

Safe-School Community *Intelligent* Digital Video Surveillance Integrated Architecture

By

Rob Merchant

MTS Consulting Services

June, 2005

Purpose

Our increased awareness to threats, both locally and globally, has called for an increased response to counter those threats. Locally, the public education community is not immune from these threats and as an institution, presents unique challenges in its ability to provide for a safe and secure education for our children. The purpose of this paper is to provide oversight into some of the issues the education community is facing regarding safety and security and provide for a view on how technology can be used to help offset those issues and challenges. In particular, the application of *intelligent* and *integrated* digital video surveillance will be discussed as a means to contend with security threats and budget constraints.

Background

There is a need for increased safety and security within our public education community. Springfield, Oregon; Columbine, Colorado; Red Lake, Minnesota. These are the headline tragedies that have recently caught the nation's attention. These are isolated incidents. However, ten percent of the nation's schools reported one or more violent crimes in the 1996-1997 school year, including murder, suicide, rape, robbery and fights involving weapons. In 2002 alone there were 659,000 student victims of rape, robbery and aggravated assault. In 2003, seven percent of students said they were bullied at school and twenty-one percent reported street gangs in their school. In 1999, nine percent of teachers were threatened with injury by a student and 4 percent were physically attacked by a student.

According to the National Center for Education Statistics, 7.2 percent of girls in grades 9-12 reported engaging in a physical fight on school property. Boys reported 18 percent. According to the Centers for Disease Control, more than

MTS Consulting Services

Managing the intersection of IT and Security

one out of every twenty high school students skipped school at least one day because of safety concerns in 2003. That number is up from 4.4 percent in 1993. This does not even consider the issues of narcotics trafficking and the unlawful presence of pedophiles within school grounds

This paper is intended to show the value of the application of intelligent and integrated digital video surveillance technology to help reduce the probability of those type of events and aid in the apprehension and prosecution of offenders. Is video surveillance a viable means to counter security threats in the public schools?

According to *The New York Times*, nearly 1,000 new public schools opened in 2002 and 75 percent of them were equipped with surveillance cameras. This is not a question of whether or not video surveillance should in the schools, but a question of how and when.

The question of privacy and rights has caused some administrators to be leery of incorporating video surveillance within their schools. According to David Rubin, a Metuchen attorney who specializes in school law, students (and teachers) have privacy rights, but classroom activities are not considered private and are sometimes observed by administrators or parents.

"Cameras themselves are not violations of the law unless they invade the private space of an individual," Rubin explained. "There may be an educational concern about cameras, but not a legal one," he added, "unless the camera recordings are used for purposes other than school security, and accessed by unauthorized people."

In most privacy cases at the state or federal level, there is a general agreement by the courts that students in a school setting have less privacy rights than when they are outside of school.

MTS suggests applying some guidelines when architecting a video surveillance solution. Cameras should not be used in an area where there is a "reasonable expectation of privacy." Examples of these are bathrooms, gym locker/changing areas, and private offices (unless consent by the office owner is given). Examples of where cameras are generally acceptable are in hallways; parking lots; front offices where students, employees, and parents come and go; gymnasiums; cafeterias; supply rooms; and classrooms. The use of cameras in classrooms is often debated by teachers who want cameras for protection and teachers who do not. At this point in time, it is probably wise to use cameras in classrooms only when the teacher is given an option and notification that a camera is to be used.

Signage can be an important legal component in the use of video cameras in schools. Also, it is important that the presence of video cameras not lead a

person to believe he or she will be rescued if attacked. Dummy cameras should not be used (which is in contrast to the "black boxes" on buses, in which cameras may or may not be located at any time). While a fake camera can create a temporary deterrent to some security incidents, the potential liability it creates due to a victim's impression of being rescued quickly is not acceptable.

