Intelligent video surveillance and GIS

by Etienne Louw, African Astronautics

IVS (intelligent video surveillance) is a state of the art technology for use in security environments allowing its users to easily monitor and secure areas with security cameras. Places of interest can easily be monitored with sophisticated software that makes detecting threats or unwanted visitors simple and effective.

IVS consists of algorithms that detect movement or changes in live and recorded video to see whether the movement or changes mean a possible threat is about to occur, occurring, or has occurred. These algorithms work by examining each pixel of the video and putting together all the pixel changes which then depicts motion or detection. Depending on the policies and alerts you have setup, you will be notified of this motion/detection; actions can be automatically taken by the software e.g. tracking the motion until it is no longer detected.

Traditionally IVS has been seen as a non geo-referenced technology – something like your TV or movie experience – it represents happenings in the real world, or for that matter the real world itself, but not in the way that we as ‘GIS people’ understand the definition of ‘real world’. Right? Wrong!

Some of the benefits of IVS

Real-time video monitoring

IVS software can display live video in real time. Also in real time are alerts for security policies you setup. These alerts will notify you immediately when there is a threat.

Improves quality of surveillance

With IVS software you have the ability to be notified immediately when unusual activity is detected. IVS software does not get tired or distracted, 24 hours a day, 7 days a week.

Accurate detection

IVS software has the ability to detect specific behaviours. For example, if someone is heading towards somewhere they should not be, you will be warned – indoors, outdoors and even in low-light situations.

Force multiplier

IVS software can be integrated with existing CCTV/analogue systems or implemented with new state of the art IP network cameras. There is no need to replace existing investment in infrastructure. IVS becomes a force multiplier when added to any existing camera network.

Optimise labour costs

Due to the IVS software handling all alerts from possible threats, less personnel is needed to view video and can be redeployed to pro-actively assist in providing on-the-ground supportive security services. With standard video systems, someone must always be watching for threats or abnormal behaviour, but with the IVS software watching for you, more video can be watched by a lower number of people. Video no longer needs to be watched live by a person 24/7. This decreases labour costs at the control centre and increases productivity.

Video analytics form an important component of IVS

Effectively manage real-time CCTV video

Video analytics allow you to effectively manage multiple CCTV cameras within a CCTV system. Some large surveillance installations require that multiple CCTV cameras are watched by just one or two security personnel. This can cause issues as each camera is not being effectively monitored as there are so many cameras. Video analytics give the capability to only push video to monitors when an actual event occurs or when a specific alarm is triggered within your CCTV system. This means the video analytics software is watching the cameras for you and only notifies you when some type of action needs to be taken.

CCTV system intelligent motion detection

Video analytics also give you the capability of advanced motion detection in your CCTV system. When a camera within the CCTV system detects motion within a specific area of the video, it will automatically trigger an alarm within your CCTV system. Video analytics offers higher reliability than standard motion detection. Video analytics software is based on various algorithms that will analyse the video to determine the type of motion. This means your CCTV system will only look for true motion of a moving person or vehicle instead of e.g. swaying trees and bushes.

License plate/vehicle type recognition

The software allows the cameras to detect and determine vehicle type and license plates which can then be integrated in the system for tolls, behaviour monitoring, anti-crime operations etc.

Object recognition

One can also monitor video footage for missing or unwanted objects. Objects that have been left behind (bag containing a bomb) can be detected when the video from a CCTV camera displays an object not part of the normal video scene. This causes it to trigger an alarm within your CCTV system. Video analytics can also do the reverse. When a camera within your CCTV system has a change in the video scene that shows that an object is missing an alarm can be triggered.

Security access points

Video analytics can determine the behaviour of people outside of an access point. This can include loitering, studying of the security cameras or
even tailgating. One can therefore better monitor traffic around security access points. Alarms can be set that will trigger when people within the CCTV cameras view are acting strangely or entering an area they are not permitted.

Advanced systems are able to detect anomalous situations by analysing inputs from multiple sensors, including cameras, fence intrusion systems, and radar systems and ensures a policy based response to threatening conditions. These systems combine GIS, advanced video analytics, and robust and open systems architecture to maximise system effectiveness and interoperation with third party cameras, CCTV systems, intrusion sensors, access control, and alarm management systems (see Fig 1).

In terms of integration, our software algorithms are combined with initial sensor feedback to both decrease false alarms and increase the confidence level of a specific event. For example, a fence integration will consist of a fence sending an alarm of an event to the IVS system. Before setting a general alarm, the system will redirect a camera to the point of intrusion and apply analytics. Perhaps executing an algorithm to verify that the intrusion is a person, versus an animal or vegetation. After validating that fence event, the system can now perform the alarming function.

