Water and Wastewater System Security: A Technical Analysis

Thomas H. Powell

The public depends on water utilities to provide clean, reliable, and safe drinking water at all times. To consistently deliver quality water to their customers, utilities must not only efficiently operate and maintain effective water systems, they also need to securely protect those systems. The primary risk of an unprotected system is not theft, but rather contamination of the water supply, which could impact public health and possibly result in a loss of public trust.

A recent situation that demonstrates the potential vulnerability of surface water supplies resulted from an industrial chemical leak of 4-methylcyclohexanemethanol in Charleston, W.Va., that contaminated the capital city's water supply in January 2014. Due to the chemical leak, the local river, which is the city's water source, was contaminated, making the water unacceptable for treatment and distribution as potable water. This example certainly highlights the need for effective security systems to protect all of the water systems in the United States.

Various chemicals are used in the water treatment process, and these chemicals are typically stored in bulk at the plant. If improperly handled, mixed, released, or discharged, many of these chemicals can be dangerous to public health. Therefore, it is of critical importance to prevent the possible theft or discharge of these potentially harmful chemicals.

Security: A Growing Concern

Public water systems, including treatment and distribution facilities, are required to be assessed and protect against threats to the system for the safety of consumers. Protection of water systems has been an important issue, even before the terrorist attacks of Sept. 11, 2011. In the U.S., the Department of Homeland Security (DHS) and the U.S. Environmental Protection Agency (EPA) have established minimum guidelines for security. In 1998, Presidential Decision Directive 63, which focused on identifying and rectifying vulnerabilities in the country's critical infrastructure, including water and wastewater systems, was issued by then-President Clinton.

The directive noted that these systems had become increasingly automated and interconnected, making them vulnerable to any number of natural disasters and other threats.

When the DHS was formed in 2002, it combined the resources and administration of 22 agencies and 180,000 employees under a new agency to foster a comprehensive, coordinated approach to protecting vital U.S. systems.

In 2003, the Homeland Security Presidential Directive 7 (HSPD –7) established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources to protect them from terrorist attacks. Through this effort, 18 critical infrastructure sectors were identified, including water, energy, transportation, dams, ports, and more.

As a result, security guidance was developed for each critical infrastructure. Guidance for water infrastructure included documents issued by the American Water Works Association (AWWA), Water Environment Federation (WEF), American Society of Civil Engineers (ASCE), Institute of Electrical and Electronics Engineers (IEEE), International Society of Automation (ISA), American National Standards Institute (ANSI), and EPA outlining standards and recommended practices that could be used as guides for system owners and consultants.

Thomas H. Powell, P.E., is the instrumentation and controls engineering group head and an associate at Greeley and Hansen in Chicago.

Evaluation and Assessment of Public Water Treatment Facilities

The sophistication and complexity of protection for a water system, its facilities, and equipment is dependent upon multiple factors, including the size and financial resources of the community being served by the system. To help illustrate the factors that should be considered, a typical municipal water system, which includes a surface water supply, a water treatment plant, pumping stations, storage reservoir, elevated tanks, and distribution piping, will be used.

The first step of the evaluation process is the physical assessment of the existing facilities, which can be done using the Vulnerability Self-Assessment Tool (VSAT). The documented evaluation is followed by the subsequent identification of proposed improvements or other alternatives that would increase the security of the water system using government and industry standards and guidelines. Once the proposed improvements are identified, engineering design and project implementation considera-

tions are established for protecting the system for the community.

These physical and security guidelines include references from AWWA (http://www.awwa.org/legislation-regulation/issues/utility-security.aspx), ISA (www.isa.org), DHS (https://www.dhs.gov/water-and-wastewater-systems-sector), and EPA (https://www.epa.gov/homeland-security-research/water-system-security-and-resilience-homeland-security-research).

As part of the evaluation, the site assets of each production or distribution facility should be identified. Some of these assets include equipment (pipes, motors, wire, etc.), raw materials and finished products, chemicals, and natural resources. Service disruptions can happen as a result of the theft of raw materials or equipment from the site, whether they are in use or just stored. For example, copper materials have often been stolen for their recycle value. Therefore, the following questions should be considered in evaluating site assets:

- What raw or recyclable scrap materials are stored on the property?
- Is fuel for vehicles or generators stored in out-of-the-way areas?
- Could any of these items provide an opportunity for a thief to enter the property and cause an immediate or future service disruption?

Water system security requires both site and equipment protection, and should consider physical, electronic, and procedural elements, and incident prevention, which involves planning and preparing for various types of scenarios, including threats. Considerations in this regard include how someone could enter a facility through abnormal methods. Once someone is inside, the following should be considered:

- What damage could be done?
- What could be stolen?
- What barriers, procedures, or other options could stop or deter the theft?

