Integration in Access Control Systems

Putting Together the Pieces of an Integrated Access Control System

An RS2 Technologies White Paper

400 Fisher Street, Suite G
Munster, IN 46321
www.rs2tech.com

Integration in Access Control Systems

Putting Together the Pieces of an Integrated Access Control System

Technologies

Table of Contents

Executive Summary

In the first two papers of the RS2 White Paper series[1], we examined the subjects of Total Cost of Ownership (TCO) and Open Architecture as they relate to access control systems. We concluded that an important element of TCO was the use of Open Architecture and that, in turn, Open Architecture was the "cornerstone of integration." We stated that this integration allowed end users to build completely integrated security systems incorporating access control, badging, CCTV, digital or network video recording and analytics, intercom, intrusion detection, wireless/IP locksets and other functions such as visitor management.

This White Paper endeavors to provide a useful definition of integration (as it pertains to access control systems), provides several examples (including diagrams) of discrete integrated systems, and discusses what the next step(s) might be along the road to even higher levels of integration. It also lists some of the questions that end users should ask the vendors of access control systems and the systems integrators who install these systems. Readers are then encouraged to apply these conclusions to their own evaluations of access control systems.

What is Integration?

System integration is also about value-adding (to the system) capabilities that are possible because of interactions between sub-systems

Not too many years ago, when defining a word, writers would quote the American Heritage or Merriam-Webster dictionaries. In keeping with the times, we find Wikipedia's definition of "system integration" to be very useful for the purposes of this White Paper:

"System integration is the bringing together of the component sub-systems into one system and ensuring that the sub-systems function together as a system.

A system is an aggregation of sub-systems cooperating so that the system is able to deliver the over-arching functionality. System integration involves integrating existing (often disparate) sub-systems.

System integration is also about value-adding (to the system) capabilities that are possible because of interactions between sub-systems."

A little long, but right on the mark for our purposes. Please note that we are using the term "system integration" almost interchangeably with

[1] Copies of the RS2 White Papers "Total Cost of Ownership of Access Control Systems" and "Open Architecture in Access Control Systems" can be downloaded by logging on to the RS2 web site (www.rs2tech.com) or by calling 877.682.3532 and requesting a copy.

"integration." In the world of access control, the distinction between the two terms tends to blur, as what is being integrated is just that – systems/sub-systems.

Perhaps equally as important as defining what integration *is*, is defining what it is *not*. Integration is occasionally used interchangeably with "convergence." In his article "Convergence 2.0", Bill Zalud, editor of *Security* magazine, says "For some, convergence is a fancy-pants term for security systems integration in which various security subsystems are connected beyond simple interfacing. In a general way, however, most security leaders see convergence as the bringing together of physical and logical – or computer – security in ways that primarily emphasize access controls and identity management."[2] We will deal with convergence in greater detail later. See "The Future of Integration: Convergence" on page 14.

Perspectives on Access Control Integration

Integration between access control and other security systems is so prevalent today that it's almost hard to remember that, as recently as a few years ago, that was not the case. However, one need only look at security trade publications from that period to find stories like this:

"A security manager for a large corporation comes in from a long Memorial Day weekend and reviews the security logs for the time he was away. He sees a line of type in his access control log saying that someone was attempting an unauthorized entrance to a highly secure area of the facility on Memorial Day itself, when no regular employees were present. He reviews his access control logs to see whose card was being used to try to enter. Unfortunately, he has no way of confirming whether that person actually was attempting entry or someone else was using the person's card because the corporation's video system is not integrated with its access control system."[3]

Today, it's difficult to find a security sub-system that **doesn't** integrate with access control.

Seems pretty primitive by today's standards, doesn't it? In fact, video was one of the very first integrations (with access control) to occur. Today, it's difficult to find a security sub-system that **doesn't** integrate with access control. While video is still the obvious hot spot, access control also now routinely integrates with intercom, intrusion detection, wireless locks, visitor management, and other systems.

[2] "Convergence 2.0", Security Magazine, February 2009, Bill Zalud. © 2009 Security Magazine.

[3] "Trends in Video Integration: The Need for 'Open Book' Design", SDM Magazine, 4/3/06, Russ Gager. © 2006 SDM Magazine.

