Considerations when selecting a Digital Video Management Platform

A Digital Video Management System acts as the front end interface to the operators of a security system. It is the most visible component in a security and surveillance installation and often the most important component to decide on. The DVMS features and level of integration with cameras and other security sensor devices will ultimately determine if it will meet the needs of your organization or customer.

The primary purpose of a DVMS is to display live video from attached cameras, record video and allow for easy investigations of security events. The DVMS often interfaces with other components of the security system such as Access Control, Video Analytics, Point of Sale terminals etc. and can act as the interface for all components in the security system.

The features which should be considered when deciding on a DVMS platform are:

- Scalability
- Cost & licensing structure
- Integration with 3rd party systems
- Video display capability and client applications
- Investigations and recorded video playback
- Rules engine (event handling) & recording engine

There are many classes of systems in this product category such as Digital Video Recorders, Hybrid DVRs, Network Video Recorders and Video Management Software.

Product Classes Advantages and Disadvantages

Digital Video Recorders

Digital Video Recorders (DVR) are designed to record video from analog CCTV cameras. The DVR is typically PC platform hardware with video capture cards installed and specialized software designed to display, compress and record video from NTSC/PAL analog cameras.

DVR systems have the advantage of being easy to setup and use. If the DVR is based on an embedded operating system, many of the complexities of Windows operating system or another background platform will not be exposed, making it easier for an operator who is not computer savvy to use the system. Additionally many DVR systems have controls on the front panel allowing an operator to quickly access functions to control the playback of video. DVRs have many disadvantages as compared to newer systems which have been developed since IP based security equipment has come to market. With regard to scalability, a DVR will not be able to expand in single camera increments. This can make it costly to work with installations requiring odd numbers of cameras. For instance, if your organization has a 32 camera system, there is no problem finding a 32 camera DVR, but if you want to add a 33rd camera additional DVRs would need to be purchased. This leads to another disadvantage which is many DVR systems will be standalone and may not integrate with other DVRs used in the security system. This is fine if the desire is to only view video from locally attached cameras but many campus environments have the need to view video across different buildings or sites. Also switching between DVRs to view video sources can be cumbersome and difficult to learn for someone new to the system. Additionally the traditional DVR may not be remotely accessible, unless it's a newer Hybrid DVR.

A DVR running on the same hardware as a Network Video Recorder (NVR) or Video Management Software (VMS) will not be able to process as many frames per second or be able to support as many cameras on a single system. The reason for this is DVRs are only compatible with Analog cameras so they cannot take advantage of edge device processing. With an NVR or VMS the connected IP cameras (or analog cameras connected via an Encoder) are transmitting video which has already been compressed at the camera. The DVR has to compress all the video streams coming to it which dramatically increases the processing power required per camera. NVRs and VMS systems can also take advantage of other edge device processing features, such as motion detection, video analytics, digital PTZ and Image Cropping. As cameras continue to develop edge processing capabilities this disparity in number of cameras and FPS per server will grow greater.

Hybrid DVR

A Hybrid DVR (HDVR) is a traditional DVR with one or more RJ45 ports and IP network communication capability. This allows the HDVR to support IP cameras in addition to Analog. The HDVR may also have the ability to integrate multiple systems, or it may have a client viewing application allowing the user to view video from cameras connected to different HDVRs. An additional benefit to both DVRs and Hybrid DVRs is having a single point of support for both the hardware and the recording software. Newer VMS systems do not have that advantage but there are downsides to this, such as being locked in to the DVR/HDRV vendor's hardware and service plans. Their hardware may be equivalent to brand name Commercial Off The Shelf (COTS) PC components but would be sold at a higher cost. This is due to costs inherent to stocking product and operating in lower volumes relative to general purpose PC hardware manufacturers. Typically the end customer of the DVR/HDVR must purchase their vendors hardware components to maintain the product warranty and to qualify for technical support. Other disadvantages are limited upgrade and storage capability, similar to DVRs. HDVRs may be able to work with Network Attached Storage (NAS) or Storage Area Networks (SAN) allowing for archiving of video to accommodate longer retention requirements but this may not be true of all products in this category. Also similar to DVRs, HDVRs would not be able to process as many FPS or cameras which are analog because any analog feeds need to be compressed.

