EVALUATING CORRECTIONAL TECHNOLOGY

What to Look for When Purchasing Perimeter Security, Communications, or Monitoring and Surveillance Systems

Over the last decade, technological innovation has spurred the development of new devices to improve efficiency in correctional institutions. Technological advances encompass many areas, and have led to changing roles for corrections personnel. Management information systems have been introduced as a more affordable and comprehensive means of tracking inmate activities. Perimeter security has advanced from reliance on the human observer to comprehensive electronic sensing devices. Similar innovations have occurred in internal security --advanced X-ray devices, closed-circuit monitoring, magnetic "friskers" and officer tracking/alerting systems. Drug and alcohol abuse testing packages, telemedicine and videoconferencing all are products of advances in technology.

This technological explosion has not, however, been accompanied by a system for evaluating the utility of the advancements or their potential impact on an agency.

Agencies are most likely to experience expanded uses of technology in the areas of perimeter security, communications, and monitoring and surveillance systems. Below, we examine each of these types of technology and provide guidelines on evaluating their efficacy for a particular agency.

Perimeter Security

A correctional facility is only as secure as its perimeter. The basic role of a perimeter security system is fourfold: deter, detect, document and deny/delay any intrusion of the protected area or facility. Six factors typically affect the probability of detection of most area surveillance sensors, although to varying degrees. These are: 1) the amount and pattern of emitted energy; 2) the size of the object; 3) distance to the object; 4) speed of the object; 5) direction of movement; and 6) reflection and absorption characteristics of the energy waves by the intruder and the environment (e.g., open or wooded area, or shrubbery).

The application of security measures should be tailored to the needs and requirements of the facility to be secured. The security approach will be influenced by the type of facility or material to be protected, the nature of the environment, the client's previous security experience and any perceived threat. These perceptions form the basis for the user's initial judgment; however, they rarely are sufficient to develop an effective security posture. The nature and tempo of activity in and around the site or facility; the physical configuration of the facility to be secured; the surrounding natural and human environment; fluctuations and variations in the weather; and new or proven technologies all are factors which should be considered when planning a security system.

Some examples of intrusion detection sensor technologies include:

Photo Electric Beam -- A photo electric beam transmits a beam of infrared light to a remote receiver, creating an "electronic fence." The sensors often are used to "cover" openings such as doorways or hallways, acting essentially as a trip wire. Once the beam is broken/interrupted, an alarm is generated.

Microwave Sensors -- These are motion detection devices that flood a designated area with an electronic field. A movement in the zone disturbs the field and sets off an alarm. Microwave sensors may be used in exterior and interior applications.

Wall Vibrations -- Vibration sensors are designed to be mounted on walls, ceilings and floors and intended to detect mechanical vibrations caused by chopping, sawing, drilling, ramming or any type of physical intrusion attempt that would penetrate the structure on which it is mounted.

Fiber Optic Wall -- A fiber optic wire sensor is in an open mesh network (quilt) applique that can be applied directly to an existing wall or roof, or installed in a wall (or roof) as it is being constructed. The fiber optic network is designed to detect the low frequency energy (vibrations) caused by chopping, sawing, drilling, ramming or physical attempts to penetrate the structure on which it is mounted.

Audio Sensors -- Audio detectors listen for noises generated by an intruder's entry into a protected area, and generally are used in internal applications, from an entrance foyer to critical data/resource storage areas.

Passive Ultrasonic -- This motion detection device "listens" for ultrasonic sound energy in a protected area and reacts to high frequencies associated with intrusion attempts.

Active Ultrasonic -- This motion detection device emits ultrasonic sound energy into a monitored area and reacts to a change in the reflected energy pattern.

Passive Infrared -- These sensors are passive; that is, they do not emit a signal. The sensor head simply registers an impulse when received. The sensor head typically is divided into several sectors, each defined with specific boundaries. Detection occurs when an emitting heat source (thermal energy) crosses two adjacent sector boundaries or crosses the same boundary twice within a specified time.

