How to Select an IP Video Management Solution

A strategy for managers to systematically compare IP video management and surveillance systems

milestone

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Table Of Contents

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Introduction

The benefits of Internet Protocol (IP) technology are driving a major change in the video management and surveillance field. Organizations are interested in IP video surveillance for:

- High quality recordings
- Fast search and retrieval
- Easy maintenance
- Freedom from dealing with tapes

They are also attracted to the networking capabilities — everything from the ability to integrate with other security equipment and business systems to the simplicity of running multiple cameras on the same network to cover larger areas more efficiently.

Yet not all IP video surveillance and management systems are the same. The rush to embrace IP technology has led some vendors to offer composite products that consist of a mix of IP and analog technology patched together with software. This has resulted in gaps between what is being claimed and what these products actually deliver. This is particularly evident in the software designed to help users manage and operate the solution.

This white paper presents a strategy for managers and organizations to systematically evaluate IP video management solutions by explaining what an IP video management system is and providing a list of criteria to consider in selecting a system.

Author:

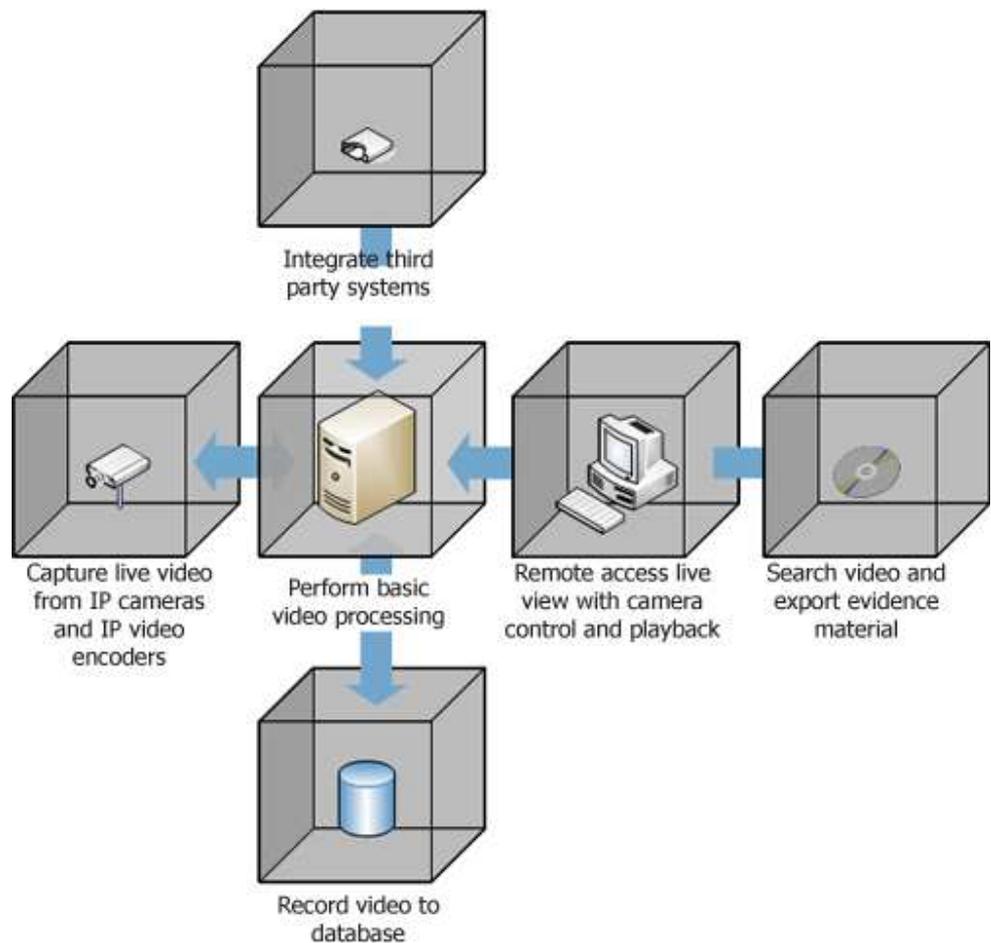Kent Sumida is the Pre-sales Support Manager at Milestone Systems Inc.

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

What is IP video management?

IP video technology provides video surveillance management software that is:

- Flexible
- Updatable
- Scalable

The ideal IP video management system provides intelligent software for the day-to-day operation of video surveillance hardware on an IP network and offers the opportunity to integrate other components of your corporate security program.

