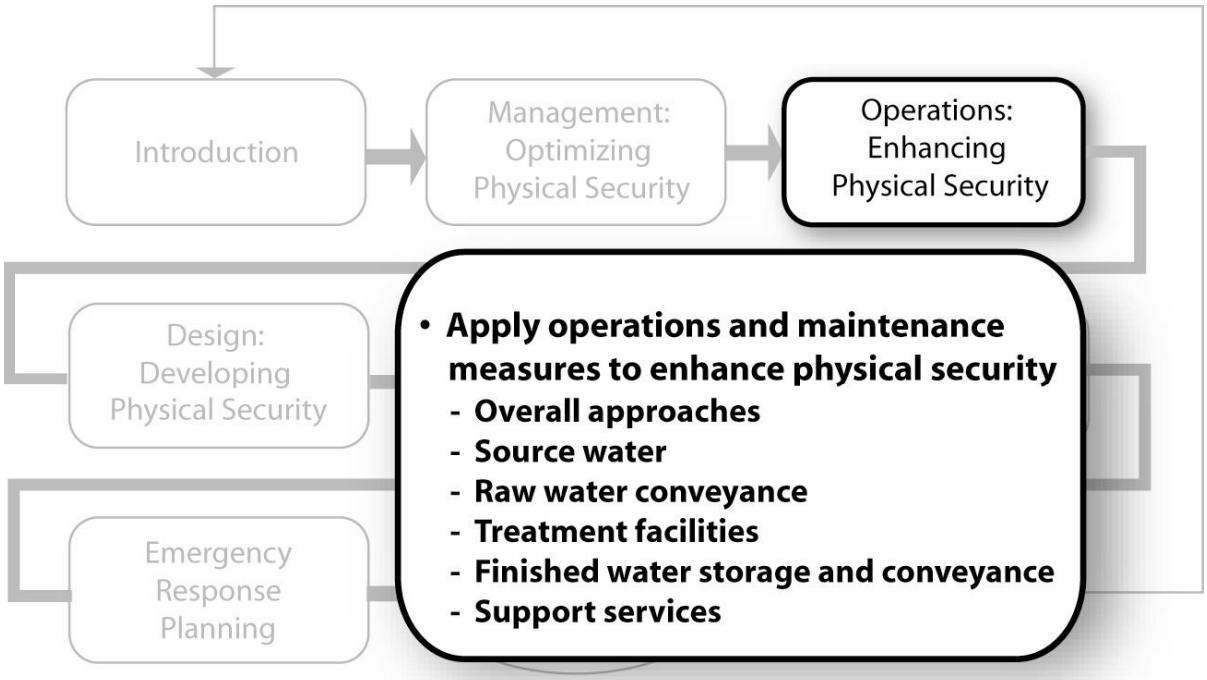
SECTION 3

Operational Considerations for Enhancing Physical Security



3.1 Overview

Water managers and operations staff have traditionally considered security to be an enhancement provided for a limited number of facilities, and have focused on electronic access control systems and CCTV monitoring. Today, water system managers, engineers, architects, and operations staff not only consider natural acts and accidents, but also security issues as an integral operational consideration for all aspects of their water systems that may potentially be threatened by acts of violence, such as vandalism, crime, sabotage, or terrorism. The objective of this section is to provide guidance that enables water utility managers, operators, and decision-makers to identify and apply operational improvements to their systems. The purpose of these improvements will be to increase the safety of utility facilities and to protect people, information, property, and assets related to the mission and goals of the utility. That universal mission is to effectively provide water that meets quality and quantity requirements for the community.

Operational changes often provide some of the more cost-effective approaches for utilities to enhance the physical security of their systems. This section provides a variety of operational approaches that water utilities may adopt to improve the security of their above ground and underground

infrastructure and support facilities. It also evaluates the applicability of different operational approaches to security for the four major threat levels from an outsider--vandals, criminals, saboteurs, and terrorists—as well as threats posed by an insider. An added benefit to addressing these threats is the enhanced capability of the water utility to respond to natural disasters and unanticipated events.

It is important to note that utilities adhering to industry-standard O&M practices contribute to their security enhancements when the operational measures identified here are included in utility O&M programs. The sources used in this section include *Water Treatment* (AWWA 1995), *Water Transmission and Distribution* (AWWA 1996), *Maintaining Distribution System Water Quality* (AWWA 1986), *Distribution System Maintenance Techniques* (AWWA 1987), *Guidance for Management of Distribution System Operation and Maintenance* (Deb et al. 1999), and *The Design and Evaluation of Physical Protection Systems* (Mary Lynn Garcia 2001). Other sources are included in the bibliography.

3.2 General Considerations

In addition to operational considerations specific to the various portions of the water system, a number of general considerations apply to water systems in general.

3.2.1 Philosophy

Physical security through operations should be addressed in a layered approach similar to the design concept of protection in depth, as described in Section 4.2.4, "Layers of Protection." 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 operational security to match the threat that may be associated with specific assets at the facility.

- 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 threats such as poorly equipped vandals and criminals.
- The site is the area between the perimeter and the buildings, structures, and other individual assets. This area provides a unique opportunity for early identification of an unauthorized intruder on the site and initiation of early response.
- The buildings and structures within a facility, such as a treatment plant or pump station, 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 protect critical assets or processes from intruders. Examples of these types of features include internal walls and doors, equipment cages, and redundant equipment.

For these layers to be effective, the proper maintenance of each layer is critical. For example, the fences and locks have to be maintained properly so that the associated layers can provide the physical security expected from them. Similarly, the proper security procedures have to be followed so that unauthorized entry is not permitted as discussed in Section 2.7, "Policies and Procedures."

The proper maintenance of infrastructure and the implementation of procedures are especially important for the distribution system because there are fewer layers between a potential intruder and the infrastructure.

3.2.2 General System Operational Practices

Table 3-1 provides general considerations for operational practices for the different layers within a facility for the key threat levels.

