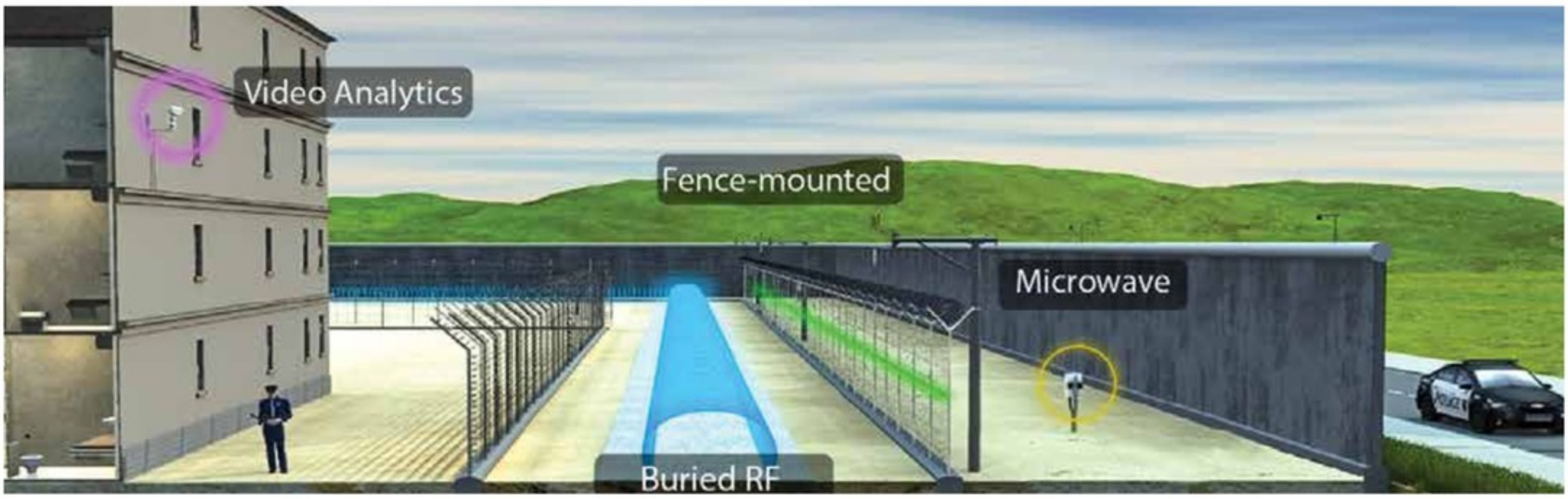

Buried RF consists of a set of buried cables that form a virtual fence of electromagnetic energy.

Intelligent, low-voltage lighting is a new trend in correctional perimeter security.

Technology Advances in Perimeter Intrusion Detection Systems

By Stewart Dewar

The end goal of using perimeter intrusion detection systems (PIDS) in correctional environments is to augment the effectiveness of both physical infrastructure and security personnel. When the technology works well, it becomes a force multiplier, freeing up officer resources and alerting staff to inmate escape attempts.

Technology that works well is the key. PIDS have been in use in correctional environments for over 35 years, and a lot has changed over time. Advances in technology have made these systems more effective, easier to install and dramatically lower in cost. This article examines which PIDS technologies are the most effective for correctional environments and how new advances can solve application-specific problems.

Protecting the Perimeter

While there are many types of sensor technologies that protect perimeters, some are more suitable for correctional facilities than others. When looking at different systems, consider these factors:

- Probability of detection: Does the system quickly and accurately detect attempts to breach the perimeter each and every time?
- Nuisance alarm rate: Does the system only generate alarms for real or simulated escape attempts? If the system generates alarms during normal conditions or high winds, security may start to suffer from complacency when responding to alarms.
- Ease of installation and configuration: How easy is the system to install and configure? Can the system be configured remotely from an equipment room, so maintenance staff can avoid travelling out to the perimeter whenever an adjustment is required?
- Integration with Security and Video Management Systems (SMS/VMS): Does the system generate information for correctional officers that improves situational awareness? For example, can the SMS use the sensor data to display the precise location on a map? Are related alarms grouped together to avoid overloading officers with redundant information? Can the alarms be integrated with the VMS for automated camera control?

Fence-Mounted Sensors

Fence-mounted sensors consist of a coaxial cable, fiber-optic cable or set of accelerometers attached directly to the fence, and detect any attempt to cut, climb or lift the fence fabric. Older systems (sometimes called "shaker systems") use electro-mechanical movement and are notorious for a high-nuisance alarm rate, leading to operator overload in the control room and alarm complacency.

