CCTV Special

>> Making **Technology** Work Around **You**

By Anthony C Caputo



We live in the world of digital interfaces; software operating systems and applications that empower us to the magic of technology. Digital interfaces, from our laptop, to the iPhone, to a Cable TV DVR, all have the ability to change our lives profoundly by making communication and thus our relationship with technology much more personal, intuitive and efficient. The digital software interface becomes an intimate lifeline and without the respective concept of personalisation, that intuitive magical relationship with the human interface can become crippling, frustrating, and an obstacle to our daily lives.

The convergence of digital technologies has created a social and economic evolution, making it possible to transform fixed hardware driven solutions into a software driven integration, providing more effective intelligence to end users and creating better efficiencies. In a physical security environment, where there are multiple required security subsystems, that means improved intelligence, delivered where you need it, when you need it, automating processes to make better decisions.

Make the technology work around operations, not operations work around the technology.

The theory behind video surveillance was founded on the same four key factors that are still prevalent today:

- Deterrence
- Efficiency
- Capable Guardian
- Detection

However, video data is one piece of the overall physical security puzzle that reinforces the effectiveness of the same four key factors. These other components are just as important in protecting and saving lives and property and can provide additional information to improve the efficiency and effectiveness of security operations. Those additional pieces include:

- Access Control
- Intrusion Detection
- Perimeter Detection
- Communications
- Keys Management
- Incident Reporting
- Panic Alarms
- Tamper Alarms
- Elevator Intercoms
- Power Management
- License Plate Recognition

These additional physical security subsystems are typically isolated systems, deployed or upgraded at various times, with separate hardware and software to manage and monitor incidents, access, alerts and alarms without consideration for the impact on operator procedural details. By providing a consultative analysis of the overall present and future requirements, not just the technology, its hardware, software and functionality and features, but understanding how this new requirement impacts the operator (the real world users). Better efficiencies may be possible through an integration of those multiple subsystems. Many times, security does not know what is possible with today's technology and the video management system (VMS) software.

The Single Interface

The graphical user interface (GUI) is the link between the operator and the system behind it. Providing a simple, single interface, with effective training can empower the user to become more efficient and effective at their jobs, whatever the role. In a physical security environment, the effectiveness of that interface is even more critical, whether that be in a command centre, a mobile vehicle or a smart phone; becoming familiar with the simple interface makes the user's capability to manage the system initiative, thus understanding the information is simple and easy. The best interfaces are always designed to be the most intelligent and intuitive.

There are many VMS software applications available. The key to choosing the right application rests entirely on the present and potential future system requirements, so the more detail included in the project requirements, the easier it is to make a decision. Keep in mind that this is the interface between your operators and security personnel and the physical security system behind it. The many choices in the market (far too many to even consider exploring here) create serious challenges, as organisations sift through all the available VMS options. In a business environment, making a wrong software decision can increase organisational risk, cause inefficiencies, hardware limitations, and eventually require costly upgrades, because no one wants to use it if it makes their job harder, not easier.

VMS systems are constantly evolving to keep up with market trends and demands. Originally developed as an interface to simply monitor video surveillance camera streams, the convergence of telecommunications, media, and security provides a new proficiency with additions such as camera tampering, auto-tracking, video analytics, people-counting, auto-tracking, and alarm management and integration for more intelligence. Avoiding pitfalls must be accomplished through informed decision-making, which includes understanding not only the full functionality and capabilities of the VMS software, but also the software company's market segmentation, distribution, development plans, and integration processes. The VMS should be a separate decision from the hardware to provide continuity to security operations.

The addition of a new VMS software or solution into the business isn't like a typical software install. Traditionally, an IT department may install a new application for the employees to use and confirm their attendance for training. The employees attend the training, pick up enough to navigate around the application, and then truly learn by using it day in and day out. Successful VMS implementations, however, are based upon how well the integrator understands the software, the industry and the internal business processes and subsystems.