*Good IP video management systems perform
all these core functions acrocss an IP network.*

The core functionality of the ideal IP video management system should include all of the following.

1. Simultaneously manage IP cameras and analog cameras together to capture live video. (Analog cameras are connected through video servers, or encoders that convert analog video

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

into digital format.) For example, it could connect more than 200 different IP cameras from over 30 vendors to capture live video, all through the same user interface.

2. Perform basic video processing like motion detection.
3. Start recording in response to triggers such as:
   - Motion detection
   - Doors opening
   - A response to rules in the software interface
4. Remote access that allows users in different parts of a building to see live camera views with complete control (pan, tilt, zoom, etc.). Other remote capabilities should include retrieval and playback of video from the archive database.
5. Integrate with third-party systems like access control and video analytics. For example, when a person enters a building, an access control system could trigger the video management system to verify that the image of the person captured from video matches the ID card/system.
6. The ability to search the video archive database (by area of interest or time period) and create a secure export of material evidence to pass on to police or other authorities.

To facilitate a systematic evaluation of an IP video management solution, this white paper provides 10 criteria that Milestone Systems has selected to be the most important.

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Reliability

Reliability is essential to any video surveillance system. Here are the main characteristics of a proven, reliable IP video management system.

Proven in daily production. Look at the solution's installed base and customer testimonials, preferably from businesses similar to yours. Both are indications of solid performance in the field.

Stable in operation 24/7/365. Ask for data to support system reliability claims.

Robust in different network environments. Verify that the solution performs in different network environments, 100MB or 1GB networks, as well as a wide area network (WAN), in real, live situations.

Smooth software upgrade path. Software upgrades are an important part of the software life cycle to keep up with new devices, drivers and operating systems. Make sure the system can implement software upgrades without requiring all hardware components to be reconfigured.

Openness

Look for a system that can connect and integrate many technologies based on an open software platform and industry standards. Some of the ways to determine openness are:

Well documented Software Development Kit (SDK). The SDK should include a rich, easy-to-use Application Programming Interface (API) that supports the most common programming languages.

Input and output support. Can you measure the inputs in the software? Can you react on those inputs to trigger events and alerts, as well as activate outputs?

Event management. Event management enables custom settings for image uploads, alarm notification, recording, input/out (I/O) control, and other features in response to events.

Support for standard protocols. This is the key to maintaining independence from any one vendor. Surveillance solutions built on proprietary systems can exclude you from future technology innovations that occur within the industry — especially those that you cannot envision today. Popular with the public

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Easy to use

Solutions that are easy to use save you time and money in both the short and long run.

Easy to learn. Ease of use means that your employees will need less time to learn the system and can get up to speed in operation more quickly. This is very important in situations where turnover is high and can have a direct impact on reducing training costs.

Make sure your vendor offers good training and that they are certified in installation and training.

Easy to install. Have the vendor demonstrate that installation procedures do not require multiple manual steps on individual servers, for example, separate tasks to copy Dynamic Link Library(DLL) files to each server.

Look for push or pull deployment options that streamline the process of updating servers and clients.

Easy to manage. Your administrator should be able to manage the solution from one central location, not having to go from station to station.

Simple, clear technical documentation. Are you able to understand the technical documentation? Does it consist of User Guides (how to use the product) and Technical Reference Manuals (quick reference on functions and procedures)?

Certified technical support. Ask to meet the individuals that will support your solution and verify that they are well trained and technically certified.

Easy to operate. When things go wrong there is usually no time to understand the system. Verify that common functions have one-click access and simple navigation — easy operation is vital for your employees to use the solution efficiently in daily tasks and maintain their ability to respond fast.

Independence

The best IP video management systems are independent of hardware and give you the freedom of choice to select the "best of breed" hardware with the best fit for your application.

Hardware and software limitations. Often, vendors offer a broad line of their own security products (alarms, cameras, access control, etc.), however, these may not all be "best of breed". A vendor may have six or seven types of products, including some that are good, but not top quality in all application categories. Likewise, sub-vendors may introduce products of lesser quality to compete on price. In general, the ability to mix and match to get the best components for different application needs enables you to achieve optimal performance.

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Open platform strategy. If you choose to engage with a vertically integrated, proprietary supplier offering everything in a one-stop solution, be careful not to get locked into "proprietary jail" and thus limit your options.

