the other possible causes of the measured changes. For this reason, the utility needs to identify the baseline water quality characteristics of its source water and its potable water in the distribution system. This baseline will require at least one year of water quality sampling and analysis of parameters monitored via an EWS, enabling the utility to better interpret whether the variations in water quality are due to contamination or other reasons.

4.5.7 Communication System Requirements

An EWS typically consists of a number of instrument platforms located throughout the water system that are operating continuously and producing large quantities of data. The data would be sent to a central data analysis facility at which they would be processed and interpreted.

The data can be transmitted to the data analysis center over existing SCADA linkages or over separately configured and managed linkages. Most utilities would probably prefer to use an existing SCADA system for these communications. For security reasons, it is better to encrypt the data., although this might create compatibility problems with an existing SCADA system.

Proper guidance for such communications is provided in Section 5, "Cyber Security Management, Operations, and Design Considerations."

4.5.8 Responses to Contamination Events

This factor is covered in Section 7, "Emergency Response Planning."

4.5.9 Operations, Maintenance, Upgrades, and Exercising the System

Pikus (2004) provides extensive recommendations regarding these factors. They cover topics such as unscheduled and scheduled downtime, preventive maintenance, built-in testing and diagnostics, integration with SCADA, supplies, spare parts, and training for staffing.

4.6 Recommendations for Source and Ground Water Facilities

In the security evaluation of water facilities, the raw water system, composed of the raw water supply, intake, pumping, and transmission to the main plant, are typically considered to be critical components of the water supply system.

Table 4-2 provides general security design consideration for surface and groundwater facilities. The following subsections provide more specific measures by facility.

TABLE 4-2
Source (Ground and Surface) Water Supply Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Malicious damage	Harden facility using cage, fencing, locks
		Use appropriate signage and lighting
		Provide intrusion alarm
Criminal	Equipment theft	Chain and lock portable equipment
		Install card access system
Saboteur/Terrorist	Destroy or disable facility systems	Install CCTV at facility perimeter
	Contaminate water	Install alarmed entry
	Injure employees	Install alarmed interior presence sensors
		Use multi-parameter water quality probe
		Restrict boat access to intake
Insider/Additional Considerations	Revenge, personal gain	Restrict access by job function

4.6.1 Wells

Consider the following security design measures for wells:

- Enclose the wellhead with cages or buildings that restrict access to avoid physical destruction or intentional contamination of well water supply. Cages can be of simple construction, such as a reinforcing bar.
- Protect gravel chutes and chemical application points with a cage to avoid intentional contamination of the water supply.
- Use shackle-protected locks to prevent the lock from being cut by a bolt cutter.
- Post warning signs on the perimeter fence for deterrence and to protect the utility from liability. Follow local ordinances when signs are installed. Depending on the diversity of the population, multi-lingual signs may be required.
- Increase site lighting to allow suspicious activity to be easily noticed by citizens or passing law enforcement. Motion-detecting lighting can be used in area where local residents are sensitive to external lighting in facilities.

- Dual utility power supplies from different substations or a backup power generator will provide a continuous supply of water even when the primary utility power supply fails.
- Provide redundancy for treatment, disinfection, and water quality monitoring structures, which typically consists of aeration, pH adjustment, and disinfection.
- Use a multi-parameter probe to measure contaminants such as pH, oxidation-reduction potential, conductivity, turbidity, chlorine residual, and dissolved oxygen in the aquifer or well discharge for early detection of chemical/biological contamination. Major deviations from the baseline of these parameters would indicate potential biological or chemical contamination of the water.

4.6.2 Rivers, Lakes, and Reservoirs

Design considerations to protect water supply from rivers, lakes, and reservoirs include:

- Source water watershed protection.
- A multi-parameter probe to measure contaminants such as pH, oxidation-reduction potential, conductivity, turbidity, chlorine residual, and dissolved oxygen in the river for early detection of chemical/biological contamination. Major deviations from the baseline of these parameters would indicate potential biological or chemical contamination of the water.
- A fence around the facility or site. However, this may not be feasible depending on the size of the facility/site and may also be opposed by the public because it will not be aesthetically pleasing.
- Consider an aquarium-type fish tank where small portion of raw water is directed to the fish tank. Effects to the fish will indicate water contamination. This is a basic system that requires operator attention, although there are more sophisticated units available to alert the operator.

4.6.3 Dams

Dam breach can have a significant impacts downstream: flooding, loss of life and property and loss of water supply source. Vulnerability assessments for dams can be conducted using the RAM-D tool developed by Sandia National Laboratories. Based on the results from the assessment, some of the following security improvements can be applied. Design considerations to improve security at dams include these:

4.6.3.1 Basic

- Restrict access to the spill way, overflow, and intake to avoid placement of explosives at these structures.
- Restrict vehicle access on the dam using locked gates or bollards.
- Warning signs on the perimeter fence for deterrence and to protect the utility from liability.

