

A Boost at the Border

Video analytics enhances perimeter security applications



Case Study:
Perimeter Security Applications

Mention border security, and you might imagine the intersection of two countries, or perhaps the border separating government facilities from private land. But border security also can be defined as perimeter security, which expands the concept to encompass walls, fences, roads and other perimeters around businesses, schools, transportation facilities, factories, resorts, prisons, utilities, research facilities, and other properties and buildings.

Because it is physically impossible to watch every foot of perimeter and border fencing or walls all the time, increasingly the security function falls to cameras. In the beginning, these cameras were primarily static, analog devices, purchased inexpensively and in large volumes to monitor long perimeters. Besides their cost-effectiveness, they were valuable because they let security officials look back at recorded footage following an incident to try to piece together—from the usually low-quality images—what happened and who was responsible.

While more expensive than the mass-purchased analog cameras, modern digital video cameras offer rich functionality to improve security functions. In fact, the advent of digital video cameras, equipped with video analytics technology, promises to turn security cameras from passive, backward-looking devices into intelligent, active partners in helping prevent incidents, as well as providing compelling evidence after the fact. The success of video analytics software, in turn, depends largely on the quality of the video picture it has to work with.

Amplified Capabilities

Video analytics technology has the potential to revolutionize how the security industry monitors borders and perimeters from a security guard function into an automated task.

Traditionally, the primary role of cameras in border and perimeter security applications has been to provide security personnel with accurate and rapid assessment of alarms. Perimeter alarm systems can use buried, fence-mounted or microwave detection, among others. The camera's job is to provide high-quality images, both day and night, in a variety of lighting and weather conditions.

Video content analysis improves the main task of security cameras by providing specific and timely alerts to security personnel, based on the camera images. As such, the video analytics system augments the detection function of the perimeter alarm system instead of simply operating alongside it.

For instance, video analytics software can instantly detect and record if a person enters a secure area or if an unauthorized person tries to cross a perimeter to the other side and, then spur action based on these observations.



Selection Factors

Regardless of camera type, factors such as camera coverage, image quality, wide dynamic range and broad coverage of large areas will be important for border and perimeter security.

Ideally, video analytics are embedded into the cameras, operating at the network edge. Locating the video analytics at the edge eliminates the need to transmit copious data from the cameras to a central monitoring facility, which can lower the infrastructure costs and make many installations more feasible. For example, it provides an attractive practical alternative to trenching fiber-optic cables across remote desert stretches of the U.S./Mexico border.

This edge-based approach creates a scalable and cost-effective system, with lower latency between real-world events and alerts to security staff. Accurate rules-based alerts provide low nuisance, such as false-positive alarm rates, and can shorten response times. Rules can specifically identify the location and behavior of people, vehicles or objects relative to defined areas, and easy-to-use filters are available to exclude alarms caused by nuisance factors such as small animals, rain, snow or falling leaves.

In addition, modern video analytics software is able to direct a PTZ camera to remain trained on a suspicious person or vehicle until security personnel can be deployed to check out the situation. What's more, some advanced video analytics solutions can automatically track an intruder from one camera to another. This can be accomplished using either fixed or PTZ cameras with hand-off capabilities that enable multiple cameras to track, for example, a person running along a fence or a vehicle crossing into and through a restricted area.

Some video analytics applications include a GPS component that is automatically tied to longitude and latitude, which enables the camera to know where it is geographically aimed. These GPS-equipped camera systems can thus produce geographically registered targets, letting security personnel know precisely where to respond to an alert.

The cameras used for border and perimeter security should not only meet the security needs of the site in question, but they also must be easily compatible with existing or planned video management, access control and alarm systems.

