Jimmy Palatsoukas discusses how unifying access control systems can strengthen surveillance initiatives across entire cities

CITY-WIDE SECURITY

©Getty Images

The days when public organisations relied solely on video surveillance to protect their facilities and citizens are almost entirely behind us. Today, both large and small cities are looking for more sophisticated platforms which centralise data from many sources and display information in real-time. Keeping terrorism, street crime and other threats at bay from their public buildings, water facilities, schools, hospitals and local businesses means that more cities are requiring the integration of other pertinent security and building systems with their video surveillance. They are seeking unification of multiple systems to improve response to emergencies by simply having more consolidated information available at the click of a mouse.

These unified solutions have been proven to help deter crime, to improve information sharing between multiple agencies like law enforcement, fire stations, and emergency response crews, to enhance response time to incidents and to keep citizens safe. More than that, unification of security information across public facilities has also been credited with reducing operational expenses whereby a city can standardise on a single solution and collaborate with other agencies to bring their individual systems into a central operating centre. This approach allows for the multiple agencies involved to share in procurement and maintenance costs while benefiting from a unified system that facilitates greater efficiency in response to events and the ability to check many more video feeds and data before dispatching manpower to a potential incident.

Chicago, Toronto, London and New York are a few examples of large cosmopolitan cities that are unifying their city-wide systems such as video surveillance, computer-assisted dispatch (CAD), gunshot detection, perimeter detection, portable overt digital surveillance (PODS), and in some cases license plate recognition systems, into a single massive crime-fighting solution. These are enormous undertakings that take many years to implement and involve many different stakeholders, but they are proving successful in these large cities. And it is not just big cities that are looking to unify their physical security environments. Smaller cities are also starting to look to big city-thinking and explore how to adapt these principles on a smaller scale to their public buildings by starting with a fundamental level of unification: IP-based video surveillance and access control.

The majority of video surveillance manufacturers offer a software development kit (SDK) that can be used to integrate live and playback video within any application. For example, some access control manufacturers use the SDK from some DVR vendors to attach an access control alarm to the associated video for quick playback. But integrating and unifying are two very different ways to go about merging video and access control systems. Integration can sometimes present limitations, such as: the access control system cannot easily be linked to cameras; intricate and time-consuming rules have to be configured to ensure door events are tagged with video; difficulties searching through all recorded video recordings from within the access control user interface; and pan-tilt and zoom (PTZ) functionalities are limited in access control as compared to the video system.

In contrast, a unified platform goes above and beyond by providing the ability within a public facility to tag or bookmark video when an access control event occurs or to unlock an access controlled door from the video surveillance user interface. It provides both a unified interface and a unified back-end server infrastructure that seamlessly links video and access control and provides built-in core functionalities like monitoring, reporting, alarm management, configuration,

Unified surveillance solutions are being used in London and New York to reduce crime, prevent terrorism and increase information sharing

©Getty Images

authentication, permissions and more. The benefits of this approach are three-fold. Firstly, it improves the operator experience. A single user interface for both video and access control allows security operators to easily and efficiently move from one security task to another, thus avoiding complicated workflows or jumping from interface to interface to reach the required window. The operator's workflows are also consistent between the video and access control functions allowing them to become more familiar with the system and to gain more confidence when learning and using it.

Furthermore, the total number of workflows is reduced by having common core functions. For example, alarm management, event to action, reporting, investigation, and incident-related workflows are all the same regardless of whether it is for video or access control. Users need only be trained on a single system, thereby saving operator training time and improving security operations within the public facility.

Secondly, unifications allows the operator to become faster and more efficient at handling events. A unified system can offer automatic correlation between video and access control events because every door card swipe can be directly linked to related video. This allows operators to easily visually track access-denied events and to visually verify who is entering an area to confirm or deny a breach in security. In other circumstances, a tailgating event could be noted by the operator on video, and they can look to the access control system to confirm if there was a single card, or multiple access cards, swiped at the door and if any alarms should be raised.

Thirdly, unification allows operators to simplify maintenance and support through one vendor. With a unified system, only a single software platform needs to be upgraded and maintained, reducing the amount of infrastructure investment and time associated with its maintenance. This ease of upgrade results in time savings and simplifies the technical support related to roll-out of new features to the video surveillance and/or the access control system.