When thinking about facility security, what type of incident could result in an unwanted news headline? Planning, protection, and prevention with security can help keep that headline out of the media.

As part of the security evaluation of the facility, the physical location must be considered; not only where the facility is located, but how the facility can be accessed. Also, what is adjacent to the facility and how can the facility be accessed from roads, expressways, urban highways, city streets, railways, or waterways?

In addition to the location, the frequency and types of visitors should be considered as well. Are there visitors other that municipal employees, customers, delivery personal, and students? Does the utility allow customers to pay service bills at the administration office?

Looking more specifically at the example water system described earlier, while the subject water treatment facility does not allow consumer bill payment service at the administration office, it does have regular deliveries from multiple package carriers for supplies, as well to meet service offerings. The plant also accepts drop-offs of water sampling and testing materials from the local water quality laboratory. Again, the quantity and type of expected visitors for a facility impacts the type of security elements that should be implemented.

This water treatment facility is surrounded by residential properties, and the facility management is very sensitive to being a good neighbor. The utility does not want to create the appearance of a fortress or isolate its neighbors, so many of the physical security elements selected for this facility have been made less obtrusive, with low impact to the neighborhood.

In the same community, the subject wastewater treatment plant is just outside the city limits, near businesses and a hospital. The plant is accessible by major city streets and bordered by both a river and an active railroad track. As part of the engineering and security evaluation for this example facility, it is important to consider what paths an intruder can use to gain access to the property and assets within the property.

Although the primary focus of a water facility is production of water and the effective maintenance of system equipment, the safety and security of both plant personnel and the system should also be an important focus. However, the primary function of staff is to maintain and oversee treatment operations, not site security. Since many facilities do not have dedicated security staff on site, these utilities must rely on the municipal police, county sheriff, or state police to respond when a threat is detected or abnormal events occur.

In the subject water treatment plant, the main process facility is fully staffed during the day shift, but with limited staff overnight. Remote sites are staffed intermittently according to maintenance needs. As such, the facility relies on the municipal police department for response to security incidents.

Security Principles and Strategies

The basic principles of physical security include three strategic components: to deter, detect, and delay.

Deterrence focuses on making facilities or equipment less available to a threat, by basically making it harder to obtain entrance into the facility. This can be done by modifying the appearance of the facility or physically changing the structure. The use of warning signs can deter less motivated intruders, and the use of visible cameras may deter pranksters or more serious threat activities. Access gates, pedestrian turnstiles, fences, moats, and movable vehicle barriers can also help deter access.

Detection focuses on the ability to monitor a facility or activities within the facility in real time. This is normally accomplished through the use of surveillance monitoring of facilities with video, motion detection, or other electronic methods.

Delay involves slowing the access either to the facility or within the facility. One of the easiest methods to delay access is to have doors that are locked and keys that are controlled. An alternative to locks and keys is to use a card access control system, which provides the same benefit of securing doors.

Security Design Elements and Challenges

Although almost any facility can be vulnerable to access by a committed threat, site access

Continued on page 26

Continued from page 25

by those threats and pranksters can be made much more difficult through the design and incorporation of various security measures. Design elements that are typically used to delay or discourage access include fences, barriers, labyrinth access, and signs, as well as physical distance and location.

For monitoring of physical space within the facility, motion monitoring equipment, door position monitoring, and video surveillance can be implemented to show when unauthorized people are in the area. The use of a card access system allows authorized people to be granted access, while providing an alert when unauthorized access is obtained.

If a card access system is part of the enterprise system for the community and is shared across multiple operating groups, additional considerations are required. An enterprise system allows for a comprehensive master database of authorized employees, but also creates other challenges. For example, a programmed system presents a challenge for timed locks and access control for holiday schedules, as well as providing temporary access for multiple contractors.

Other challenges to site monitoring may be related to climate or specific location conditions, such as frozen soil in cold climates, or surface rock terrains, which can restrict certain monitoring technologies, including vibration monitoring. Wildlife (deer, coyotes, and other large animals), normal pedestrian traffic, significant temperature changes, and seasonal variances to the facility can also affect site monitoring equipment.

In winter, snow piles from clearing roads and parking may restrict monitoring, while in the summer building ventilation needs may reduce compliance with closed-door requirements. Thermal cameras detect the heat of an approaching person or object, which works well in cooler temperatures, but as the temperature approaches 100 degrees, the images of people blend into the background. When foliage changes seasonally, the images viewed by cameras can change significantly, including blockage of security critical images. The extent of foliage change varies by geographic area, and successful implementation may require increased grounds maintenance to minimize foliage obstructions.