Who and what drove the change? And why did it occur so quickly? The "who" are, literally, all the stakeholders: suppliers, integrators, and end users. The "why" essentially boils down to economics – on the part of all three groups. In a series of articles in 2006, *SDM* magazine examined integration from all three perspectives. There were certainly differences between the three groups. Suppliers were looking for a competitive advantage; integrators were looking for products that would improve their profitability; end users were looking for single-platform systems that were easy and cost-effective to operate:

Suppliers:
"Integration is not a buzz word anymore – it is already here. People are trying to understand it better. As manufacturers are getting to understand the importance from a market development standpoint, the end users are beginning to realize the importance of getting as much as possible out of the investment."[4]

Integrators:
"What integrators also look for is manufacturers that typically enable the integrating company to make money, and how you do that is limit distribution so not everybody sells it, and you don't sell directly to end users. . .Manufacturers who sell directly to end users are avoided by most integrators."[4]
(Note: From its founding in 1998, RS2 Technologies has never sold to end users.)

End Users:
"For us here, the bottom line is dollars."[4]

"Better integration would economize on the biggest expense of installing security equipment – not the equipment itself, but running the wire for it."[4]

And, in a more recent (June 2008) article entitled "Feature Sets that $ell", the "Big 3" features are identified as integration, open platform, and ease of use: "Integration with video, or any other system, is a boon to customers in today's economy. 'The way things have matured, CCTV, access, and alarm management were traditionally separate systems,' says Matt Barnette . . . AMAG Technology. 'Today, we are finding more customers trying to do more with less. They need systems that play into that.'"[5]

[4] "Integration: The Suppliers' Perspective", SDM Magazine, 5/1//06, Russ Gager. © 2006 SDM.
"Integration: The Integrators' Perspective", SDM Magazine, 6/1//06, Russ Gager. © 2006 SDM.
"Integration: The En d Users' Perspective", SDM Magazine, 7/1//06, Russ Gager. © 2006 SDM.

[5] "Feature Sets That Sell", SDM Magazine, June 2008, Karyn Hodgson. © 2008 SDM Magazine.

How Integration Works

"I know you. You know me."

- from "Come Together", the Beatles, 1969

It's a pretty safe bet that, when John Lennon wrote "Come Together" in 1969, he wasn't thinking about security system integration. Nevertheless, those 6 words are a succinct description of what happens in an integrated security system. Literally, the individual sub-systems recognize and talk to each other through the access control system, allowing them to "come together" as an integrated system. Many integrated systems started out as one or two sub-systems that were integrated with the access control system. In the RS2 experience, video and CCTV were among the initial physical security sub-systems to be integrated with access control, followed quickly by intercom and intrusion detection. Most recently, wireless/IP lock-sets are being integrated with access control.

How do all the pieces go together? The following series of diagrams shows how various sub-systems are integrated with RS2's Access It!® access control systems. As shown in Figures 1-6, each system utilizes the Local Area Network (TCP/IP) to configure any number of components.

Integration with Closed Circuit Television (CCTV)

In the case of CCTV, the Access It!® system connects through the LAN either directly to IP cameras or through the access control server and a CCTV matrix switch to an unlimited number of dome cameras. Using interactive graphical display maps, users can direct cameras to preset positions based on alarms or events, control cameras with full PTZ (pan-tilt-zoom) capability, view live events on demand, and perform other functions.