Network Video Recorder (NVR)

The term NVR is sometimes used interchangeably with the term Video Management Software, but for these purposes an NVR is a PC computer preloaded with Video Management Software. An NVR is like an HDVR but only supports IP Cameras and Analog cameras connected to the IP network via an Encoder.

Some Video Management Software companies offer their software preloaded on a PC computer. The advantage is a user gets the benefits of a true digital/IP solution and a single point of support. Also NVRs are easier to specify than Video Management Software sold separately from the hardware. Hardware and preloaded software sold from the same vendor is guaranteed by the vendor to work together. There are also fewer vendors to work with so vendor management is easier and the user gets a single point of support on the video management system. The disadvantage to this is again, limited hardware choices. The vendor's hardware may not be preferred or accepted by an organizations IT department. The warranty may be void (and support unavailable) if COTS hardware components are used to expand or replace parts in the system. Also Analog cameras will need to be connected by encoders which may be more expensive then connecting to a system with PC capture cards when you account for the cost of the encoder and network ports the encoder needs to connect to.

Video Management Software (VMS)

A VMS platform is software which an organization installs on separately purchased computers to record video for IP cameras and encoders. Additionally the VMS may integrate with many other 3rd party systems and act as an interface for the entire security system. There are no physical limitations to interconnecting systems with IP based equipment therefore professional VMS packages are typically designed to scale to any number of cameras, across any number of servers and sites. Because VMS vendors focus on software, they're systems may be more feature rich and support more 3rd party equipment then DVR/HDVR Digital Video Management Systems.

The advantages and disadvantages of VMS systems are common to NVR systems. Because Video Management Software is sold separately from the hardware it is more difficult to specify and there is no single point of support. Of course a VMS can be installed on any brand PC hardware and use COTS replacement parts. The expandability of the hardware the VMS is installed on is only limited by the operating system running (barring limitations in available hardware).

Digital Video Management Systems; Features and Cost Considerations

Scalability

The first consideration should be scalability. If you are working with a four camera system which will never expand, then you have a lot of choices. As systems become larger and needs to accommodate future expansion one needs to consider the system's ability to grow and be managed through a centralized management application. Also the ability for a system to integrate with complimentary security products, such as Access Control, and complimentary authentication directories, such as Active Directory, needs to be considered.

Many VMS and NVR platforms are marketed as enterprise systems but in reality only the client applications which view video are designed to interconnect servers. A client application may be able to view cameras which are being recorded to different servers, but the platform may not include a management application which allows for updates and configuration to be managed across multiple servers simultaneously.

More advanced systems may have failover capability which allows for recording of cameras to continue on a failover server if the primary server goes down.

Cost & Licensing Structure

The cost of DVRs are typically based on a per box price determined mostly by the number of video channels the device supports, warranty and storage space provided. This is true for HDVRs as well although there may be optional IP camera licenses which are sold on a per camera basis in addition to the cost of the HDVR.

VMS and NVR licensing is more complex. Most vendors have similar licensing models which can be broken down into three parts; per-video-channel license, server fee and a maintenance fee or upgrade subscription. The cost per video channel is most common and it is simply a license charged for each video device (IP camera or individual channel on an encoder) used with the system. Although uncommon, some vendors tie the license to the hardware device used by MAC address. This is undesirable because if cameras or encoders need to be replaced it can be cumbersome to get the DVMS vendor to issue a new license for the replacement camera/encoder. Additionally, setup of the DVMS is complicated by having to compile a list of video device MAC addresses for the license keys.

