The Olympic Challenge – Securing Major Events using Distributed IP Video Surveillance

The homeland security issues facing major sporting events such as the 2010 Winter Olympics in Vancouver and the Football World Cup in South Africa are massive. With the experience of supplying digital CCTV solutions to several Olympic Games and numerous sporting events, Oliver Vellacott, IndigoVision CEO, explains how a distributed IP Video system is fundamental for surveillance at such events.

The major security risk at any large sporting event is people. They not only attract fans, but also criminals, traffic chaos and potential terrorist attacks. CCTV surveillance is therefore a key component of the integrated security solution at these events.

The major security risk at any large sporting event is people

Enabling multiple agencies and operators to view high-quality video from key locations and to quickly identify potential problems and incidents is fundamental to the smooth operation and security of any event. The only technology capable of reliably and cost-effectively supplying such a surveillance solution is distributed IP Video.

IP Video Architecture

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. And just because a surveillance system is based on digital network technology, it doesn't mean the architecture is suitable.

The scale of the problem can be seen from the system deployed in Athens for the 2004 Olympics. Figure 1 shows the Command Center Structure used during the games.

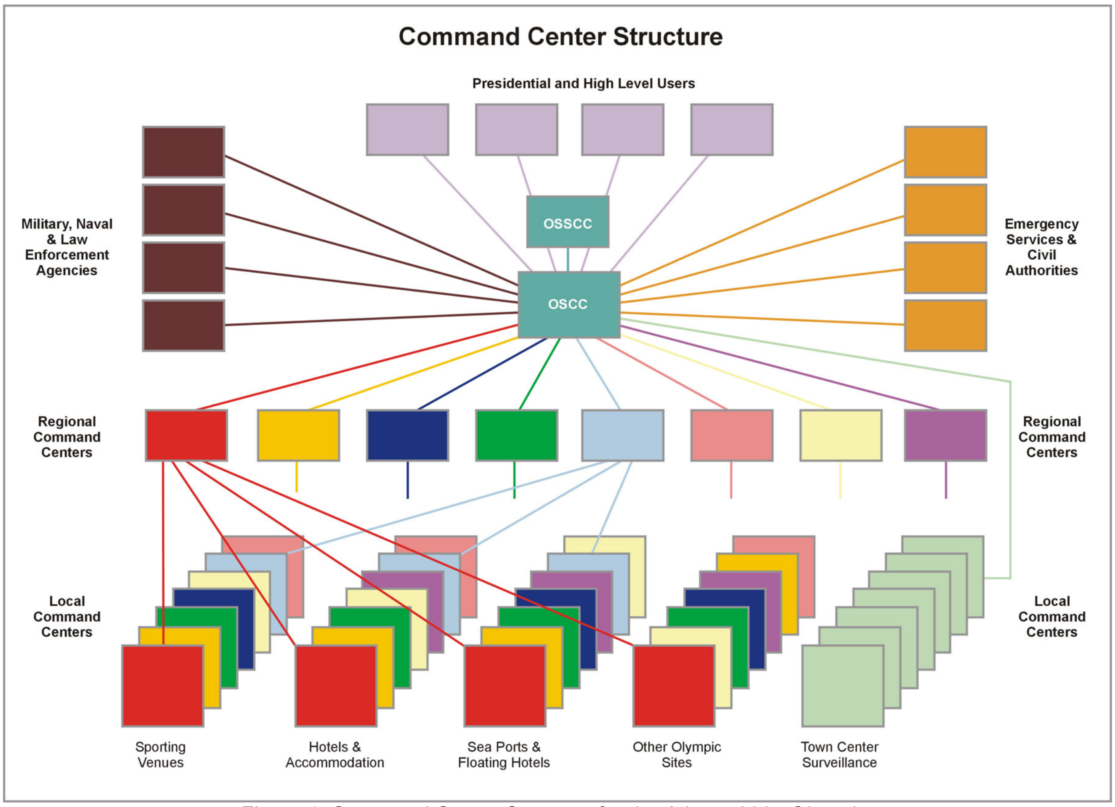

Figure 1. Command Center Structure for the Athens 2004 Olympics

There were 63 command centres with 1250 operators, monitoring 47 venues spread out over an area of 250 square kilometres. Operators worked for many different agencies each with their own interest in the CCTV video feeds. Law enforcement, emergency services, military, traffic management, coastguard and local security all required, to some degree, access to all or part of the system and so every operator had to be given unique access rights to particular components. This provided a high degree of redundancy, ensuring control could be transferred to any of the other centres should any command centre become inoperative.