An Integrated Access Control & CCTV System

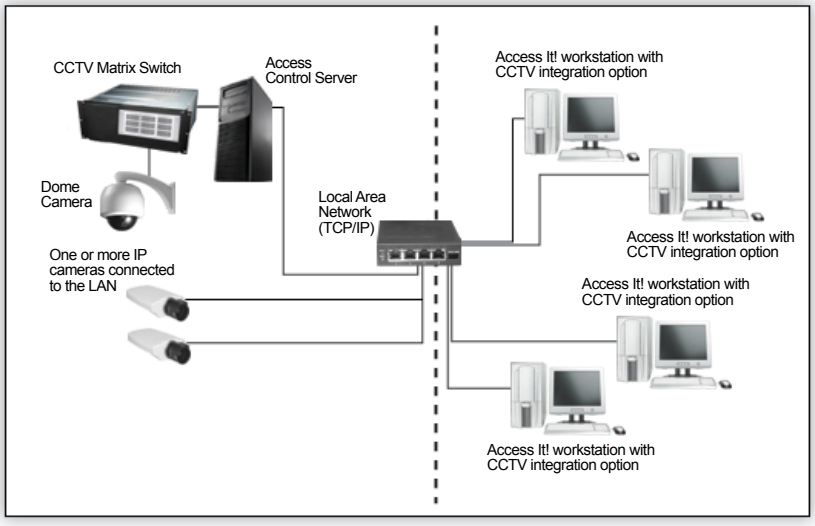

Figure 1: This diagram shows the network setup for an RS2 Access Control System that has been integrated with a CCTV system.

Integration with Digital and Network Video Recorders

With digital and network video recorder systems (DVRs and NVRs), users can perform all of the same functions as with the CCTV system (i.e., PTZ camera control, live camera view on demand, etc.), and have the added capabilities of video playback on demand (or tied to alarm/event time and data), hyperlinking to video from access control history reports, simple GUI (graphical user interface) for faster incident investigations, and many other functions. Because of the popularity of video analytics, RS2 integrates with more than a dozen DVR/NVR manufacturers, and incorporates a "Universal DVR/NVR Viewer" into its Access It!® software.

An Integrated Access Control & DVR/NVR System

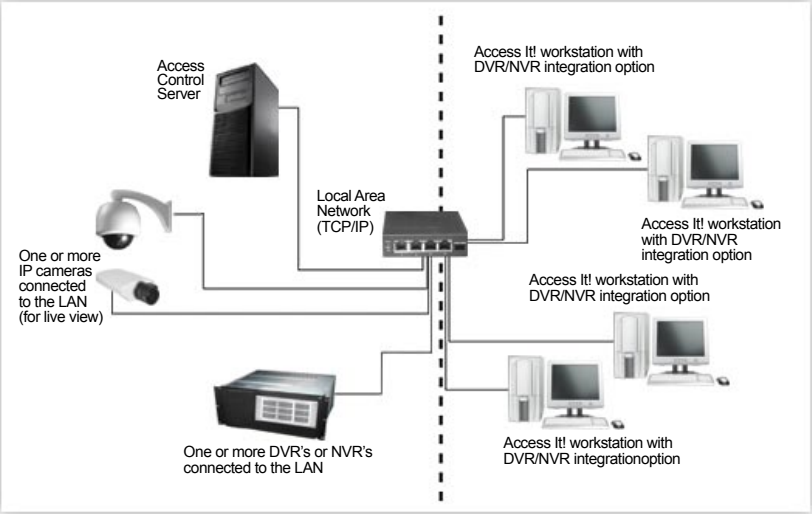

Figure 2: This diagram shows the network setup for an RS2 Access Control System that has been integrated with a DVR/NVR system.

Video –and the analytics associated with it– is certainly the fastest-developing area that is integrating with access control. New developments allow users to choose "intelligent" cameras that have built-in content analytics that can not only see the scene but can also interpret it using computer algorithms that analyze what the camera is seeing. These analytics-enabled cameras supplement the analytics software that resides on the application server. Writing about these cameras in the March 2009 issue of SDM magazine, in an article titled "Where's Everyone Going?", Gadi Piran, president and chief operating officer of On-Net Surveillance Systems, points out:

"Their capabilities include detection of specific movements and behaviors, such as:

- *Motion detection (the size/shape, speed, and direction of a moving object)*
- *Non-motion detection, such as stalled vehicles or an abandoned object*
- *Behavior analysis, such as tailgating at entry points or loitering*

continued on page 8

continued from page 7

- *Accurate optical character recognition (OCR) for applications such as license plate recognition"*

In the same article, Piran also discusses the advantages of using PoE (Power-over-Ethernet) and wireless technology to enable users to extend the reach of their video-integrated access control systems to areas without a power supply, similar to what is being done with wireless/IP locksets (see page 10 of this White Paper).

