

Guidelines for selecting video surveillance systems for school security

MTS Consulting Services
2005
Revised Summer 2006

Technology Considerations

- Digital Video Surveillance (DVS)
 - Analog-based recorders are virtually obsolete, however, analog transmission cameras are not
- IT based (Network Video Recorder (NVR) vs Digital Video Recorder (DVR)); standards
 - Video Recorder should be software-based and be able to be hosted on Standard Information Technology computers. (See MTS DVS Evolution) This allows organizations to take advantage of current IT standards, processes, policies, learning, maintenance programs, etc. It also avoids being tied to proprietary hardware. Wherever possible, standards within database, video format, and networking should be adhered to.
- Adjustable, flexible
 - Video surveillance solutions need to be able to be calibrated and adjusted to accommodate differing conditions, to include:
 - Surveillance distance and width
 - Lighting
 - Day/Night (for outdoor)
 - Low light conditions
 - Backlighting
 - Storage requirements (variable/selectable per camera)
 - Recording and monitoring Resolution (variable/selectable per camera)
 - Ability to support different camera types within a single architecture including analog, IP, PTZ
- Fixed vs. PTZ considerations
 - School security personnel are typically under-manned and on the move. As such, cameras typically need not be 'operated' but need to be fixed on surveillance locations wherever feasible as PTZ cameras typically require operators. Also, even on 'patrol', PTZ cameras present coverage gaps, higher cost, and higher failure rates. However for some select applications, PTZ cameras may be more effective. When a school resource officer is included, PTZ cameras may be desirable for key surveillance areas.

However, we recommend supplementing PTZ with fixed cameras to ensure full time coverage.

- Alarm/Event Based
 - School security personnel are typically not in the mode of monitoring cameras. The video surveillance system should be configured to accommodate security policies and processes. As such, with the use of schedules, zones, and rules, alarm and alerts should be programmed into the system whenever possible to avoid ‘monitoring’ and increase ‘alerting’
- Internetworking
 - True internetworking, that is TCP/IP standard networking between servers and between clients and servers, is essential. Critical to this is true bandwidth management. The ability to match the video stream to the appropriate available bandwidth. For schools, this may also need to be adjusted during normal school hours when networks are primarily used for eLearning. This system should also have the ability to incorporate gateway technology such that multiple video streams (multiple clients looking at multiple cameras) can be ‘served’ via a single gateway, significantly reducing bandwidth requirements. This is especially important for remote viewing and monitoring.
- Export to Standard Format
 - To aid in prosecution and discipline, video recording software must be able to export video and still frame images to a industry standard format (such as AVI)
- Scheduler
 - Ability to create policies within the software to have the ability to operate under different rules during different times of the day, different days of the week. This is important in both bandwidth management, and alarming/alerting. This is also important when police are involved in monitoring (police may only monitor off hours vs. full time)
- Licensing Costs
 - Software should be licensed such that adding clients and/or cameras should not be extensive costs. Typically, client additions should be under \$50-75 per client and the same or less per additional camera
- Intelligent Features
 - More and more intelligent features are being developed. System should be able to accommodate these type of features when the become desirable and affordable, without a need to change any hardware or core architecture
- Camera and Lens selection
 - Flexibility in selecting cameras to include PTZ and fixed, indoor and outdoor, vandal-proof, low-light, etc. This is also important to be able to use different (and appropriate) lenses. Greater distances can be accommodated via larger telephoto lenses (such as 100mm) where wide areas may need wider viewing lenses (5mm) and aspherical lenses. This also includes Auto Iris lenses for outdoor, fixed and electronic shutter.

Bottom line is all lenses are not for all applications. Many video surveillance vendors use one camera and one general purpose lens.

- Support of NTSC and IP based cameras
 - Video recording software should be able to accommodate both NTSC and IP-based (MJPEG, MPEG) video formats
 - Regarding camera selection, price points, image quality, features, and lens format are all considerations. The ability to add intelligent features is also a consideration. Finally, for IP cameras, the true bandwidth available within a network must be factored in to fully understand network loading. MTS foresees IP cameras becoming more capable, and more cost effective in the near future, however, at the time of this writing, NTSC format cameras have a more favorable price point and performance. What is important is the infrastructure can accommodate both and the ability to transition from NTSC to IP be seamless.

- Scalability
 - System should support both horizontal (multiple servers) and vertical (growth within a server) scalability. Regarding horizontal scalability, this should not be 'stacked' DVRs but true peer-peer growth.
- Enterprise Architecture
 - School IT systems are evolving as is the need for surveillance. The surveillance technology architecture should be able to be defined at an enterprise level (school district) then have subordinate schools (servers) within that hierarchy. This permits the organization to define rules, security policies, and sharing policies within that enterprise architecture. This also permits the organization to build the architecture one school at a time or in incremental building blocks without:
 - The need to throw out existing purchases
 - Penalty in hardware, software, or licensing purchases
 - Complex re-definitions of architecture
- Fault Tolerance
 - The system should have the ability to recover from power outage automatically (application load on power reboot) and the ability to recover upon disk corruption (full backup on separate disk). Video, O/S, Backup, and Audio should not be stored on the same disk drive
- Archive
 - The ability for the system to easily provide archive capability in either compressed or uncompressed format, preferably selectable by the operator on a per-camera or per time segment basis
- Alarm/Alert-based
 - The ability for the system to be event-based. This includes detection of motion for both alerting (alarming) and for management of video recording. The system should not record video that is not event-driven. Also, the system should be able to have scripts (macros, scripting language) applied to the alarming rules to establish more comprehensive alerting criteria to better enforce security policies.
- Analysis tools
 - The system should include/support tools to aid in identification and analysis such as digital zoom and image enhancement