The integration with GIS provides many innovative features not found in other “intelligent” video systems. Combined with a flexible open architecture these features include:

- Geographic map-based command and control user interfaces that provide enhanced situational awareness, and automates PTZ camera steering tasks.
- Wide-area surveillance and perimeter intrusion detection: when integrated with perimeter intrusion systems one can provide automated video corroboration of intrusion events without using camera presets, which reduces cost and increases flexibility.
- Advanced scene analysis turns cameras into object detection and tracking sensors. Objects, once detected and reported in the database, become full geo-objects, ready for manipulation within a GIS environment.
- Point-and-click interfaces that control multiple PTZ cameras simultaneously through interaction with both maps and video images.
- Automated policy-based detection rules and alarm notification ensures that the proper responses are carried out for any given type of alarm. And because every alarm triggered is a geo-object, all typical GIS-related response mechanisms can be utilised, e.g. automated vehicle response etc.

Automated wide area surveillance systems – technical detail

Advanced systems also provide automated wide area surveillance capabilities that provide complete solutions for digital surveillance of remote sites and large outdoor environments. Distributed computing architectures utilise TCP/IP networking to provide maximum flexibility for component deployment.

While the security industry has invested a lot of effort into migrating CCTV systems onto digital platforms to ease the burden of managing the volume of video data, almost no attention has been paid to the ergonomics of operators interacting with digital video systems and PTZ cameras.

This deficiency can be addressed by utilising camera control technologies to make operators more efficient by automating PTZ camera steering, making it easier for operators to interact with the cameras, and providing them with truly useful feedback about where each camera is looking. This feedback is portrayed directly onto either a 2D or 3D GIS display (see Fig. 2).

Advanced systems will be able to directly interface with the majority of PTZ cameras and matrix switches on the market. They will also be able to utilise feedback from PTZ cameras to provide real-time positional information feedback to operators on a GIS display, dramatically enhancing situational awareness for operators that aren’t intimately familiar with the environment being monitored. This allows users to see on a map, in real-time, which direction a PTZ camera is pointing and to simultaneously steer multiple cameras to view a location by clicking on any location on a map, instead of using a joystick.

Advanced systems are able to completely eliminate camera-based presets and the use of contact-relay closures from intrusion sensors to steer PTZ cameras to a finite number...
of different locations. This has several advantages:

First, because all camera control is virtualised, all 'presets' become software-based instead of hardware-based – typically, 'no go' areas can now be set simply by drawing a polygon on the map view.

Secondly, and perhaps more importantly, these systems can automatically drive PTZ cameras to look at arbitrary geographic locations based on the location of events. This has tremendous cost-saving implications when monitoring large perimeters. You can then take alarm information from video analytics, fence detection sensors, GPS, and other intrusion detection systems and relate those alarms, through the use of mapping technology, to specific geographic locations.

The system can then steer one or more cameras automatically to that location to provide automatic video verification of perimeter alarm events without using any hardware or software presets. After the system steers cameras to the correct location of detection, the operator can take control of the PTZ camera to further assess the situation or the system can provide automated tracking.

**Intelligent video**

Advanced systems have video analytics that permit reliable alarming based on object detection and tracking, all designed to eliminate or reduce the false and nuisance alarms traditionally associated with 'intelligent' video systems. A common source of false alarms when performing motion and object detection is the motion of the camera itself, either under the control of an operator, or due to wind, weather or vibrations.

Pole-mounted cameras are particularly prone to low frequency, high amplitude oscillations in even moderate winds or vibration effects, and this can wreak havoc with 'intelligent' video systems. To overcome this problem, the usual solution is to use expensive hardware video stabilisers, or to reinforce the camera mounting, which is also an expensive proposition. More advanced systems solve this problem by stabilising video images in software, which is a unique capability among leading vendors of 'intelligent' video systems. This allows video analytics software to function even in the presence of significant camera motion or vibration.

Video analytics are able to classify and track an object based on size (animal, human, car, truck, etc), speed (slow moving, fast moving), shape, and direction of movement in changing lighting conditions (overcast, moving clouds, night), and alarms can be raised based on upper and lower thresholds for any of these attributes. These features are available for all video sources, including infrared and thermal cameras. Video analytics also provide diagnostic capabilities, such as detecting possible camera tampering due to lens blockage or gross physical movement.

**Behaviours**

These systems also have the ability to classify objects in relationship to environmentally changing backgrounds and then track those objects within video space. This functionality results in the ability to identify typical security behaviours or situations: Detecting stopped vehicles, human/vehicle piggybacking, crowd detection, left-behind or removed objects, etc.