4.6.3.2 Advanced

- Use boom systems or turbidity curtains, as shown in Figures 4-6 and 4-7, to restrict boat access to the intake to avoid contamination of water.

FIGURE 4-6
Boom System

- Use video cameras for alarm assessment to verify whether the alarm is real or a nuisance alarm so that the utility can take appropriate action.
- Limit switches on gate operators to alert the operator when someone is closing or opening the gates on dams.
- Increase lighting so that suspicious activity can be easily noticed by citizens or passing law enforcement.

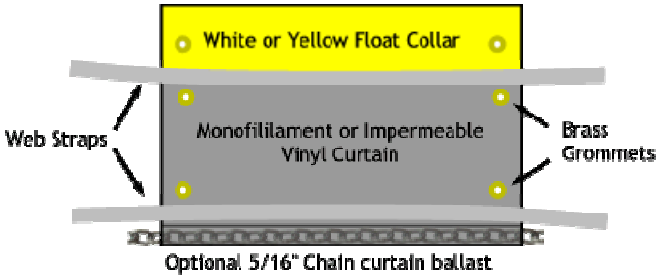


FIGURE 4-7
Turbidity Curtain

Design considerations to improve security at intake, pretreatment, and water quality monitoring structures include:

- If the utility is considering a second intake, it is recommended to spatially separate the two intakes so that an impact on one intake does not affect the other.
- An intruder alarm can alert an operator when an unauthorized person gains access to the facility.
- Video camera for alarm assessment can verify whether the alarm is real or a nuisance alarm so that the utility can take appropriate action.

4.7 Recommendations for Raw Water Conveyance Facilities

Table 4-3 provides general security design considerations for raw water conveyance facilities. The following subsections provide more specific measures by facility type for utilities to consider.

TABLE 4-3
Raw Water Conveyance Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Cause malicious damage	Harden facility using cage, fencing, bolting
		Use appropriate signage
		Provide intrusion alarm
Criminal	Steal equipment	Lock access

TABLE 4-3
Raw Water Conveyance Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Saboteur/Terrorist	Destroy or disable facility systems	Implement alarmed entry
	Contaminate water	Implement CCTV at pump station
	Injure employees	Install pipelines below ground
Insider/Additional Considerations	Seek revenge, personal gain	Restrict access to facility by job function

4.7.1 Pump Stations

Redundant units and adequate capacities under peak flow conditions with at least one unit out of service is generally considered a standard for design of pump facilities. Pump stations can be designed to enable removal of pumps and motors for repair while maintaining the operability of the facility at full capacity. If possible, at least two discharge pipes and two discharge locations should be considered in the design to provide additional redundancy. Consider restricting access to the pump station using access control systems.

4.7.1.1 Perimeter/General Site Security

- Install chain-link fence with three strands of barbed wire, break-away stanchions, and signs 50 feet apart.
- Use shackle-protected locks to prevent the lock from being cut using a bolt cutter.
- Use video cameras for alarm assessment to verify whether the alarm is real or a nuisance alarm so that the utility can take appropriate action.
- Increase lighting so that suspicious activity can be easily noticed by citizens or passing law enforcement.

4.7.1.2 Electrical Supply and Equipment

- Provide a redundant utility power supply from a different substation, pre-wired connection for a backup generator, or a portable backup generator.
- Match the plug on the portable generator to the emergency power receptacle at the pump station.

Tips For Small Utilities

Smaller utilities can coordinate with other local utilities or rental companies for generators and pre-wire the facility to accept the generator.

4.7.1.3 Control Room

- Use card access to restrict access to the control room to authorized personnel.
- Install a door status switch and motion sensor to alert operator when an unauthorized person gains access.

4.7.1.4 Pumps and Appurtenances

Consider redundancy of critical components.

4.7.2 Pipelines and Appurtenances

When adding a second pipeline to meet additional demands, bury the second pipeline in a trench that is physically separated from the first pipeline.

4.7.2.1 Underground and Aboveground Pipelines

- Reduce the area of aboveground exposure for the pipeline.
- Use high-pressure pipeline material (such as ductile iron) in exposed areas if the DBT includes small explosive capabilities. If a significant threat exists, consider using Schedule 80 piping.

4.7.2.2 Pipelines on Bridge Crossings

- Use high-pressure pipeline material (such as ductile iron) in exposed areas if the DBT includes small tools or small explosive capabilities. Consider using Schedule 80 pipe if a significant threat exists.
- Protect the pipeline with fan structures or concrete encasement to restrict access.
- Replace overhead pipelines with pipelines in tunnels under the river or creek if the DBT includes significant explosive capabilities.

4.7.2.3 Distribution System Appurtenances

- Add bolts that require a special wrench to unlock (where generally available screw drivers and wrenches would not work) for access hatches and valve vaults.
- Add protective cages over aboveground appurtenances to restrict access.