A camera's ease of use while on-site can make the difference between a smooth and a rocky installation process. As an example, Lumenera's Pixim-Powered Li045C-DN intelligent camera—with OnBoard embedded video analytics software

licensed from ObjectVideo—not only addresses the special requirements of IP cameras, but also includes an analog output for use by CCTV installers. This feature allows the installer to mount and focus the network camera via a compact, portable flat-panel display or CRT without worrying about the network configuration, having a computer present or contacting a control room by phone or radio. In this manner, each camera can be installed correctly the first time, saving time and money.

Extending Human Capabilities

In the past, it took dozens of security guards patrolling an area—or dozens or hundreds of cameras transmitting stagnant video to a video monitor watched by security guards—to detect an intruder or other incident. Video analytics handles the tedious task of monitoring scenes to concentrate instantly on the types of events that security personnel need to know about. As a result, border security workers remotely can survey and track a wider area with fewer people in the field.

While video analytics is an automated function, it depends on human operator for optimum results. When a video analytics system detects a potential intruder, it can create an alert. Still, it's up to the security operator to take appropriate action, whether that means a closer look at live or recently recorded video surveillance images or the dispatching of security officers to the site.

Taking advantage of video analytics solutions, operators can identify and respond to intruders or other incidents quickly and more accurately. In this way, video analytics functions can reduce operator fatigue and improve both decision-making and response time. For instance, rules-based content analysis embedded in the security cameras can provide operators with an automated display that clearly highlights and logs a potential intrusion alarm. As a result, security personnel spend less time chasing false alarms, and the presence of specific, visually highlighted alerts helps them take fast and appropriate action.

Nuisance alarms are a significant waste of time for staff who monitor borders and perimeters. These false alarms also can create a “boy who cried wolf” mentality, sometimes leading security staff to ignore, tamper with, or even disable important system functions that deliver nuisance alarms too often. By improving the accuracy and ease of use of the camera system, video analytics capabilities lead to better effectiveness and improved motivation of security staff, as well as more confidence in their security tools.

A Good Picture

Regardless of the capabilities of any video analytics solution, the software can perform only as well as the quality of the images. For border and perimeter security, it is important that a camera maintains high-quality images both during the day and at night, performs well in bright, low light and high-contrast lighting situations, captures high-quality images when there's strong glare or reflections, maintains accurate color in all lighting conditions, and minimizes image artifacts, such as pixel blooming, vertical smear and color aliasing. It's also important that a security camera has excellent image quality in both live and recorded (compressed) images and includes component parts, such as chipsets and other electronics, that can withstand extremes of heat, cold or vibrations.

Traditional analog charged-couple devices struggle with providing image quality sufficient for today's video analytics requirements. Constantly generating high-quality images—regardless of lighting conditions, temperature and other environmental fluctuations—while avoiding false alarms is possible only with the latest generation of digital image sensors.

With an all-digital camera, including embedded video analytics, there is no need to re-sample and convert data from analog to digital. Embedded video analytics takes place on the edge of the network, rather than after transmission to a central server. This approach has the added advantage of transmitting only significant events over the network, which dramatically reduces network traffic, false alarms, time and data storage requirements.

Video analysis depends on security cameras with image sensors that deliver wide dynamic range, high signal-to-noise ratio, minimal image artifacts and accurate color reproduction. Let's take a closer look at these factors:

- › WDR, which is measured in decibels, refers to a camera's ability to capture image details and accurate color in both the lightest and darkest portions of a high-contrast scene, and everything in between, simultaneously.
- › SNR measures the amount of usable visual information—signal—compared to the amount of noise, or spurious, non-content visual information, especially random noise generated by the image sensor or processing in the camera.

- › Image artifacts include vertical smear, pixel blooming, color aliasing and interlace artifacts surrounding both still and moving objects.
- › Accurate color reproduction is challenging in lighting situations such as bright sunlight, glare, reflections and high-contrast lighting.

To be effective, video analytics software requires a camera that can provide 100 dB or more dynamic range with high SNR, minimal noise, few or no image artifacts, accurate color and precise details throughout all the lighting ranges of a scene. Such a camera can deliver the consistent, high-quality data needed to optimize video analytics applications' algorithms.

