

IP Video Surveillance Technology for Local Government Agencies

Ojo Technology, Inc.
48890 Milmont Drive
Suite 101D
Fremont, CA 94538
www.ojotech.com

Abstract:

The purpose of this white paper is to provide an overview of IP surveillance including government-specific requirements. This paper also contains a section on potential cost savings when using an IP video surveillance system.

Overview of IP Surveillance Systems

Government Agencies have been successfully implementing Closed Circuit Television (CCTV) as a safety measure for citizens in parks, government offices, water treatment facilities and even school districts. However, CCTV systems have proven to be expensive and inflexible, which has limited their wide-spread use and kept them from becoming a key component in many cities' safety and protection plans. A key cost factor for CCTV is the expense of the long-distance, dedicated cabling from the cameras to the viewing station. Another limiting factor is the inability to view the video from police squad cars.

Networked (Internet Protocol or IP-based) camera systems are now replacing traditional CCTV. Most local government agencies are finding that the newer IP Surveillance systems are significantly lower in cost. Furthermore, the flexibility and the remote monitoring capabilities inherent in IP Video Surveillance systems make them much more practical for public safety implementations.

An IP video surveillance system consists of the following:

- One or more digital "network" cameras
- A standard Ethernet network, either shared or dedicated
- A central management server
- One or more client viewing stations
- A digital storage unit

Cameras

IP cameras contain a digital CCD or CMOS sensor with an embedded microcomputer to do image processing and interface to the network. Both the digital video output frames from the camera and camera control information flow through a standard Ethernet connector. There are a wide range of cameras that work under different lighting conditions including infrared cameras for night-time viewing.

Network

The standard computer network that supports the digital video flow and the camera control information are identical to those that support the data flow between office computers, servers, and printers. Network cable, switches and wireless interfaces are standard hardware products, widely available and inexpensive. The network for the IP surveillance cameras is often shared with an existing, installed data network. This is appropriate if the current network is 100base-TX or Gigabit Ethernet. Some companies may desire to run a dedicated network, or a partially dedicated network for the IP surveillance system. Sometimes government facilities choose to upgrade an older network, providing improved computer functionality as well as supporting networked cameras.

“The idea is to give people a higher level of security so that they can enjoy themselves. The reality is that we can’t afford to put an officer on every corner.”

-- David Ready,
City Manager,
Palm Springs.
California State
Library, Public
and Private
Applications of
Video
Surveillance
and Biometric
Technologies

Server

The central server is often a standard Windows-based desktop computer, typically running the camera server software as a dedicated application. The server may physically connect to the network at any point. A standard mouse, keyboard and computer monitor connected to the server typically function as a real-time monitoring station.

The combination of the server, plus storage, is often called a Network Video Recorder (NVR).

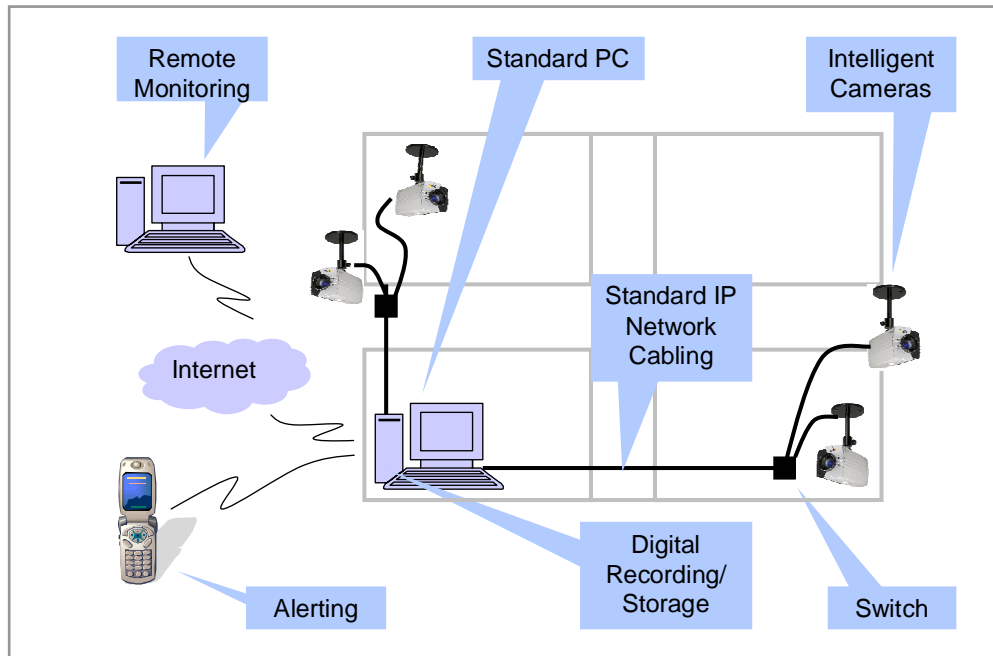
Viewing Stations

The client viewing stations are standard office PCs or laptop computers. The client viewing is either through a simple Windows application or a standard web browser. Multiple client viewing stations are easily supported anywhere on the network, or anywhere on or off-site, connected to the server via the Internet, if desired.