Audio recording is often considered to be of greater legal concern than video recording in most States. The recording of conversations is viewed as more of an invasion of privacy, as conversations often take place where the participants do not expect to be overheard. ¹

Reality within the education institution

There is not a school system in this country that is not facing budget limitations and scrutiny on how the budget is being spent. Increased security, albeit a common desire by faculty, parents, and students, typically represents a cost that traditionally hasn't been fully accounted for. This paper suggests there are ways to leverage other technology investments in schools to improve security through the careful design of the DVS architecture and the application of key technology.

Related to budget constraints are limitations within the administrative structure. Most schools do not have dedicated security personnel available to monitor schools via video surveillance technology full time. Even those schools that do have dedicated personnel, these typically are in large schools with thousands of children and multiple buildings. How can we expect these individuals to watch everything, even with adequate surveillance camera coverage?

Many of these incidents are virtually undetectable. Schools face two forms of security threats – internal and external. Internal threats stem from within the school grounds, and from either students or faculty. Depending on the school grade, this can range from schoolyard fights to more violent acts for the older grades. External threats occur when individual(s) who are not permitted or authorized on school property transcend the perimeter and threaten our children and teachers. Typically, this can be threats from narcotics trafficking, pedophile assault, or violence from outside individuals. Finally, infrastructure security is a growing concern and growing cost and ranges from vandalism to theft and destruction.

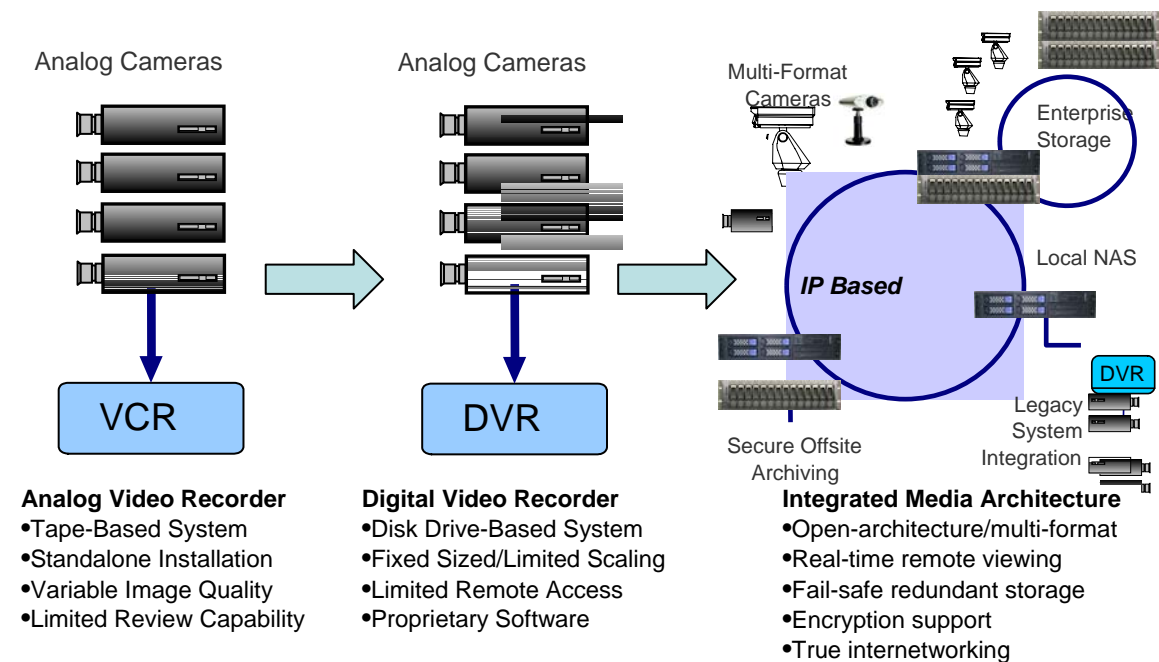
¹ U.S Department of Justice, Office of Justice Programs, National Institute of Justice

Why Video?

