

Safe Community Digital Video Surveillance Integrated Architecture

By

Rob Merchant

MTS Consulting Services

May 2005

Background

Our increased awareness to threats, both locally and globally, has called for an increased response to counter those threats. 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 Command and Control information to battlefield commanders or helping prosecute shoplifting in a retail store, 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. Experience 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, then those systems will be ignored and unused.

Many communities have grown and as such, have a growing infrastructure to protect. Transportation, tourism, hospitals, airports, universities, and recreational facilities represent revenue into the community and benefits for the citizens of the communities, but also represent growing challenges for safety and security. This paper talks to the benefits of integrating the various elements of the community together for safety and security, providing value to those participants as well as distributing the burden of cost. This paper is organized to provide a brief background on Digital Video Surveillance (DVS) technology, and then introduce the concept of an integrated safe community.

[For the context of this paper, we will break-down safety and security incidents into three time phases: Pre-event, event, and post-event. During pre-event, emphasis on deterrence and prevention is placed. During the event itself, there is emphasis on stopping or minimizing the event to regain control. Post-event activities may include prosecution, assessment, information or knowledge exchange, and the application of lessons learned to help thwart future events. Information collection, dissemination, and analysis are critical during all three phases of safety and security events.]

Digital Video Surveillance Technology

Digital Video Surveillance (DVS) technology is the current standard for video surveillance. It has replaced its predecessor, Closed Circuit Television (CCTV), which used analog video recording as the mechanism for the application of video surveillance for safety and security. This new

technology basically encodes analog video captured from a camera into digital data, and then manipulates the data (analyzes, disseminates, stores) in the same manner as 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 assist 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 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 into an index 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 organizations have existing Information Technology (IT) 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.

Video Surveillance technology can be applied in many different ways. It can be applied to promote tourism (webcams), provide assistance (traffic or weather updates), can aid in management functions (remote monitoring of employees and actions), and policing and protection. With regards to policing, we believe there are five basic functions for video surveillance. They are:

1. **Discrete Surveillance** of known and unknown criminals
2. **Command and Control** to act as a force multiplier for police and first responders
3. **Provision of Evidence** by increasing guilty pleas and reducing the time and expense of the prosecution processes
4. **Deterrence** when used as part of an overall policing or protection strategy
5. **Re-assurance** to help increase the public confidence through crime reduction and other factors

Intelligent and Informed Response – Policing in a Safe Community

This paper describes the capabilities resulting from the *application* of a number of technologies to create an integrated, community DVS architecture. For the pre-event scenario, deterrence and assurance are the most relevant factors. The obvious placement of cameras and signage identifying police monitoring can help deter crime and security-related events. This can also help boost the community's comfort in the security of the area or be used to promote tourism and actually function as a revenue recovery technology. However, the bigger benefit of an integrated DVS architecture comes in the event and post-event stages.

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 detection (bomb prevention)
- Perimeter intrusion detection
- Face capture (for identification)
- Iris scan (for identification, verification, and validation)
- Facial recognition (for identification, verification, and validation)
- Fare evasion detection (for transportation community)
- Suspicious vehicle movement detection
- Crowd gathering detection
- Traffic analysis (speeding, license plate recognition, red light/stop sign offense)
- Others