Storage

The digital storage unit is a standard disk subsystem consisting of one or more disk drives that is used to store any type of digital data. Often, multiple disks are used to provide fault tolerant video storage and to store many days of video automatically. A RAID-5 system that holds 14 days of video is the most common configuration. The disk subsystem is normally connected to the server; however it may be placed anywhere on the network, or even remotely via the Internet.

Figure 1: IP video surveillance components



“Video cameras are a relatively inexpensive and very useful tool in both preventing crime and terrorism and also enabling a better response to crime and terrorism.”

-- Michael Chertoff
Homeland Security Chief on NPR 2/08/06

The Need for IP Surveillance in Government Facilities

The needs of government agencies are as broad and diverse as the agencies themselves. However, they share common goals in terms of public safety, crime prevention, employee protection and customer service.

Public safety/crime prevention is a primary reason for many government agencies to install video surveillance, whether it is monitoring water and power supplies or parks. Providing the police service easy access from cameras around the city provides the public with peace of mind and the police force the ability to act with better information. Many cities across the United States have found that installing cameras in high-crime areas is a deterrent to crimes being committed as well as a way for the police to better identify criminals when crimes do happen. The best example in recent history of video surveillance used to identify criminals was with the London bombing in July of 2005. Investigators in London relied on hundreds of cameras in the underground transit system to help identify and capture suspects responsible for the attacks.

Employee protection is always a priority. IP surveillance helps monitor working conditions and watch for safety issues. In areas where employees work late shifts, surveillance of exits, entrances, and parking lots can provide peace of mind to employees.

Vandalism is a costly problem for many cities. The graffiti and disfiguration of city property such as statues gives the city a “black eye”. Video surveillance has proven to be a powerful deterrent against such crimes.

Customer Service is often a priority for city agencies. Video monitoring of lobbies and lines allows management to know when extra personnel are needed in a given area or when an area needs cleaning.

Government-Specific Requirements for IP Surveillance

Though each agency has its own unique needs based on the size, function, and individual requirements, there are several requirements that are common to many government agencies.

Ease of Storage and Retrieval

Finding the video sequence that captures an act of vandalism or a crime required a lot of work with older CCTV-video tape based systems and yet time is often the most critical factor in the apprehension of criminals. IP-based systems make it very easy to isolate an event based on time and motion detection. IP-based systems also make it easy to search across video from multiple cameras.

Connection to Local Law Enforcement

For water districts, parks, and city streets, local law enforcement needs a way to quickly view a situation and to understand where to send enforcement personnel. An IP-based surveillance system allows an immediate connection from the cameras to the local law

enforcement offices or even to patrol cars. With budgets keeping the police stretched thin, video surveillance can make each officer more effective.

Ease of Expansion

Once an IP surveillance system is installed and running, a government agency often finds that it is invaluable in deterring vandalism and crime. It is common for the agency to want to expand an installation to include more cameras and additional monitoring capability. IP-based surveillance systems can be easily expanded to meet these needs.

Flexible Monitoring

It is not uncommon for different people to monitor the cameras at different times. For example, cameras placed in a Post Office may need to be monitored by the Postmaster. However, cameras placed at Post Office entrances and exits may need night-time monitoring from a central security personnel located off-site. IP surveillance systems allow monitoring from any PC. These systems can be set up so that only certain cameras can be monitored by certain individuals if desired.

Specialized Alerting Capability

Instead of constantly monitoring the cameras “alerts” can be set up for unusual circumstances. Alerting saves manpower by not having to have personnel monitoring the video. Alerting can provide more privacy for citizens because video is recorded only when something unusual is happening. The better specialized the alerting capability; the less video that has to be recorded. Specialized software can provide alerts under the following circumstances:

- People traveling the wrong way in crowded environments such as airports
- Motion in just one section of the camera view
- People creating motion as opposed to an animal
- An object that is removed from a location
- A new object appearing in a scene, such as a package left under a seat

All of the above can create a virtual “trip wire” that sends out an alert to a PC, pager, or cell phone.