The timely exchange of *current, relevant, and accurate* information is an essential component to safety and security. Historically, the more detailed and timely the information is the more informed law enforcement and others responsible for the protection of people and infrastructure become. This enables a more effective prevention or response to a safety or security incident. Whether it's providing the police information to apprehend schoolyard drug deals or helping administrators discipline violent students, information is the key. As important as information is to the protection of people and infrastructure, too much information, irrelevant, or untimely information can actually inhibit those in the safety and security business from an effective response. False alarms and over-reaction can be a significant hindrance. History also tells us that if the systems that are put in place to provide the information are too complex to operate or require too much time to obtain meaningful results, than those systems will be ignored and unused.

Evolution of Video Surveillance

The figure below illustrates the ongoing evolution of video surveillance.



Digital Video Surveillance (DVS) Technology is the current standard for video surveillance. It has replaced its predecessor, Closed Circuit Television (CCTV), which uses analog video recording, as the choice for the application of video surveillance for safety and security. The technology basically encodes analog

video captured from a camera into digital data, and then manipulates the data (analyzes, disseminates, stores) in the same manner any computer system would. In some instances, digital transmission cameras can be used to eliminate the encoding step as the encoding process is built into the camera. The hardware technology used to manage and manipulate the data is essentially a computer. This paper is not intended to be a dissertation on DVS technology, but provides some basic background to help with the discussion. Some of the advantages of DVS technology over analog video recording technology include:

- **Information Storage.** Information can be stored on a variety of digital data media including Optical (CD or DVD), computer Storage Area Networks (SANs), computer disks, or tape. Analog video traditionally is stored on tape.
- **Search and Retrieval Capability.** DVS stores the data into a database, similar to any computer program with large amounts of data. Search engines can be used to tap the metadata indexing scheme to almost instantly find exact video segments based on a variety of search criteria (time, event, camera location, etc). Analog search requires a mechanical time search of tapes.
- **Dissemination.** DVS video segments can be transferred over data networks or accessed from servers. Analog video cannot and must be mechanically transferred (copy of tape) or streamed over an analog network.
- **Application of pixel-based analysis tools.** DVS can use a variety of analytics to aid in the search process or to help trigger alarms/alerts. Analog typically can only use motion to trigger an alarm.
- **Infrastructure cost.** Most safety and security organizations have existing Information Technology infrastructure in place (such as office automation or computer aided dispatch). The addition of DVS can be accomplished via *software* with minimal hardware upgrade. Analog video systems are standalone.

The list goes on with advantages for DVS over analog. The importance to this paper is this is where the technology is at and where research and investment dollars are being applied. The cost of DVS technology is dropping and will continue to drop while capability increases.

DVS Technology – A Mission Critical Application

The evolution to DVS technology has taken a number of steps. Initially, analog recording devices or Video Cassette Recorders (VCR) were replaced with digital recording devices or Digital Video Recorders (DVR), while the remainder of the infrastructure remained as is. These DVRs were essentially commercial off the shelf (COTS) computers, modified to perform specific digital video applications

MTS Consulting Services

Managing the intersection of IT and Security

with proprietary encoder inputs and proprietary database schemes. You were buying a black box with its own maintenance, warranty, and specific training requirements. However, the industry trend is to move towards software-based DVS applications that run on standard IT computers or servers. This way safety and security professionals can migrate to DVS without the costly investment of DVRs and can take advantage of current IT infrastructure. With this approach, DVS technology can be managed in the same way as any other mission critical application – similar to Computer Aided Dispatch (CAD) systems for police or Student Information Systems (SIS) for schools.

Infrastructure – leveraging Information Technology Investments

Typically, the most costly components of any DVS installation is cabling and storage. Both are controllable with the application of some basic architectural principles. There basically two types of cameras on the market today – analog transmission cameras and IP based cameras. Analog cameras transmit a composite video signal similar to what your home TV uses, typically NTSC standard while IP cameras transmit TCP/IP data, much like a computer. Traditionally, NTSC video format was transmitted over coaxial cable while IP cameras transmit over conventional Ethernet means, which includes coaxial cable, unshielded twisted pair (UTP) – much like phone wires, or more recently wireless.