In addition to the per-channel licensing a server fee may be charged for the software. The server fee may increase based on the number of cameras used with the system and it may be charged for each server the software is installed on. Some companies offer the server fee as a site license, charging once for each site the software is installed in regardless of the number of physical servers used. Others may charge it as an organizational license charged once for the entire organization regardless of the number of physical servers the software is installed on. Vendors may also have a hybrid approach to these models, such as a high server fee and a lower fee for each additional server the recording engine is installed on.

When the DVMS is purchased the user is buying only the currently released version of the DVMS software. Many companies offer upgrade subscriptions in 1 year increments for up to 3 years after the original purchase date. The upgrade subscription entitles the user to download and deploy new versions of the software at no additional cost. The upgrade subscription is paid up front, at the time of purchase. Many vendors will also allow users to ‘trade in’ their old software for a newer version, but this would cost more than the upgrade subscription.

When all the costs for a system are added together then broken down to the cost per camera, the cost of a software VMS can range from Free to over $1000 per video channel. Some camera manufactures offer free software to compliment their cameras but it typically only scales to around 16 cameras, only supports their product line and lacks features. Very sophisticated enterprise systems can cost over $1,000 per camera if purchased in small quantities. Several excellent enterprise-level, scalable systems can be purchased for $200-$500 per camera.

Although not part of the main licensing model many companies charge for add-on client applications which such as a Virtual Matrix, PDA client, Video Investigations tools etc.

Integration with 3rd Party Systems

In some cases the DVMS is chosen based on the integrations with complimentary systems which an organization may already have in use. For example, an organization may have an Access Control system in place and wants to add video. If the DVMS also supports the existing Access Control system then the user can have a common interface for both systems, or alarm based recording and searches are possible between the systems.

DVMS platforms can be found that integrate with Access Control, Video Content Analytics (VCA), Point of Sale terminals, SCADA systems, Building automation, HVAC and other systems. Using integrated systems, video recording can be triggered on event from the 3rd party system. Also, video information can be tied to meta-data from such systems. An example of this may be information on movement and behavior received from a Video Content Analytics engine. This meta-data tied to the video may allow for the user of the DVMS to search for all instances of someone walking the wrong way through an airport terminal exit, instead of searching through hours of video for such an event. In fact, if recording is triggered on the event instead of recording on a schedule the user of the integrated system may save significantly in storage costs.

The level of integration between systems varies widely. Integration can be as simple as receiving alarm events from a complimentary system, and the DVMS can trigger recording on those alarm events. More sophisticated integrations can allow for searches of video specific to the integrated system. For example, in the case of a PoS terminal being integrated, the DVMS playback interface may bring up a view of the transaction data (a receipt) alongside the video. The user can click on any line item in the receipt and view the associated snapshot of the item being scanned. A user may be able to do specialized searches, such as a search on all 'exceptions' at a certain register then view video of those transactions to quickly identify fraud and theft.

The integration at a deep level can allow for the DVMS to control configuration of the other system, so both viewing and management can be handled through one interface.

Video Display and Client Applications

The interface quality and usability can vary greatly between DVMS systems. The basic viewing application will allow for a tiled display of multiple video feeds. Typically, the viewing panes can be configured in different sizes to display some cameras in a larger resolution than others. Sometimes applications only allow for a few fixed tiled configurations. Enterprise-level applications usually allow for any configuration the user or administrator desires. More feature rich clients offer features like hot-spot windows, video pop-up on alert or a color indicating activity, instant replay, full screen mode switching or cycling between cameras and more.

