

# SECURITY CAMERA EVALUATION GUIDE

By: John Honovich

[jhonovich@ipvideomarket](mailto:jhonovich@ipvideomarket)

<http://ipvideomarket.info/>

646 867-1965

1. What type of security cameras should I use?
2. How should I connect cameras to video management systems?
3. What type of video management system should I use?
4. What type of storage should I use?
5. What type of video analytics should I use?
6. How should I view my surveillance video?
7. How should I integrate video with my other systems?

## 1. Security Camera Selection

Security cameras are literally the eyes of a video surveillance system. Cameras should be deployed in critical areas to capture relevant video.

The two basic principles of camera deployment are (1) use chokepoints and (2) cover assets.

Chokepoints are areas where people or vehicles must pass to enter a certain area. Examples include doorways, hallways and driveways. Placing cameras at chokepoints is a very cost-effective way to document who entered a facility.

Assets are the specific objects or areas that need security. Examples of assets include physical objects such as safes and merchandise areas as well as areas where important activity occurs such as cash registers, parking spots or lobbies. What is defined as an asset is relative to the needs and priorities of your organization.

Once you determine what areas you want to cover, there are four camera characteristics to decide on:

1. **Fixed vs. PTZ:** A camera can be fixed to only look at one specific view or it can be movable through the use of panning, tilting and zooming (i.e., moving left and right, up and down, closer and farther away). Most cameras used in surveillance are fixed. PTZ cameras are generally used to cover wider fields of views and should generally be used only if you expect a monitor to actively use the cameras on a daily basis. A key reason fixed cameras are generally used is that they cost 5 to 8 times less than PTZs (fixed cameras average \$200 to \$500 USD whereas PTZ cameras can be over \$2,000 USD).
2. **Color vs. Infrared vs. Thermal:** In TV, a video can be color or black and white. In video surveillance today, the only time producing a black and white image makes sense is when lighting is very low (e.g., night time). In those conditions, infrared or thermal cameras produce black and white images. Infrared cameras require special lamps (infrared illuminators) that produce clear image in the dark (but are significantly more expensive than color cameras - often 2x to 3x more). Thermal cameras require no lighting but product only silhouettes of objects and are very expensive (\$5,000 to \$20,000 on average) In day time or lighted areas, color cameras are the obvious choice as the premium for color over black and white is trivial.
3. **Standard Definition vs. Megapixel:** This choice is similar to that of TVs. Just like in the consumer world, historically everyone used standard definition cameras but now users are shifting into high definition cameras. While high definition TV maxes out at 3 MP, surveillance cameras can provide up to 16 MP resolutions. In 2008, megapixel cameras only represent about 4% of total cameras sold but they are expanding very rapidly.

4. **IP vs. Analog:** The largest trend in video surveillance today is the move from analog cameras to IP cameras. While all surveillance cameras are digitized to view and record on computers, only IP cameras digitize the video inside the camera. While most infrared and thermal cameras are still only available as analog cameras, you can only use megapixel resolution in IP cameras. Currently, 20% of cameras sold are IP and this percentage is increasingly rapidly.

Most organizations will mix and match a number of different camera types. For instance, an organization may use infrared fixed analog cameras around a perimeter with an analog PTZ overlooking the parking lot. On the inside, they may have a fixed megapixel camera covering the warehouse and a number of fixed IP cameras covering the entrance and hallways.

## 2. Connectivity

In professional video surveillance, cameras are almost always connected to video management systems for the purpose of recording and managing access to video. There are two main characteristics to decide on for connectivity.

- **IP vs. Analog:** Video can be transmitted over your computer network (IP) or it can be sent as native analog video. Today, most video feeds are sent using analog but migration to IP transmission is rapidly occurring. Both IP cameras and analog cameras can be transmitted over IP. IP cameras can connect directly to an IP network (just like your PC). Analog cameras cannot directly connect to an IP network. However, you can install an encoder to transmit analog feeds over IP. The encoder has an input for an analog camera video feed and outputs a digital stream for transmission over an IP network.
- **Wired vs. Wireless:** Video can be sent over cables or through the air, whether you are using IP or analog video. Over 90% of video is sent over cables as this is generally the cheapest and most reliable way of sending video. However, wireless is an important option for transmitting video as deploying wires can be cost-prohibitive for certain applications such as parking lots, fence lines and remote buildings.

