



Integration Soon to be the Only Game in Town

BY GINNY LU

In years to come, stand-alone security equipment will no longer be available; all solutions will be integrated. The question is when this phenomenon will take place. A&S investigates advancements and challenges.

Increasingly, multinationals are globalizing security operations to increase business efficiency, improve risk management, control processes, and deliver greater transparency and consistency in business operations, said Laird Hamberlin, Regional General Manager, Southeast Asia, Tyco Fire & Security Services Asia. Certain considerations, however, are preventing companies from implementing integrated systems, namely cost, language and local regulations.

Industry integration has taken place over three generations, explained Ken Francis, General Manager, Access Control and Integrated Solutions Platforms, GE Security. The first was emergence of enterprise or IP security. The second involved multiple best-in-breed products, whereby end users

integrated important security products to create one platform. Today's third generation entails fully integrated all-in-one platforms manufactured by a single vendor.

The essence of the slower-than-expected uptake with integrated systems is twofold, said John Katnic, Chief Operating Officer for Synectics Systems. "First, the security response to a given threat is not that of a complete system from day one. This means that systems evolve over time, responding to specific security needs with piecemeal buying.

Second, complete security solutions have multiple layers, each of which tends to address a particular facet of the solution. These layers are often very different disciplines."

"We are not seeing large demand for integrated systems, whereby multiple subsystems (such as video and access control) are provided

by the same manufacturers," said Robert Grossman, who runs his own consulting firm. "Initially, we were surprised by this; on the video side, we hear concerns about going sole-source to avoid integration issues between cameras, digital recording and network clients; but access control seems to be more best-of-breed than sole-source."

The three reasons for less-than-expected demand, said Grossman, are integration through acquisition, open standards and departmental turf battles. "Most manufacturers who offer both video and access control did so through acquisition, not development. This means that they are essentially two different product lines owned by the same company but developed at different times by different teams."

As most access control players started out as independent

companies, they learned how to integrate well with a variety of manufacturers, said Grossman. One of Grossman's casino clients has Human Resources in charge of access control, and Security and Surveillance in charge of video and alarm point monitoring. "The two systems were purchased from different integrators and are maintained by different departments (IT and surveillance). As such, they have different upgrade cycles. In fact, in the gaming market, they are almost always controlled separately."

Francis seconded this assessment: "End users, whose budgets remain separated into security, building management and IT, are less likely to be early adopters of fully integrated solutions."

According to Francis, institutions looking to upgrade video surveillance networks may not delve into fully integrated solutions, but limit technology purchase investigations to only cameras and recording. Modular designs allow for flexible purchases of video or access control. Thus, an end user who is well-informed about technology trends is more likely to be open to advanced, fully integrated solutions.

"Often, systems have different construction priorities, which contribute to separation of systems," Grossman continued. "When a team is hired to do video work, often the access control contract is added too late in the construction cycle for the team to bid the jobs together or sole-source a manufacturer."

"With larger projects, there are often two different integrators involved, recommending two different product lines," added Grossman. "At other times, the camera manufacturer may not

have an access control line (Pelco, for example, only recently added access control when it was acquired by Schneider Electric); or the access control manufacturer may not have a video line that is sufficiently sophisticated. Without real advantage to purchasing the various systems from a single source, and given the operational obstacles, it is not surprising that the markets remain separate, even when sharing parent companies."

Cost can have a negative effect on desire to adopt integrated solutions, said André Cardyn, International Sales & Business Development Director, Genetec. The fact that there are so many different vendors also poses problems since not all vendor solutions integrate easily.

Public purchasing departments and those run by city, state, local or federal authorities are more likely than other verticals to buy older technology. End users coming from these entities may wish to have next-generation solutions, but find themselves constrained by procedures dictated by documents containing outdated specs. The security staff in these departments often lacks access to



▲ Magnus Jonsson, CEO of Pacom Systems

non-vendor-specific expertise to update knowledge and procurement procedures.

In government entities, even those with large security budgets, there is often no provision for consultancy services — funds are allocated to equipment only; this is a pity as the vertical makes up as much as 15 percent of integrated security spend. Lack of an IT department is another drawback.

STAND-ALONE SYSTEM BENEFITS

"There are some advantages to not using converged security systems," said Magnus Jonsson, CEO of Pacom Systems. "If you focus only on one aspect of the system, such as managing access control, you have more functionality for indepth management than you would with a system converged with surveillance and intrusion. Convergence platforms that are horizontally integrated offer limited functionalities. Additionally, many manufacturers of sophisticated stand-alone systems are not willing to open their technology to other vendors, so end users who need specialized solutions often find that integrated security solutions do not meet their needs."

Integration platforms differ. According to Jonsson, some have strengths in access control for enterprise systems (headquarters), others in monitored intrusion for a limited number of buildings. Still others deliver remote management through overviews of multiple sites using alarm management software packages. Frequently, security needs for headquarters are very different from those for branch sites. End users who have installed a converged solution, therefore, may

use stand-alone systems for more complex security needs.

Even converged solutions, which allow for management of disparate needs at both headquarters and branches, rarely have equal strengths in both remote, less complex security management and in enterprise security. Furthermore, there are not many integration platforms available that integrate video, intrusion and access control. Those that do exist generally retrieve and manage video. If, however, the company is using a particular video vendor's enterprise solution, then said vendor is likely to have more advanced software for video. Other examples are video analytics and remote troubleshooting: video manufacturers have dedicated software for these, which converged systems lack.