A very popular type of client application is a mapping client. A mapping client allows the administrator to import an image file and overlay icons representing cameras on the map. This will show an operator exactly where a camera is in the facility making it much easier to learn the system and track activity across cameras. Mapping interfaces vary in features but many applications offer hyperlinked maps, allowing a user to start with a campus map, then click on building and bring up those cameras, then click on a floor and bring up a floor plan with associated cameras and so on. Most mapping clients allow the administrator to have an arrow near the camera icon representing the direction the cameras is pointing in. More sophisticated maps allow for cones to be drawn from the camera, representing the field of view; also the cones may change color indicating motion, events etc. Some maps include geospatial data (typically from Physical Security Information Management vendors, not DVMS) to locate security assets with precision on the map. This is also useful if security assets (such as guards) are moving, which can be tracked live on the map.

Alarm clients are sometimes offered. An alarm client will display a blank video screen until activity occurs on associated cameras. Only video triggered by motion or alarm will display which helps prevent the operator from being bombarded with potentially irrelevant video information. Some alarm clients include a history list of events, so an operator can click on an item in the list and quickly playback video of the event.

Virtual Matrix applications are intended to replace the analog video matrix. A PC running Virtual Matrix software can replace racks full of analog matrix switchers, and can provide huge cost savings in terms of equipment, power, rack space etc. Virtual matrix clients are typically very feature rich and may be designed to control a video wall with everything from a mouse to a touch screen interface. Some DVMS systems can use video clients to populate a video wall or multi monitor display with tiled camera views, maps etc.

Other clients are sometimes available such as PDA/Smart Phone clients and web interfaces. PDA or Smart Phone clients are not as frequently used because most organizations don’t have roaming guards outfitted with wireless PDAs or Smart Phones. It’s an area of interest for many organizations and an application users may want to explore.

Web Interface clients have the advantage of not requiring software to be installed (with the exception of an ActiveX or other browser plug-in) but sometimes lack features and operate slower as compared to installed client applications. This is due to limitations and overhead of running in a browser environment. Because the web client can offer access to video without installed software it can be useful for the occasional viewer of the DVMS or first responders. In the case of first responders, often police will have laptops and wireless/cellular internet access in their cars which can be used to access the security system of a school for instance, if an incident were to occur.

Many enterprise systems have the benefit of lots of features but suffer in usability. Oftentimes applications are designed with functions buried under menus and it takes many mouse clicks to perform a function. This can be hard for someone who is not computer savvy to learn. Ease of use and ease of training are a primary concern for organizations that have guards monitoring the video.

Investigations and Recorded Video Playback

The ability to investigate an incident and find relevant video clips is an important consideration for selecting a DVMS. Most platforms offer single camera playback, multi camera playback and 'smart search' functions. Single camera playback allows the user to chose a camera, time & date and pull up a list of recorded events which fit that criteria. The user may be able to filter events by recording type (show only motion recordings) and a snapshot picture from the clip may be displayed. Playback controls should include play, stop, fast forward, rewind & frame-by-frame advance and reverse. Some clients display a histogram representing motion in a scheduled recording for easy identification of activity in the camera view.

Multi camera playback allows the investigator to play recorded video from many cameras (usually up to four) simultaneously. This is especially useful if tracking a suspect through hallways, for instance. It is much easier to track an event in this view than to switch between individual cameras if the investigator does not know the path a suspect has taken. A graph of the camera's recordings over time is displayed in high-end clients. This is useful if cameras are recording on motion; the graph would allow one to see when motion occurred in one camera relative to the others.

Smart Search is a feature that allows an investigator to search for activity in an area of the camera's field-of-view. First the user selects a camera and a time period to search through. Next, one or more zones can be drawn in the camera field of view to search for motion in. Lastly some clients allow the user to select the level of activity to search for. The DVMS then searches for motion in the recorded video which meets the defined criteria. The speed of the Smart Search can be extremely slow. A large batch of video bring processed for motion is very processor-intensive and depending on the system the search is conducted on, it can take up to four minutes per hour of video being searched through. Some DVMS applications record meta-data along with the video which contains information about motion levels and what part of the scene the motion occurs in. These types of recording engines allow for extremely fast smart searches as compared to less sophisticated systems. In either case the Smart Search allows an investigator to easily locate relevant video if they know where an event occurred but not when. For instance, if a camera overlooks a room with a window which was broken overnight, the investigator can highlight the window in a Smart Search and quickly locate the relevant clips without manually watching eight or more hours of video.