## 3. Video Management System

Video management systems are the hub of video surveillance solutions, accepting video from cameras, storing the video and managing distribution of video to viewers.

There are four fundamental options in video management systems. Most organizations choose one of the four. However, it's possible that companies may have multiple types when they transition between one to another.

- **DVRs** are purpose built computers that combine software, hardware and video storage all in one. By definition, they only accept analog camera feeds. Almost all DVRs today support remote viewing over the Internet. DVRs are very simple to install but they significantly limit your flexibility in expansion and hardware changes. DVRs are still today the most common option amongst professional buyers. However, DVRs have definitely fallen out of favor and the trend is to move to one of the three categories below.
- **HDVRs** or hybrid DVRs are DVRs that support IP cameras. They have all the functionality of a DVR listed above plus they add support for IP and megapixel cameras. Most DVRs can be software upgraded to become HDVRs. Such upgrades are certainly a significant trend and is

attractive because of the low migration cost (supports analog and IP cameras directly).

- **NVRs** are like DVRs in all ways except for camera support. Whereas a DVR only supports analog cameras, an NVR only supports IP cameras. To support analog cameras with an NVR, an encoder must be used.
- **IP Video Surveillance Software** is a software application, like Word or Excel. Unlike DVRs or NVRs, IP video surveillance software does not come with any hardware or storage. The user must load and set up the PC/Server for the software. This provides much greater freedom and potentially lower cost than using DVR/NVR appliances. However, it comes with significant more complexity and time to set up and optimize the system. IP video surveillance software is the hottest trend in video management systems currently and is the most frequent choice for very large camera counts (hundreds or more).

#### 4. Storage

Surveillance video is almost always stored for later retrieval and review. The average storage duration is between 30 and 90 days. However, a small percentage of organization store video for much shorter (7 days) or for much longer (some for a few years).

The two most important drivers for determining storage duration is the cost of storage and the security threats an organization faces.

While storage is always getting cheaper, video surveillance demands huge amount of storage. For comparison, Google's email service offer about 7 GB/s of free email storage. This is considered to be an enormous amount for email. However, a single camera could consume that much storage in a day. It is fairly common for video surveillance systems to require multiple TBs of storage even with only a few dozen cameras. Because storage is such a significant cost, numerous techniques exist to optimize the use of storage.

The type of security threats also impact determining storage duration. For instance, a major threat at banks is the report of fraudulent investigations. These incidents are often not reported by affected customers until 60 or 90 days after the incident. As such, banks have great need for longer term storage. By contrast, casinos usually know about issues right away and if a problem is to arise they learn about it in the same week. Casinos then, very frequently, use much shorter storage duration (a few weeks is common).

Three fundamental types of storage may be selected:

- **Internal** storage uses hard drives built inside of a DVR, NVR or server. Today this is still the most common form of storage. With hard drives of up to 1 TB common today, internal storage can provide total storage of 2TB to 4TB. Internal storage is the cheapest option but tends to be less reliable and scalable than the other options. Nonetheless, it is used the most frequently in video surveillance.
- **Directly Attached** storage is when hard drives are located outside of the DVR, NVR or server. Storage appliances such as NAS or SANs are used to manage hard drives. This usually provides greater scalability, flexibility and redundancy. However, the cost per TB is usually more than internal storage. Attached storage is most often used in large camera count applications.
- **Storage Clusters** are IP based 'pools' of storage specialized in storing video from large numbers of cameras. Multiple DVRs, NVRs or servers can stream video to these storage clusters. They provide efficient, flexible and scalable storage for very large camera counts. Storage clusters are the most important emerging trend in video surveillance storage.

## 5. Video Analytics

Video analytics scan incoming video feeds to (1) optimize storage or (2) to identify threatening/interesting events.