4.8 Recommendations for Water Treatment Facilities

Two key design approaches for limiting negative impacts to treatment plants are redundancy and adequate capacity. Redundancy in design that is geographically distant 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 adversaries. Whenever feasible, consider providing multiple trains for each process unit with bypass systems to enable an individual process train to be removed from service. Similar redundancy for auxiliary and support processes and equipment such as chemical feed pumps should be evaluated. Redundancy can be extended to entire treatment trains of multiple process units that are, if possible, separated by a physical distance but connected for maximum operational flexibility.

Flexibility to respond rapidly to unplanned shutdowns of process units should be considered during design by allowing channels, gates, pumps, valves, and piping to enable tanks and pumps to be used for different processes. Critical valves, gates, and transfer pumps can be automated to allow for quick shutdown or diversion of flows. However, in the event that automated controls or SCADA systems are compromised or inoperable, a means to operate the processes manually is recommended.

On-the-shelf spares, such as process pumps, motors, valves, meters, and controllers, provide redundant critical components. Redundant utilities, particularly electrical power, are vital to a secure operation. In addition to the need for at least two independent main power supplies to the treatment facility, looped power distribution networks within the treatment plant should be considered to enable rapid isolation and removal of a damaged power feed or inoperable electrical equipment from the power net.

The approach for adequate design capacity works in tandem with redundant unit processes. At a minimum, the design for individual processes should be conservative and meet peak demands with one unit out of service. For treatment plants with multiple trains, consider peak demands with one train out of service. Higher redundancies should be considered for critical processes, such as disinfection systems, where redundancies are often 100 percent of design capacity.

Where practical and feasible, tanks and open channels should be covered, and the access doors and hatches should be secured. Critical components such as pumps, motors, motor control centers, and SCADA components can be secured within enclosures and hidden from view. Where feasible, piping and appurtenances can be installed below ground or within secured structures. Locking mechanisms can be considered for critical valves and gate operators.

However, designers should consider the impacts of limiting access to normal O&M activities. Adequate access and room for routine maintenance and repair can be considered in the layout of individual unit processes. The ability to remove enclosures may be necessary to replace or repair equipment.

Table 4-4 provides general security design considerations for water treatment plants. The following subsections provide more specific measures by facility type.

TABLE 4-4
Water Treatment Facility Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Cause malicious damage	Harden facility using fencing, locks, and bollards Install appropriate signage and lighting Provide intrusion alarms
Criminal	Steal equipment	Lock access ladders, hatches, buildings, and gates Install a card access system for building entry Harden windows, doors, and other entry points Provide signage with no asset information

TABLE 4-4
Water Treatment Facility Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Saboteur/Terrorist	Destroy or disable facility systems Contaminate water Injure employees	Install CCTV at facility perimeter Install alarmed entry Install alarmed interior presence sensors Use multi-parameter water quality probe Provide vehicle inspection area Install vehicle barriers Install redundant power connections Install tamper-switches on SCADA panels Install duress switches for operators Install bolting for critical valve vaults
Insider/Additional Considerations	Seek revenge, personal gain	Restrict access to areas by job function Provide secure fence to isolate critical assets within facility

4.8.1 Conventional Treatment Processes

The WTP unit processes for conventional treatment usually consist of pretreatment; flocculation and sedimentation and filtration (supplemented by the backwash of the filters using a backwash supply tank); and disinfection (including the use of a clearwell for storage and contact time).

4.8.1.1 Pretreatment System

Special considerations are required where the DBT includes adversaries with explosives. Individual concrete structures, such as splitter boxes and pump stations, may serve as single points of failure that can be hardened against the threat, or duplicated and separated to preserve functionality if one unit is damaged.

4.8.1.2 Flocculation/Sedimentation and Filtration

- The redundancy of the flocculation/sedimentation trains reduces the criticality of each individual train; however, loss of flocculation system could adversely impact water quality. The flocculation basins are potential points of contamination. Limiting access, intrusion detection
- Maintain the effectiveness of filtration through an effective backwash or cleaning system. Interconnected, dual backwash systems, each with a capacity for 50 percent of the peak flow, can provide the redundancy desired. Chemical systems used to enhance filtration can also include a measure of redundancy. Consider storing replacement media in a secured storage building away from the filters.
- If pneumatic valves are used for the filter inlet/outlet control valves, consider a backup air compressor for the pneumatic valves. Also, a pressure transmitter on the air supply to detect loss of air supply to the valves can be added.
- Consider a backup power supply for key electrical valves.

4.8.1.3 Backwash Supply Tank

For plants with one backwash tank, obtain redundant backwash supply from tapping the finished water discharge with appropriate pressure-reducing valves (PRVs).

4.8.1.4 Disinfection – Chlorination, Ozonation, Ultraviolet

Typically, the final step of water treatment is the disinfection process, a key process in the treatment train. Adversaries may target this process in an effort to discredit the utility and promote concerns and fear within the general public about the quality of the finished water. Increased security approaches, such as more restrictive access control and hardened physical protective systems, are warranted for this process. Regardless of the type of disinfection system used (i.e., chemical or ultraviolet light), provisions or plans can be considered for a backup disinfection system using a liquid disinfectant such as sodium hypochlorite. This backup system could consist of temporary pumps, tanks, and piping.