Advanced features such as a Video Queue, or Bookmarking may also be available. Bookmarking in a DVMS works much like Bookmarking in a web browser. The investigator can mark a clip so it can be retrieved easily. Sometimes the Bookmark can contain a text description of the clip. A Video Queue allows an investigator to mark many clips in a list which can all be exported simultaneously once the investigation is finished.

Exported file formats are typically available in a standard format and a proprietary database format. The advantage of the common format (such as AVI or ASF) is the file can be played in a common media player, like QuickTime. The advantage of the proprietary database format is often them DVMS can export the video with a 'watermark'. The 'watermark' is actually the result of a mathematical equation run on the video to allow for verification that is has not been tampered with. The same equation is run when played back. If the results of the equations match the video is verified as original. Also exporting in a common format may require conversion to the format which can cause a loss in quality of the video. This is not always the case and some DVMS platforms can export to a common format while maintaining the original recorded data and including a method of verification. This is possible because some common file formats can act as container files and maintain the original recorded data.

Rules and Recording Engine

The 'engine' of the DVMS controls the recording of cameras on schedule and event. Most engines support scheduling recordings at various frame rates, resolutions and compression levels at various times of day on a per-camera basis. The event functionality varies by DVMS. Defining rules or events to record on can be as simple as recording when motion is detected, or events can tie recording and actions together. For instance an engine may trigger both a Pan Tilt & Zoom camera to go to a preset position, begin recording on a separate camera and several other actions based on a motion detection, alarm event or an event received from another sensor.

The recording engine itself should support many common compression formats, such as Motion JPEG, MPEG4 and H.264. The DVMS needs to support many compression formats to take full advantage of newer cameras supporting H.264. Some advanced DVMS engines can transcode between formats. This is especially useful when using megapixel cameras. MPEG4 and H.264 are often times not supported on megapixel cameras due the greater processing requirements to encode those compression formats. An advanced DVMS can take the MJPEG video and transcode it to H.264 for instance, which can save significant costs on the storage required for the security system. The downside is more processing power is required on the server, but a well optimized, multi-threaded engine can deal with this well.

DVMS systems handle the recording of video in different ways. Many systems will record video to a database, where clips or frames are stored in records of the database along with meta data, time information or audio. Some proprietary databases have limitations, which in entry level systems may limit the amount of frames you can record per day. Other systems record to the database for a long time before closing it and starting a new database file. In the event of a system failure (power outage etc.) the database may have to be 'rebuilt', or 'recovered' before your recordings are available. This process sometimes fails and long time periods of video may be lost. DVMS systems which manage files in smaller chunks are less prone to these types of problems.

Archiving of video is typically handled as a function of the DVMS, and most DVMS systems will not work with professional backup and archiving software. As compared to professional 3rd party backup software, the archiving function in most DVMS systems lacks many configuration options. Most allow all video to be archived to a single location one time per day. Sometimes the time of day the archive occurs is not configurable. More advanced systems can offer archiving up to once per hour, but typically the archiving feature does not match what's available in 3rd party software. Some DVMS systems do integrate with 3rd party backup software which can be a big advantage for IT managers working with the DVMS.

Conclusion

In conclusion many DVMS systems are very feature rich, and can act as the 'glue' of the security system bringing all the sensor devices together under a common interface. Systems with similar feature sets are sold at significantly different prices. It can be complex to specify the correct DVMS but it pays to research available options to ensure a cost effective and scalable security system.

About the Author: Brian Carle is the Product Manager for Salient Systems Corporation. Prior to Salient he worked as the ADP Program Manager for Axis Communications.

Brian.carle@salientsys.com