It is clear from the Athens example that a truly distributed IP Video system is required. So what is meant by a distributed system? One way to explain this is to look at the alternative to a distributed system, that is one that is centralised.

Many IP network surveillance systems are based on centralised architectures and they have some major drawbacks for large mission critical applications. In these types of 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, and in some cases continuously, communicate with the central office in order to check for changes and updates in the Site Database. This includes checking for valid licenses or storing recording and alarm data.

A centralised architecture has four major drawbacks:

1. **Cost** - All users continuously communicate with the central office. On a LAN that means buying expensive high-end switches and on a Wide Area Network (WAN) it means using up precious bandwidth.

2. **Reliability and Resilience** - What happens when the WAN or LAN breaks? Remote users can be left stranded with no access to the live and recorded video from cameras which are actually located locally to them on a working LAN.

3. **Single point of failure** - What happens if the server hosting the Site Database fails? All users of the system rely on access to the Site Database. For example, to get login credentials verified or license permissions checked. If the Site Database server fails, the whole Security Management system goes down.

4. **Scalability** - As more cameras and users get added to each remote site and as more remote sites get added to the network, everything gets congested. The local LAN's, WAN links and Central Server all get congested coping with increasing levels of traffic checking for Site Database changes, valid licensing and storing recordings and alarms.

So for large sites, such as the Athens Olympics, the system needed to be distributed. In a distributed architecture each remote video management workstation keeps a copy of the overall Site Database. Configuration data does not change very frequently. This means the information can be synchronised between the Central Server and the remote workstations, either according to a managed schedule or on-demand when a change happens. In the event that the Central Server, a LAN switch or the WAN fails, users at workstations can continue to work using their locally cached Site Database.

Similarly, rather than continuously streaming recording and alarm data back from the remote sites to the central site across the WAN, it is much better to keep the data locally on the LAN. One or more local Network Video Recorders (NVRs) at each remote site can reduce traffic across the WAN and allow users at the remote sites to access recordings and alarms even when the WAN is not available.

Dual streaming can also be deployed by the cameras, enabling a low-resolution stream to be transmitted for live viewing and a high-resolution stream for recording. This way evidential forensic quality video is available for post-event analysis. Being able to distribute NVRs to the edge of each network improves redundancy and resilience.

Wide Area Surveillance

The ability to deliver high-quality video over very large distances is again a fundamental requirement for an Olympic surveillance system. The issues with long-distance transmission of video are network bandwidth and latency. If too much bandwidth is required to deliver the video then a costly network infrastructure is required. This will also lead to high-latency, i.e. a delay in the video transmission. This makes it difficult for operators to smoothly control camera PTZ movement remotely over large distances.

The key to overcoming this is to deploy the very best compression technology. There can be significant differences between vendors' IP Video solutions, which is often down to how well the MPEG-4 or H.264 compression standards are implemented. The data rates from different manufacturers' cameras can vary significantly (often as much as 5 or 6 times higher), even when comparing cameras implementing H.264. This not only has an impact on network bandwidth, but also on NVR disk storage.

This issue becomes even more important when considering megapixel HD video. HD cameras can provide much greater detail allowing faces and licence plates to be easily identified. They also offer a much larger field of view, enabling a single HD camera to replace a number of standard definition cameras.

As part of a major upgrade programme and in preparation for the 2010 Winter Olympics, the Canada Border Services Agency (CBSA) installed 500 HD IP cameras, the largest HD IP Video system to be deployed at the time, to monitor their customs operation on its US-Canadian border crossings and at Vancouver Airport.

