Maximizing Municipal Investment:
The Importance of Openness

By **Mitchell Kane**
President, Vanderbilt

We've come a long way. Today, the industry demonstrates a commitment to delivering open systems solutions through its compliance with open standards and vendors' close collaboration with aligned technology providers. This is quite a change from the days in which one manufacturer's products would only communicate with devices from the same manufacturer.

If you're new to the security market or just need a refresher course, here is how and why we transitioned from a closed model to one that promotes interoperability and information sharing.

The Industry's Evolution

IFor many years, manufacturers produced technology that worked really well … with its own family (i.e. the same brand of products). End users were locked into purchasing solutions from a single manufacturer, which limited freedom to choose a best-in-class system. This became even more challenging when IP systems entered the picture.

Systems integrators had to work overtime to try to manually integrate systems if a customer requested it. Software development kits promised close integration between networked devices but often times the communication between systems was cumbersome. Purchasing was complicated, options were limited and installations were complex. There had to be a better way.

ONVIF was formed in 2008 as a global industry forum dedicated to the development of a global open standard for the interface of physical IP-based security products, such as video surveillance and access control. The ONVIF specification aimed to achieve interoperability between network video products regardless of manufacturer.

The advent of digital technologies, the evolving security landscape and the growing need for more intelligence drove a great shift in the development and sustainability of open-platform technology. Today, ONVIF has moved beyond standards for IP video surveillance and developed Profile C, which enables interoperability between clients and devices of physical access control systems and network-based video systems.

Profile C-conformant devices are able to provide information about doors and access points in the access control system while enabling the monitoring of doors, access control decisions and alarms.

Advantages of Open Platforms

Open-platform technology delivers the freedom and flexibility to use the hardware and software that will be the best fit municipalities need – whether it's from a single manufacturer or a number of them. Systems integrators have the advantage of recommending products that will suit the specific needs of their customers and promote increased ROI. As a result of the ability to customize a security solution, a city's total cost of ownership is reduced significantly.

Additionally, many cities must maximize older – yet still functional – video cameras or access control solutions when upgrading various pieces of the puzzle. Without
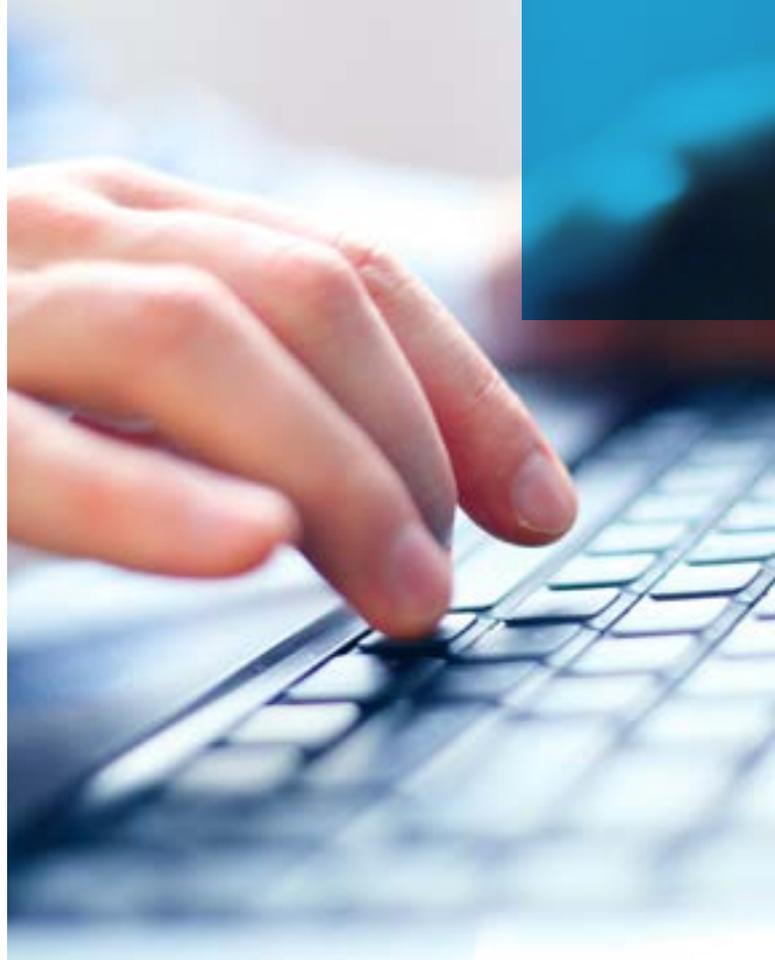
open-platform capabilities, extensive investments would need to be made. Open-platform technology protects existing investments while also allowing cities to take advantage of new advancements in security technology, keeping innovation at the heart of everything they do.

Many cities are also seeing extensive growth, meaning more cameras, alarms and access points. With open platforms, scaling is made easier as needs change.