The migration of government and public facilities towards IP-based access control is driven by a number of key benefits, including the ability to roll-out, or migrate to, a more open and flexible access control system. Today, truly open IP-based access control software is available and has the ability to not only support multiple door controllers and readers but also to offer a common user interface to configure and manage these various models. Through interoperability, an open architecture access control system provides the ability to select one or more device models to meet a public facility's varying needs, and also becomes a long-term investment strategy with huge savings down the line. Cities rolling out IP-based access control software in one or more of their facilities can benefit from preserving existing hardware, having the flexibility to choose from multiple card formats as their needs change, or the ability to incorporate newer hardware technologies over time; this could include implementing wireless or PoE locks in buildings where wiring might be cost-prohibitive or on doors that are in difficult-to-reach locations.

Other benefits of IP-based access control are faster communication speeds between controllers and software, support for a significantly greater number of devices sharing the same network, and the move away from a polling architecture towards one that is event-driven. In an event-driven architecture, door controllers communicate with the security software only when there is an event as opposed to the polling mechanisms typically found in legacy solutions.

Case study

Unification at Sanford Public Safety Complex

A few years ago, this Florida-state city with a population of just over 53,000 unveiled a new 75,000 square foot public safety complex housing both Sanford's fire and police headquarters. Serving as the city's emergency operations centre, the new state-of-the-art complex was equipped with Security Center, a unified security platform by Genetec, comprising both Omnicast video surveillance and Synergis access control systems. A major factor in choosing Genetec for Sanford's security needs was its ability to unify video and access control security operations into one interface while also allowing for centralisation of several distinct city facilities, including a water treatment plant, under one single system.

When construction was complete, 83 cameras were installed inside and outside the complex. The Synergis system included 78 access-controlled points covering a myriad of uses such as parking gates and sally ports for detainees. Sanford put the open and flexible access control system to the test by incorporating a number of third-party hardware integrations, including duress buttons in interview rooms which trigger strobe light alerts, microphones and alarm triggers connected to perimeter and rollup doors, as well as storage facilities. They also incorporated a variety of PoE access control readers, including some biometric keypad smart card readers for high-security areas such as the evidence room and armoury.

Integration between the various components has allowed normally unrelated pieces of hardware to interact with each other, creating an efficient and responsive system able to handle all the needs of this highly sensitive environment. For example, when certain doors are forced open or held open for a period of time, the door contacts trigger output modules to alert a third-party security monitoring panel, which then sends an alarm to an offsite monitoring company. Simultaneously, the system pulls up the appropriate camera on the monitoring panel, facilitating timely response to any potential threat.

"One of the great things about this system is how easily it can be expanded," explained John Grocke, Design Engineer and Project Manager at SiteSecure, the integrator overseeing the project. "In a critical facility like this with such complex security needs, it's great to be able to quickly add a new piece of hardware without having to reconfigure or rewire the whole system. Using PoE reduces complications and costs, and the extra money can go towards more doors or cameras, creating an even larger coverage area. Plus, the edge devices and distributed architecture have allowed us to significantly downscale the amount of physical space we devote to IT equipment – now it's just the size of a broom closet instead of a whole room!"

"Genetec's Security Center has met all of our sophisticated needs for video surveillance and access control, and afforded a few additional perks above and beyond. As an example, the ease and speed with which we can navigate video footage allows us to efficiently use our archives in an audit capacity if a concern arises about evidence handling. All the data is organised in an intuitive manner, and we can go back after the fact to track an item from the time it landed in our hands to the time it left, moment by moment, to assuage concerns or prove validity in a court of law," elaborated Nicholas McRay, Senior Project Manager at the City of Sanford.

Jimmy Palatsoukas is a senior product marketing manager with Genetec, overseeing product messaging, market and competitive analysis, sales enablement and product launch activities. He has been with Genetec since May 2006 and led the Synergis access control and security centre unified platform solutions as a senior product manager. He previously worked in various technological industries.

Locked down: Sanford's Public Safety Complex

©Genetec