American Water Works Association

PRACTICAL IDEAS FOR WATER OPERATORS

Opflow

VOLUME 43, NO. 5 MAY 2017

WATER LOSS CONTROL
System Size Can Determine Water Loss Control Challenges

TOTAL WATER SOLUTIONS
What Is Membrane Bioreactor Technology's Role in Water Reuse?

SYSTEM SECURITY
Optimize Perimeter Defense for Utility Security

WATER QUALITY MONITORING
Robust Sampling and Lab Prep Bolsters Incident Response

STORAGE TANKS

MAGNETIC BRACKETING AND MOUNTING SYSTEMS HEIGHTEN WATER TOWER SAFETY

http://dx.doi.org/10.5991/OPF.2017.43.0031

Tom Wallace is western regional manager of Southwest Microwave (www.southwestmicrowave.com), Tempe, Ariz.

Optimize Perimeter Defense for Utility Security

Water and wastewater facilities are critical components of any country's infrastructure. Knowledge of potential threats and technology limitations are essential to designing an effective perimeter security system. BY TOM WALLACE

WATER SUPPLIES and treatment facilities must be protected to ensure public health. Although cybersecurity is a common concern, physical security—such as protecting the exterior perimeter of water and wastewater treatment facilities—is equally important to provide early warning of attempted intrusion. Knowledge of potential threats, as well as available intrusion-detection sensor technologies and their limitations, is essential for achieving the primary objectives of a perimeter security system:

- Deterrence—physical and visual
- Detection—early warning of unauthorized access
- Delay—physical barriers such as walls or fences
- Assessment—ability to visually assess activity at alarm occurrence
- Response—in-house local security force or local law enforcement

SECURITY CONSIDERATIONS

Conducting a vulnerability assessment will help users identify areas of concern and assets to protect. Common questions to address include the following:

Who poses a threat to critical water infrastructure? The list may include terrorists (foreign or home-grown), thieves, disgruntled former employees, or vandals.

How knowledgeable is the intruder? Is he or she familiar with the facility, operations, schedules, or security and video surveillance system?

What tools might be available to the intruder? For example, what would happen if an intruder used hand tools, power tools, a ladder, or a vehicle?

What level of damage can an intruder cause to a facility or community? Potential concerns include water contamination, destruction of equipment, or release of untreated waste or chemicals.

What's the real cost of an intrusion? Physical damage and repair costs seem obvious and easy to equate to a dollar value, but other costs can be more difficult to assess, such as facility downtime, liability claims for injuries or death, and bad publicity.

All these concerns play a part in determining the required level of security and the sensor technologies needed to secure a given facility.

TYPES OF SENSOR TECHNOLOGIES

Although many different perimeter sensor technologies are on the market, they can be categorized into five main types: fence or fence-mounted, line of sight, buried or covert, video analytics, and thermal imaging. All these options can be effective for water and wastewater utilities.

Fence and Fence-Mounted Sensors. These sensors make up the largest group. Some sensor systems are part of a physical fence such as a *taut-wire fence*, which comprises multiple strands of barbed wire strung between posts that incorporate position sensors for each wire. When a wire is pulled, pushed, lifted, or cut, it actuates one or more of the post sensors and generates an alarm. Another fence type is an *electric-field fence* (different from an electrified fence), which consists of multiple strands of nonbarbed wire, with one wire acting as the field-generator and the others acting as the sensing wires. An alarm is generated when an intruder interrupts the field created between the wires. *Electric fences*, or "shock" fences, are also composed of a series of electrically charged wires that can deliver a potentially lethal jolt of electricity and generate an alarm when that occurs.

Fence-mounted sensors can include special sensing cables or small wired mechanical modules attached to existing fences. These can be made of several different technologies. *Electro-mechanical* or *piezoelectric sensing modules* are attached to a length of wire or cable and spaced at 10- to 20-ft intervals along a fence. Fence vibrations cause the device within the module to move and generate an alarm. *Microphonic cables*, whose sensing is based on either a change in capacitance or magnetic properties, can detect fence vibrations and generate an alarm. *Fiber-optic sensors* consist of fiber-optic cable that operates from a laser diode source and responds to minute "light bending" when the fence is vibrated or cut, thereby generating an alarm. *Point-location sensors* operate from a pulsed processor and use a special sensor cable that detects cutting and climbing attempts on a fence and can locate the point of attempted breach to within 10 ft.

Vulnerability assessments help users determine the required level of security and the sensor technologies needed to secure a given facility.

PHOTOGRAPH AND FIGURE: SOUTHWEST MICROWAVE

Line-of-Sight Sensors. The two most common line-of-sight sensors are *bistatic* (point-to-point) *microwave sensors* and *active-infrared* (photo beam) *sensors*. A microwave sensor consists of a separate transmitter and receiver that may be located up to 1,500 ft apart. Between them, they create an invisible volumetric (length, width, and height) detection field. The receiver detects changes in the received signal when an intruder enters the detection field and generates an alarm.

Active-infrared sensors consist of two or more emitters within a transmitter module that are aimed at a receiver module up to 1,000 ft away. This produces a narrow detection field of multiple invisible infrared beams that, when broken or interrupted by an intruder, generates an alarm.