Interior Active Infrared -- Interior active infrared sensors generate a certain pattern of modulated infrared energy and react to a change in the modulation of the frequency or an interruption in the received energy. Both of these occurrences happen when an intruder passes through the protection zone.

Exterior Active Infrared -- Exterior active infrared sensors generate a multiple beam pattern of modulated infrared energy and react to a change in the modulation of the frequency or an interruption in the received energy. Both of these occurrences happen when an intruder passes through the area covered by the beams.

Dual-Technology Passive Infrared/Microwave -- These sensors use a combination of microwave and passive infrared technology to provide a lower false alarm rate than either of the sensors independently. This category of sensors typically is referred to as dual-tech.

Electric Field -- Electric field sensors generate an electrostatic field between and around an array of wire conductors and an electrical ground. Sensors in the system detect changes or distortion in the field. This can be caused by anyone approaching or touching the field.

Electrified Fence -- Positioned between double perimeter fences, an electrified fence serves as an unmanned lethal barrier or deterrent. It consists of galvanized posts spaced approximately 30 feet apart

supporting wires powered with high voltage and is located approximately 10 feet from the outer perimeter fence and approximately 15 feet from the inner perimeter field.

Capacitance -- These sensors detect changes in an electrostatic field created by an array of wires installed on the top of a fence. A low-voltage signal is induced in the wire array, creating an electrical field with the fence serving as the electrical ground. A sensor processor continually measures the differential capacitance between the sensing wires and the ground. Once a change in the signal is detected at the processor, a filter screens the signal and allows signals which meet the parameters deemed characteristic of an intruder to be forwarded. When this occurs, an alarm signal is generated.

Strain Sensitive Cable -- Three line sensors use electric energy as a transmission and detection medium. The sensors maintain uniform sensitivity over the entire length of the protection zone. The cable runs from the signal processor to an end-of-line resistor, which guards against cutting, shorting or removing the cable from the processor.

Fiber Optic Fence -- Light is used rather than electricity for transmission and detection. Optical fiber is a fine, strong strand of glass or other optical medium. The optical fiber guides light waves from a light source at one end to a detector at the other end of the fiber. In operation, light is pulsed through the fiber in a manner similar to an electric signal through a wire. Fiber optics, however, offer several distinct advantages over other conductive materials. Optical fiber is immune to electrical interference and electrical magnetic interference disruption. It is intrinsically safe and uses very stable equipment, making it highly reliable overall. Depending on the processor used, two basic types of fiber optic sensors can be employed: fiber optic continuity, which requires the fiber optic strand to be broken to initiate an intrusion alarm; and fiber optic microbending, which detects alterations in the light pattern caused by movement of the fiber optical cable.

Taut Wire -- The taut wire sensor is a series of micro-switches connected to tensioned barbed wire installed on the top of a chain-link fence or installed as the fence itself. The sensors detect changes in tension on the fence fabric. Taut wire sensors are used to protect perimeter fence lines. These are very reliable, and provide a high probability of detection and an extremely low false alarm rate. They are one of the most expensive fence sensor systems because of the laborious installation and maintenance time required.

In-Ground Fiber Optic -- Fiber optic sensors can be used as an in-ground, pressure-sensitive detection system. The system contains an electro-optics unit, which transmits light using an LED for the light source. The light travels through the fiber optic and is picked up by the detector, which is very sensitive to alterations in the transmission caused by vibration and strain in the burial medium caused by walking, running, jumping or crawling. When an adequate alteration in the light pattern takes place, an alarm signal is generated.

Ported Coax Buried Line -- Ported coax buried line sensors are coaxial cables that have small, closely spaced holes in the outer shield. These openings allow electromagnetic energy to escape and radiate a short distance. Emissions from these cables create an electric field that is disturbed when an intruder enters the field. When an intrusion is attempted, the pulse signature changes radically and is picked up by the signal processor. If the variation falls outside allowable parameters, an alarm signal is generated.