For treatment plants using gaseous chlorine and/or gaseous ammonia, special design considerations are required if the DBT includes saboteurs and terrorists, as these chemicals are highly toxic and have the potential for significant and dramatic impacts on employees and area residents if released into the atmosphere. Standard design considerations for handling and use of these chemicals include, but are not limited to, separate rooms and ventilation systems or independent buildings for storage and feed equipment, leak detection and alarm systems, automatic shut-off valves if leaks are detected, and air scrubbers for containment and neutralization of a release of the entire contents of the largest cylinder or tank in the storage room. For threats including saboteurs and terrorists, countermeasures can include an additional layer of security that includes secure fencing, detection devices, and monitoring as described below.

In addition to very restrictive control of individuals authorized to enter these facilities (if deemed appropriate to the threat), the design can include sufficient stand-off distances (parking lots are away from these areas) and structural hardening to prevent damage and rupture to the gas cylinders or tanks. Delivery areas and loading areas can also be tightly controlled and monitored. The following security features can also be considered.

- Install a security fence to isolate toxic chemicals to prevent unauthorized access to these sensitive areas. Figures 4-8 through 4-10 show desirable secure fencing characteristics.
- Use shackle-protected locks prevent the lock from being cut using a bolt cutter.
- Install motion-sensors to alert the operator when there is an unauthorized person onsite.
- Use a video camera for alarm assessment to verify whether the alarm is real or a nuisance alarm so that the utility can take appropriate action.

FIGURE 4-8
Secure Fencing with Aircraft Cabling

FIGURE 4-9
Fencing with Openings Too Narrow for Adversary to Get a Handhold or Toehold

- Increase site lighting so that suspicious activity can be easily noticed by utility employees.
- Use a card reader or key pad to limit access to only authorized utility employees.

The best defense may be to avoid the use of extremely hazardous chemicals (chlorine and ammonia), replacing them with less dangerous chemicals (sodium hypochlorite and liquid ammonium sulfate), and installing physical treatment processes where possible.

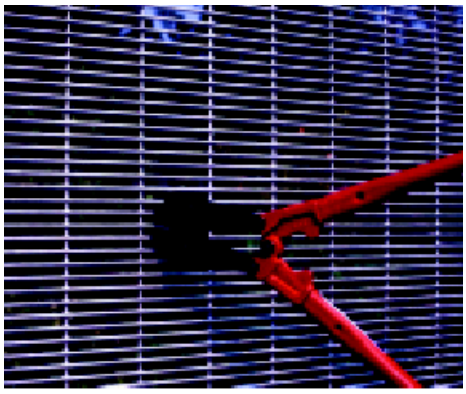


FIGURE 4-10
Fencing with Openings Too Narrow for Cutters to Grip

4.8.1.5 Clearwell

- If there are two or more clearwells, ensure that one can be isolated if it is contaminated to provide finished water from the other clearwells. The utility should consider installing a multi-parameter probe to measure contaminants such as pH, oxidation-reduction potential, conductivity, chorine residual, and dissolved oxygen in the clearwells for early detection of chemical/biological contamination. Major deviations from the baseline for these parameters may indicate potential biological/chemical contamination of water.
- For clearwell hatches, use unique shackle-protected locks and not locks that use a master so that only authorized utility staff have access to minimize an insider threat.
- For clearwell vents, consider installing goosenecks with thick, double-meshed, offset screens that cannot be easily cut to prevent chemicals from being introduced through the vents. For greater protection, add internal baffles and a structure around the vent that would make chemical addition more difficult while still providing an opening for ventilation.
- Use tide valves on clearwell overflow pipes in lieu of a flapper valves to minimize the ability to introduce chemicals into the pipe.
- Add intrusion alarms on clearwells that are coupled with automatic effluent shut-off valves for immediate isolation.

4.8.2 Auxiliary Systems/Components

Utilities have numerous opportunities to increase security throughout a facility as shown below.

4.8.2.1 Perimeter/General Site Security

- Install chain-link fence with three strands of barbed wire. Consider a fence detection system such as fiber optic or taut wire.
- Post warning signs on the perimeter fence for deterrence and for liability to protect the utility. Follow local ordinances when signs are installed. Depending on the diversity of the population, bilingual signs may be required.
- Install aircraft cable for perimeter fence where the fence is potentially exposed to adversaries in high-speed vehicles to prevent forceful entry onto plant site.
- Add concrete vehicle barriers at the entry gate to slow traffic to prevent vehicles crashing into the property, as shown in Figure 4-11.

FIGURE 4-11
Example of Vehicle Access Approach to Reduce Speed

- Lock entry gate operator enclosures with a shackle-protected pad lock.
- Provide a system, such as a Knox box, to allow emergency response personnel to gain access to the facility during an emergency when utility employees are not at the site or are unable to open the entry gate. Consider a small side-entry man gate.