TABLE 3-1
General Considerations for Operational Security at a Water Facility

Threat Type	Perimeter	Site	Building	Building Systems
Vandal	Keep gates locked during non-working hours Repair breaks in fence Ensure all locks are functioning	Keep site illuminated	Lock buildings during non-working hours Keep windows closed and locked during non-working hours Follow intrusion alarm response protocol	Employ motion detector alarms
Criminal	In addition to the above: - Post guards at access locations during non-working hours	Keep site illuminated	In addition to the above: - Restrict access to building - Supply employee/ visitor ID badges	In addition to the above: - Restrict access to critical areas
Saboteur/ Terrorist	In addition to the above: - Conduct perimeter security inspections - Post guards 24/7	In addition to the above: - Conduct video monitoring 24/7		In addition to the above: - Conduct video monitoring 24/7
Insider				Apply dual employee requirement for critical areas

3.2.2.1 Basic

Utilities may want to consider the basic general operational practices to improve physical security as they identify ways in which to make their unique facilities more secure.

- **Application of Visitor Control Policy.** Visitors to facilities can include a number of different groups such as employee guests, the public (tour groups), vendors, and contractors. All visitors should be accompanied by an employee when they are going to sensitive areas. Site tours should be accompanied by an employee at all times, and should also be restricted to non-sensitive areas

of the facility. Some utilities have recently started requiring background checks on visiting international groups.

Vendors and contractors who have been cleared through background checks and have been assigned badges could sign a log when entering and exiting the utility. In all cases, prior to granting entry to a visitor, a security staff member can collect the following information from the visitor: the visitor's name, identification, company, the name of the employee being visited, and the purpose of visit. Additional guidance is provided below under "Delivery Access Control."

- **Alarm Response Protocols.** Utilities can develop alarm response protocols for security-related alarms. Utility staff can be trained in these protocols to understand their specific roles and responsibilities. By following the alarm response protocol for each category, staff members with proper training can then address the problem upon receipt of alarm notification.

  Alarm response protocols should provide guidance to identify false alarms, unverified alarms, panic and distress alarms, etc. Otherwise, false or non-urgent alarms will eventually render responses to alarms ineffective as the staff will start to ignore them. The interrelationship and interaction between security alarms and operational systems needs to be recognized and understood.

- **Application of Key Control Policy.** A strict key control policy can be implemented by water utilities. Features of the policy should include: 1) a limit to the number of employees with keys, 2) a ban on providing keys to contractors, 3) a prohibition on the duplication of keys, 4) use of patented keys that prevent the unauthorized duplication of keys (patented key blanks are protected and proprietary), 5) periodic and random change of keys, and 6) return of all utility keys from employees when terminating employment with the utility.

  Use of coded or cipher-based alternative keyless locks could also be considered. These include (Garcia 2001, U.S. Department of Commerce 2003) mechanical combination, electromechanical combination, mechanical entry control, and electromagnetic keyless control locks. Their main advantages are simple operation and ease of code change, thus they are especially suitable for smaller utilities. However, they are used primarily for access control and do not provide a high degree of security when used alone. Some models have time-penalty and error-alarm features and can be tied to alarm systems.

- **Alarms and Set-points.** Doors and windows that provide access to critical areas can be alarmed so that any unauthorized entry will alert security personnel. Responses to such alarms should be addressed in the alarm response protocols discussed above.

- **Lock Control.** Utility facilities often have multiple locks hooked together in a daisy chain to allow easy access for other groups, such as contractors or other groups. The removal of daisy chains and the development of an operational procedure for utility personnel to coordinate facility access with non-utility groups is recommended.

- **Scheduling of Annual Maintenance Activities.** The most critical times of operations occurs during peak demand periods. During these times, operations require as much system redundancy as possible to allow for reacting to both simple and complex operational issues. Large annual maintenance activities should be scheduled during periods when the demands of the system are at their lowest. This schedule should also include major shutdowns related to construction activities at the water treatment plant or other impacted critical facilities. Coordinating major annual maintenance activities, such water main flushing and valve exercising in distribution systems, during low-demand periods reduces the system vulnerability because the system has redundant capacity available.
- **Application of Access Control Policy.** Utility personnel, as part of their functional duties, have different access requirements to the various facilities. Employee access to each facility should be restricted based on job requirements. Limits to access can be accomplished through simple key control or more sophisticated access control systems. Highly sensitive areas, such as those with SCADA equipment and the operational control room, could have additional operational controls requiring two-employee identification prior to allowing access.
- **General Maintenance.** Utilities need to keep the general facilities in repair, including lighting, fencing and gates, doors, and windows. Similarly, distribution system air relief valves and air vents in storage tanks need to be regularly maintained. Poorly maintained facilities can increase the ease of unauthorized access.
- **Clearzone Areas.** An important concept in perimeter access control is a clearzone on both sides of a fence. A clearzone is an area surrounding the perimeter of a facility that is free of shrubs and trees and features well-maintained landscaping that does not provide hiding places for an adversary. Similarly, no materials should be stored by the utility near the fence to obstruct view. Clearzones enhance visual observation by security personnel and create a demarcation zone that makes unauthorized persons more noticeable. Clearzone distances will vary based on siting constraints; clearzone areas ranging from 50 to 100 feet from perimeter fence to building exterior are common for new facilities and are typically smaller for existing facilities that are space-limited. In either case, utilities are encouraged to maximize the space available.

  Lighting is frequently is enhanced within clearzone areas, making it easier for employees and passersby to observe and identify intruders. Within the clearzone space surrounding the critical buildings, motion detection is sometimes installed, with instant-on, high-visibility lighting (3 to 5 foot-candles of illumination) that activates when people approach the building.

  Critical facilities located within neighborhoods may be affected by zoning rules or neighborhood covenants that, for example, specify or prohibit certain landscaping and fencing features. Utilities can work with their governing municipalities to have the perimeter of critical facilities zoned as clearzone areas, as is the case with military installations and airport runways.