Using Wireless Ethernet Bridges to extended networks to areas that would be costly or impossible to reach with network cabling is an established solution, particularly in wide-area surveillance applications. Again low bandwidth transmission of video is fundamental to maximise the benefits of wireless network links.

CBSA has installed 500 HD IP cameras to monitor their customs operation on its US-Canadian border crossings and at Vancouver Airport.

Multi-Vendor Integration

CCTV is often the system most used by operators working in an integrated environment, so it's important that the IP Video solution can 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 located in the Eastern Cape province of South Africa installed an integrated security solution. The metro area is home to over 1.3 million people, covers an area of 2000 km^2 and includes the towns of Uitenhage and Despatch, together with Port Elizabeth which will be a host city for the competition.

The integrated security system includes CCTV, access control, intruder detection, perimeter security and fire detection. The systems are fully integrated across a 1 Gbit LAN running on a fibre backbone, with wireless network links for more remote sites. The system also provides services such as IP telephony and intercoms.

Integration of various systems across an IP network can provide the user with very powerful tools for managing the security environment. Alarms from one system can trigger an action in another. For example, an access control alarm from an illegal door entry can cause the nearest CCTV camera to be panned to a preset position and the video feed automatically displayed to the operator.

Often traditional analogue CCTV systems in satellite venues or existing transport infrastructures already exist and budgets aren't available to upgrade these systems to IP Video. However, the flexibility of IP Video allows these systems to be easily interfaced to the wider CCTV system, creating a hybrid solution.

Analytics & Alarms

The 2006 Winter Olympics in Turin, Italy deployed a 500-camera distributed IP video system for its surveillance. As with any large monitoring project it was important to provide tools that allowed operators to prioritise and manage the many hundreds of video feeds they were responsible for.

In Turin, video analytics were used to automate the low-level scene monitoring functions, freeing the operators to monitor higher risk areas. This could simply have been motion detection, or more advanced functions such as virtual tripwires, abandoned object detection, congestion detection or counter flow monitoring.

The analytics were processed in real time at the edge of the network in the IP transmitter modules that were connected to the analogue cameras. When the analytics function triggered an alarm the Security Management Software automatically alerted the operator and displayed the appropriate camera feed on a spot monitor.

The 2006 Winter Olympics in Turin, Italy deployed a 500-camera distributed IP video system for its surveillance

Alarms from other third-party systems can also act in the same way as analytics, automatically triggering actions in the Security Management Software. This cause and effect allows the system to operate in what is known as a 'black' or 'dark' screen monitoring mode, where video is only displayed on alarm. The result is quicker incident response and a more overall efficient surveillance operation.

Regeneration

Regeneration is a very important issue for any modern games. Re-using the investment in new sporting venues, athlete's accommodation and transport and regenerating the local area is a key outcome for the organisers. The IP Video system has its part to play in this, due to its flexibility. A distributed network surveillance system allows any component - video management workstation, camera or NVR - to be located on any part of the network. This also means that it is very easy to change the configuration of the system after the games as use of the facilities change.

Local authorities can also expand on the systems left behind after the event to further enhance security in their area, as was the case in Stuttgart, Germany, following the 2006 Soccer World Cup.

Using an IP Video solution, Stuttgart extended its existing analogue CCTV infrastructure to provide central monitoring for the city's transport network in a 30Km radius around the existing football stadium. The CCTV surveillance inside the stadium was also updated to IP Video to provide a totally integrated solution that delivered continuous high-quality, full-framerate video to several control centres around the city. After the World Cup, Stuttgart expanded the system further by adding additional cameras to the network for the monitoring of tunnels, roads and pedestrian areas.

About the Author

Oliver Vellacott founded IndigoVision in 1994. He was previously a product manager with a background in intelligent camera products. Oliver studied piano at the Guildhall School of Music before gaining his first degree in Software Engineering from Imperial College London and then a PhD in Electrical Engineering from Edinburgh University.

Dr Oliver Vellacott, CEO,
IndigoVision Group plc,
Charles Darwin House
The Edinburgh Technopole
Edinburgh, UK, EH26 0PY
Tel: +44 131 475 7200
Fax: +44 131 475 7201
www.indigovision.com