FIGURE 4-12
Example of Drop-Arm Crash Beam Vehicle Barrier

- Install drop-arm crash beam type vehicle barriers at the vehicle entry gates to restrict forceful entry of unauthorized vehicles, as shown in Figure 4-12.
- Add fixed security cameras at the main gate to record entry/exit events (e.g., date and time) and to provide a means for the receptionist to verify (e.g., call to find out if there is supposed to be a delivery) or record (e.g., in case there is a question about a delivery later) who is at the gate before opening the gate.
- Increase site lighting so that suspicious activity can be easily noticed by citizens, law enforcement, or utility employees. This is discussed in detail in Section 3.

4.8.2.2 Finished Water Pump Station

- Consider redundant (stand-by) pumps and other critical components.
- Provide intrusion detection on doors to alert operator when there is an intruder.
- Provide access control on doors to restrict access to authorized personnel only.
- Design backup or redundant power supply.

4.8.2.3 Chemical Storage and Feed Systems

Utilities typically use numerous chemicals at a WTP; these include liquid ferric sulfate or alum, liquid oxygen, aqueous or anhydrous ammonia, chlorine gas or sodium hypochlorite, sodium hydroxide, hydrofluorosilicic acid, and polymer. Depending on the specific chemical in use, the chemical and its feed equipment can be targets of saboteurs and terrorists. Based on the DBT, chemical buildings or chemical rooms within buildings can be provided with a higher security, as can outside chemical storage areas, using methods such as these:

- Consider visual access so that chemicals can be observed from outside without going into the building.
- To provide adequate redundancy, keep at least two storage tanks per liquid chemical on hand.
- Provide adequate spill containment and control or all storage tanks, and separate containment structures for each chemical. It is standard practice to design the containment to hold the volume of the largest tank within the containment.
- Include spill detection systems in the design of storage and feed areas to assist in detecting theft or release of the chemical. Typical systems include liquid levels in containment sumps.
- Include instrumentation to alert the operator when there is an overdosage of chemicals.

4.8.2.4 Electrical Supply and Equipment

The following considerations can be taken into account to improve security for electrical supply, which is one of the most critical assets at a treatment plant:

FIGURE 4-13
Bollards Protecting a Fence from Vehicle Entry

- Redundant utility power supplies from different substations or a backup generator. Provide bollards to protect intentional or accidental damage of power transformers, as shown in Figure 4-13.

- Isolate critical electrical components such as switchgear from the rest of the plant using secure grills, as shown in Figure 4-14. Tampering with switchgear can result in a loss of power failure for an entire facility.

FIGURE 4-14
Example of Sensitive Equipment Isolated by Secure Grills

4.8.2.5 SCADA/ Control System Equipment

- Provide lock and intruder switch on control panel.
- Provide signal supervision and tamper alarms to detect loss of signal and tamper attempts.

4.8.2.6 Control Room

- Limit access to the control room with a card reader or key pad.
- Provide employee-activated as well as "deadman" duress switches to alarm station operator, control room operator, personnel working alone in remote facilities, and other key personnel.

4.8.2.7 Administrative Area

- Limit access to the administrative areas with a card reader or key pad.
- Upgrade door hardware on mission-critical facilities as follows:
  - Install tamper-resistant hinges (tack-weld hinge pins at minimum) and security pins into doorjamb or use Z-strip (a protective shroud that safeguards hinges and doors from tampering).
  - Use shackle-protected locks that are hardened to provide delay values consistent with other door delay values.
  - Install balanced magnetic switches tied into central alarm system to alert the operator.
  - Install expanded metal grating on interior of door louvers and 3/8-inch (or thicker) Lexan® on interior of door windows to prevent forceful entry into a room through these openings.
  - Install tamper-resistant panic door hardware on all exterior doors to provide additional delay in forceful entry.
  - Replace doors that have glass windows with solid metal doors to provide additional delay.
- Upgrade windows:
  - If windows must be capable of opening for ventilation, install a securely-attached expanded metal grating on interior. One-quarter inch anchor bolts inserted a minimum of 1 inch into the window frame is recommended. Anchor bolt head should incorporate a tamper-resistant fitting so that a specialized socket is required for removal.

- If windows are not required to open, install an expanded metal grating or 3/8-inch Lexan® on interior of windows.
- If a room is alarmed, install glass-break sensors to provide earlier detection of penetration attempts at highly critical facilities such as chlorine storage.

4.8.2.8 Laboratory

A water utility's laboratory typically contains sophisticated and valuable analytical equipment, as well as computer hardware and software that may be a target of vandalism and theft. In addition, laboratories have various hazardous reagents and, consequently, may be targets of saboteurs or terrorists. As with the other security measures described in this document, the design considerations discussed in this section should be employed based upon the identified DBT. 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. Chemicals or gases (in cylinders) that are stored outside of the laboratory can be secured with lock and chain and enclosed in a cage in accordance with the determined DBT.