- **Fences.** Security fences, such as chain-link fences, typically do not prevent intrusion to a facility. Even the use of barbed wire or barbed tape concertina may not provide significant delay for intruders. However, by posting signs on the fence that trespassing is a criminal offense, fences can provide some deterrence to vandals. Thus, fences need to be inspected, maintained, and repaired as necessary to maintain their level of deterrence from vandals.
- **Delivery Access Control.** Deliveries present a difficult security challenge for facilities. Particularly for water systems that have regular chemical and other material deliveries, additional access control policies may be warranted:
  - Physically inspect vehicles before allowing them to enter a facility perimeter.
    - Construct a pull out area to stage delivery vehicles outside of the fence line.
    - Require the supplier to provide the manifest and driver name, and coordinate delivery time in advance.
    - Adopt a procedure that requires faxed or electronically transmitted copies of delivery bills-of-lading information and driver identification sent to the security office prior to the truck arriving onsite.
    - Have a trained security staff member meet the vehicle; physically inspect the driver, vehicle, and cargo for contraband; and test the cargo for correctness, concentration, and purity (if applicable) before it is allowed onsite. Unverifiable, unscheduled, or late deliveries should be refused.
    - Training security personnel regarding the necessity of keeping detailed logs of deliveries and pick-ups, including driver information and destination.
  - The same procedure can be accomplished prior to allowing a vehicle to depart the facility, checking for short deliveries, theft, or contraband.
  - Consider adding a CCTV video surveillance system. Deploy cameras to capture the vehicle license plate and driver facial features.
  - Implement a procedure for ensuring that a driver who regularly picks up or delivers hazardous materials, such as hazardous chemicals, is previously identified, given proper identification badges, and trained in the facility security requirements.
- **Vehicle Checkpoints.** A vehicle checkpoint area for detaining vehicles for identification is recommended in a perimeter access control system. The purpose is to screen all vehicles or pedestrians prior to accessing the property. The key to this practice is that the perimeter fencing must be as strong as the gate facility, based on the old concept that a chain is only as strong as its weakest link.
  - In a simple system, a vehicle checkpoint can consist of a gate with an intercom and video surveillance system. When a vehicle approaches, the driver requests permission to enter the facility using the intercom. After security staff has visually identified the visitor, access may be granted or denied from within the facility. Adding an exterior card reader on a pedestal outside the gate can serve to grant access to employees.

- In more elaborate security installations, a guardhouse facility may be located at the entrance to a facility. A security officer, who screens all vehicles entering the site, staffs the guardhouse. Vehicles that are not permitted to enter the site are turned back.
- High-security applications use vehicle sally ports to detain and screen incoming vehicles. A vehicle sally port consists of interlocking gates within a fenced area. Incoming drivers pass through the first gate and stop at the second gate. Once both gates are closed and the vehicle is captured within the sally port, a security guard may confirm the identity of the driver and, if necessary, search the vehicle to confirm the contents. Once the vehicle and driver are approved, the second gate opens and the vehicle may drive onto the facility.

3.2.2.2 Advanced

- **Reevaluation of Minimal Accepted Personnel Staffing Levels.** If the facility cannot be operated in a manual mode with the existing staff, this is a significant operational vulnerability that must be addressed. The utility ERP should have an emergency staffing plan that should include hiring of temporary employees or contractors for the duration of an emergency. This plan should also include staffing of facilities that are operated remotely. (For additional information about protecting remote facilities, see Section 5, "Cyber Security Management, Operations, and Design Considerations.")

3.3 Source Water

Source water marks the beginning of the utility water system and provides the first opportunity for disruption of water service to customers. Loss of source water supplies through contamination or disrupted delivery will have varying degrees of impact on a utility based on the utility's redundancy of raw water supplies, delivery capabilities, and finished water storage in the distribution system.

Contamination of actual source water supplies is difficult to accomplish because of the large volumes of water involved. The most vulnerable areas are typically associated with the transmission mains that deliver water to the treatment facility or directly into the system (groundwater wells). The raw water intake from lakes, reservoirs, dams, or wells can be monitored for entry control and access if feasible and practical. Intake water characteristics can be monitored for changes, such as the presence of petro-chemical contaminants. If a flammable or toxic substance is introduced into the intake system, it is possible that this contamination may be discovered by plant operations personnel who monitor water quality. Changes in the constituents of the water, such as color, pH, and odor, may also be identified by operations, maintenance, or lab personnel. During periods of elevated security risk, operators should make such inspections frequently and randomly throughout the day.

3.3.1 Groundwater

Groundwater supplies can be divided into two categories: 1) groundwater originating from a protected aquifer and 2) groundwater under the influence of nearby surface water. These systems have different vulnerabilities.

3.3.1.1 Protected Groundwater Supplies

Protected groundwater supplies are unlikely to be intentionally contaminated through the environment (e.g., spills) because of the depth of the groundwater, protective clay lenses, and the volume of water. On the other hand, a well head provides a more vulnerable target. The two intrusion points of a well head are the site inspection tube and the wellhead sample port. Either component can act as a potential conduit for the introduction of contaminants.

Wellheads equipped with intrusion alarms can trigger an automatic shutdown of the well. This would allow operations staff to inspect the facility for potential contamination prior to introducing the well water back into the system.

3.3.1.2 Unprotected Groundwater Supplies

Unprotected groundwater supplies can be potentially influenced by nearby surface water sources and percolation of contaminants through the soil. These sources typically lack protective clay lenses and are relatively shallow supplies, which make them more vulnerable to contamination events. The vulnerable components of these unprotected groundwater supplies are the water source, the site inspection tube, and the wellhead sample port. Each of these components can be a conduit for the introduction of contaminants.

Unprotected groundwater supplies typically go through additional treatment similar to surface water sources prior to distribution. Online monitoring could be used for unprotected groundwater supplies to provide early detection for unusual water quality changes that could be associated with a contamination event. In addition, the wellheads can also incorporate the same types of operational approaches identified above for protected wellheads.

3.3.2 Surface Water

The two common types of surface water supplies are reservoirs/lakes and streams/rivers. Both of these types of supplies require treatment at water treatment plants. Operational considerations to enhance security in both type of supplies include:

- Continuous raw water monitoring for surrogate parameters (such as pH, conductivity, total organic carbon [TOC], and toxicity). The implementation of this measure will greatly depend on the financial resources of the utility, as some of these monitors currently have relatively high life-cycle costs. Furthermore, the interpretation of the measurements depends on an intimate familiarity with baseline water characteristics and behavior under different conditions. Regardless, the development of a raw water baseline sampling program followed by the installation of inexpensive monitors for surrogate parameters would be a good start for most utilities. After establishing baseline water characteristics, utilities might enhance their monitoring with more advanced monitors, resources permitting. Information on online monitoring systems both for source water and the distribution system can be found in Grayman et al (2001), Hergesheimer, et al. (2002), and Pikus (in press).
- Site inspections are conducted at random times of the day.

3.3.2.1 Reservoirs/Lakes

Reservoirs and lakes are typically large bodies of water, significantly reducing the potential for introducing a contaminant at a dose high enough to be of concern. Additional operational considerations to enhance security include those listed below.

