IP video networking systems drive access control innovation

Integration between the two most common and active systems in a security environment, video management systems (VMS) and access control systems (ACS), will soon offer security managers a powerful tool to incorporate ACS access and biometric data with video surveillance footage. Currently, there are integration options available, but not all solutions offer a seamless link-up of the traditional ACS data with the IP network. This is according to Marc van Jaarsveldt, consultant, The Surveillance Factory, a video surveillance system-integrator.

"There are some convincing implementations locally, where the integration is solid and results are positive. We have no doubt that the integration will improve over time, but for now users need to be aware of the pitfalls," says van Jaarsveldt.

What is making a difference and an impact on the ACS market is the continued growth and acceptance of IP networking as the de facto standard for video management systems. "We have seen that several access control (AC) vendors have started to offer IP interfaces with their hardware because of the prevailing nature of the network-based security technology. Some examples are Suprema, which produces biometric units with IP interfaces and Genetec that offers an end-to-end AC plus VMS system, including hardware and full integration.

Van Jaarsveldt explains that typically the AC unit (a car or fingerprint reader)) is IP enabled and uses a UTP network cable to allow communication with the LAN, but it still retains traditional signaling interfaces like Wiegand or RS485, which need to be wired in via an IP enabled controller. Examples of these devices are made by Axis, a market leader in network video. In some cases the IP link-up happens where the main AC controller resides, but door units are still wired the traditional way: "Even though there are various levels of integration, the ability to incorporate AC data with video surveillance footage has changed the game plan somewhat for ACS vendors. It has also had a positive impact on the role of biometric data within an overall VMS."

The main advantage of this approach is that it allows biometric data or AC information to be extracted and displayed on a suitable PC. It is here that the VMS comes in. Once that IP interface is available,

developers can write a specific software program to interrogate the AC device and bring biometric or simple access data into the VMS and incorporate it with video.

"The data will be included with the video footage, providing a deeper layer of security information as the video system now displays all AC data including personnel information, credentials and video images. This enhances security and situational awareness. The great thing is that in this instance, operators are now using a single interface for video and AC, as opposed to separate interfaces," explains van Jaarsveldt.

An example, he says, is that you are not just viewing a person as they enter the building, but now having access to all the data about that individual embedded or included with the video. In doing this, companies are able to set up alarms that allow for rule or exception management, which is a powerful security tool.

"Integrated ACS and VMS systems are no longer science fiction. They are an important part of the future of the security industry. Locally, we still have a long way to go to get the integration with VMS seamless and deliver acceptable outcomes. Companies need to understand and have a quality VMS system installed first, and then work towards adding value and extra layers of security such as the integration of AC," concludes van Jaarsveldt.

Tips for choosing your system:

1. Choice of VMS and ACS is critical because it will define which hardware can be integrated. Most VMSs offer basic AC integration with a very limited sub-set of brands.

2. Realise that there is *intelligent integration* where the door or biometric unit integrates fully with the VMS and all of its functionality is supported versus *un-intelligent integration* where the unit communicates with the IP LAN via a simple controller that allows the RS485 cable to be plugged in. These will only support basic functionality and limited data integration.

3. With very long cable runs, or in very noisy environments, you may need to stick with traditional RS485 and cabling and link to the IP network on the backend.

4. When the integration plug-in is written by a 3rd party company (as

is often the case), keep in mind that VMS version upgrades or ACS firmware upgrades can break the inter-device communication.