Integration with Intercom Systems

In an integrated access control and intercom system, the Access It!® workstations connect through the LAN and access control server to an intercom switch serving multiple intercom stations. Integration between the access control system and the intercom stations allows automatic connection to those stations during alarm processing. If an employee presses an emergency call button during an incident, an alarm is generated in the Access It!® system, prompting a security officer to acknowledge the alarm. This automatically connects the master intercom station to the emergency call box, giving the security officer full audio of any ongoing incident.

An Integrated Access Control & Intercom System

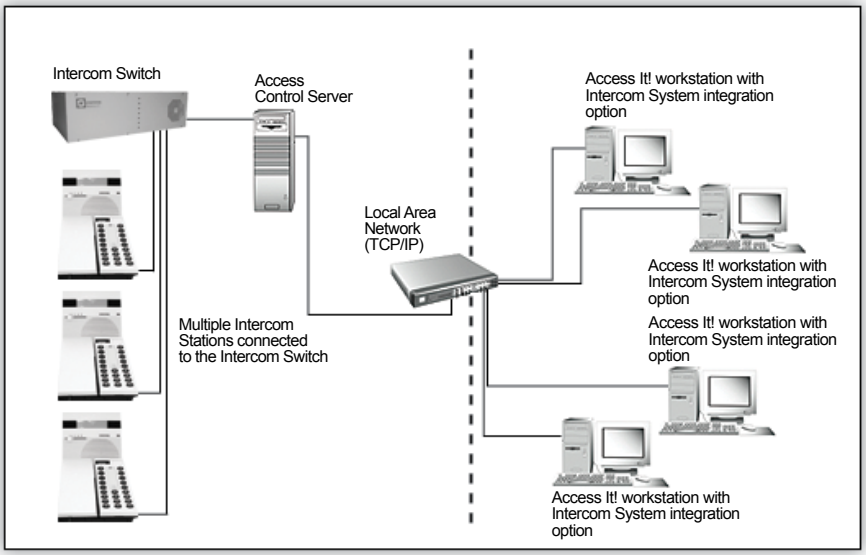

Figure 3: This diagram shows the network setup for an RS2 Access Control System that has been integrated with an intercom system.

Integration with Intrusion Detection

The integration of access control systems with intrusion detection is an excellent example of how systems integration not only provides end users with greatly increased functionality, but can also reduce overall security system costs.

In the past, intrusion detection systems and access control systems were installed using separate cabling, door contacts, etc., which increased system installation costs. Also, the systems did not share data, making it difficult to associate intrusion alarms with access control events. By integrating access control with intrusion detection products, end users now use a single, consistent GUI (graphical user interface) for both the access control system and the intrusion detection system. This allows them to monitor intrusion events and alarms, execute access control system tasks based on those same events/alarms, record alarm event data in the access control system events database, and even control day-to-day intrusion detection system operations (arming/disarming zones, etc.) via the access control system. (See Figure 4.)

An Integrated Access Control & Intrusion Detection System

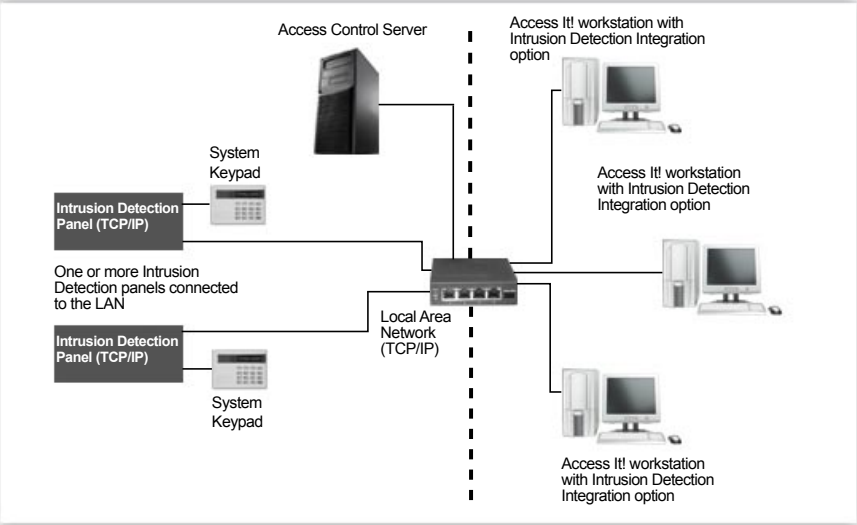

Figure 4: This diagram shows the network setup for an RS2 Access Control System that has been integrated with an intrusion detection system