Basic

- A neighborhood watch program with local park staff and other community users of the reservoir/lake observing conditions at the site
- Inspection of dams under a dam safety program managed by FEMA or the appropriate state agency to identify the vulnerabilities of the dam

Advanced

- Source water watershed protection agreements with other agencies (state or local watershed districts) in which source water protection is a top priority for district managers

3.3.2.2 Streams/Rivers

Streams and rivers have a higher potential for short-term contamination events due to intentional dumping or accidental releases of contaminants upstream of the raw water intake structures. Additional operational considerations to enhance security include these:

Basic

- Coordination with local police departments, sheriff's departments, and other agencies, including the Coast Guard and Harbor Patrols, where appropriate, to develop early warning systems (EWSs) for reporting illegal and accidental discharges into the river or stream

Advanced

- Development of an integrated water quality monitoring response program that evaluates surrogates that are indicative of an unusual and unanticipated change in water quality

3.3.3 Raw Water Intake

Raw water intake structures for both reservoirs/lakes and streams/river systems are among the vulnerable facilities in the raw water system. The intake structures are typically located in remote locations (resulting in a slow response time), are gravity fed (allowing easier introduction of contaminants), and are often single of points of failure for the raw water delivery system (easily allowing disruption of raw water deliveries). Some operational considerations for ensuring the security of raw water intake structures include those listed below.

3.3.3.1 Basic

- At random times of the day, site inspections conducted of screens and bars by operations staff during elevated alert periods, and temporary use of guards during emergencies
- Coordination with other agencies and community groups to develop an "alert" program

3.3.3.2 Advanced

- Fencing installed on the land side of the intake structures with intrusion alarms and CCTV cameras for utilities that have the resources.
- Hatches and valves secure from tampering and entry attempts into the intake structure
- Daily, randomly timed site inspections of screens and bars by operations staff during elevated alert periods, and temporary use of guards during emergencies
- Coordination with other agencies and community groups to develop an "alert" program

3.4 Raw Water Conveyance

Raw water conveyance facilities are sometimes located in remote locations, making supervision of the facilities relatively difficult for operations staff. Some typical operational practices include improved awareness, site visits by operations staff, and physical protection system monitoring. These practices are described below.

3.4.1 General Considerations

General security considerations for raw water conveyance facilities are divided into Basic and Advanced categories.

3.4.1.1 Basic

Increased Awareness. A heightened awareness of utility staff, other local government employees, and the public observing trespass and physical disturbance is critical to keeping remote facilities secure.

Operator Visits. Although the trend over the last one to two decades has been to reduce the frequency of utility staff visiting remote facilities, for high-level threats reversing this trend may be reasonable. Coordinating with local police on facilities critical to the water system can add to the routine presence of authority and reduce the response time, if notified. This is especially true for master pump stations, tanks, or reservoirs that serve significant portions of the service areas. Site visits by operations staff should be scheduled at random times of day.

3.4.1.2 Advanced

Physical Protection and Monitoring. Remote pump stations, tanks, and reservoirs should be monitored by intrusion alarms, SCADA systems, and CCTV if threat levels warrant. Utilities should have procedures to ensure perimeter fences are maintained, gates are locked, and hatches are secure. Security audits of remote facilities can be performed every 6 months, or more often for critical facilities or if high threat levels exist.

3.4.2 Pump Stations

Raw water pump stations are typically located in remote areas and are unmanned, increasing the vulnerability of these facilities to malevolent acts. Operational considerations specific to raw water pump stations are provided below.

3.4.2.1 Basic

- Routine testing of stand-by pumps
- Maintenance of a spare part inventory for critical components in secure location apart from the pump station

3.4.2.2 Advanced

- At random times of the day, site inspections conducted by operations staff during elevated alert periods
- Automatic shutoff for pump stations with open wet wells that are susceptible to introduction of a contaminant

3.4.3 Pipelines and Appurtenances

Raw water pipelines create a unique problem in terms of protection from malevolent acts. The pipeline typically extends for many miles, realistically cannot be fenced off and protected, and provides a number of areas of exposure (e.g., exposed pipeline sections, airvacs, and vent pipes). Operational considerations for raw water pipeline security can include daily pipeline inspections by operations staff during elevated alert periods, including inspection and repair, as necessary, of air vent screens.

3.4.4 Raw Water Storage Tanks

Raw water delivery systems often include storage tanks upstream of the pump stations to serve as wet wells for the pumps. The major vulnerability for the tanks is intentional contamination through hatches and vent structures. The general operational considerations for raw water conveyance listed above can also be applied to raw water storage tanks. Additional operational considerations are provided below.

3.4.4.1 Basic

- Daily site inspection by operations staff during periods of high alert
- Response protocol for bypassing the tank when unauthorized intrusions have been detected

3.4.4.2 Advanced

- Hatch and vent intrusion alarms that automatically activate the tank effluent valve to isolate the tank

3.5 Treatment Facilities

Water treatment facilities are designed to include multiple barriers to malevolent acts by incorporating redundancy in treatment processes. The advantage of the multiple barrier approach is that if one barrier is breached, the plant will still have the capability of producing water that meets regulatory requirements. Additional information on operational measures for treatment facilities can be found in Water Treatment (AWWA 1995).

3.5.1 Treatment Processes

The typical treatment processes in a water treatment facility include:

- Pre-treatment, which includes screening to remove debris (in a surface water source), presedimentation to remove sand, addition of chemicals such as chlorine for slime control and oxidation of some metals and organics present in water, and potassium permanganate for taste and odor control
- Coagulation, flocculation, and sedimentation, which involve the addition of chemical coagulants (e.g., aluminum salts, ferric salts, and polymers), rapid mixing, and sedimentation to enhance removal of solids from the raw water
- Filtration, which is accomplished using conventional media filters (e.g., sand, garnet, and anthracite) or membrane filters (microfiltration or ultrafiltration) to provide final solids and microorganism removal, and polishing of the water
- Disinfection, which is typically accomplished using gaseous or liquid chlorine to deactivate any remaining microorganisms in the water prior to delivery to customers for consumption
- Treated water clearwell and pump stations, which deliver the treated water to the water distribution system

Each of the unit processes typically has redundant trains that allow periodic maintenance to be performed while the water treatment plant remains in operation. Operational security considerations for water treatment facilities include:

- Routine maintenance performed during low-demand periods of the year to ensure continuous operations during emergency events
- Construction-related shutdowns scheduled during low-demand periods of the year to ensure continuous operations during emergency events
- Cross-training of operations staff for improved response capabilities
- Development and testing of response protocols for unit process failures and upsets to verify the potability of water leaving the water treatment facility
- Restriction of access to critical facilities and utilization of the buddy system if insider threat is a concern