The subject water and wastewater facilities were geographically located in the north, so they experienced both winter freeze and 100-degree summer heat conditions, with a vigorous growing season for summer foliage. The geographic location of facilities impacts the required engineering decisions for implementing security measures.

With recent advances in analytics and algorithms, video monitoring can detect movement and activate alarms based on predicted behaviors and motion. For example, large animals can be interpreted to be intruders and, conversely, intruders can attempt to mimic animal behavior. Technology continues to advance in both hardware and software.

At the subject facility, motion monitoring is provided up to the facility fence line. Challenges for motion detection at this facility include students walking to a neighborhood school along the fence line, wildlife, and overhanging foliage from neighboring yards.

The owner or operator of a public potable water facility should discourage access to those who are not authorized using fencing, signs, and other methods to limit access.

With elevated tank leases, nonmunicipal employees have access to the site and to the top of the tanks and, therefore, potentially to the finished water. While the municipality can confirm the background of their employees, they do not have access to the records of the employees of the companies that service the equipment.

Valve and metering vaults may allow ground-level access to finished water. To reduce potential for contamination, the physical improvements for the subject facility include manhole drip trays, warning signs, and video monitoring,

A well-illuminated facility provides fewer shadows for hiding, is more inviting to visit, is potentially safer for workers, and provides a more attractive workplace than a facility with limited lighting. A suitable level of illumination also assists in video monitoring, with improved color rendering and object recognition.

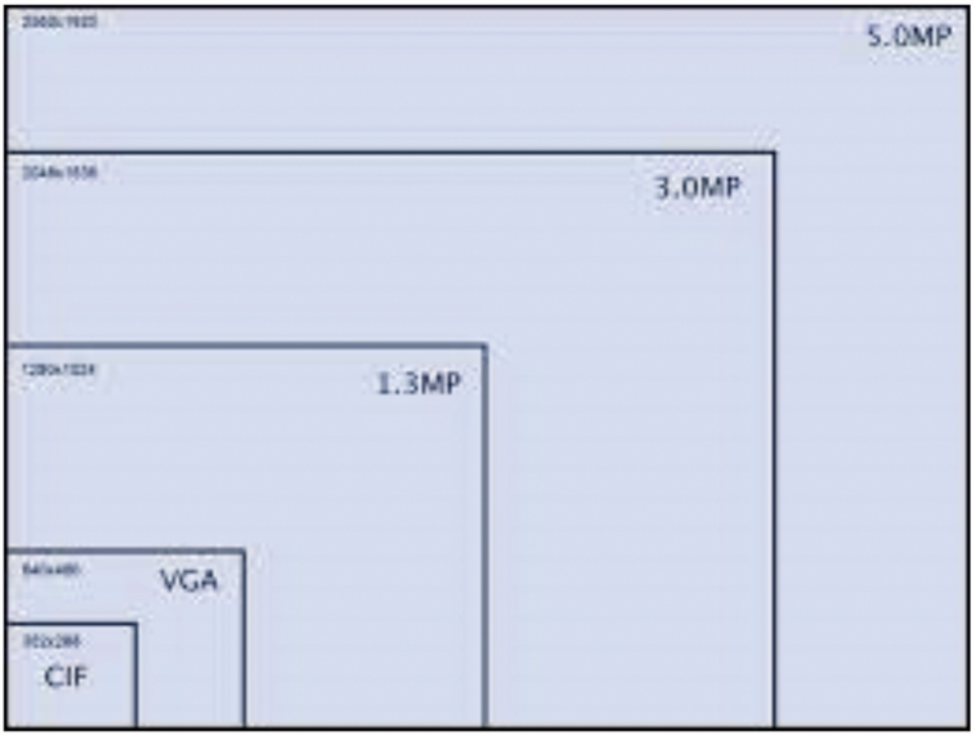

Figure 1. Size Differences in Video Graphics Array Immages

A Security-Focused Culture

Employees are the most valuable asset in any security system. They need to be trusted and trained to do their normal job and functions, as well as support security efforts and procedures.

Therefore, it is important to develop a security-focused culture that is fully embraced by management and staff within each facility. Ultimately, the best security features in a facility may be the eyes of your employees. Regular staff members are the ones who can often notice minor or major changes, as well as abnormal events. As part of this culture, respect is key and should be extended both inside and outside the facility fence. Respect includes avoiding profiling visitors, employees, and guests and establishing a system that does not monitor activities that should be considered private.