4.9 Recommendations for Finished Water Storage and Distribution System

Table 4-5 provides general security design considerations for the finished water storage and distribution system. The following subsections provide more specific measures by facility type.

TABLE 4- 5
Finished Water Storage and Distribution Facility Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Cause malicious damage	Harden facility using cage, fencing, locks, and bolting
		Install appropriate signage and Lighting
		Provide intrusion alarms
Criminal	Steal equipment	Lock access ladders, hatches, and hardened entry points
Saboteur/Terrorist	Destroy or disable facility systems	Install CCTV at facility perimeter
		Install alarmed entry
	Contaminate water	Install alarmed interior presence sensors
	Injure employees	Use multi-parameter water quality probe
		Install tamper-switches on SCADA panels
		Install motion-sensor (dual technology) for storage tank ladders
Insider/Additional Considerations	Seek revenge, personal gain	Restrict access to areas by job function
		Provide electronic key that provides access to only authorized personnel

4.9.1 Storage Tanks/Reservoirs

- Use locks or hatches on storage tanks/reservoirs.
- Consider security cameras only at mission-critical sites for alarm assessment.
- Consider intrusion alarms on control panels that are mounted outdoors to alert operator.

Tips for Small Utilities

Small utilities can consider welding a bar over hatches to restrict access into tanks.

- Consider intrusion alarms on hatch covers that are interconnected with automatic shut-off valves on tank discharge line.
- Increase site lighting so that suspicious activity can be easily noticed by citizens or passing law enforcement.
- Replace existing non-bolted covers on valve vaults with bolted covers or add bolts that require a special wrench to secure the existing covers.
- Consider an anti-climb shield, such as the one shown in Figure 4-15, with lock-on storage tank ladders. Add a bulkhead (e.g., a reinforced door) to stairs to restrict access to top of the storage tank. Alternatively, ladders can be removed so that a portable man lift or ladder is required for utility staff to access the top of the storage tank for maintenance.
- Consider a dual technology motion sensor (both microwave and passive infrared) on storage tank ladders. This sensor is designed to pick up any intruder approaching the top of the tank, and would not generate nuisance alarms from birds or other objects.

FIGURE 4-15
Example of a Protected Access Ladder to a Storage Tank

4.9.1.1 Perimeter/General Campus Security

- Provide shackle-protected locks or an electronic lock that can be programmed to open only for authorized utility staff for the entry gate. Use locks or hatches on storage tanks/reservoirs. Consider non-duplicate keys that are specifically made for the utility.
- Post warning signs on the perimeter fence for deterrence and for liability to protect the utility. Follow local ordinances when signs are installed. Depending on the diversity of the population, multi-lingual signs may be required.

4.9.1.2 Hatches

- Provide shackle-protected locks.
- Weld bar on top of hatch to restrict access (for tanks that require infrequent access).
- Interconnect intrusion alarms to automatic tank discharge shut-off valves to isolate the tank if there is an indication of a potential threat to water supply.
- Consider dual hatches for additional delay on critical valve vaults for higher level DBTs.

4.9.1.3 Air Vents

- Consider installing thick, double-meshed, offset screens on vents.
- Install baffles to prevent insertion of contaminants into tank.

4.9.2 Pipelines and Appurtenances

Underground and aboveground pipelines are discussed in this section, as well as pipelines on bridge crossings, appurtenances, fire hydrants, and monitoring equipment.

4.9.2.1 Underground and Aboveground Pipelines

- Reduce area of aboveground exposure for pipelines.
- Use high-pressure pipeline material (such as ductile iron) in exposed areas if DBT includes light explosive capabilities. Consider using Schedule 80 pipe if the threat level warrants.

4.9.2.2 Pipelines on Bridge Crossings

- Use high-pressure pipeline material (such as ductile iron) in exposed areas if DBT includes light explosive capabilities.
- Protect pipeline with fan structures of concrete encasement to restrict access.
- Replace overhead pipeline with a tunnel under the river or creek if the DBT includes substantial explosive capabilities.

4.9.2.3 Appurtenances

- Add bolts that require a special wrench to unlock (where generally available screwdrivers and wrenches would not work) for access hatches and valve vaults.
- Secure transfer valve vaults with bolting between pressure zones.
- Add protective cages over aboveground appurtenances.

4.9.2.4 Fire Hydrants

To minimize tampering of fire hydrants, install special nuts or caps, such as the ones shown in Figures 4-16 through 4-19. These devices require wrenches that are only sold to fire departments and water utilities.

To minimize the risk that firefighters would be unable to use the hydrant during a fire, consider these actions:

- Training on the use of specialized equipment should be provided to 100 percent of the personnel in local fire departments and all other fire departments with which there are mutual aid agreements or that would respond to an emergency.
- Provide the appropriate wrenches to all fire departments that may use the hydrant when responding to an emergency.