- Ban on public tours in critical areas of the facility
- Staff escorts to accompany visitors (e.g., vendors, contractors, and tours) while inside the boundaries of the facility

3.5.2 Chemical Delivery (Chemical Systems)

Water treatment facilities use a variety of chemicals as part of the treatment process. There are four major areas of concern regarding chemical feed systems: 1) loss of chemical feed systems that can result in the inability to properly treat the water, 2) introduction of contaminated chemicals into the process, 3) release of chemicals into the environment endangering the safety of workers and the public, and 4) mixing of certain chemicals, such as ammonia with liquid chlorine, on site where hazardous conditions are created. These events have the potential to impact public health and the environment. General operational security considerations for chemical storage and feed systems include those listed below. Following the general considerations are more specific considerations for gaseous and liquid chlorine (hypochlorites), the most common disinfectants used in water treatment, and other water treatment chemicals.

3.5.2.1 Basic

While chemical shipments are outside of utilities' direct control, utilities can work with their suppliers (especially chlorine suppliers) to identify ways to address potential hazards.

- Reject or batch test chemical deliveries that are suspect (e.g., those with a broken seal or late delivery). When possible, screen deliveries before offloading into storage tanks.
- Contact the vendor if chemical delivery has not occurred at the specified time to verify the status of the shipment, both for utility security as well as the safety of delivery personnel.
- Develop protocols with chemical suppliers minimize the potential for tampering during transit and to identify whether tampering has occurred upon arrival at the facility.
- Continuously monitor chemical feed systems and development of operational response to system failure.

3.5.2.2 Advanced

- Continuously monitor performance surrogates for processes using treatment chemicals to identify trends in reduced performance.
- Develop procurement specifications that require use of anti-hijacking technology and proof of compliance with the security guidance developed by the Chlorine Institute.

3.5.2.3 Gaseous Chlorine

Gaseous chlorine is stored in 150-pound cylinders, 1-ton cylinders, tanker trucks, or, at times, railcars. The highest area of concern for gaseous chlorine is a sudden release into the atmosphere due the failure of a tank or valve placing employees and nearby public at risk. The second area of concern is

the loss of chlorine disinfectant for use in finished water, which could potentially cause a public health problem. Operational security considerations for water treatment disinfection include the following.

Basic

- Continuous monitoring using a chlorine gas leak detector and trained operations staff available for small leak response.
- Coordination with local hazardous materials (HazMat) teams for response to large chlorine gas releases.
- Continuous monitoring of chlorine residual and testing of operational protocols to respond to loss of residual.
- Minimal amounts of gaseous chlorine stored onsite.

Advanced

- Change of the type of disinfecting chemicals to a less volatile type.
- Safety devices, such as self-contained breathing equipment, emergency repair kits, and adequate ventilation equipment, provided at every chlorination facility. Furthermore, these devices are to be regularly checked for proper operation and repaired as necessary.

3.5.2.4 Hypochlorite

In the past hypochlorination was typically used by smaller systems. However, due to security and safety concerns, larger plants have shifted from gaseous chlorine to hypochlorite. The most common forms are calcium hypochlorite ($Ca(OCl)_2$ in dry granules, powder, or tablet form) and sodium hypochlorite (NaOCl in liquid form). Operational security considerations for hypochlorite include the following:

- For $Ca(OCl)_2$, special storage must be provided to avoid contact with organic materials. Contact with organic material can generate enough heat and oxygen to start a fire. Similarly, when mixing with water, heat is generated; therefore mixing of with water to generate liquid chlorine must be done by adding the calcium hypochlorite to water to minimize the generation of heat. Thus, storage areas must be secure and must not contain any organic matter or water that adversaries can use to start a fire.
- For sodium hypochlorite (which has a pH of between 9 and 11), attention must be given to its corrosivity. Sodium hypochlorite must be stored away from equipment susceptible to corrosion damage. Otherwise, adversaries can use it to damage plant equipment.

3.5.2.5 Ammonia

Ammonia is used in the chloramination of finished water to maintain a disinfectant residual. Ammonia and chlorine added to water form chloramines, which remain in water for a longer duration than free chlorine as disinfectant. Ammonia can be added to water as anhydrous or aqueous ammonia (liquid form) or ammonium sulfate (powder form). The liquid form is volatile and

explosive, and is thus considered a safety hazard. Spills or leaks may require evacuation of the treatment plant, warehouse, or surrounding areas. Thus, operators must inspect ammonia tanks at every shift to ensure that there are no leaks.

3.5.2.6 Fluorides

Fluoride is added to water to reduce tooth decay in children. Fluoride compounds used in water treatment include sodium fluoride (powder or crystal), sodium fluorosilicate (powder or crystal) and fluorosilicic acid (liquid). As an acid, the liquid form is of special concern as it is very corrosive and can cause skin irritation. It is clear, colorless to yellowish, and generates fumes with a pungent odor.

Fluoride is available in 13-gallon and 55-gallon drums for small users, and in tank cars or trucks for large users. Operators must handle it with caution and must inspect containers for leaks at every shift. For the powder forms, operators must ensure that any spillage is quickly cleaned up to avoid the inhalation of the dust. In addition, because fluoride overdosing would not be detected by taste or odor, its potential as a hazard is increased. Utilities may want to verify that their water treatment facilities' feed systems have been designed to make accidental (or intentional) overdosing unlikely.

3.5.2.7 Lime Softening

Water softening is used to precipitate the naturally occurring minerals found in water. The chemicals most commonly used for this purpose are lime (either as hydrated lime [i.e., calcium hydroxide, CaOH2] or as quicklime, [i.e., calcium oxide, CaO]), soda ash (Na2CO3), and caustic soda (sodium hydroxide, NaOH). Hydrated lime, quick lime, and soda ash come in powder or granular form.

When lime is slaked for addition to water, great amounts of heat is generated, creating potential safety hazards. Corrosivity of softening chemicals is also of concern, one requiring that they are handled with care. Similarly, their dust can pose a health hazard. Dust control equipment must be well maintained and used while handling these chemicals.

An additional chemical that is sometimes used to stabilize softened water is sulfuric acid. It has the same safety issues of other corrosive chemicals used in water treatment plants.