Storage optimization is the most commonly used application of video analytics. In its simplest form, video analytics examines video feeds to identify changes in motion. Based on the presence or absence of motion, the video management system can decide not to store video or store video at a lower frame rate or resolution. Because surveillance video captures long periods of inactivity (like hallways and staircases, buildings when they are closed, etc.), using motion analytics can reduce storage consumption by 60% - 80% relative to continuously recording.

Using video analytics to identify threatening/interesting events is the more 'exciting' form of video analytics. Indeed, generally when industry people talk of video analytics, this is their intended reference. Common examples of this are perimeter violation, abandoned object, people counting and license plate recognition. The goal of these types of video analytics is to pro-actively identify security incidents and to stop them in progress (e.g., perimeter violation spots a thief jumping your fence so that you can stop them in real time, license plate recognition identifies a vehicle belonging to a wanted criminal so you can apprehend him).

These video analytics have been generally viewed as a disappointment. While many observers believe that video analytics will improve, the video analytics market is currently contracting (in response to its issues and the recession).

## 6. Viewing Video

Surveillance video is ultimately viewed by human beings. Most surveillance video is never viewed. Of the video that is viewed, the most common use is for historical investigations. Some surveillance video is viewed live continuously, generally in retail (to spot shoplifters) and in public surveillance (to identify criminal threats. Most live video surveillance is done periodically in response to a 'called-in' threat or to check up on the status of a remote facility.

Four fundamental options exist for viewing video:

- **Local Viewing** directly from the DVR, NVR or servers is ideal for monitoring small facilities on site. This lets the video management system double as a viewing station, saving you the cost of setting up or using a PC. This approach is most common in retailers, banks and small businesses.
- **Remote PC Viewing** is the most common way of viewing surveillance video. In this approach, standard PCs are used to view live and recorded video. Either a proprietary application is installed on the PC or a web browser is used. Most remote PC viewing is done with an installed application as it provides the greatest functionality. However, as web applications mature, more providers are offering powerful web viewing. The advantage of watching surveillance video using a web browser is that you do not have to install nor worry about upgrading a client.
- **Mobile Viewing** allows security operators in the field to immediately check surveillance video. As responders and roving guards are common in security, mobile viewing has great potential. Though mobile clients have been available for at least 5 years, they have never become mainstream due to implementation challenges with PDAs/phones. Renewed interest and optimism has emerged with the introduction of the Apple iPhone.

- **Video Wall Viewing** is ideal for large security operation centers that have hundreds or thousands of cameras under their jurisdiction. Video walls provide very large screens so that a group of people can simultaneously watch. This is especially critical when dealing with emergencies. Video walls generally have abilities to switch between feeds and to automatically display feeds from locations where alarms have been triggered.

## 7. Integrating Video with Other Systems

Many organizations use surveillance video by itself, simply pulling up the video management systems' client application to watch applications. However, for larger organizations and those with more significant security concerns, this is an inefficient and poor manner to perform security operations. Instead, these organizations prefer an approach similar to the military's common operational picture (COP) where numerous security systems all display on a singular interface.

Three ways exist to deliver such integration with video surveillance:

- **Access Control as Hub:** Most organizations have electronic/IP access control systems. These systems have been designed for many years to integrate with other security systems such as intrusion detection and video surveillance. This is the most way to integrate video surveillance and relatively inexpensive (\$10,000 - \$50,000 USD). However, access control systems are often limited in the number and depth of integration they support.
- **PSIM as Hub:** In the last few years, manufacturers now provide specialized applications whose sole purpose are to aggregate information from security systems (like video surveillance) and provide the most relevant information and optimal response policies. These applications tend to be far more expensive ((\$100,000 - \$1,000,000 USD) yet support a far wider range of security manufacturers and offer more sophisticated features.
- **Video Management System as Hub:** Increasingly, video management systems are adding in support for other security systems and security management features. If you only need limited integration, your existing video management system may provide an inexpensive (yet limited) solution.

## Conclusion

If you feel comfortable with the key decisions to be made, you may want to start examining what companies provide the best products for your need. You can learn more about companies for each component at the [IP Video Market Companies Overview directory](#).