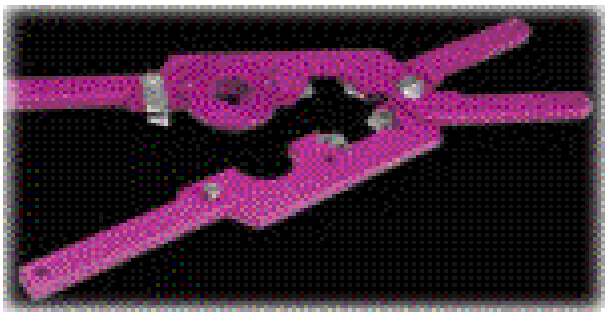


FIGURE 4-16
Example of a Special Fire Hydrant Locking Wrench

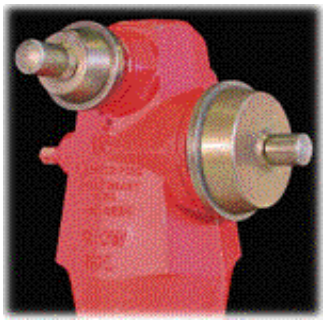


FIGURE 4-17
Example of Hydrant Locking Caps

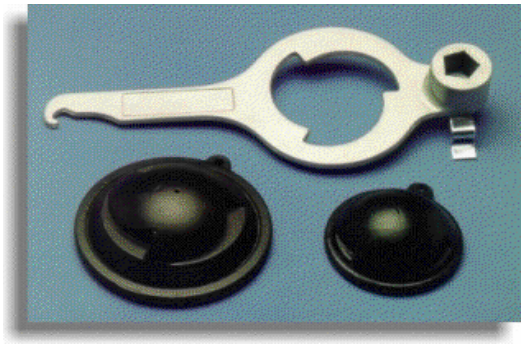


FIGURE 4-18
Example of Hydrant Locking Caps and Wrenches

FIGURE 4-19
Example of Special Fire Hydrant Locking Wrench in Use

4.9.2.5 Monitoring Equipment

The technologies for distribution system monitoring are rapidly advancing. Simple techniques such as measuring chlorine residual and pressure loss can sometimes be effective in determining if a chemical contaminant has potentially affected the system or if the system has been physically compromised. With new technologies being developed, utilities can determine if it is necessary to upgrade their existing monitoring systems after evaluating new technologies and case studies.

- Install a multi-parameter probe to measure pH, oxidation-reduction potential, conductivity, temperature, chorine residual, and dissolved oxygen in the distribution system for early detection of contamination in storage tanks.

4.9.3 Pump Stations

Security information regarding pump stations includes site security, electrical supply and equipment, SCADA/control system equipment, the control room, pumps, and appurtenances.

4.9.3.1 Perimeter/General Site Security

Post warning signs on the perimeter fence for deterrence and for liability to protect the utility. Follow local ordinances when signs are installed. Depending on the diversity of the population, multi-lingual signs may be required.

4.9.3.2 Electrical Supply and Equipment

- Provide an emergency receptacle for the backup power supply that matches the plug on a portable generator.
- Provide a redundant utility power supply from a different substation, a pre-wired connection for rental generators, or a backup portable generator.

4.9.3.3 SCADA/Control System Equipment

Provide signal supervision and tamper alarms to detect loss of signal and tamper attempts.

4.9.3.4 Control Room

Provide employee-activated as well as "deadman" duress switches to alarm station operator, central control room operator, personnel working alone in remote facilities, and other key personnel.

4.9.3.5 Pumps and Appurtenances

Secure sampling point stations with an enclosure and a shackle-protected lock.

4.10 Recommendations for Customer Connections

Table 4-6 provides general security design considerations for customer connections. The following subsections provide more specific measures by facility type.

TABLE 4-6
Customer Connection Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Cause malicious damage	Install locks
Criminal	Steal equipment	Install special bolting
Saboteur/Terrorist	Destroy or disable systems	Install backflow protection
	Contaminate water	Install dual check valves with residential meters (advanced practice)
Insider/Additional Considerations	Seek revenge, personal gain	Restrict access to areas by job function
		Provide electronic key that provides access to only authorized personnel

4.10.1 Construction Meters

Install integrated reduced-pressure backflow devices to prevent intentional or accidental contamination of water through this temporary meter connection.

4.10.2 Meters

- In high-risk areas for commercial properties such as hotels and motels, consider meters that have an appropriate level of backflow protection and anti-tamper devices to prevent the introduction of chemicals through a sink.
- Secure the water meter with a special bolt or use a locking meter, as shown in Figure 4-20, to protect from tampering.
- Consider automatic meter reading to continuously monitor flow for detection of unusual flow patterns.

FIGURE 4-20
Example of Locking Water Meter

4.10.3 Backflow Prevention Devices

Backflow prevention devices for the following areas can be considered to prevent intentional or accidental contamination of water.