3.5.3 Facility-wide Treatment

There are a number of operational considerations that can be applied to typical water treatment plant processes. A brief description of key operational practices is provided below.

- **Hatch/Vaults.** Hatches and vaults can be locked when plant staff is not using them. These appurtenances often provide direct access to critical processes or assets that, if attacked, could provide significant damage to the facility operations. The integrated use of remote detection devices, covered in Section 6, "Choosing the Optimal Physical Security Equipment," can help utilities to monitor portions of the system that are not regularly checked by utility personnel.
- **Valve/Sluice Gate Operators.** Valve and intake gates can be locked out in the normal operating configuration to avoid malicious tampering or an unintentional action by an employee. Utilities have used chains and locks effectively for years for this use.

- **Electrical Panels, Control Boxes, and Motor Control Centers.** These devices can have locking mechanisms that, when kept locked at all times, can help to prevent unauthorized access. Unrestricted access to this equipment could allow an immediate shutdown of unit processes and control systems, creating a high-level operational emergency. The integrated use of remote detection devices for these items is covered in Section 6.
- **Standby Equipment.** Standby equipment (e.g., generators, tanks, and pumps) should be rotated into operating mode routinely. The advantage of rotating equipment is to allow minor maintenance activities to be conducted routinely so that standby capacity is readily available.
- **Spare Equipment.** Critical spare equipment, such as pumps, should be stored in a location away from the operating equipment (e.g., in another building). This protects the equipment from a malevolent act that is directed at damaging the operational systems and allows the utility to quickly restore operations after an event occurs.
- **Power Supplies.** Loss of power can result in the failure of a water system to achieve its mission. Operational approaches to rapidly respond to localized or large power failures include these:
  - **Power Failure Emergency Plan.** Response to a power failure is an essential component of the emergency operations plan. The plan needs to identify the strategy that the utility will take (a systematic shutdown or continuous operations). The strategy selected will help to determine the requirements of secondary power needs. This, in turn, will identify the best way to supply alternate power, either through a secondary power supply or backup generation.
  - **Backup Generators.** Utilities can either purchase backup generators or rent generators using standing, guaranteed contracts with local equipment providers. Advance preparation for the use of backup generators includes installing and testing switchgears and pre-wiring the system to accept the alternate source of power. Switchgears are generally critical assets with a high vulnerability to risk, requiring special protection to prevent the loss of facility power.
- **Security Guards.** Temporary use of security guards during emergencies should also be considered during periods of high alert for those assets that do not have remote detection devices attached.

3.6 Finished Water Storage and Conveyance

Finished water storage and conveyance is the backbone of supplying treated water to customers. Failure of storage and conveyance facilities would have a major impact on customers. The finished water storage and conveyance systems comprise water storage tanks, pump stations, transmission mains, distribution system lines, service lines, and various appurtenances. Additional information on operational measures for finished water storage and conveyance systems can be found in Water Transmission and Distribution (AWWA 1996), Deb et al (1999), and Von Huben (1999). Operational security considerations for these areas are discussed below.

3.6.1 Storage Tanks/Reservoirs

Treated water is stored in water storage tanks at key locations in the water distribution system for a multitude of reasons. These include (AWWA 1996):

- Equalizing supply and demand
- Increasing operating convenience
- Leveling pump requirements
- Decreasing power costs
- Providing water during power source or pump failure
- Providing large quantities of water to meet fire demands
- Providing surge relief
- Increasing detention times
- Blending water sources

Storage tanks typically supply water to the water system either by gravity or pump stations. Areas that provide access to the water stored in the reservoirs include hatches and cleaning pipes. Cleaning pipes are installed on the roofs of some tanks for vacuum cleaning by divers. These access points are typically 1½- to 2-inch pipes with simple galvanized, unsecured screw caps. Removal of the cap provides direct access to treated water. Operators need to ensure that these caps are locked and cannot be removed by unauthorized persons.

Another access point in storage tanks is air vents that provide free flow of air in the tanks during filling and draining cycles. Their protection is limited to simple mesh screens. Depending on the design of the tanks, these vents may be directly accessible or accessible only by climbing the reservoir. Inspection of the screens needs to be included during the inspection of the tanks.

In general, operational security considerations for water storage facilities include:

- Development of a protocol for hydraulically isolating a storage reservoir when intrusion alarms are activated and tampering at the tank is verified
- Integration of intrusion alarms with automatic isolation valves for discharge lines when activated
- Development of a protocol for identifying contaminants, cleaning the tank, and restoring service
- Establishment of a neighborhood watch program in the community surrounding a storage facility

3.6.2 Pump Stations

Treated water pump stations are placed at key parts of the water distribution system to boost water to higher elevations for direct delivery to customers or storage reservoirs. Pump stations that supply water directly to customers without backup storage are often identified as critical facilities. The criticality of other pump stations in the water distribution system is dependent on the water demand

on the system and the amount of storage available to meet short-term fire flow requirements. Because an unmanned pump station can be an effective injection point for a large-scale intentional contamination, utilities may want to closely evaluate the security at critical pump stations. Operational security considerations for pump stations include the following.

3.6.2.1 Basic

- Maintenance of a spare pump and critical replacement part inventory in a location away from the pump station
- Routine testing of standby pumps and rotation of the standby pumps into service

3.6.2.2 Advanced

- Development and testing of an operations protocol to run the distribution system in a pressure mode in the event that a water storage tank is out of commission
- Development and testing of a protocol for turning off the pump when intrusion alarms are activated and tampering at the pump station is verified

3.6.3 Transmission Mains

Transmission mains are generally large diameter pipelines with no service connections. They are commonly greater than 24 inches in size and convey finished water from the water treatment plant to the distribution system or wholesale customers. Transmission mains are primarily located outside the service areas, placing them in more isolated areas. Depending on the topography and the distance covered, stretches of the mains may be alternately buried, exposed, suspended, or elevated. These exposed stretches pose a particular vulnerability to physical, vehicle, and outsider access. Access to transmission mains can also occur through air- and pressure-relief valves when the valves are exposed. Thus, routine, periodic inspection of exposed areas and air and pressure relief valve screens is suggested.

3.6.4 Distribution System Mains and Appurtenances

Distribution mains convey water from the transmission main to service lines and typically are less than 24 inches in size. These mains are located within the service area and are rarely exposed at ground level. However, access to the distribution mains can occur at numerous locations such as fire hydrants, air-relief valves, storage or surge tanks, pump stations, pressure-relief valves, and service connections within buildings. Access through fire hydrants and other appurtenances described above provides a potential means of contaminating particular services areas. Because of the lack of control and the inability to secure the different components, the distribution system is considered to be the most vulnerable part of a water system.