Buried or Covert Ground Sensors. *Buried radio frequency* sensor cable systems are frequently used when covert detection is needed. Such systems commonly comprise two sensor cables—one transmitting and one receiving—that create an invisible detection field above and slightly below the ground's surface. The detection field typically measures 6 to 10 ft wide and about 3 ft high. Sensor cable spacing can affect the detection pattern width with little effect on the detection pattern height. Successive processor modules and cables can protect 10,000 ft or more.

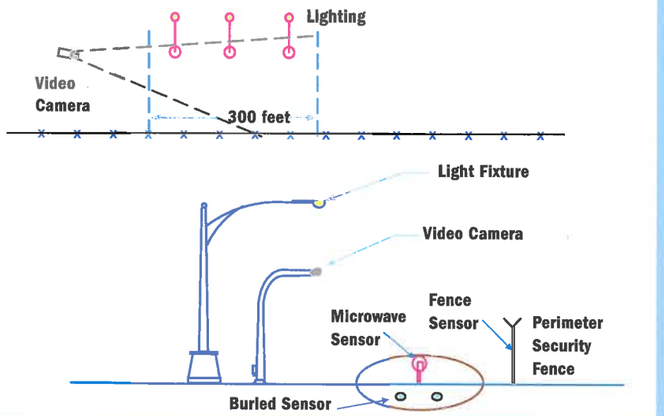
Fiber-optic sensor cables are sometimes used as a buried sensor. The operation is similar to that used for a fence-mounted system, but the deployment is different. Special ground preparation is required, and the fiber-optic cable is typically "snaked," or looped back and forth, to form multiple "S" shapes in the ground to provide some detection width. Ground vibrations are sensed by the fiber-optic cable, and an alarm may be generated. *Seismic* ground sensors are another sensor type that detects vibrations in the ground in which they're installed. Some seismic ground sensors are wired, and some are wireless. Such systems frequently establish a series of invisible detection "circles" where the sensors are installed.

Video Analytics. Although part of a video surveillance system, video analytics can also be part of a sensor system. Depending on the detection level required, this technology may reside in the video camera or in a powerful computer. Such a system can detect visual changes within the camera's field of view, display the information on a video monitor, and generate an alarm.

Thermal Imaging. Part of a video surveillance system that uses a special camera, also known as a *thermal camera*,

Layered Defense

Effective security systems include more than cameras. Several technology options should be considered for water and wastewater facilities.



thermal imaging can detect small temperature differences within the camera's field of view. Infrared radiation emitted by objects within the camera's field of view creates an electronic image that can be displayed on a video monitor. Significant changes within the field of view can also generate an alarm.

SITE CONSIDERATIONS

Weather, climate, terrain, water, animals, and vegetation contribute to a sensor technology's selection and effectiveness. Weather and climate can affect some sensor technologies more than others. For example, a foggy environment will adversely affect some infrared sensor technologies and some video surveillance systems without affecting microwave sensors, fence-mounted sensor systems, or buried sensor cable systems.

Terrain variations can also affect various sensors and technologies. Rolling or hilly terrain isn't suitable for line-of-sight, or field-of-view, sensors such as infrared, microwave, video surveillance, and laser. Obstructions, such as trees, shrubs, and structures, also limit the sensors and technologies that may be deployed. Buried sensor cable systems or fence-mounted sensor systems are recommended for hilly terrain and can also be deployed and positioned around major site obstructions.

Pooling or flowing water, perhaps from drainage, can affect radio frequency or radiating sensors more than others, including some buried sensor systems and microwave sensors. Fence-mounted sensors and active-infrared sensors aren't affected by pooling or flowing water. When only a small portion of a facility is likely to experience pooling or flowing water where sensors are needed, it may be possible to direct the water away from the sensor's detection area or fill in a depressed area where water tends to collect. Such adjustments may allow the use of additional sensor technologies, such as microwave sensors or buried sensor cable systems.

Animals can be another concern. Small animals, such as birds and rodents, are normally too small to cause false alarms. Larger animals, however, such as deer, larger dogs, coyotes, and bobcats, may be detected.

Vegetation within the desired detection area also must be controlled or removed to eliminate false alarms. Fence-mounted sensor systems perform best when they aren't subject to fence-rattling vibrations caused by tree or shrub branches that hit the fence during windy days. Line-of-sight sensors can be easily affected if vegetation grows too high. Maintaining groundcover vegetation to a height of no more than 6 in. is recommended.

LAYERED DEFENSE

Best practice includes layered technologies or in-depth defense. This entails implementing different technologies that complement each other and work together as a system.

Video surveillance is almost always one of the technologies included. Intrusion detection without assessment or response is nearly useless. Video surveillance is needed for visual alarm assessment, and a local or remote audio response is beneficial to alert an intruder of the detection and surveillance of his or her presence. Timely response is crucial; otherwise, the intruder may have time to evade apprehension, or the response force may be sent to the wrong location.

Without visual or video assessment, responders have no idea what they may be up against. Was the alarm from an intrusion attempt by one or more individuals, armed or unarmed? Perhaps it was a deer, a vehicle that breached the fence, or a tree that fell into the detection area during a storm. Such information is essential to responders so they're correctly prepared.

ENSURING SUCCESS

Exterior perimeter detection provides the earliest warning or alert to unauthorized intrusion. All exterior systems must operate and be effective in all weather environments. Best practice typically entails using perimeter sensors and video surveillance. Successful and reliable security systems depend on careful selection and planning, collaborative design, appropriate installation, training of personnel, and maintenance.