Integrating Video and Access Control

Many buildings are monitored from a central location using a streamlined access management system that openly communicates with the various doors and readers that are regularly accessed. But there is real value in ensuring that access control is seamlessly integrated with video functionality in an effort to maximize investment, surveillance and evaluation.

Video surveillance, when coupled with access control data, allows an operator to continuously monitor the activity on a site. For example, a busy courthouse might have several access points – some of which are carded and some that are open to the public. However, within the building, there are many areas – such as judge's chambers or in the courtroom itself – where security is paramount and activity must be monitored more closely. In these

instances, operators that have the ability to oversee the management of visitors while seeing what is happening on video in real-time are better able to protect visitors, employees and assets from threats.

It is critical for these systems to talk to each other and seamlessly integrate. Access control systems can generate alarms based on invalid badges, doors held or forced open, and more irregular events, which can alert the operator to investigate the source. Video helps augment this alert by allowing the operator to know which door is being affected while also seeing the incident as it unfolds. When interoperability and integration aren't in place, operators can lose critical response time by having to "shift" from one platform to another, and this time can mean all the difference in the event of a severe threat.

Integrating video and access control also allows officials the ability to examine incidents after they occur, bringing critical pieces of the puzzle together to aid in legal investigation and prosecution of serious crimes.

Bringing Networked Devices Together

Access control and video are just two pieces to the puzzle, and more and more cities are initiating Safe City programs that integrate several systems together in an effort to deliver more information to officials. Surveillance cameras, encoders, IP video management systems, video analytics software, license plate recognition, fire alarms and other sensors can be integrated to form a comprehensive security solution that spans multiple buildings and industries across an entire city.

Bringing all of these sensors together into a single solution that is managed from a central location offers officials greater situational awareness, streamlined response and the ability to efficiently and effectively investigate incidents. Utilizing a platform that is open and offers interoperability as a standard feature not only allows officials to take advantage of new technologies as they
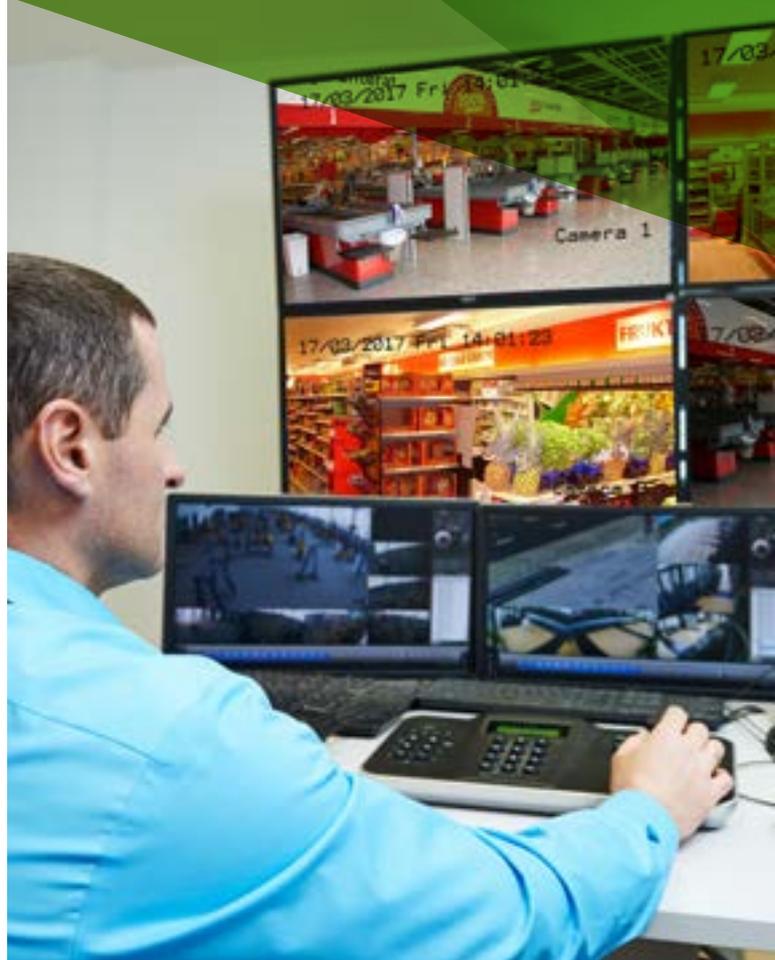
become available, but also ensures the best value when expanding the system. This component is critical to a Safe City solution's return on investment.

Open systems benefit the entire security marketplace and it is clear that we as an industry are dedicated to promoting open solutions that allow stakeholders to expand systems as security needs evolve over time. With open platforms, it is clear that customers face a more streamlined path to move beyond proprietary hardware to more feature-rich access control solutions.

The interconnection of various solutions and devices with other IP-enabled systems aids in the aggregation of security and business data, helping organizations realize new levels of situational awareness. The result? Users can improve security staff productivity, increase security intelligence and be more proactive to risk mitigation. Isn't that what we're all working toward?