3.6.4.1 General Considerations

In general, the following operational considerations apply to distribution systems and their appurtenances. Note that most of these items are often part of industry-standard practices for utility O&M programs.

Basic

- Protective covers for all appurtenances, secured at all times
- Development of an emergency isolation and flushing protocol for the distribution system
- Development of a disinfection and testing protocol for distribution system pipelines
- Maintenance of a replacement part inventory for critical pipeline appurtenances and a replacement pipe inventory or a standing, guaranteed contract for emergency delivery

Advanced

- Locking covers for fire hydrants installed in coordination with fire departments
- Backflow devices on appurtenances to reduce the potential for intentional or accidental back siphoning into the distribution system

3.6.4.2 Construction Meters

Utilities often maintain little or no control over construction meters used by contractors throughout the distribution system. Construction meters provide direct access to the water distribution system and, in uncontrolled situations, can create confusion over authorized use areas. Some of the effective operations approaches that have been used by utilities include the following:

Basic

- Installation of all construction meters by the utility and tracking of the locations of current meters installed.
- Use of Reduced Pressure Principle Devices (attached to construction meters) to prevent accidental contamination from backflow into the water system.
- Inspection of construction meter activities on a routine basis promotes compliance with utility requirements.
- Establishment of standard points of use and possible establishment of water stations controlled by the utility for contractor supply.
- Use of utility personnel, other local government employees, law enforcement, and "Neighborhood Watch" groups to maintain vigilance with respect to permitted construction meters. Section 3.6.5, "Increased Awareness," provides additional discussion on such approaches.

Advanced

- Implementation of "construction meter" program elements developed by utilities that have implemented comprehensive security programs. These elements include 1) regulating the issuance of such meters, 2) controlling access to hydrants for construction use through a permit program, 3) inspecting and approving all permittee equipment to be used to connect to utility

infrastructure, and 4) establishing a labeling system for permittee's equipment that clearly identifies the equipment that may be connected to utility infrastructure.

3.6.4.3 Meters

Most utilities in the United States meter the finished water delivered to residential and commercial customers. In areas of the United States where freezing temperatures are common, water meters are often located inside and openly accessible to the occupant. Locking lids on water meters can provide greater security. Limited operational security considerations for water system meters are adding locking lids to meters. In addition, the implementation of industry-standard practices for utility O&M programs, which include meter testing and replacement, important enhances the security of a utility.

3.6.4.4 Backflow Prevention Devices

Utilities have routinely practiced backflow prevention on industrial and commercial facilities that pose a risk to the domestic water system. Residential meters have not traditionally been backflow-protected because they have been considered to be low risk to water systems and the high cost to implement an effective program.

Most state drinking water programs have regulations in place with regard to cross-connection control. Utilities should be, and should continue to be, in compliance with state and local cross-connection regulations. Those that are not in compliance need to enforce these regulations to protect one of the most vulnerable areas of the water systems.

Another operational security consideration for backflow protection is the continued use of an industrial/commercial backflow protection program. This program employs the appropriate types of devices for the annual inspection of high-risk applications. Implementing industry-standard practices for utility O&M programs that include cross-connection surveys and backflow prevention programs is critical in enhancing the security of a utility.

3.6.4.5 Valves

Multiple types of valves for various purposes are found in a distribution system. These include:

- air/vacuum-relief valves
- butterfly valves
- check valves
- control valves
- diaphragm valves
- gate valves
- globe valves
- needle valves
- pinch valves
- plug valves
- pressure relief valves

The value of system valves is their function in operating the system, especially in the event of an emergency. Valves serve many purposes, including regulating or shutting off flow, releasing pressure or air, allowing air to enter the system, preventing flow reversals, separating zones of different pressures, and regulating tank levels. Most valves do not present an avenue for introduction of

contaminant into the distribution system; however, due to their criticality in system operations, their proper operation is of utmost importance, especially when trying to isolate sections of the system during emergencies. Operational security considerations for valves include:

- Routine exercise and replacement programs for water distribution system line valves
- Maintenance of a replacement inventory for critical valves

3.6.4.6 Hydrants

Fire hydrants are typically located at street intersections or intermediate points. Hydrants provide adversaries the opportunity to introduce large volumes of contaminant directly into the distribution system. As mentioned above, the implementation of industry-standard practices for utility O&M programs that include the inspection and testing of hydrants is important in enhancing the security of a utility.

3.6.4.7 Blow-offs

Blow-offs are small diameter pipes (2 to 4 inches) extending from mains to above the ground surface. Used to flush water mains where there is not a hydrant, they often are located at distribution system dead ends and at low points for sediment removal. Blow-offs are direct points of access for injection of contaminants into the distribution system; therefore, they are to be inspected periodically for tampering and to examine the condition of their screens.

3.6.4.8 Access and Inspection Hatches

Access hatches and vaults are part of most assets of a distribution system such as large mains, storage tanks, and pump stations. These vaults are secured either by padlocks or bolts. At a minimum, utilities could harden these access points with better locks and inspect them on a regular basis.

3.6.4.9 Service Lines

Ranging in sized, service lines convey water from distribution mains to the customers. Because they are connected to the customers' piping, they provide a point of access into the distribution system. This access can occur at the customer meters or taps, providing an intentional or unintentional source of contamination of the water system. Unintentional contamination can occur through cross-connections. Residential customers may have cross-connections from chemical dispensers on garden hoses, water softeners (drain connected to sewer), sprinkler systems, submerged garden hoses (such as filling a pool or hot tub) or taps (particularly those extended with hoses), etc. Commercial customers may have cross-connections at chemical vats and laboratory washing equipment, for example. Intentional contamination can occur using commonly available equipment to exceed service pressures and pump contaminant into the distribution system.

3.6.4.10 Sample Taps

Sample taps for water quality monitoring are located at various locations within the distribution system, sometimes next to fire hydrants and within pump stations, buildings, storage tanks, and vaults. Operators can check the locks of the sampling station boxes or vaults to determine whether there has been tampering.

3.6.5 Increased Awareness

Increased public awareness of water distribution system operations is an effective way to increase the utility's knowledge of unauthorized activities and potential malevolent acts. The two primary groups that can be effectively engaged in this process are utility employees and the public.