Video Motion Detection -- These image sensors use closed circuit television (CCTV) systems to provide both an intrusion detection capability and a means for security personnel to immediately and safely assess alarms (possible intrusions). CCTV systems offer the added benefit of documenting the events of an intrusion and the characteristics of the intruder. Video motion detection sensors detect changes in the monitored area by comparing the "current" scene with a pre-recorded "stable" scene of the area. Video motion detectors monitor the video signal being transmitted from the camera. When a change in the signal is received indicating an alteration in the image composition caused by some sort of movement in the field of surveillance, an alarm is generated and the intrusion scene is displayed at the monitoring station.

Radar -- This is an active sensor that has under gone substantial refinement and enhancement since its first operational use as a detection sensor in the early 1940s. Radar uses ultra-high frequency radio waves to detect intrusion of a monitored area. The radar signal "bounces" off objects in the detection zone and the reflected signal is then analyzed by a processor to determine the relative size and distance of the object. The information then is converted to symbols and displayed as part of an integrated presentation.

Acoustic Detection -- Acoustic air turbulence sensors detect low frequencies created by helicopters that are in their final landing phase or at close range (one to two miles). These sensors "listen" for basic sound pressure waves generated by helicopter rotor blades. Once frequencies are detected, the acoustic air turbulence sensor sends the signal to a processor that filters out frequencies not associated with helicopter flight. If the signal passes through the narrow acoustic band filter, an alarm signal is generated. This sensor can be useful in detecting helicopter-borne intrusion attempts, which otherwise would bypass normal perimeter sensors (fence and in-ground).

Ideally, before any decisions are made about perimeter security systems, agencies should familiarize themselves with the advantages and disadvantages of each option and apply these considerations to their own sites. Each factor should be weighed in light of the demands it makes on staff time and its relative importance in maintaining security. Only after there is a clear understanding of what each system has to offer to a given facility should the choice of perimeter technology be made.

One of the factors to be considered is ease of maintenance. The new technology must be compared with the maintenance demands of the existing system. This is best done by establishing a routine, written maintenance schedule. Routine preventive maintenance will warn of problems early enough to secure parts and make adjustments before the zone or the system becomes inoperable. Also, a written log will establish the criteria against which to measure technology to be purchased.

Any plan for preventing problems ideally will include programs that not only maintain equipment, but also train staff in operating the system. Scheduled training, including refresher courses and regular equipment checks, will help keep all perimeter zones functioning.

The following issues should be considered when evaluating a perimeter security system:

Determine the hazards or risks to the facility's perimeter.

Consider relevant environmental factors when planning for a new or upgraded perimeter system.

Determine which perimeter technology is least susceptible to the particular environmental factors present at the facility.

Contact other users of the equipment to learn its weaknesses and strengths.

Include in the planning process considerations regarding redundancy so that weak points in one system will be covered by another technology. Ensure that the systems being installed are integrated with existing ones.

Examine the size of the perimeter security zones. (Smaller is better because it is easier to localize alarms, speed up response and minimize interruption of the facility's operations.)

Purchase equipment for which parts are readily available and will remain available, once the system is installed, and for which there are local contractors who can provide 24-hour service.

Determine whether the facility has the appropriate electrical wiring for the system being considered.

Determine if the system has a good warranty -- one that is explicit about what is covered.

Consider if the system will meet the facility's projected needs for the next five years.

Check plans for perimeter security system installation prior to installation.

Have a trained staff member monitor installation to ensure that the installers are properly trained and working appropriately.

Plan to conduct defeat-testing of the system, postinstallation, in situations that simulate actual operations.

Ensure that the installer, vendor and/or manufacturer are under a performance bond. Determine how the bond will be enforced in the event there are problems with the system.

Have the vendor provide detailed drawings of the system after it is in place to simplify maintenance and repair.

Obtain schedules for maintenance and repair from the manufacturer, vendor and/or installer and a schedule for appropriate testing methods.