Integration with Wireless, IP and PoE Locksets

One of the most recent examples of integrating access control with other physical security systems is that of wireless, IP, and PoE (Power-over-Ethenet) locksets. RS2 Technologies was one of the pioneers in partnering with the manufacturers of both the IEEE 802.11 and 900 MHz technologies, which allowed users to extend the reach of their access control systems through their existing wireless and IP infrastructures. Users can add openings to their systems in locations that were previously difficult or cost-prohibitive to incorporate using hard-wired technology. These wireless locks not only provide centrally managed access control to these types of locations, but they do so without much of the cost, labor and infrastructure upgrades associated with traditional hard-wired systems.

As with the example of access control/intrusion detection integration, wireless locks lower costs by reducing installation labor, simplifying project management (fewer trade personnel), and leveraging existing infrastructure. (For example, a typical hard-wired access-controlled opening takes an average of 8 hours to install and bring to operational status, whereas wireless locks take about an hour to install by a single technician.)

An Integrated Access Control & Wireless/IP Lockset System

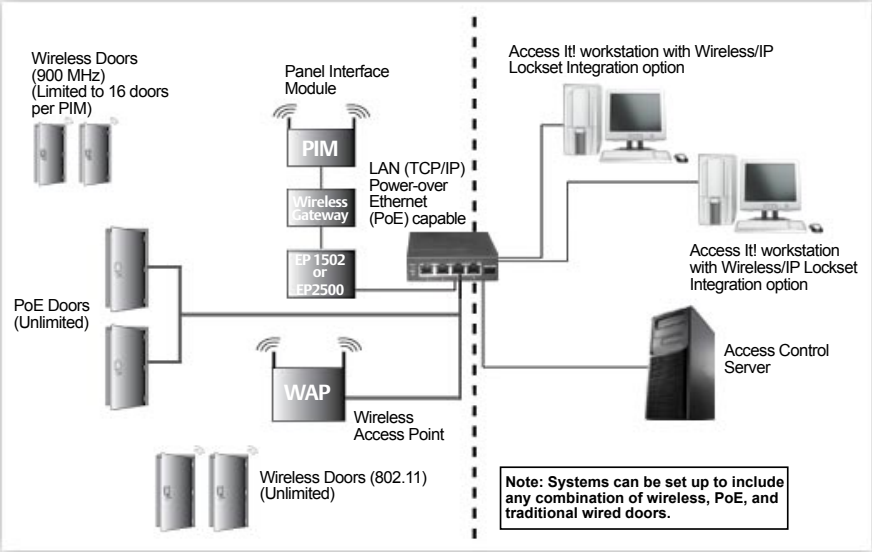

Figure 5: This diagram shows the network setup for an RS2 Access Control System that has been integrated with wireless, IP, and PoE lockset systems.

Completely Integrated Systems

The adage “The whole is greater than the sum of the parts” is frequently used to describe conditions or systems in which the synergistic effect of combining individual parts or sub-systems produces a significantly enhanced outcome. Completely integrated security systems (a term which should be used with considerable caution, as there will always be additional functions and sub-systems that can be integrated into systems that were previously considered “complete”) which combine several –or all– of the functions described in Figures 1-5 are a good example of that maxim. Figure 6 below illustrates how a “completely integrated security system” might combine elements of CCTV, video surveillance & analytics, intercom, intrusion detection, and wireless/IP and PoE locksets through the same Local Area Network.