3.6.5.1 Employees

Given that distribution systems are underground and can cover wide areas, it is impossible to constantly monitor a distribution system. Consequently, it is important to rely upon the utility staff to be cognizant of anomalies that may indicate a breach of security in the distribution system or pumping stations. While traveling along daily routes or from job to job, employees should take notice of any security discrepancy. Any persons or equipment, other than those of the utility or utility contractors, around water facilities should raise suspicion and be reported according to standard operating procedures.

In addition to utility employees monitoring the security of the distribution system, management should work with other local government departments and agencies to train their employees to be aware of any unauthorized entry into water system vaults, pump stations, or tampering with fire hydrants. In addition to the police, refuse haulers and road crews can also be made aware of water system security because of their frequent travels across a municipality.

3.6.5.2 Public

Given the large number of points of entry to a water distribution system, heightened awareness by the public is valuable for identifying unauthorized access to these systems. Water utility managers should work with those involved in community policing programs, such as Neighborhood Watch, to educate citizens on distribution system security. Identification of unauthorized tapping of fire hydrants, vandalism, and open or damaged fences and hatches should be reported. Individuals who note suspicious behavior and know how to contact the authorities can act as a deterrent and significantly reduce the risk to the system. In areas of low visibility or in remote areas, however, installation of fire hydrant locks and anti-theft devices, in coordination with the local fire departments, are recommended.

3.7 Support Services Facilities

Support service facilities include maintenance shops, warehouses, and storage facilities; administrative offices; fleet; and laboratories.

3.7.1 Maintenance Shops, Warehouses, and Storage Facilities

Utility maintenance facilities provide a central location for the utility to conduct routine repair and maintenance of equipment. Especially critical maintenance facilities include ones that store the various chemicals discussed above and large amounts of fuels such as gasoline, diesel, natural gas, or propane. For large facilities, temporary use of security guards during emergencies should be an option.

Similarly, warehouse facilities are used to store supplies for utility operations. These facilities serve an important function for providing key supplies during emergency events. Loss of the utility warehouse will impair the ability of staff to rapidly respond and correct system problems. Table 3-2 describes the potential threat and operational considerations for maintenance shops and warehouses.

TABLE 3-2
Maintenance Building and Warehouse Threat and Operational Considerations

Threat Type	Threat	Operational Considerations
Vandal	Malicious damage	Keep facility locked during non-working hours
		Employ intrusion alarm response protocol
Criminal	Equipment theft	Provide employee and visitor identification badges
	Injury to employees	Lock tools in protected cages
Saboteur/Terrorist	Use of equipment or fuels to destroy or damage property	Establish emergency contracts with local businesses and suppliers
		Establish operational procedures to isolate and shut off fuel valves in maintenance buildings
		Post guards
Insider	Revenge, personal gain	Restrict access to maintenance buildings and warehouses

3.7.2 Administrative Offices

Utility administrative offices provide the business functions (e.g., human resources, billing, and purchasing) that are required to keep the utility operating. The administrative offices contain sensitive information about employees, customers, and utility operations. Many of the utility administrative functions are not easily contracted out and need to be functional quickly after an incident occurs. Table 3-3 describes the potential threat and operational considerations based on the adversary type.

TABLE 3-3
Administrative Offices Threat and Operational Considerations

Threat Type	Threat	Operational Considerations
Vandal	Malicious damage	Keep facility locked during non-working hours
		Employ intrusion alarm response protocol
Criminal	Property theft	Provide employee and visitor identification badges
	Injury to employees	Store sensitive documents in secure location
Saboteur/Terrorist	Destruction or disabling of utility operations	Establish back-up locations to quickly restore business functions
	Damage to revenue stream	Isolate the management system and use third-party billing and collections
	Injury to employees	
		Post guards
Insider	Revenge, personal gain	Restrict access to sensitive documents and areas

3.7.3 Fleet

The utility fleet typically includes personal vehicles (e.g., trucks and cars) and large construction machinery (e.g., backhoes and tractors) that are critical for routine operations and emergency response. Although the utility fleet is an essential component for operations, in most cases, local business can supply short-term rentals in the case of emergencies. Table 3-4 describes the potential threat and operational considerations for the four types of outsider threat.

TABLE 3-4
Fleet Vehicle Threat and Operational Considerations

Threat Type	Threat	Operational Considerations
Vandal	Malicious damage	Keep facility locked during non-working hours
		Employ intrusion alarm response protocol
Criminal	Property theft	Provide employee and visitor identification badges
	Injury to employees	Lock vehicles in protected compound
		Install geographic positioning system (GPS) tracking in vehicles
Saboteur/Terrorist	Disruption of ability to operate and respond	Establish emergency contracts with leasing companies
		Post guards
	Injury to employees	
Insider	Revenge, personal gain	Restrict access to vehicle keys
		Install GPS tracking in vehicles

3.7.4 Laboratories

Water quality and process laboratory facilities provide operational and regulatory testing for the utility. These facilities are considered to be less critical because the work can sometimes be outsourced to contract laboratories on a short-term basis, if needed. Security considerations for laboratories include those listed below.

3.7.4.1 Basic

- Use a chemical receipt log that indicates the name of chemicals received and the name of the person to whom the chemical is released.
- Create and maintain an inventory of chemicals kept at the laboratory.
- Remove chemicals that are consumed in process, disposed, or shipped from laboratory inventory logs.
- Secure laboratory reagents and limit access only to authorized personnel.
- Store highly toxic materials and hazardous materials in locked cabinets, freezers, or refrigerators. This applies to sodium cyanide, potassium cyanide, arsenic compounds, select agents, and other materials that may be readily recognizable as poisons.
- Limit the number of staff that are authorized to purchase chemicals and supplies.
- Establish arrangements with other laboratories to be used in situations where the utility's lab does not have a certain analytical capability, is overloaded with work, or is unable to provide service. Maintain an up-to-date list other laboratories and the types of analyses performed.

3.7.4.2 Advanced

- Limit the amount of chemicals that are stored at the facility.
- Protect laboratory gas cylinders, service and spare, in secure wire mesh cage.
- Limit the amount of chemicals that suppliers can provide at one time.
- Establish a secondary location at the treatment facility for conducting process control-related analysis.
- Consider the use of RFID tags for valuable instrumentation such as the gas chromatograph/mass spectrometer.