Integration Considerations

- Ability to grow without penalty
 - Integration should be designed such that the system can be built in multiple pieces or all at once. The cost between the two should not be very different at all.
- Support for future
 - Expansion. Ability to add schools, cameras, clients, or features without any changes to the core enterprise architecture
 - Technology changes/updates. Ability to add/modify components of the architecture. This includes, but not limited to:
 - O/S updates
 - Application version updates
 - Server updates
 - Networking updates/additions (e.g. The addition of wireless)
 - Storage updates
 - Intelligent features
 - Video format changes
 - New Features and capabilities
 - Ability to grow in capability as these become desirable and affordable
- Head-end standards and best practices
 - Video surveillance is analogous to a data system in that it is a large investment and represents mission critical infrastructure. It is also vulnerability to the same system management issues as IT. Wiring, termination, labeling, cable management, system documentation, change management rules, etc are all important criteria for integration design and selection.
 - MTS recommends the use of CAT5e or CAT6 cabling for surveillance systems such that consistent polices can be applied as with Data cabling, and the ability to transition (or hybrid) with IP cameras is already built in. With that, termination, punch-down, labeling, and conventions (e.g., EIA-568a standards) should be adhered to.
 - Wherever feasible, all DVS systems should be head-ended in a 19" rack with neat cable management, consistent, clear labeling, and capacity accommodations
- Lighting considerations
 - Lighting is one of the most critical issues in camera/lens selection and camera placement. It is important that the integration design takes into consideration all hours of surveillance (especially outdoors) and all possible lighting conditions. Selection of which direction cameras are aimed, angles, and other integration criteria are all important factors in overcoming lighting issues. Low-light cameras, manual/electronic

shutters, Auto-iris, Back Light Compensation (BLC), and filters are all effective tools that can and should be used to maximize the viewing capabilities of a camera

- Ability to use video for discipline and prosecution
 - Many video surveillance integrations are focused on area of coverage per camera in an effort to increase profit while meeting stated requirements. For schools, one of the primary functions required of the video surveillance system is to aid in the analysis of events and provide evidence that can be used to discipline or prosecute individuals who perpetrate those events. With that, there are several very important factors to achieve this:
 - The ability to recognize the individuals (surveillance that provide face identification)
 - The ability to rapidly search multiple cameras for common criteria
 - The ability to provide the video in an easy to read (e.g., CD) and open format (e.g. AVI), such that others who need to view the video do not have to have proprietary systems
 - Design such that the recording of the video can be adjusted to capture pre and post motion detection
- Documentation
 - Documentation should be provided prior to agreement/commencement of integration that details all the features/functions of the system, identifies the threats and vulnerabilities that the system is intended to counter, and identifies specific standards, camera placement/type, cabling considerations, etc. This should form the basis for the design document/agreement. After installation, 'as built' documents should be provided that cover:
 - Physical layer installation (cable, cable labeling scheme, rack-level diagrams, and physical plant layout (camera locations, numbering)
 - Logical layer installation (addressing, VPN associations (if applicable), host naming conventions
 - Software layer installation (configuration of servers, clients, etc)
 - Training Documentation
 - User and Administrator manuals

Integrator Considerations

- Understands Security Policy
 - The DVS system is to help enforce security policy. Integrator should possess and demonstrate an understanding of security policy development, administration, and execution
- Understands security model
 - The integrator should demonstrate an understanding of how the school administers their security policy, how security personnel are used within the model, and how they will use the security system. This includes demonstration of how administrative rights would be configured in the surveillance solution
- Threat and Vulnerability understanding
 - The integrator should demonstrate an understanding of the differences between a threat-based system and a vulnerability-based system and should know generic threats and vulnerabilities of school environments including the differences between the different grade levels and geographic variants
- Value of deterrence and re-assurance
 - The integrator should demonstrate an understanding of the value of deterrence as applicable in a school system and help coach the organization to maximize that value (through signage, camera placement, policy development, etc)
- Understands policing policy to help with law enforcement relationship
 - Video surveillance is a key component in policing at schools and it is important that the integrator demonstrate an understanding of how police use surveillance to help in prosecution of offenders, command and control response to incidents, and in the provision of evidence
- Mandatory recalibration process
 - The integrator should include re-visiting the installations periodically to recalibrate viewing angles, configuration settings, lighting accommodations, etc as the organization gets more versed in operations and uncovers conditions that were not obvious during system design/installation
- Total Responsibility end-to-end
 - Many DVS vendors are hands off, that is the developer of the product is independent of the distributor, who is independent of the designer, who is independent of the integrator. With those disconnects comes a lack of end-to-end responsibility. Integrator selection should take into consideration those linkages and selection should include integrators who demonstrate an end-to-end responsibility. 75% of DVS installations are performed by integrators who are completely independent of both the designer and distributor/developer. These integrators are typically not very familiar with the design criteria or the system capabilities and features