It is these algorithms that differentiate between foreground and background and between still and moving objects; that can tell the difference between a target or event of interest and a video artifact or other sensor error; that can recognize the difference between a small animal and a human being; and that can alert humans to an out-of-place person, object or activity.

Furthermore, it is the quality of the original camera images that enables more accurate identification of faces, license plates and other important details in a scene needed to anticipate or prevent incidents, or to provide forensic details for effective investigation and prosecution after the fact.

Pixim's Digital Pixel System® ultra-wide dynamic range technology delivers image quality that is optimal for video analytics: crisp, clear, color-accurate images even in situations of strong backlight and other high-contrast and difficult lighting conditions; in all temperatures; and with minimal image artifacts. This technology makes it possible to record and review high-resolution, clear images of intruders, loiterers, escapees, or anyone or anything else attempting to cross a secured perimeter without permission.

Border and perimeter security poses significant inherent challenges. Through sophisticated video camera systems, equipped with the latest video analytics software and powered by all-digital image sensing and processing chipsets, border and perimeter security professionals can significantly augment the skills of their staff and potentially do a better job of monitoring and securing the perimeters they must protect.

Video content analysis improves the main task of security cameras by providing specific and timely alerts to security personnel, based on the camera images. As such, the video analytics system augments the detection function of the perimeter alarm system instead of simply operating alongside it.



Special Challenges

Borders and perimeters may vary in size, structure or purpose, but they share certain challenges when it comes to security, and specifically the use of video cameras.

Almost all border and perimeter security takes place outdoors, so cameras must be weatherproof and tamperproof. That often requires enclosures appropriate to the site where they are installed. Also, effective border and perimeter security systems must be able to distinguish between potential intruders and small animals entering the field of view, and they must deal effectively with natural elements such as trees, shadows and insects on the lens.

The cameras and all the components inside—including the image sensors, video processing chips and other electronics—must withstand temperature and humidity extremes. This might be sweltering summer heat or freezing, icy conditions. As a result, rugged design is important.

Because they are installed and expected to work 24 hours a day, the cameras and lenses must provide the appropriate sensitivity, adaptability and reliability to capture useful images in a variety of challenging lighting conditions. They must have a wide dynamic range, which is the ability to maintain consistent image quality and accurate color in high-contrast scenes, such as bright light and deep shadow, simultaneously.

One major challenge of border and perimeter security is ensuring sufficient camera coverage. With today's cameras, this means not only enough cameras mounted in the right locations, but also sophisticated video analytics software that dramatically improves the security function at borders and perimeters.

Pixim's Digital Pixel System® Technology

Pixim's Digital Pixel System ultra-wide dynamic range technology, a true breakthrough in imaging technology, delivers unprecedented image quality in all lighting conditions. Cameras powered by Pixim's specialized image processing chipsets can significantly enhance perimeter and border security through the following capabilities:

- › **Widest dynamic range:** Captures highlight and shadow detail in the same scene.
- › **Highest total resolution:** Makes it easy to distinguish fine image features and details.
- › **Superior color rendering:** Accurately displays color even in difficult lighting such as bright sunlight, glare, and high-contrast lighting.
- › **No "sun blindness":** "Sun blindness" is common in east-facing CCD cameras in the morning and in west-facing CCD cameras in the afternoon.
- › **No "camera blindness":** Eliminates the vertical smear, pixel blooming, and other image artifacts commonly encountered in high-contrast scenes.
- › **High image compression:** Improves image quality with smaller file size – allowing DVRs to record with higher frame rate or higher resolution, or both, while maintaining the same total recording time.
- › **Less need for DC auto iris:** Saves money and greatly improves camera reliability.



› Significant loss of information in strong backlight

› Superior image quality despite harsh lighting conditions



1395 Charleston Road
Mountain View
CA 94043

P: 650.934.0550
F: 650.934.0560

www.pixim.com

Updated 05/2008