This advice should not be confused with a Systems Integrator who integrates "best of breed" components from multiple vendors into a full solution.

Flexibility

In today's business environment change happens faster and faster making flexibility more essential today than ever before.

Security requirements are not static. Expansions, relocations, mergers, new regulations or advances in technology all force change on your security solution. A solution that has the flexibility to adapt to the changing needs of your organization can save you money and increase the return on investment (ROI) in the long-term.

Choose standard components. Select standard servers, switches, storage hardware, software, and surveillance hardware (cameras, access control etc.).

Innovation

IP technology is established as the future carrier for surveillance and access control. Creating a successful solution requires a new type of vendor that has skills in both physical security (positioning cameras, lens selection, etc.) and IT/network infrastructure (Ethernet, structured cabling, systems management, etc.). The leading manufacturers are actively building this new channel by helping their partners acquire these new skills through certification and training.

Research & Development. Protect your company's future and avoid legacy solutions by verifying the investment in research and development in each supplier you consider.

Pace of development. Does your potential supplier have a documented roadmap of future upgrades? Do these upgrades represent significant increases in functionality that will help you leap-frog your competitors, or are they bug fixes?

Product maintenance agreements (PMAs). A PMA reduces the cost of keeping your solution up-to-date as new software upgrades are released. The cost is usually a small percentage of the product price. A well thought out PMA program will extend the life of your solution, and significantly increase your return on investment (ROI).

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Scalability

Scalability ensures the ability to expand your system in synch. with your company's needs. For example, adding new buildings to accommodate increases in staff may require an upgrade from a single-server localized solution to a multi-server solution. Mergers and acquisitions often require upgrades to a distributed solution across several sites. Make sure none of these will be a "fork-lift" upgrade.

Have channels to spare. Implementing a single-server system that only handles 16 channels limits your options for growth. To expand with one more channel typically requires adding another server with a further 16 channels and having the two systems run side-by-side. With 17 channels, only 53% of the new hardware is being utilized initially.

Implementing a solution that can scale from one to an unlimited number of devices, and one that can grow smoothly in step with your needs, is a more efficient approach that avoids the duplication and under-utilization of hardware.

Old and new technology side by side. To protect your investment in hardware, your solution must incorporate new technology as it becomes available, for example, megapixel and day/night cameras, side by side with existing devices.

Anticipate extra data capacity. As your solution grows by adding cameras or specialized devices, the demand for Central Processor Unit (CPU) and other resources on the video recording system increases. To maintain overall performance and fast response times, the system must be able to manage a distributed solution in which the load is shared across multiple, geographically separate servers.

Plan for future storage needs. At 4 frames per second (FPS) and recording 24 hours a day, a single megapixel camera (100KB per frame) will require 12 Terabytes (TB, $12 \times 10_6$ Megabytes) of storage during one year of operation. To manage storage capacity you will need to implement a company policy for archiving and storage, for example, periodic archiving to CD or DVD. Milestone's storage calculator will help you estimate the initial storage requirements for your solution. See:
www.milestonesys.com/support/questions_and_answers/estimator_and_calculators?.

Always plan for overcapacity on storage from the beginning, and verify that the solution you implement can accommodate several types of storage solution and expansion options.

Supplier licensing schemes. Most surveillance solutions require a separate license for all devices on your system, as well as a new license for each device you add. Clearly, licensing schemes can become complex and unwieldy. Ask potential vendors to demonstrate that their licensing scheme is simple and easy to manage, especially as you start to add new devices.

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Performance

When you are recording multiple video channels, system performance depends on both software and hardware.

Remote access. Fast, reliable remote access depends on the server — how quickly it can serve clients, and how fast the client can decode the video. To analyze an incident you will typically need to view multiple cameras using simultaneous, time-synchronized playback (all cameras playing back on the same time-line). To provide this functionality the software must synchronize views from all cameras and will require a powerful server and a good quality high-definition monitor.

Ask your vendor to demonstrate how many cameras you can view on the same server in simultaneous, time-synchronized playback.

Network utilization. A one megapixel camera at 10 frames per second requires approximately 10 megabits per second in bandwidth. If your surveillance solution requires many megapixel cameras, the server's network adapter can quickly become a bottleneck.

Verify that you can easily configure the solution to share the load across multiple servers, switches and interfaces to maintain performance.