The evolution of video continues in cabling in that basically, either IP-based or analog-based cameras can use most any of the cabling available to them, with the addition of baluns to allow for the transmission of composite video signal over UTP. What does this mean for the schools? Typically, many schools have made investments in computer technology including wiring the schools for Ethernet. Very few network installers will install the minimum required number of pairs of UTP cable – typically the cable comes in bundles of many pairs and the excess is used for growth. MTS recommends evaluating your school's Ethernet cable infrastructure to determine if it is reusable, to some extent, to carry either IP-based video over the Ethernet or to simply utilize the UTP cabling infrastructure. More than likely some cabling will need to be performed but in almost all instances, cable infrastructure (or Ethernet) can be leveraged.

MTS recommends using standard Information Technology computer systems for digital video surveillance. For storage, this equates to cost effective hard drives, CD/DVD Read/Write drives and for some schools, network attached storage (NAS) drives, as applicable. The key to keeping the storage costs down is to store what you need. The analog VCR world taught us to record everything and put it on tape, then replace the tape with a new one. DVS technology allows us to record only *meaningful* events and at varied video frame rates, thus optimizing the storage efficiency. For schools, typically 7 days of storage is sufficient, which can typically fit on standard hard drives of computers.

MTS Consulting Services

Managing the intersection of IT and Security

The *hidden* costs of DVS are the same as standard Information Technology – operations, maintenance, upgrades – all the components of running a computer system. By taking the approach of treating DVS as an application on a computer system, schools can leverage their understanding of computer technology, as well as maintenance contracts, training, and spare parts.

Intelligent and Informed Response – Application of Intelligence for school video surveillance

This paper describes the capabilities resulting from the *application* of a number of technologies to create an integrated safe-school community DVS architecture. For pre-incident, deterrence is the most relevant factor. The obvious placement of cameras and signage identifying police monitoring can help deter crime and security-related events.

As mentioned above, one of the main advantages of DVS over analog is the inherent ability to apply pixel-based analysis techniques to the video stream, either post-event for analysis or real-time for alarmed-based monitoring. There are a number of emerging companies that are dedicated to developing algorithms and techniques to analyze digital media. Already available, tested, and deployed include such algorithms as:

- Rioting and assault detection
- Object-left-behind (bomb prevention)
- Perimeter Intrusion
- Face Capture (for identification)
- Iris Scan (for identification, verification, and validation)
- Facial Recognition (for identification, verification, and validation)
- Fare evasion (for transportation community)
- Suspicious vehicle movement
- Crowd gathering
- Traffic analysis (speeding, license plate recognition, red light/stop sign offense)
- Others