Determine if maintenance and repair of the system will be accomplished by facility staff or through a maintenance contract.

Specify the amount and type of training required for staff. Plan to train staff on how to operate, maintain and repair the system. Try to arrange the training as part of the sales contract.

Plan how follow-up training will be provided for both present personnel and new hires.

Consider if this system is necessary to answer the needs of the facility for perimeter security or whether it is a case of electronics for electronics' sake.

Communications Technologies

Information is crucial to a well-run correctional system. Knowing what is happening gives correctional administrators the power not only to react to problems promptly, but also to anticipate and prevent

them. The key to this kind of knowledge is a well-designed communications system, one based on state-of-the-art technology that is simple to operate and that will perform continuously even while its components are being maintained and updated. Some examples of communications technologies include:

"Smart Cards" -- A smart card is a standard-sized plastic card with an embedded computer microchip containing a central processing unit (CPU) and up to 8K bytes of electronic, updatable memory. Smart card technology has been emerging over the past two decades and there now are millions in circulation.

The card stores all types of information about an inmate, including his or her movement, medical care, commissary purchases, treatment needs and meals eaten.

Personal Locator Device -- This device provides users with a wireless transmitter that is small enough to fit in a pocket or on a keychain. This capability enables staff and inmates to have their locations monitored within the facility. Applications that require multiple-building protection can communicate via fully supervised, long-range wireless transceivers, which are deal for campus-style facilities.

Personal Duress Alarms (PDA) -- When the user perceives a threat, he presses the button on the transmitter of his personal duress alarm. Once activated, the system instantly relays critical information about who is in danger and his whereabouts. Strobe lights, voice alerts, sirens or CCTV cameras and intercoms can be triggered to further deter would-be attackers until help arrives. PDAs operate by wireless signal from an unobtrusive transmitter that can be activated either manually or automatically. Personnel who are not desk-bound often wear these alarms, especially when operating outside the immediate presence of other staff members.

Panic Button -- A kind of duress alarm, usually affixed to a wall in a remote location within a cell block or another area where staff members must operate on their own. When pressed by a staff member, it sends a signal that identifies the specific site location.

Vehicle Radio -- Radio communication system in which at least one end of the radio path terminates in equipment carried in a vehicle or on a person riding in a vehicle. It can function with one or both terminals in motion. These devices typically are used when the institution employs a roving patrol around its perimeter.

Walkie-Talkie -- Hand-held, two-way radios that allow staff to talk with one another or with the control center. Many walkie-talkies can be programmed to sound an alarm when a staff member is thrown to the ground or if the radio is laid horizontal.

Communications technology must anticipate the possibility that a proscribed technology that works in one place may not work in another. In other words, it must be customized to meet the unique characteristics of a single site. In no facility is it possible to keep all inhabitants, both inmates and staff, in sight at all times, or even much of the time. Consequently, personnel must rely on communications technology to maintain contact.

Additionally, communications systems must be flexible enough to meet changing conditions, because in many facilities, the mission and demographics of the population change after the facility has opened. Moreover, no one has enough staff. Shrinking budgets require reductions in operational costs, and this

almost inevitably leads to a higher inmate-to-staff ratio. At the same time, the inmate profile is changing. Not only are there more inmates, but some may be more aggressive.

All these factors make the need for instantaneous communication imperative, preferably while maintaining an ability to convey as much information as possible.

Correctional administrators, planners and fiscal officers are faced with a myriad of choices when acquiring or upgrading communications systems for new or existing institutions. Managers should review available comparative information and consult with communications experts prior to making these decisions.

When communications systems are being installed and/or upgraded, the following issues should be considered:

Prepare a list, with input from staff, of the requirements the new system should meet.

Consider all possible solutions to meet the communications system requirements in order to make the most cost-efficient decisions.

Check plans with colleagues in other institutions to benefit from their experiences.

Ensure that equipment is purchased for which parts will be readily available, and for which parts will remain available once the system is installed.