Modern systems use a variety of sensing techniques (time-domain reflectometry or accelerometers, for example). These advances allow for features such as environmental compensation algorithms, precision ranging, cut immunity and low-voltage power over sensor cables.

Coaxial-based sensors are generally highly economical and easy to deploy. Fiber-optic sensors require zero electronics on the perimeter and may be more cost-effective for larger facilities.

New fence sensor products can report the precise location of a disturbance. This ranging capability is a major improvement over previous "block" sensors. Not only can ranging information be used to direct surveillance cameras, it enables sensitivity levels to be adjustable for specific areas of the fence (for example, to accommodate for changes in fence construction). Ranging capabilities can reduce nuisance alarms as well, since the system can distinguish between site- or area-wide disturbances caused by high winds and a legitimate escape attempt. Finally, ranging reduces operational costs by enabling maintenance staff to quickly locate and resolve issues.

Sliding gates have always posed a problem for cable-based sensors. Traditionally, a mechanical cable retraction system is used to manage the routing of the sensor cable from the fence to the sliding gate panel. These systems are expensive, cumbersome and prone to failure. Fortunately, there is now a much better solution: wireless gate sensors. An embedded accelerometer analyzes gate movement in three dimensions, enabling the sensor to distinguish between gate activity, intrusion/escape attempts and environmental conditions. The sensor communicates with a nearby processor over an encrypted and monitored wireless link. If any suspicious event occurs — an intrusion or escape attempt, communication link failure or an attempt to remove the sensor from the gate — an alarm is immediately generated.

Volumetric Sensors

Volumetric sensors emit an RF/microwave energy field between a transmitter (Tx) and receiver (Rx) pair. The most common type is microwave, which generates a cigar-shaped field between a pair of post-mounted units. The main advantage of current microwave systems is that they typically perform well in extreme weather conditions such as heavy snowfall or dense fog and are easy to retrofit within existing sites.

While their coverage makes microwaves well-suited for open areas, such as the secure area between inner

and outer fences, their primary use is to monitor sallyports. When designing the sensors for a sallyport, integrators should be aware that a single event (e.g., the entrance of a delivery truck) can trigger alarms on multiple microwave pairs if used in close proximity. In these cases, the SMS should be able to merge the related events together to avoid overloading the control room officer with redundant alarms.

Buried RF, on the other hand, consists of a set of buried cables that form a virtual fence of electromagnetic energy. Being covert, it is considered impossible to defeat and is highly suited to detecting the presence of intruders in no-go buffer areas, such as near the fence or in the space between fences. Buried RF systems work well when the area is clear and there is good drainage. Because of the need to bury the sensor cables, an RF cable system is one of the more expensive systems to install.

Video Analytics

Video analytics have greatly improved over recent years, benefiting from today's higher-performance, lower-cost computing resources as well as HD cameras with impressive low-light, IR and thermal capabilities. Advances in computer vision research have led to the development of sophisticated video analytic software optimized for outdoor/indoor people tracking, left/removed object detection, auto PTZ, face and license plate recognition, crowd detection and much more. These software modules may be included as part of a Video Management System (VMS) or embedded on individual cameras.

Rather than being an alternative to traditional PIDS, video analytics offer an exciting new set of technologies that greatly enhance perimeter security at relatively low cost. For example, video analytics can leverage a facility's existing camera infrastructure to detect and track people near both sides of the perimeter fences, providing early warning of potential security events before they can occur.

Intelligent Lighting

Intelligent, low-voltage lighting is a new trend in correctional perimeter security. Installed on the fence, the LED-based luminaires provide uniform, wide-spectrum illumination targeted along the fence line. This improves the quality of video feeds by avoiding hot spots while a high Color Rendering Index (CRI) value means colors are accurately shown (greatly assisting officers with identification). LED-based lighting also dramatically reduces electrical consumption while a 10-year-plus lifespan virtually eliminates maintenance.

These benefits are useful, but how do they relate to perimeter sensors? This is where the word "intelligent" comes into play. Sensors embedded in the luminaires themselves can detect the fence vibrations caused by someone attempting to cut, climb or lift the fence fabric. In addition to notifying the SMS/VMS, the lights in the immediate area can instantly switch to full power or strobe. Knowing they are detected, potential escapees may rethink their actions.

New- and future-generation perimeter sensors (and accompanying video analytics) can certainly meet the goal of reliably detecting attempts from inmates to bypass perimeter fencing and gates. The key concerns when evaluating these systems are to ensure that they are cost-effective, do not burden correctional staff with large numbers of nuisance alarms and can be properly integrated so as to enhance overall security response capabilities.

Stewart Dewar is the product manager for Senstar, a global company that provides one of the largest portfolios of perimeter intrusion detection products.