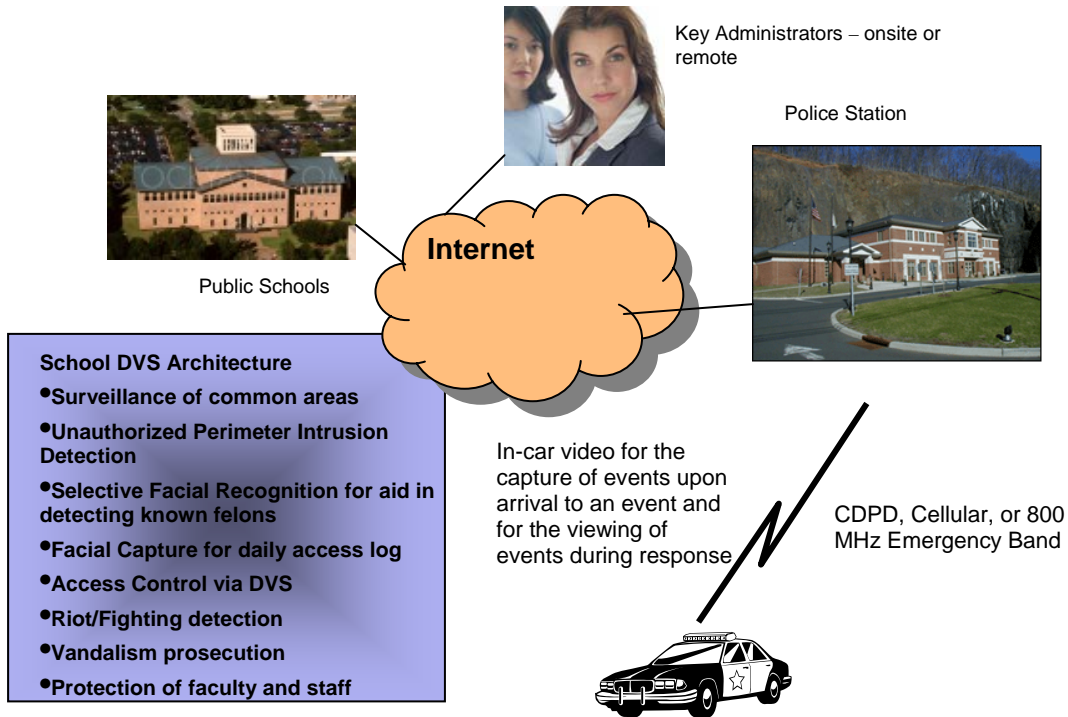
As such, the application of analytics to help *trigger* alarms and *focus* the attention of individuals responsible for the monitoring of the area is crucial during the event phase (or identification of an event). First, it allows for more accurate detection of potential safety and security incidents while second, it allows an individual to be more versatile in being able to monitor a larger area (more cameras) more effectively, acting as a force-multiplier. Different companies apply different techniques to video algorithms and are at different stages of maturity in their development. With that, it is imperative to maintain an awareness of who is developing what and understand this rapidly evolving technology.

MTS Consulting Services

Managing the intersection of IT and Security

Paramount to the safe community concept is the integration of the public school systems into the architecture. Our children are our future and their safety cannot be compromised. There are many threats that face our children at school, depending on the schools location, the grades served, and other external factors. Drug trafficking, schoolyard violence and pedophile assaults are some of the more prominent issues we must face. We believe there are technology-based solutions that may help reduce the probability of such events and are more than justified in their implementation. Schoolyard violence can be detected using crowd gathering and assault detection algorithms to help focus security personnel to the event. Facial capture and facial recognition can be used to help identify known pedophiles and drug dealers when they come within unsafe distances of the school. 24 hour monitoring helps thwart vandalism and theft while using DVS technology to aid in access control and audit for school visitors makes false identification more difficult.

MTS believes that creating a 'good guy' list – the identification of those individuals who are supposed to be on school property, is an excellent way of focusing attention on those who are not. By creating a database of faculty and students, facial recognition can help point out those who warrant validation and verification of identity. Using License Plate Recognition by first ruling out faculty, student, and parent vehicles aids administrators and security officials in investigating potential unauthorized access. Linking the schools video environment into the police station also has several distinct advantages. One, it *may* help augment school security staff with additional trained personnel. This is especially helpful during non-school hours to help prevent vandalism and theft. Two, it allows the police to better interpret the severity of the incident to institute the proper level of response. Three, it enables a more *informed* and *intelligent* response by directing the police to the appropriate area within the school, providing them with a first hand look at the potential perpetrator(s) and victim(s) (to aid in apprehension), and can arm the responding police with timely, first hand *visual* information of the event during the response. Upon arrival on school property, the in-car viewing station can switch over from a highly mobile, low bandwidth data link (CDPD or Cellular) to a more robust wireless network (802.11) to gain better access to digital media information.