A Completely Integrated Security System

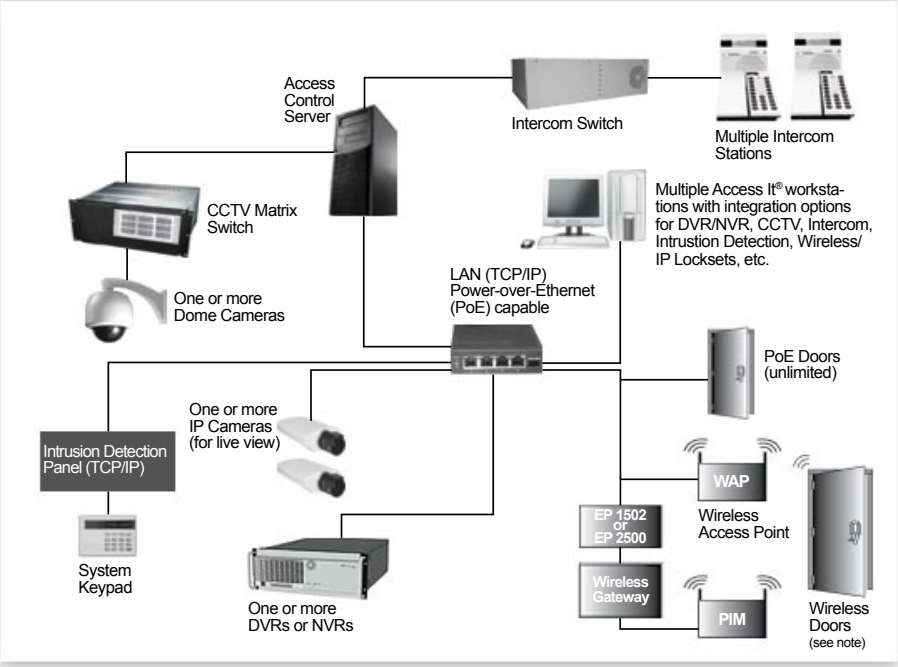

Figure 6: This diagram shows the network setup for an RS2 Access Control System that has been integrated with video surveillance, intercom, CCTV, intrusion detection, and wireless/IP and PoE lockset systems.

Note that in the case of wireless/IP locksets, systems operating on 900 MHz are limited to 16 doors per PIM (Panel Interface Module). With IEEE 802.11 systems, there are no limits. PoE systems can also have an unlimited number of doors. Systems can be set up to include any combination of wireless/IP, PoE, and traditional wired doors.

Integration with Software and Other Systems

Integration between access control systems and other elements of a security system is not limited to physical sub-systems, but can also include integration with other software systems. A good example is electronic visitor management. For those not familiar with the subject, electronic visitor management systems were created more than a decade ago to address what Mark Eardley, in an article in Hi-Tech Security Solutions, called "the big loophole in access control." His point was that access control systems did a great job of tracking employees, but not quite as great of a job of tracking visitors.[6] Up through the mid-90's, visitor management consisted of visitors and contractors signing a paper log with names that were at best, illegible, and at worst, false. In the event of an emergency such as a fire, it was impossible to quickly determine who was still in the building. To address these issues, companies and organizations started to install stand-alone electronic visitor management systems about 10 years ago and, within the past few years, began integrating them with access control systems. However, even as recently as 2008, estimates Howard Marson, CEO of visitor management supplier EasyLobby, Inc., "no more than 15% of visitor management systems are integrated with access control."[7]

Integration with access control is not limited to physical sub-systems, but can also include other software systems.

Comprehensive visitor management systems electronically scan the visitor's ID (business card, driver's license or passport), and automatically capture name, company, title, contact information, etc. into a database file, with photo and signature, name of the person being visited, reason for the visit, and entry and exit times. Multiple stations can share a central database over the network for monitoring and reporting. And, enterprise-level systems can also track incoming packages and even visitors' vehicles.[8]

In terms of integrating with access control, while the visitor management system does, indeed, have physical equipment such as badge printers, turnstiles, and self-serve kiosks (for un-manned lobbies), these are generally controlled directly by the visitor management software. Integration between it and access control software such as RS2's Access It!® Universal occurs within the same SQL server where both the visitor management and access control databases reside. An example would be the integration between Access It!® and EasyLobby's SVM™ visitor management system, in which the SVM™ software includes a configuration and installation utility that allows users to

[6] "Visitor Management", Hi-Tech Security Solutions, June 2007, Mark Eardley. © 2007 Hi-Tech Security Solutions.