Traditionally, vendors in the access control field who state that they have integrated intrusion in their systems merely have technology that allows for alarm inputs from different devices, said Jonsson. "Most end users want the ease of alarm setting through a keypad rather than alarm management through software. These access control vendors do not usually offer this type of intrusion capability."

End users who take the time to evaluate and understand the exact nature of their security requirements are more likely to see benefits of an integrated system. These do not constitute a majority, since businesses are driven to decrease costs, and thus see security as a grudge purchase.

WHERE IS INTEGRATION OCCURRING?

"Global networking that allows ease of operation and business continuity planning is desired," said Hamberlin. "This makes IP access



▲ Laird Hamberlin, Regional General Manager, Southeast Asia, Tyco Fire & Security Services Asia



▲ Robert Grossman, President, R. Grossman and Associates

control and video surveillance the most common type of integrated security solutions in Asia as it provides ease of operation and faster access to important information."

"In government facilities, video integration to access control is commonly applied," said Katnic. "Rather than scanning random cameras, alarms sound and/or video can be automatically presented anytime a sensitive door is opened. Operators can even lock or unlock magnetic doors without taking their eyes off of a subject in live video."

According to Jonsson, integration between video and access control is the most widely available type of integrated system, possibly because there are some fundamentals in video, such as transmission, which makes integration a simpler process.

Also, he explained that integrated solutions are widely found in enterprise buildings, which have historically been heavy access control users. Since there is a higher number of access control than intrusion incidents, it makes sense to integrate video with access control so that each

incident does not take away from valuable manpower time.

"In the manned control room where operators are running a mission-critical system 24/7," said Katnic, "there are many examples of user interface software bringing together alarms to operators for auctioning. In major surveillance control rooms in gaming and public spaces, integration software brings together video with alarms to create powerful environments. With ability to integrate alarms via intelligent software and more efficient encoding, such as H264, functionality is increasing while transmission and storage costs are falling."

Intrusion systems are being integrated with access control, said Mo Hess, Global Security Segment Manager, TAC at Schneider Electric, because they can replace each other if regulations allow. Francis expanded on this: "Connecting an intrusion point to access control hardware makes it less expensive to access video of your intrusion system. Basically, this is more affordable than having a motion sensor on your

access controller.”

In high-security and defense environments utilizing integrated solutions, Katnic explained that, when a radar or sonar system detects a target, coordinates are sent to a pan tilt zoom, which automatically zooms in on the suspected location and presents a map and live video to the operator. The integrated system is used to open and close draw gates and bollards, monitor barrier intrusions, and process IR and RF alarms on real-time maps.

Most Asian companies are not receptive to RFID, which makes it the least common type of integrated system. “While most retailers are aware of RFID and its benefits in supply chain management, it is still in the early stage and not many retailers have implemented it,” said Hamberlin. “There have been trial implementations in some markets but, generally, due to the high cost in implementation as well as tags and labels, companies have been slow to adopt this product offering.”

Another factor impeding faster adoption of integrated systems may be unavailability of systems integrating access control and fire

or video and fire. Fire is a heavily regulated sector; some U.S. states require approval from fire marshalls before a fire product can be installed.

GUIDE TO INCREASING END USER TAKEUP

Vendors who offer integrated solutions and wish to win over stand-alone system end users need to develop advanced systems that offer unique, flexible or expandable capabilities, said Jonsson. A vendor whose solution is geared toward remote monitoring needs to expand technology to manage more sites remotely. When a bank with 4,000-plus branches needs a firmware (operating system for panels) upgrade, this means sending out an installer to each and every branch.

A vendor that allows such an upgrade centrally will win out because its system will enable multinationals to achieve central management of security from different regions depending on the time of day. When the North American station closes for the day, the European station can then take over and, in turn, the Asian one will continue the latter’s work.

It is worth noting that most integration vendors today have a physical security background, such as providing video or access control. In this case, integration vendors who have telecommunication backgrounds have an advantage because their starting point is the network rather than security systems or products. Adoption of integrated solutions may be affected by the fact that the latter type of company, which has a stronger IT and R&D background, is in the minority.

Since today’s technology partnerships consist of a hardware company

collaborating with a software company, or vice versa, Francis opined that vendors that are both hardware and software providers will be able to deliver more mature hardware and software solutions, thus enabling them to offer functionalities that far exceed those of solutions stemming from hardware or software-only vendors. A software company working with several hardware partners may choose to limit its functionalities to those which all partner products have in common.

In contrast, a vendor in control of both hardware and software is positioned to react more rapidly to changes and can work with a more diverse group of technology providers. Such a vendor can also make longer commitments to end users to provide functionalities that meet their needs. To pursue higher market penetration, and to become a leading innovator, such a vendor needs to ensure that its integrated solutions offer significant and undisputable cost and functionality advantages. This means increased investment in vertical marketing.

“End-user certification and training courses are restricted by budget and space. Not every sector is being addressed,” said Francis. “Estimates suggest that only 10 percent of end users currently have access to training courses. That said, momentum in fully integrated systems is picking up, and this is resulting in steady adoption. End users are increasingly better informed about how the industry’s solutions meet their needs.” **AS**



▲ Ken Francis, General Manager, Access Control and Integrated Solutions Platforms, GE Security

READER FEEDBACK

What do you think about this story? Please send all your comments and suggestions to as-pr@asmag.com, thank you!