Consider available optional telephone features, such as interface with pocket pagers, group-calling capabilities, automatic call-back, and dedicated emergency phones, off-the-hook alarms, call override, cellular phones, recording capabilities, monitoring features and hearing-aid compatibility. Also consider the following:

Whether the intercom network should be part of the telephone system or separate;

Whether to use the telephone system for paging

Whether certain numbers should be blocked so that inmates cannot dial them; and

Where in the facility the telephones should be installed.

Check with phone companies regarding possible profit-sharing plans.

Determine the number of inmate telephones needed in relation to the size of the population.

Develop telephone procedures to reduce the likelihood of fraudulent use by inmates.

Take into consideration environmental factors that may affect a radio system's effectiveness, such as the following:

Configuration of the buildings;

The amount of metal in the buildings;

Obstacles that might affect clear transmissions (trees, hills, etc.);

Nearby institutions that might be using the same radio frequencies;

Long transmission distances that may require powerful radios;

Potential blind spots that may require extra wiring or antennas for clear transmission.

Consider battery life and recharging capabilities for walkie-talkie radios.

When determining the number of walkie-talkies to be purchased, consider the need for back-ups when radios are being recharged and/or repaired.

Develop accountability procedures for signing out communications equipment.

Consider audio monitoring as part of the housing units' intercom system.

Ensure speakers are installed to be easily heard but out of reach of inmate tampering.

Check plans for communications system installations using realistic, simulated situations prior to activation.

Ensure that the various systems being installed can be integrated with each other. Test system components.

Ensure that the vendor provides detailed drawings of the system after it is in place to simplify maintenance and repair.

Have a trained staff member monitor installation to ensure that the installers are properly trained and working effectively.

Make decisions as to whom on staff should be trained to operate each system and what training schedule will be followed.

Ensure that the manufacturer provides a preventive maintenance schedule at the time of installation.

Have the manufacturer provide a maintenance contract.

Select equipment for which local contractors can provide 24-hour service for each system.

Ensure that warranties are explicit about what is covered. Make sure the system's warranties cover not just communications equipment, but transmission lines and wiring.

Ensure that the contractors have a performance bond, and then require the bonded contractor to fix any post-installation problems.

Consider and plan for expandability. It is always cheaper to plan ahead for growth.

Monitoring and Surveillance Systems

On the theory that the best way to control inappropriate behavior is to prevent it, correctional administrators have long used monitoring and surveillance technology. The primary intent of this technology is to prevent access and/or alert staff when intruders (inmates or unauthorized individuals) are in off-limits areas and acting inappropriately. The use of monitoring and surveillance systems reduces the likelihood of escapes and diminishes threats to the orderly running of the facility. Thus, these systems help protect inmates from one another and aid in the prevention of disturbances within institutions.

Examples of monitoring and surveillance technologies include:

Global Positioning Satellite -- Global Positioning Satellite (GPS) receivers have been in use since the 1980s. The GPS or Navstar is a constellation of 24 satellites in 12-hour orbits of high inclination, containing on-board atomic clocks. The satellites are operated by the U.S. Department of Defense providing 24-hour-a-day, worldwide service. A system has been developed to monitor offenders using cellular technology combined with GPS. As with the regular electronic monitoring system, each offender wears an ankle bracelet, but he or she also carries a portable tracking device (smart box), programmed with information on his or her geographical restrictions. If an offender violates his or her boundaries, the information can be transmitted directly to the police, along with the offender's geographic location. The smart box and the ankle bracelet also squawk loudly when boundaries are breached, alerting potential victims.

Access Control Systems -- These systems allow certain designated persons to enter otherwise secured areas. Several types of systems are push-button code and card-access control. Push-button code systems have keypads installed at the entrance to each controlled-access area. Those authorized to enter are given the combination to be punched into the keypad. There is no keyhole to allow locks to be picked and locks are easily re-coded if prior combinations have been compromised or if there are staff changes. Card-access-control systems use card readers instead of keypads. Authorized individuals are given programmed cards that allow entrance into a given area. Magnetic key-card systems use a plastic card containing thousands of magnetic particles that are arranged to match the pattern set up in the card reader. When a match is made, the locking system is activated.