[7] "Beyond the Visitor Ledger", SDM Magazine, October 10, 2008, Joan Engebretson; and "Visitor ID Integrates with Access", Security Magazine, October 8, 2008. © 2008 SDM Magazine and Security Magazine.

[8] "Tracking People, Packages and Vehicles", Security Magazine, February 1, 2009. © 2009 Security Magazine.

install the integration between the two systems and configure a variety of settings. Once the integration is established, operators use the Access It!® GUI to create access levels equivalent to those assigned by the visitor management software.

The Importance of Partnering in Integration

Powerfully integrated systems start with powerful integration partners. RS2 has partnered with a number of the leading manufacturers of DVRs, NVRs, CCTV and intercom systems, and intrusion detection panels, as well as with companies offering employee and visitor management systems and other access control products that can add value to our systems. Our integration partners include such names as ABM Data Systems, Altronix, ASSA ABLOY, AWID, Bioscrypt, Blackboard, Bosch, Costar Video Systems, Dedicated Micros, Digiop, Digital Watchdog, DMP (Digital Monitoring Products), EasyLobby, Exacq Technologies, Farpointe Data, HID, Integral Technologies, Integrated Engineering, IR Schlage, March Networks, Mercury Security, Milestone Systems, On-Net Surveillance Systems, Inc., Panasonic, Pelco, RTS Sentry, Stentofon (Zenitel), Toshiba, Vicon, Vision Controls, XceedID, and others.

The Role of the Systems Integrator

The importance of the professional systems integrator organization in the planning, installation, and servicing of a successfully integrated access control system simply cannot be overstated. And, it seems so obvious to us that we will not devote more than a few paragraphs to cite the opinions of other observers:

The importance of the systems integrator to a successfully integrated access control system cannot be overstated.

"We try to work with integrators that we have relationships with, and we feel are qualified and will give us good service and pricing. As you get a few systems under your belt, that relationship and trust begins to build. We are achieving seamless integration at this point. Speaking for myself, low cost isn't always the determining factor. For me, it's actually fairly low on the list in determining who will get a job." [9]

Throughout its history, RS2 Technologies has endeavored to work with top-notch systems integrators who are viewed by end users as "security system experts" and "security partners", and not as vendors.

"Integrators often specialize in high-end systems, but are either familiar with all others or can easily figure it out. They are at their best in complex projects that join parts of separate systems to function with core usability." [10]

[9] "Integration: The End Users' Perspective", SDM Magazine, 7/1//06, Russ Gager. © 2006 SDM.

[10] "The Integrator Relationship", Security Magazine, April 2009, Bill Zalud. © 2009 Security Magazine.

For a list of integrators in your area that can plan and install an integrated access control system, end users should contact the RS2 Regional Sales Manager in their area or RS2 Corporate Headquarters. For that contact information, see page 17 of this White Paper.

The Future of Integration: Convergence

What is the future of integration in access control? Certainly, we will see more discrete systems join the current list of those that integrate with access control. Beyond that, however, will be a new level of integration that most observers define as "convergence." But, what is convergence? "In the past few years, perhaps no security industry buzzword has been defined in articles and promotional materials more than 'convergence'", writes Honeywell Senior Product Manager Beth Thomas, in an article in *CSO Online*. "These definitions have most commonly referred to the integration of physical security and IT systems, with occasional elements of building control."[11]

Most security leaders see convergence as the bringing together of physical and logical security.

E. John Sutton, security and integration manager of the Port Authority of NY and NJ, offers that "Enterprise level systems combine many security functions within one system; this is convergence at some defined level." [12]

However, as we quoted Bill Zalud of *Security* on page 4, "most security leaders see convergence as the bringing together of physical and logical – or computer– security in ways that primarily emphasize access controls and identity management."[13] That, it seems to us, is the most useful definition. How will this be accomplished? Most indications are that, as was the initial experience with integration, it will again be the joint efforts of manufacturers, integrators and end users that determines the final shape of convergence. The difference will be that, at the end user level, IT professionals will be a bigger part of the mix.

[11] "Industry View: Checklist for Converged Access Control", CSO Online, June 2008. © 2008 CXO Media, Inc.