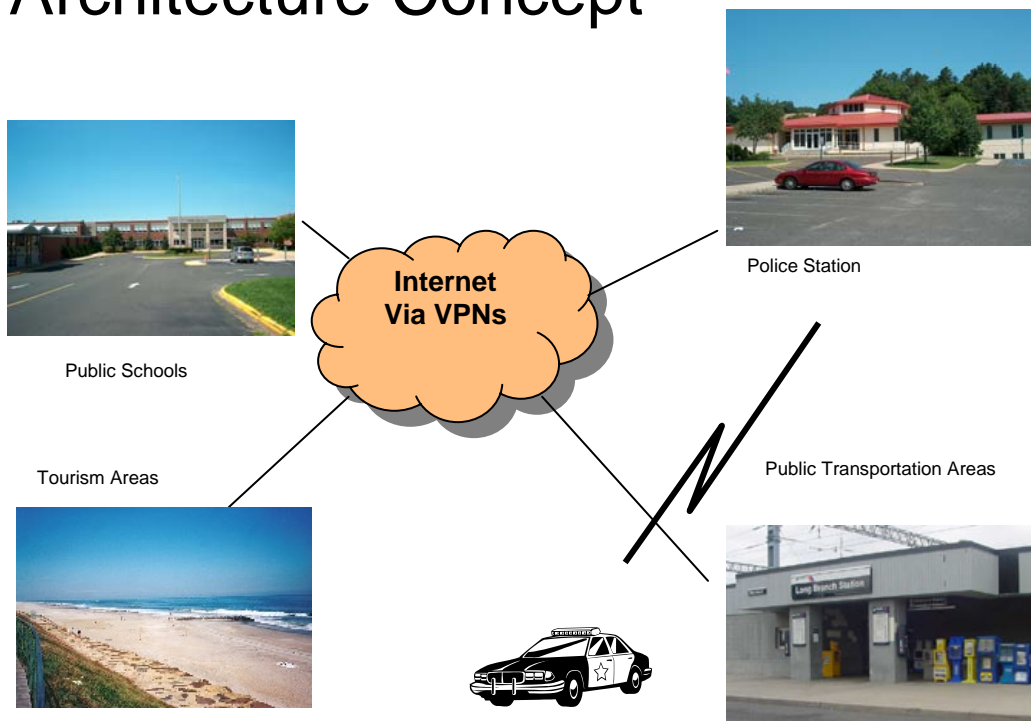
As such, the application of analytics to help *trigger* alarms and *focus* the attention of individuals responsible for the monitoring of the area is crucial during the event phase (or identification of the event itself). First, it allows for more accurate detection of potential safety and security events 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.

Paramount to the safe community concept is the architectural integration of key infrastructure such as the public school systems, assisted housing, recreational facilities, transportation facilities, and tourism centers. For these applications, our children, citizens and tourists are our primary focus and their safety cannot be compromised. For example, there are many threats that face our children at school, depending on the school's location, the grades served, and other external factors. Drug trafficking, schoolyard violence, bullying, and pedophile assaults are some of the more prominent issues we must face. These same threats are pervasive in high tourism

areas such as boardwalks. As such, 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 school administrators 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. Using License Plate Recognition (LPR) technology can identify those same individuals as they cruise near the school's perimeter. Linking the sub-community (school) video environment into the police station also has several distinct advantages. One, it *may* help augment security staff dedicated to that facility with additional trained personnel. 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 facility, 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.

For communities with tourism or recreational areas, integrated DVS enables the law enforcement community to more adequately patrol and respond to key tourism areas, such as parks, beachfronts and boardwalks. The ability to monitor such areas for fighting and violence and to be able to help prosecute offenders is of high value to undersized police forces. Implementing surveillance in a high tourism area may have other benefits such as the use of the video infrastructure for the promotion of tourism. This can actually serve as a revenue generation mechanism. Additionally, it can reduce liability.

Architecture Concept



The diagram above depicts the architecture of integrating the police, the police vehicles, the education community, and the retail community together for the sharing of digital media. 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.

An integrated DVS community also provides for significant capability during the post-event phase. For police, the value of video as evidence has already proven itself. High quality video capturing the incident increases guilty pleas and reduces the number of cases that go to trial. With technology such as watermarking, already-approved anti-tampering technology can be applied to simplify the evidence management process. 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 ease of 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 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 shoplifter pictures within retail 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 community happen - the technology infrastructure upgrade and agreement among community stakeholders. The technology infrastructure upgrade may at first appear like a costly investment. However, as an integrated community, the benefits are shared among the various stakeholders as is the cost, making this a much more achievable architecture in times of tight budgets. Additionally, 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. There are also savings that can be realized in the reduction of overtime pay as well as liability insurance costs.

Paramount to establishing a safe 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

MTS Consulting Services

Managing the intersection of IT and Security

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 exists 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 community. What's in it for me? How it can prevent security-related events and crime, better enable the policing community to perform their duties, and provide for a safer and more secure 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. Already, supermarkets use video of criminals to share between stores in a region for the prevention of crime, why can't other community stakeholders do the same?

For more information on this topic or related topics, please contact Rob Merchant at rob.merchant@mts-consultants.com. Updated on April, 2006