Closed-Circuit Television -- This is an arrangement in which television cameras, placed in potentially vulnerable areas within an institution, can be monitored by staff. It usually is located in a control center. Typical camera locations are at entrances and sally ports, in visiting areas and along the facility's perimeter.

Motion Detectors -- These devices use infrared light waves, radio frequency transmission, ultrasound or microwaves to detect changes that occur in a previously empty space when a human body enters it. They detect a change in volumetric pressure or temperature changes as a consequence of radiant body heat.

Audio Monitors -- This technology is similar to CCTV, but rather than conveying an image, it picks up and transmits sound through a closed-circuit audio system to one or more locations staffed by facility personnel. Existing public address systems, with the speaker turned into a microphone, can listen to sounds in the protected area and then trigger an alarm relay when an intrusion takes place.

As with most technology, an important component in monitoring and surveillance systems is the staff who use it. System planning should incorporate both a facility's security needs and staff requirements into the design process.

The agency should retain specialized personnel who understand the problems to be solved, from both management's and users' perspectives. Administrators then can review the proposals that are most appropriate. The agency should address the following:

Identify all facility hazards or areas that require monitoring.

Determine precisely what problems the monitoring and surveillance technology should address.

Identify potential environmental problems (e.g., lighting for CCTV or noise levels for audio-detection) and ensure that equipment will be able to avoid their detrimental effects.

Determine if the facility has the correct wiring for the new equipment.

Determine if the benefits expected from the equipment outweigh the costs of its purchase, installation and maintenance.

Contact other users of the equipment to be purchased to benefit from their experience.

Purchase monitoring and surveillance equipment for which parts will be readily available, and for which parts will remain available once the system is installed and for which there are local contractors who can provide 24hour service.

Determine whether or not the system has a good warranty -- one that is explicit about what is covered.

Develop a plan for on-site support.

Ask the vendor to provide detailed documentation of the monitoring and surveillance system.

Obtain schedules for maintenance and repair from the manufacturer, vendor and/or installer, and a schedule for appropriate testing methods.

Determine if maintenance and repair of the system will be accomplished by facility staff or by a maintenance contract.

Make sure the amount and type of training is specified. Plan for staff to be trained in how to operate, maintain and repair the system. Try to arrange the training as part of the sales contract.

Decide the level of staff that will be trained and ensure that management as well as support staff are included.

Plan how follow-up training will be provided for both present personnel and new hires.

Consider whether or not the monitoring and surveillance system can be expanded to meet future needs of the facility.

Conclusion

The key to maximizing the use of technology in perimeter security, communications, and monitoring and surveillance systems in corrections is research and evaluation. The technology to be implemented needs to be fully researched and evaluated to determine its utility and benefit to the agency. Several states have established technology review committees to evaluate technology before purchase or use. The benefit of such committees is that the corrections agency becomes more knowledgeable about its technological needs and requirements, and will know what to ask and request of the vendor or manufacturer. Having a formal review and evaluation process improves the chances of success and satisfaction.

It also is beneficial to interrelate with other corrections agencies at the local, state and federal levels prior to making key technology purchases. Often, other agencies already have addressed the same or

related issues, and another's success or failure can save precious time and resources. In addition, ask vendors and manufacturers to provide you with a listing of their last several installations or sales so that you can check with your peers to determine a technology's strengths and weaknesses before urchasing. Reputable technology firms should have no problem providing you with this type of information. Research and evaluation is critical to achieving satisfaction in the use of new technology within your agency. Don't sell your agency short by shortcutting this important process.

~~~~~~~~

By Kevin Jackson

Kevin Jackson is a senior technology program manager for the National Institute of Justice.
~~~~~~~~