- Evaluate appropriate backflow protection for all high-risk industrial and commercial facilities.
- Consider installing backflow protection c on residential properties in conformance with the Universal Plumbing Code for high-risk applications (e.g., pools, irrigation systems).
- Consider installing dual check valves with residential meters for additional backflow protection in high-risk areas. Meter installations will require the use of an expansion chamber downstream of the backflow device for protection of the residential water system.

4.11 Recommendations for Support Services/Facilities

Protecting utilities' support services and facilities can be equally as important as protecting the more high profile water system components.

4.11.1 Maintenance/Equipment Storage/Warehouse Facilities

Criminal theft of equipment, chemicals, and tools should be the minimum DBT for maintenance shops, warehouses, and storage facilities. At the threat levels of saboteur and terrorists, consideration should be given to providing a higher layer of security for these facilities and locating them a substantial distance from the treatment processes that they serve. Thus, should damage occur to the treatment process units, repairs can still be made—spare parts, replacement equipment, and materials such as filter media will still be available for use.

- For saboteur and terrorist threat levels, design delivery areas for equipment and supplies, as well as for chemicals and fuel, to consist of an inspection area that is separated from the eventual

destination to allow for inspection of the delivery vehicles and contents of the delivery. The inspection area can be designed to allow multiple inspections should more than one delivery vehicle be detained for inspection. The inspection areas can also 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.

- Utilities with vehicle fueling stations should be located at a sufficient standoff distance of 200 to 300 feet from treatment process units and inhabited buildings based upon the DBT.

Table 4-7 provides general security design considerations for support facilities. The following subsections provide more specific measure by facility type.

TABLE 4-7
Support Facility Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Cause malicious damage	Keep doors locked
		Install appropriate signage and lighting
		Provide intrusion alarms
Criminal	Steal equipment	Install card access system for building entry
		Harden windows and entry points
		Use signage that provides no asset information
Saboteur/Terrorist	Destroy or disable facility systems	Install CCTV at facility perimeter
	Contaminate water	Install alarmed entry
	Injure employees	Install alarmed interior presence sensors
		Install duress switches for operators
Insider/Additional Considerations	Seek revenge, personal gain	Restrict access to areas by job function

4.11.2 Remote Control Facilities

- Provide employee-activated as well as "deadman" duress switches to alarm station operator, control room operator, personnel working alone in remote facilities, and other key personnel.
- Upgrade door hardware on mission-critical facilities:
  - Install tamper-resistant hinges (tack-weld hinge pins at minimum) and security pins into doorjamb or use Z-strip (a protective shroud that safeguards hinges and doors from tampering).
  - Harden locks to provide delay values consistent with other door delay values.
  - Install balanced magnetic switches tied into the central alarm system.
  - Install expanded metal grating on interior of door louvers and 3/8-inch (or thicker) Lexan® on interior of door windows. One-quarter inch anchor bolts inserted a minimum of 1 inch into the window frame is recommended. Anchor bolt head should incorporate a tamper-resistant fitting so that a specialized socket is required for removal.

  - Install tamper-resistant panic door hardware on all exterior doors.
  - Replace doors that have glass windows with solid metal doors.
- Upgrade windows:
  - If windows must be capable of opening for ventilation, install a securely-attached expanded metal grating on interior.
  - Install glass-break sensors to provide earlier detection of penetration attempts through windows.

4.12 Recommendations for Administrative Facility Security

Loss of the business functions provided in administrative facilities may not necessarily disrupt the water supply, but may instead disrupt the ability to handle the financial and management duties that keep the utility running smoothly. Table 4-8 provides general security design considerations for administrative facilities. The following subsections provide more specific measures by facility.

TABLE 4-8
Administrative Facility Threat and Security Design Considerations

Threat Type	Threat	Security Design Considerations
Vandal	Cause malicious damage	Keep doors locked
		Provide intrusion alarms
Criminal	Steal equipment	Install card access system for building entry
		Install harden windows and entry points
		Install CCTV at parking areas
Saboteur/Terrorist	Destroy or disable facility systems	Install CCTV at facility perimeter
	Contaminate water	Install CCTV at building interior/public areas
	Injure employees	Install lock-down means at building lobby
		Install alarmed entry
		Install alarmed interior presence sensors
		Install duress switches for operators
Insider/Additional Considerations	Seek revenge, personal gain	Restrict access to areas by job function
		Install card access

4.12.1 Control Access to Buildings

The minimum DBT for administrative offices will most likely be theft, although a saboteur or terrorist may target the utility's management and administrative staff as well as the treatment plant infrastructure. Administrative offices of any organization are typically the target for an insider threat on management. Thus, consideration should be given to an increased threat level for administrative offices, even if the DBT of the surrounding facility is at a vandal or criminal threat level.

If applicable, designs for administrative offices should include 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 can alert local law enforcement of malevolent acts.

4.12.2 Safeguard Employees

- Provide employee-activated as well as “deadman“ duress switches to alarm station operator, control room operator, personnel working alone in remote facilities, and other key personnel.
- Provide a public address system to contact employees in a timely manner when there is imminent threat.