[12] "Convergence 2.0", Security Magazine, February 2009, Bill Zalud. © 2009 Security Magazine.

[13] Ibid.

Questions to Ask Access Control Manufacturers and Systems Integrators

As in our first two White Papers, we offer a list of questions that purchasers of Access Control Systems should ask the manufacturers of those systems – in relation to the integration of the system with other sub-systems. (For copies of previous lists of "Questions to Ask Vendors", please download our White Papers on Total Cost of Operation and Open Architecture.) Because this White Paper deals with the integration of access control with other systems, and because of the importance of the systems integrator in the installation of such an integrated system, we have expanded the list to include questions that should be asked of systems integrators. Like all such lists, this list is not all-inclusive, but a good basic list of questions would include:

Questions for Access Control Manufacturers:

- **What other security systems does your system integrate with (e.g., CCTV, intercom, intrusion detection, visitor management, etc.)?**
- **How long have you been integrating in each of these areas?**
- **Specifically, which manufacturers of each of these types of systems do you integrate with?**
- **Does your Dealer List include systems integrators who have experience in installing complex integrated systems?**
- **Can you provide a list of such integrators in our area?**
- **What kind of a relationship do you have with these integrators?**
- **Can you provide a list of projects that have involved integration of your access control system with other systems?**
- **How familiar are you with our business sector (e.g., education, banking, hospitals, etc.)?**
- **Do you have integrated installations in our business sector?**
- **Can you provide references at those installations?**

Questions for Systems Integrators:

- **In what types of systems do you specialize?**
- **What manufacturers' products do you install?**
- **How many systems have you installed that have involved integration between access control and at least one other sub-system?**
- **Can you provide a list of these, with names and numbers of references?**
- **How many project managers, installation technicians, service technicians, and account managers work from the office that would install and service our system?**
- **What kind of relationship do you have with the manufacturers of each of the systems that would be part of our project?**
- **If applicable to the project: Do you have personnel who have IT/IP knowledge?**

For a more complete list of questions for systems integrators, see "The Integrator Relationship", April 2009 *Security* Magazine.

Conclusions

Stand-alone, un-integrated security systems and sub-systems are a thing of the past. They are neither operationally effective nor cost effective. The security system of today is a system that efficiently and effectively integrates access control with multiple sub-systems, both physical and software. The security system of tomorrow will be a system that accomplishes the convergence of physical and logical (IT) security.

End users who are contemplating the purchase and installation of new access control systems (or the upgrade/expansion of existing systems) should do their research on integrated systems with manufacturers and systems integrators by asking them – at a minimum– the questions outlined in this White Paper. First and foremost, they should seek out a systems integration organization that has experience in the installation of complex integrated systems, and should develop a long-term partnership with that organization.

About RS2 Technologies, LLC

RS2 Technologies, headquartered in Munster, Indiana, is a technology-driven developer and manufacturer of cutting edge access management hardware and software. The company's hardware line includes a wide range of system control processors, input/output modules, multiplexers, card readers and proximity and smart cards. RS2 also offers the industry's most advanced, easy-to-use software with its **Access It!**® line of access control software. RS2 is a Microsoft Certified Partner with ISV (Independent Software Vendor) software solutions competency status.

For more information, visit our web site at www.rs2tech.com or contact:

Corporate Headquarters
Gary Staley National Sales Director
877.682.3532
gstaley@rs2tech.com

St. Louis Office
David W. Barnard
Director of Dealer Development
877.682.3532
dbarnard@rs2tech.com

West Coast Sales Office
Ty Caudill
Western Regional Sales Manager
877.682.3532
tcaudill@rs2tech.com

Southeast Sales Office
Ed Sims
Southeast Regional Sales Manager
877.682.3532
esims@rs2tech.com

Northeast Sales Office
David Bensky
Northeast Regional Sales Manager
301.524.2971
dbensky@rs2tech.com

European Sales Offices
UK (London): 0207.993.4737
Italy (Milan): 029.175.4046

Asia Sales Offices
Beijing: 86.10.58630222 ext. 315
Hong Kong: 852.2893.8899 ext. 308