Cost Justification

In most government agencies, public safety and security is prioritized above the need to cost justify the purchase of a video surveillance system. However, there are often other benefits that can provide real cost savings and can provide a smoother process for the approval of the system.

The cost, for example, of someone poisoning the public water system would be staggering, but installing cameras in all access points also allows easy monitoring of

The city of Chicago has over 2000 cameras that were paid for with the help of a \$5M grant from the Office of Homeland Security Crime has been down since installing the cameras.
-- NPR, All Things Considered 02/08/06.

water levels and cost savings on personnel traveling to those locations. Below are some other potential cost savings:

- Annual cost of repair from acts of vandalism – Statues in parks are often targets of vandalism. Video surveillance in the park will provide a feeling of security to the public, but also deter vandalism and thus eliminate the cost of clean-up.
- Potential cost of a fire – Fires are a special act of vandalism that can have a devastating impact. Even a small fire has significant costs associated with repair. It is clear that if the system prevents just one fire, then it can pay for itself many times over.
- Decreased cost of security personnel required to monitor facilities – Cameras in parking lots can make employees feel safer without having to add expensive security personnel.
- Dumping – Many cities have properties that are currently unoccupied. Unsightly dumping at these sites makes the city look bad and paying for continuous clean-up can be costly. Installing cameras provides a deterrent, but also allows the perpetrator to be caught and fined. Many cities have saved a substantial amount of money by installing cameras on unoccupied properties.
- Service Monitoring – Smaller airports are often not staffed during all operating hours and rely on a trust system to pay for services. Cameras provide assurance against lost revenue when working on the honor system. The cameras also allow monitoring of supplies so that they can be replenished when inventory levels get low.

Privacy Implications

Even though safety is a primary motivator for installing video surveillance systems, there are privacy advocates who are concerned about video surveillance in public places. The public transportation agencies have been using video surveillance for years. According to the National Transportation Research Board, signs should be posted in all vehicles and premises notifying the public of the cameras and that information is being gathered and recorded via the surveillance system.¹ These signs are often a deterrent by themselves.

There have been several court cases that have brought charges that video surveillance violates the right to privacy, but the courts have generally ruled that people do not have a reasonable expectation of privacy when in public because their actions are readily observable by others.²

Special Considerations

When designing an IP surveillance system, there may be special conditions that dictate a specific type of camera equipment or a unique site design. These conditions include the following:

- Covert or semi-covert operation
- The requirement for real-time monitoring
- The requirement for the need to see a long distance

- Upgrading an existing CCTV camera or system
- Cameras in a hard to access or high location
- Unusual lighting, like sodium lamps
- The need for auxiliary lighting
- Ultra-sensitive night vision
- Cameras requiring wireless networking
- Cameras requiring Pan-Tilt-Zoom capability
- The requirement for a camera to monitor more than one area
- Cameras requiring special enclosures
- A vandal-prone location

An experienced installer of IP surveillance systems can help you with site design and work through any special conditions that may exist at your site.

About Ojo Technology, Inc.

Ojo Technology is a solution provider and systems integrator with expertise in both security and in data networking. Ojo specializes in complete customer specific solutions for IP surveillance systems in local governments, manufacturing facilities, and educational institutions. Ojo has installed IP video surveillance systems in a range of government installations including:

- Municipal water districts
- City streets
- City offices
- Police stations
- Airports
- Schools
- Powerplants

Whether developing a completely new IP surveillance solution, or upgrading and enhancing an existing analog video surveillance platform, Ojo Technology delivers the complete solution including consultation, design, hardware, software, data cabling, electrical, installation, maintenance, and support services. Ojo Technology also provides complete user training. Learn more about Ojo Technology online at www.OjoTech.com.

Ojo Technology, Inc., 48890 Milmont Drive Suite 101D, Fremont, CA 94538
Tel 510-249-9540 Fax 510-249-9545 email: info@ojotech.com.

¹ Public and Private Applications of Video Surveillance and Biometric Technologies, by Marcus Nieto, Kimberly Johnston-Dodds, and Charlene Ware Simmons, Ph.D. Available at <http://www.library.ca.gov/crb/02/06/02-006.pdf>

² Legal Issues Related to Silent video Surveillance, Alexandra, VA: Security Industry Association, 1999. Available at http://www.securitygateway.com/E/E3_4.html