**Geo-referencing tracked objects**

The advanced systems that are integrated with GIS are capable of converting the positions of objects or events tracked through video analytics into geographical latitude and longitude coordinates, which can then be displayed as an icon on a GIS map (see Fig. 3). Through the use of advanced camera control capabilities and user interface, an operator can then click on the icon on the map to steer one or more PTZ cameras to the object's location automatically.

**Emergency/crime response**

A command and control user interface which leverages GIS technology can be used in emergency/crime responses to locate intruders and response vehicles and personnel on the geographic map as well. This enables security personnel to orchestrate a coordinated response.

From the central command centre, security personnel get a bird's eye view of the situation. They are able to visually locate both the perpetrator and the response vehicles. They can steer cameras to critical locations simply by clicking on the map or the system can automatically steer the cameras based on any geographic coordinate on the map from GPS or other sensor inputs. Response officers can transmit an alarm with their GPS position from any GPS transmitting device and these systems can automatically steer the camera to this location. This can greatly increase the safety of the response team and
aid in orchestrating a successful response.

Remote access to video and alarms

Native support for Pocket PC-based PDAs also exists to receive alarms, view live video, control PTZ cameras, and provide alarm acknowledgments. Advanced PTZ camera control capabilities (point-and-click, drag-to-zoom) are also available through the PDA software, and the operator can dynamically adjust the video stream frame rate and the quality to suit the available network bandwidth (see Fig. 4).

Forensic search

Digital storage of video provides for seamless searching of video through forensic analysis or date-time queries for each camera, whether the video is stored locally or centrally. Advanced searches allow a user to add forensic analysis capabilities to the query, such as looking for motion or objects in certain parts of the camera’s field of view, or looking for objects that meet certain size, speed, or directional criteria. An example may be searching for movement within a keep-out zone.

Edge device - managed bandwidth

In South Africa bandwidth is always an issue. One can overcome the problem by using an edge device that operates within the wide-area surveillance system, which monitors, detects and reports on multiple types of threats.

The edge device can also act as a stand-alone remote sensor, detecting and reporting threats or seamlessly integrating into your current enterprise surveillance solution. These devices can be used as input logic for smart threat detection or can be activated by the central control room system based on the identification of a threat.

When integrated into your enterprise surveillance system, the edge device lets the system scale video much more affordably. Offloading image processing allows your network video server to receive a higher number of inputs – helping you save money. The edge server also removes the need to stream video all the time, and therefore requires less network bandwidth and less storage.

The edge device can be programmed to store information until such time that it is requested, or to continuously send information. It may also be programmed to only send text information, jpeg alarm images, video clips of events, or full frame rate video. It is like having your own personal security guard on duty out in the wilds, 24/7, never sleeping.

Potential benefits to critical facilities

To illustrate a few of the powerful capabilities and resulting benefits that these geo-referenced IVS solutions can provide to a critical facility, consider the following scenarios.

Scenario A: A thief is crawling towards the facility in an attempt to enter illegally. The system will monitor for changes in the background and identify objects which are anomalous or changing over time, while filtering out changes due to lighting and environmental conditions. When conditions are met, the appropriate security protocol will be initiated (see Fig. 5).

Scenario B: A gang has cut through a critical facility’s chain link perimeter fence with the intention of sneaking into the facility. The system will detect a person(s) cutting through or climbing over a facility’s perimeter fence. When integrated with fence
detection sensors, the system can automatically command multiple cameras to the point of intrusion. When this happens, an alarm will notify security personnel and the system will display a map with the exact location of the intrusion while continuing to track, identify and record the suspects. Further, such a system also allows operators to control cameras using a point-and-click interface, allowing them to fully understand the situation before implementing an emergency response.

Scenario C: A truck containing hazardous material departs the facility in several hours. As a security precaution, the facility has declared that the truck cannot be accessed by anyone until just prior to departing the facility. Using the visual interface feature, an operator can draw a ‘virtual’ perimeter zone around the vehicle. If a person crosses that region during this monitoring period, the system will alarm, notify security and track the offending person or object.

Scenario D: A criminal steals an employee’s access card, allowing them to gain entry to the facility’s unauthorised zones. The system can be integrated with a facility’s card access system, wherein every time a facility employee scans his/her access card, the system provides security personnel with a comparison of a live image of the person against an archived still image. Alternatively, the system can be integrated with a facial recognition system that will automatically verify the individual entering the facility against an archived database of faces.

Contact Etienne Louw, Director Spatial Security Solutions, African Astronautics, Tel 082 453 5475, elouw@afrinautics.com @