The diagram above depicts the architecture of integrating the police, the police vehicles, the education community, and key administrators together for the sharing of digital media. Other first responders, such as the fire department, can benefit from video access as well. Key to the success of such an architecture is recognizing the limitations of the network connections. Shared internet access is very different than dedicated circuits and the various forms of wireless communications are extremely limited in the transmission of digital media. With these limitations, the dissemination of only critical information is the key. Passing of face capture still images (vs. video) during response provides the responding officer with a current photo of the suspect which is more than sufficient for apprehension. Transmitting the results of a license plate recognition (LPR) query requires much less bandwidth than transmitting the license plate image itself.

An integrated DVS safe-school community also provides for significant capability during the post-event phase. For police, the value of video as evidence has already proved itself. High quality video capturing the incident can leave defense lawyers speechless. With technology such as watermarking, already-approved anti-tampering technology can be applied without effort. There is no ‘physical’ evidence security needed, the data is secured within the system and rendered untouched. Equally important is the ability to search and find significant case data to help strengthen the prosecution of criminals and the dissemination of that information to the appropriate judicial community. In the event the suspect evades capture, the dissemination of digital media is a powerful way to help

MTS Consulting Services

Managing the intersection of IT and Security

prevent additional crimes and to help aid in the capture of the individual. Criminals follow patterns and have been known to target similar institutions and situations. Disseminating the information in a timely way (pedophile pictures within neighboring schools or gang member pictures within the greater community) can help in the apprehension of the individual and the protection of the people and community infrastructure.

Conclusion

There are two things needed to make an integrated DVS safe-school community happen: technology infrastructure upgrades and agreement among community stakeholders. The technology infrastructure upgrade may at first appear like a costly investment. However, by leveraging some of the guidelines presented in this paper, significant infrastructure re-use can greatly reduce the cost needed to implement such a concept. Implementation in phases can be linked to school budget cycles. There are also savings that can be realized in personnel reduction and potentially insurance costs.

Paramount to establishing a safe-school community architecture is the application of standards (where they exist) and to institutionalize an open architecture. Inevitably, different community stakeholders will deploy different manufacturer's video surveillance technology. There will be a mix of analog and digital with different network capabilities. What is important is to strive for an open architecture embracing standard Information Technology (IT). Using encryption over the internet allows for the sharing of digital media between stakeholders. Implementing DVS technology via software, not hardware allows for cost effective upgrades to analog systems and avoids the tendency to get trapped in a proprietary system that presents interoperability issues. Within the police architecture, the systems deployed in the police vehicles should to be compatible to (or the same) as the system that is in place at the police station to better facilitate the management of the digital media. Linking the system to traffic intersection cameras is also a consideration when deploying license plate recognition algorithms to aid in the apprehension of suspects. In parallel to the evolution of the internet, where there originally was a series of disparate networks, independent of each other that ultimately became one ubiquitous network, sharing information on a global basis, digital video can follow a similar course. There currently are a variety of video surveillance systems within a community. In police cars, in public buildings, in banks, on roadways, in retail stores, schools, gas stations. Linking together the systems that make sense, providing the policing community with access to viewing incidents will allow for a more capable surveillance system that can better serve the community.

Obtaining agreement among community stakeholders is a matter of helping to visualize the benefits of what this type of architecture can do for the education community. What's in it for me? How it can prevent security-related events and

MTS Consulting Services

Managing the intersection of IT and Security

crime, better enable the policing community to perform their duties, and provide for a safer and more secure education environment?

Finally, having multiple communities linked in a hierarchy to county, state, regional, and federal levels provides for a powerful way to share information. Should there be a regional incident, protection and response can be coordinated in unprecedented ways. If felons approach one school within a community, what is to stop them from moving on to the next school, within the same community or a neighboring community?

MTS Consulting Services is focused on the convergence of security and Information Technology for the education and local government communities.

For more information on this topic, related topics, or services, please contact Rob Merchant at **rob.merchant@mts-consultants.com**