Process Improvement - Case Study

Navy Pier is the largest entertainment and retail multiplex in downtown Chicago, Illinois (USA) that reaches outwards into Lake Michigan for three-quarters of a mile and is completely surrounded by water on three sides. Originally, their physical security subsystems included four separate undocumented monitoring analogue systems, and two separate alarm systems, with over 300 alarm functions. The Panic Alarms, located in the garage facilities provided patrons with an emergency call button and siren. Originally, when someone pressed the panic button, a single nearby camera would appear on the alarm monitor. The operator would answer the phone and determine the level of urgency and make the decision to dispatch security. In order to deactivate the alarm and siren, they would dial in a code number onto the phone. If that didn't work (and it rarely did) a hardwired switch was added to cut power. The operator would then move to another physical computer within the Command Center to file an incident report on another separate system.

Genetec Omnicast was the chosen VMS software for the new system, which satisfied two primary requirements, 1) integration into the city's 911 Center, and 2) gave them the flexibility to integrate any existing assets including older Panasonic, Pelco, and Bosch cameras and accept the new Axis cameras. Genetec is a software company that is hardware agnostic. If a camera is not listed in their huge compatibility list, they will write the code for it. Omnicast also provided Alarm Management capabilities (as do Milestone and OnSSI), so by using the existing I/O ports of the Axis encoders used to integrate the analogue garage cameras, the Panic Alarms were moved from the legacy system into the Genetec interface. Now, upon activation, up to three of the closest PTZ cameras move to a preset position to view the area from various angles, and those video streams populate special armed tiles within the software interface. The video can be a live feed and/or a pre-recorded playback to review the location, seconds before the specific alarm activation, and the Command Center is instantly alerted with audio, colour-coded room lighting, email and/or messaging signals. The alerts, audio, video and archived footage provides enough information to make a better decision. The operator may not see anyone on the live footage, and concerned for the safety of their patrons, immediately dispatch security personnel. However, the arm tile that depicts the archived video footage may show a group pressing the button and running away. The alarm is acknowledged within the same interface with an incident reporting field where the incident is then recorded within the database for future review.

The Stain Glass Museum includes silent parameter and pressure sensitive tamper alarms for the protection of the museum exhibits and informs the personnel in the Command Center in the same manner as the Panic Alarms. Prior to this implementation, the Stain Glass Museum tamper alarms presented a preset PTZ camera to the stain glass cabinet, with no additional information or intelligence. Typically, once the alarm was triggered and the PTZ camera moved to that location, the potential threat may be gone. Security personnel were required (for insurance coverage) to physically investigate. The new integrated system provided the operators with the following scenario:

1. Someone touches a stain glass display
2. Shattered glass audio alarm sounds in Command Center
3. Lights in Command Center change unique identifiable colour
4. Video Management System Software presents live view (depending on location, up to three cameras) in armed tiles and archived from five seconds prior in another armed tile
5. Intelligent information presented: patron leaned on display when taking a picture. No security dispatch required

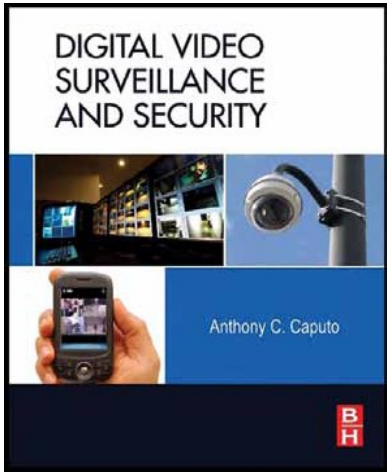
Summary

The right VMS software, that meets business requirements, can and has been proven to improve business processes, producing measurable results. If the VMS software can make technology work for you, why work around the technology?

When choosing the right VMS solution, it's important to consider the following lessons learned:

- Due-diligence: make sure the VMS system chosen can accomplish all the video requirements (e.g. compression technologies, integration, etc)
- Are your existing reusable assets listed within the compatibility list?
- Research any compatibility issues with existing devices that will require integration
- Make sure there is enough storage capacity and bandwidth for all devices for the required timeframe
- Establish a secure, well-protected connection between all clients and the VMS server
- Limit the amount of users with access to the system from outside the working environment and scale the system for the amount of users
- Is your network either configured or disabled for multicast traffic? ■







About the Author
Anthony C Caputo is currently a Technical Architect for IBM's Solution Design Centre of Excellence (SDCoE) specialising in Digital Video Surveillance for Homeland Security and the author of Digital Video Surveillance and Security (Butterworth-Heinemann, 2010, ISBN-13: 978-1856177474). His blog is at **www.dvsbook.com**