Video Surveillance Considerations

Video systems are the eyes that never sleep or take a vacation. Part of the design includes

Continued on page 28

Continued from page 26

determining if the system is to be visible—using an obvious camera—or unobtrusive. Both types of systems can be effective. Cameras can be placed to blend into the walls or ceilings, or in locations where they can be easily noticed. The system can be limited to a few strategically placed cameras, or have many of them. Keep in mind, however, that the number of cameras can impact the communication bandwidth and security network performance.

In addition, when using cameras, the type of signage that is required by the local community to properly notify the public when they may be on camera at a public or private facility must be considered.

Electronic adjustable cameras (pan, tilt, or zoom) allow real-time adjustment to the image when needed. Adjustable images can be fixed once electronically set without requiring physical adjustment on a ladder or scissor lift, and can also be easily adjusted to avoid interference with seasonal direct sunlight.

The size of the desired image is another design consideration. Figure 1 shows the relative size differences between video graphics array (VGA) images: a 1.3 megapixel (MP) image to a 5 MP image. The larger the image size in MPs, the more clarity the image will have when stored and reviewed, whether for recognition, personal recognizable characteristics, or reading license plate characters.

The many elements related to the selection of video monitoring hardware includes the physical camera, the lens, the image size or resolution, the focal length, the ability to change the view, how to store and retrieve the images, the ability to use the same camera for day viewing and night viewing, and more.

Privacy Considerations

Video surveillance and security includes monitoring of both the facility and of people (the people who are supposed to be there, as well as the people who aren't). The key concept is that people are being monitored by people.

While monitoring can help improve the security within a community, the images can also potentially be misused. Establishing a published video management policy may be beneficial to increasing trust not only with employees, but also the public.

Electronic Security Considerations

Electronic security and cyber hardening is recommended by several organizations, including ISA to protect electronic networks. These organizations have standards on cybersecurity and protection of electronic assets. Recommended protection includes restricting access, monitoring and controlling access and usage, implementation of firewalls, layers of protection, and establishing network rules. The rules should be applied systemwide, be uniform, and apply to all users, including contractors and visitors. Establishing an independent visitor network can successfully limit the access to the primary control system and increase its security. Electronic networks need to be protected from eavesdropping (stealing of data), theft of service, denial of service, and hijacking the control of equipment.

There are fundamental differences in securing a control system from an information technology (IT) system. The IT systems typically have a service life of three to five years, while control systems typically have a 20-year life. The systems deploy antivirus software and are regularly updated, while control systems, with their executable code, typically do not deploy. Control systems have a constant uptime requirement (greater than five-nines reliability at 99.999 percent) while IT systems can accept outages. The IT systems that are three-nines reliable (99.9 percent) allow for up to 8.75 hours of outages in an 8760-hour year. The IT server rooms are typically secure, with control system hardware located in control rooms with general access only permitted once after gaining access in the building.

In the Aug. 2, 2013, issue of *Technology Review*, a decoy water plant (virtual) was established as a test of control system security. The outcome of the test was that the decoy water authority control system was hacked by a foreign army. This means that there are people "out there" who could hack your system if they can find it, so system security is required.

The Department of Energy (DOE) has published 21 steps to improve cybersecurity of supervisory control and data acquisition (SCADA) networks. These steps provide guidance for hardening against cyber attacks, which may include prevention for uploading of viruses, worms, or malware. The guidance also protects against actions that include data theft, denial of service, and pranks.

Planning and Preparation

Part of security is planning in advance for how to best respond to various types of attacks. Tabletop training exercises designed specifically for a facility and team are available. These exercises are planned by experts to obtain response from the facility team during a simulated event and allow for procedural and operational changes. After the simulation, improvements to operating plans and facility are typically implemented based on the results of the simulation.

A plan for emergency response is critical. The security design or master plan should include a facility command center, with internal and external communication systems, and real-time process information and security information. A facility without a command center will not be able to respond as quickly to an emergency.

Training on how to effectively use the system and respond to both normal and potential security events is essential. The first time an alarm occurs in the middle of the day or night, the employees need to acknowledge it and be ready to properly respond.

Water and wastewater system security includes multiple elements, and surveillance is just part of the protection. Security includes physical security, access control, network security, cybersecurity, operational culture, operations and maintenance, and, most importantly, planning, which includes considering all potential threats to the system.

Keeping water and wastewater systems safe requires vigilant observation to identify unusual or suspicious activities through a security-focused culture that engages facility staff and embraces security processes and technology systems. Developing a comprehensive security plan is key to providing safe, clean, and reliable drinking water to the public at all times. The subject facilities in this discussion became more resistant to anticipated security threats as a result of the implemented design. Given evolving threats to critical infrastructure and changing worldwide conditions, regular and reoccurring evaluations of physical and cybersecurity is strongly recommended for each facility. ◊