

Examining Best Practices for Outdoor Events

Large events require comprehensive solutions. With experience in supplying digital video solutions to several Olympic Games and numerous sporting events, Oliver Vellacott, CEO of IndigoVision, explains how a distributed IP video system is fundamental. John Romanowich, CEO of SightLogix, explores outdoor installation tips for video and intelligent analytics.

SUBMITTED BY INDIGOVISION AND SIGHTLOGIX

THE OLYMPIC CHALLENGE: SECURING MAJOR EVENTS USING DISTRIBUTED IP VIDEO SURVEILLANCE

The security risk at any large sporting event is people. There will be nearly 8 million spectator tickets available at the London 2012 Olympics. Large sporting events not only attract fans, but also criminals, traffic chaos and potential terrorist attacks. Video surveillance is a key component for integrated event security.

Enabling multiple agencies and operators to view high-quality video from key locations and to identify potential problems is fundamental to the smooth operation and security of events. A technology which reliably and cost-effectively supplies such surveillance is distributed IP video.

Choosing the correct IP video architecture is fundamental to a surveillance system that has to monitor huge areas with multiple remote sites and offer multi-agency access at any location. The 2004 Athens Olympic Games were secured by 63 command centers with 1,250 operators, monitoring 47 venues spread out over 250 square kilometers. Law enforcement, emergency services, military, traffic



Athens 2004 Olympic Games opening ceremony
(Image courtesy of IndigoVision)

management, coast guard and local security all required access to the system, so every operator had to be given unique access rights. This provided a high degree of redundancy, ensuring control could be transferred to any of the other centers, should any command center become inoperative.

It is clear from the Athens example that a truly distributed IP video system is required. Many IP network surveillance systems are based on centralized architectures. Centralized systems have four drawbacks: Cost, network reliability, a single point

of failure on the site database and limited scalability. In these systems, a central control room houses the overall site database on a central server and video recording servers. Every camera and workstation in each remote location must regularly communicate with the central office to check for changes in the site database.

For large sites, the system needs to be distributed. Each remote video management workstation keeps a copy of the site database. If the central server, a LAN switch or the WAN fails, users at workstations can continue to work using their locally

cached site database.

Delivering high-quality video over long distances is a fundamental requirement for an Olympic surveillance system. The issues with long-distance transmission of video are network bandwidth and latency. This issue becomes more pressing when considering high-definition (HD) video. In preparation for the 2010 Winter Olympics, the Canada Border Services Agency installed 500 HD network cameras to monitor their customs operations on US-Canadian border crossings and at the Vancouver International Airport.

An IP video solution must offer excellent alarm handling features and a seamless interface to integrate third-party security systems across IP networks. In preparation for

the 2010 Soccer World Cup, the Nelson Mandela Bay Metropolitan Municipality in South Africa installed an integrated security solution. The metro area is home to more than 1.3 million people and will be a host city for the competition. The integrated solution includes video, access control, intrusion detection, perimeter security and fire detection. The systems are fully integrated across a 1-Gigabit LAN running on a fiber backbone, with wireless network links for more remote sites. The system also provides services such as IP telephony and intercoms.

The 2006 Winter Olympics in Turin, Italy, deployed a 500-camera distributed IP video system. Video analytics automated low-level scene monitoring functions, freeing the

operators to monitor higher risk areas. When the analytics triggered an alarm, the security management software automatically alerted the operator and displayed the appropriate camera feed. The result was quicker incident response and more efficient surveillance operation.

HOW TO ALARM-PROOF OUTDOOR VIDEO AT LARGE SITES

Nuisance alarms are the bane of the security industry. Whether false alarms come from burglar alarms, outdoor sensors or some other system component, they can undermine security effectiveness and cause security teams to lose trust in their systems. Repeated false alarms can eventually condition

security operators to ignore valid alerts. Nuisance alarms can become part of the “background noise” of a dysfunctional security system and can negatively impact accountability of the entire security organization.

Some facilities are plagued with hundreds of nuisance alarms every week. Outdoor detection systems are especially prone to nuisance alarms, which must operate in uncontrolled environments subject to weather changes, random movements from trees, shadows from clouds, and small animals that can inappropriately trigger alerts. One cause of these nuisance alerts in outdoor systems comes from deploying intelligent video systems originally designed for static indoor environments. When these indoor systems are misapplied to protect a facility's perimeter or buffer zone, the recurrence of nuisance alarms can undermine the important mission of perimeter security to serve as the first line of defense. There is a high likelihood that such systems will never detect the threats that they were intended to stop.

For these reasons, providing effective outdoor security systems without nuisance alarms requires

intelligent surveillance systems designed for outdoor applications. A number of camera features engineered specifically for outdoor surveillance enables such a system to provide accurate detection in the outdoor environment, despite uncontrolled factors.

For example, sufficient onboard image processing can be used to accurately discriminate legitimate targets from extraneous surrounding motion and clutter. Such processing power within the camera can be used to stabilize the image electronically, before video content analysis takes place. This removes camera motion as a source of nuisance alarms, since video analytics cannot detect an object entering into view if the whole scene is moving from wind.

Sufficient in-camera processing can eliminate water reflections and tree motion as sources of nuisance alarms, and dynamically correct lighting to detect events that would otherwise be missed. Additional environmental factors that need to be addressed in the outdoors include the sun moving across the sky, clouds constantly in motion and shadows moving through a scene, all of which must be filtered so as not to appear to the camera as targets on which to alarm.

When sufficient processing is placed in the camera, 100 percent of the

raw scene data is available to make accurate determinations. Such extra processing can also be used to register the camera's field of view to GPS coordinates and provide operators with accurate determination of target location, size, bearing and speed. This information becomes critical when protecting large outdoor areas.

The economics of covering large outdoor areas is different. Outdoor surveillance involves additional infrastructure costs, including engineering design, construction, trenching, camera poles, network connectivity, video display and storage. By providing the appropriate level of computational power, such outdoor cameras are able to cover three to five times the distance — more than 10 times the area — of indoor surveillance cameras. This reduces the number of cameras, infrastructure and associated costs. While outdoor cameras may have a higher cost per unit, their extended range from extra processing leads to an overall reduction in deployment cost.

Applying outdoor solutions to outdoor problems is the key to eliminating nuisance alarms. Using appropriate tools designed for the task realizes the benefits of intelligent video and delivers new levels of efficiency for security personnel. **AKIS**



John Romanowich,
CEO of SightLogix



Oliver Vellacott,
CEO of IndigoVision



Outdoor monitoring applications require proper setup of video surveillance equipment. (Image courtesy of Messe Frankfurt)