Connect multiple users. A typical surveillance operation requires multiple users to access live video from each camera. For example, in a city-wide surveillance operation, many different users such as police, firemen, and ambulance personnel may need high performance access, say, at 30 frames per second (fps), to view video from each camera and usually different levels of access and control. In this real-life situation the server can provide better performance to many users than could be achieved by connecting individual users directly to each camera.

Given the debate about "pushing functionality out to the edge of the network" (meaning at the cameras), is this a better solution?

A camera typically has a small CPU and can handle a small number of channels. As little as three to five users accessing a camera simultaneously and requiring 30 fps can cause inconsistent levels of performance from the camera and may result in a significant performance drop for all users.

A server, on the other hand, is designed to connect to large numbers of simultaneous users and can deliver a high performance to each one. The camera connects to the server using a single channel and is consequently never overloaded. The server can easily distribute the video to many users providing a consistent, high level of performance to each, even at 30 fps.

Uni-casting vs. Multi-casting. Uni-casting streams video by sending separate packages to each user. However, the server only sends the packages to users that are requesting the video.

Multi-casting streams video by sending one package to all users on the network at the same time. Only those users who want video pick it up.

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

If all users are viewing the same video at the same time, multi-casting can appear as a good solution, however, consider the citywide surveillance example above that is more likely to have many users who need to view different cameras at different times. This surveillance situation creates problems for multi-casting solutions by sending all the video streams to all users whether they are requesting it or not (depending on how the routers are set up, video may even travel to remote IP sub-nets).

Even 10-20 cameras in a multi-casting setup will take a lot of bandwidth and can seriously affect system performance unnecessarily considering that not all users may need access to the video from all cameras. Before implementing a multi-casting setup, confirm that your solution needs simultaneous viewing from multiple clients.

Remote locations and mobile devices. Implement low bandwidth optimization features such as image-size reduction and adjustable frame rates. For low-bandwidth requirements, verify that the system can be optimized manually or automatically to reduce image size and adjust frame rates.

Fast access to the latest video. To reduce storage costs and capacity requirements, store only the most recent video on fast access storage devices. As time elapses and the video gets older, migrate your video archives from faster to slower disk storage systems. The older the data becomes, the less likely it is that you will need to retrieve it for review.

Integrity

Here are some of the important factors to consider to manage access and maintain data integrity in your solution.

Authentication and authorization. The solution should provide a role-based access to the system for all users based on:

- Authentication—verifying that the user is who they say they are
- Authorization—managing/restricting access to features and data in the system

Most surveillance solutions require the administrator to be able to determine which cameras a user can view and when.

Logging system. Verify that the solution provides a continuous log with time stamp so you can trace the activity and use of your system. You will need to set up procedures for your operators to audit these log files to assess if someone has tried to break in to the system.

Encryption. Verify that the solution encrypts all data that is transmitted across unsecured networks. The encryption algorithm must be sophisticated enough to prevent network sniffers or wiretaps from being able to capture and decode confidential video, and secure data like passwords.

Secure, reliable evidence. Ask the vendor to demonstrate that video evidence that has been exported from the system is both encrypted

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

and access-protected by passwords. It is important that the solution can validate that evidence has not been tampered with during the "chain of custody." If tampering has occurred, you must be able to easily check the integrity of the evidence and identify when the tampering occurred and by whom.

Watermarking. This is the process of applying an identification mark to video to verify that it has not been changed since it was recorded. From a "chain of custody" point of view, it is only allowable to apply a watermark at the camera when the video is recorded. Any addition of a watermark after the camera may be interpreted as tampering if the evidence is presented in court. For this reason, our recommendation is to avoid solutions that apply watermarks at the server.

Availability

To be effective, a video surveillance solution must be fully operational 100% of the time. In designing your solution you need to plan for all contingencies, for example, power outages, hardware failure, system issues, etc. Here are some of the requirements you should consider.

Redundancy. Run hot standby systems in parallel with your active systems that duplicate both hardware and software. Provide redundant power supplies and cooling from all servers and networking equipment.

Redundant Array of Inexpensive Disks (RAID). A RAID-5 setup provides redundancy in storage through parity striping. In this technique each disk in the array duplicates enough data from the other four disks so the complete data set on any of the five disks can be recreated if one fails.

Archiving and backup. In addition to your on-site archive, plan for long-term, off-site storage to enable fast data recovery after a catastrophe, like a fire in the server room.

Failover. The degree to which you implement failover in your solution depends on cost and the business priority of the data to be protected. Failover can be either "cold" or "hot."

A "cold" failover has a standby server that is off-line and has to be powered-up to take over. There is a chance that you may lose data during the time it takes to power up the standby server.

A 'hot' failover is where the standby server is powered-up and on-line so it can take over immediately preventing any data loss.

A potential drawback with a failover approach is that there may be gaps in the data on the active system when it resumes control after repair. Verify that the failover strategy you implement includes synchronization between all servers to keep the data set intact.

Monitoring software. You can improve availability by employing software solutions that continually monitor the status of all the devices on your system. If there is a problem with any component, the

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

monitoring software sends an alert to a master control panel, or via email, enabling your staff to respond quickly to rectify the problem.

In response to an alert, the system can re-direct a PTZ camera to continue surveillance in mission-critical areas where a camera has failed.

Milestone White Paper
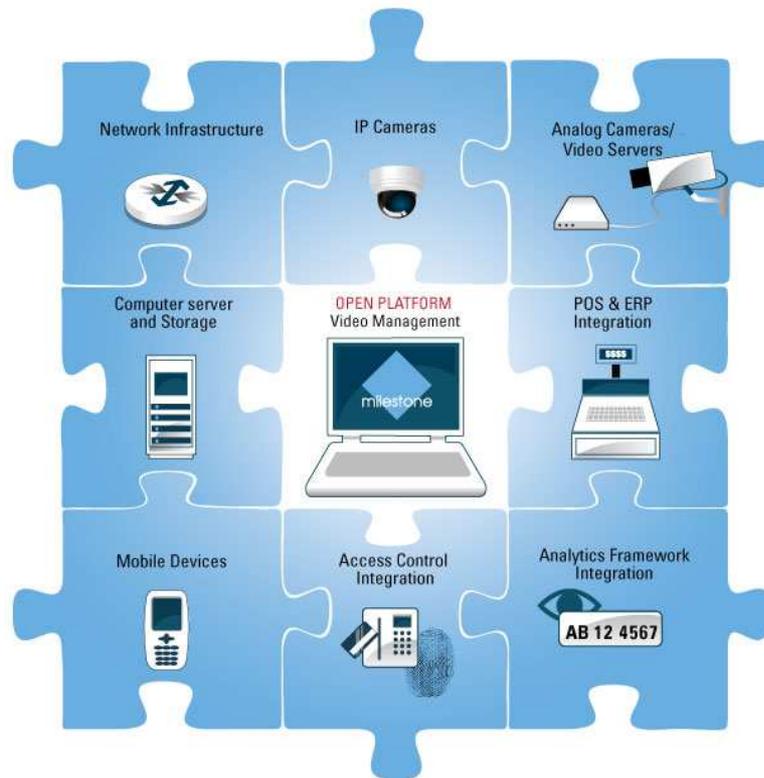How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Milestone Systems

Innovator. Milestone Systems is internationally recognized as an innovator and thought leader in open platform IP video management software. Milestone's XProtect products operate as the core of surveillance systems: connecting, sharing and managing all devices through a single interface that is easy to learn and operate.

Easy to use. The XProtect platform is easy to use, proven in operation and scales to support unlimited devices. XProtect products support the widest choice of network video hardware and are designed with an Application Programming Interface (API) that integrates seamlessly with other manufacturers' systems.

Best-of-breed. Using XProtect, you can build scalable, "best of breed" solutions to reduce cost, optimize processes, protect assets and ultimately increase value in a company's products and services.
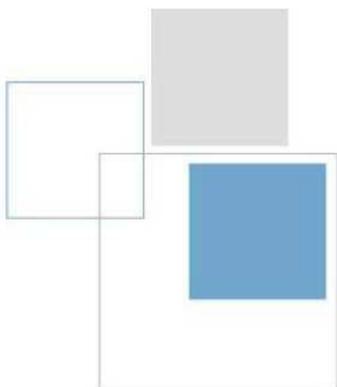

© Copyright Milestone Systems 2008

Milestone White Paper
How to Select an IP Video Management Solution
— A strategy for managers to systematically compare IP video management and surveillance systems

Founded in 1998, Milestone Systems is the global industry leader in true open platform IP video management software. The XProtect™ platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-of-breed solutions to 'video enable' organizations – reducing costs, optimizing processes, protecting people and assets. Milestone software is sold through authorized and certified partners. For more information please visit www.milestonesys.com.