Underutilization of Features in Access Control Systems

Getting Your Money's Worth When Specifying & Buying an Access Control System

An RS2 Technologies White Paper

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

Underutilization of Features in Access Control Systems

Getting Your Money's Worth When Specifying & Buying an Access Control System

Table of Contents

Information contained within this document is intended for general educational purposes and is subject to change without notice. It is considered to be accurate at the time of publication, but RS2 Technologies, LLC assumes no liability and makes no warranties, express or implied, with respect to the accuracy of the information or its use for any purpose.

Executive Summary

In previous papers of the RS2 White Paper series, we have examined subjects such as Total Cost of Ownership (TCO) and Integration as they relate to access control systems. In our White Paper on TCO, we concluded that specifiers of access control systems should evaluate competing systems – and base their purchasing decisions – on the total cost to own the access control solution. In our White Paper on Integration, we concluded that un-integrated security systems are neither operationally effective nor cost effective. This White Paper, the fourth in our series[1], builds on these conclusions by addressing the issue of underutilization of features in access control systems. As the subtitle suggests, the paper also addresses some issues which – when properly and thoughtfully addressed – will help end users "get their money's worth" when specifying and purchasing an access control system.

Many security consultants, systems integrators, and end users of access control systems simply aren't as knowledgeable as they should be about the systems they specify.

This White Paper endeavors to provide a useful definition of underutilization (as it pertains to access control systems), provides several examples of access control system features that users might not be taking full (or any) advantage of, and discusses how users can greatly improve the utilization and cost effectiveness of their access control system by spending a relatively few extra dollars on integrating some of the features and equipment that they plan to purchase. 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 Underutilization?

Basically, there are two main types of underutilization relating to access control systems. The first and most obvious type occurs when users pay for features or equipment – knowingly or unknowingly – that they don't end up using. How does this happen? Most frequently, the answer is that specifiers (and this can include security consultants, systems integrators, or end users themselves) simply aren't as knowledgeable as they should be about the features of the access control systems that they have specified, installed, or purchased.

The second type of underutilization occurs when an end user makes a considerable investment in installing an access control system and also spends money on a sub-system such as video, but does not spend the comparatively few extra dollars required to integrate the two systems.

[1] Copies of all RS2 White Papers can be downloaded by visiting the RS2 web site (www.rs2tech.com) or by calling 877.682.3532 and requesting a copy.

Why does it matter? Isn't there a little bit of underutilization in almost everything we do in business? Maybe so, but considering the economic downturn of the last few years, security professionals should be especially focused on getting their money's worth out of their access control and overall security systems. In an article in the May 2009 issue of *Security Director News*, Noelle Britton, Director of Marketing for the Security Solutions Business Unit of Siemens Technologies, makes the point that "conducting a thorough cost analysis can help you maintain the value of your security investment."[2] She cautions security directors that they "are responsible for protecting the people, property, and assets in your organization. On top of that, you have to account for and justify every dollar that you spend on security."[3] And, in a June 2009 article in *SDM Magazine*, Karyn Hodgson writes "The downturn in the economy has shifted the focus of many end users from a goal-oriented approach to a value-oriented approach."[4]

Security managers should be focused on getting their money's worth out of their security systems.

Buying More Than You Need

"You can't always get what you want. But if you try sometimes, you just might find, You get what you need."

- from The Rolling Stones, 1968

Actually, in the world of access control utilization and underutilization, it's usually just the opposite. Customers can almost always get what they want (or think they want). But sometimes, they find that it's *more* than they need.

Client Licenses

Within this first category of underutilization, there are a couple of sub-categories. The first centers around the issue of "client licenses." Client licenses, also sometimes referred to as "seats", are the one-time licensing fees that a customer pays for workstation licenses controlled by the server. Frequently, a customer will pay for too many seats because they are not aware that the software can be "shared" (also called concurrent licensing) by more than one user. Let's take the example of a customer who wants the access control software to be available to the General Manager, Security Director, Human Resources Manager, and three shifts of guards. Many times, the customer will order six client seats/licenses. They could have gotten by with just four seats by having the three guard shifts share one client seat. Access control software such as RS2 Technologies' Access It!® Universal software features a concurrent licensing model that controls the total number of workstations that can be in use at any given time, which allows the software to be installed on any desired number of workstations.

[2] "Maximizing the Value of Your Security Investment", Security Director News, May 2009, Noelle Britton. © 2009 Security Director News.

[3] Ibid

[4] "Prioritizing Value", SDM Magazine, June 2009, Karyn Hodgson. © 2009 SDM Magazine.

In addition to paying too much for client licenses, customers might also be setting themselves up for years of ongoing costs because many access control software manufacturers also charge for software maintenance agreements that are coupled to each client seat. The resultant added cost can significantly increase the lifetime TCO of the system. (For a detailed treatment of the costs of such items as software maintenance agreements, software "add-ons", client licenses, reader licenses, per-device integration fees and other items that increase TCO, see our White Paper entitled "Total Cost of Ownership for Access Control Systems." See footnote number 1 on page 3 for details on how to obtain this White Paper.)

Overspecifying

Another sub-category of purchased feature or equipment underutilizaton involves customers who –either through a lack of knowledge or as a result of inaccurate advice from a security consultant or installer – pay for and install door monitoring hardware that they have no plans to use. This usually occurs when a customer gives an installer general directions such as "Give me access control on these three doors." What can then happen is that the installer will misinterpret this seemingly simple but overly broad instruction. While the customer means that he/she wants just the electronic lock and card reader that constitute the elements of basic keyless entry, the installer (or specifier) will include a door contact (position switch) and a Request to Exit (REX) device such as a motion sensor or button.

If you're never going to actively monitor the door, don't pay for the hardware & cabling to do so.

These additional elements are required for true door monitoring. These additional devices and their requisite wiring can add $300-$350 per door in additional costs, so in our example of the customer who requested "access control" for three doors, the system will cost an additional $1,000. This is fine if this customer truly wants door monitoring, either now or in the not too distant future, but if he's never going to monitor these three doors, he's just wasted $1,000. Conversely, if the plan is to eventually monitor a particular door, the customer should go ahead and have the installer put in the necessary cabling at the same time he's "dragging cable" to the door for the lock and card reader.

These additional elements are required for true door monitoring. These additional devices and their requisite wiring can add $300-$350 per door in additional costs, so in our example of the customer who requested “access control” for three doors, the system will cost an additional $1,000. This is fine if this customer truly wants door monitoring, either now or in the not too distant future, but if he’s *never* going to monitor these three doors, he’s just wasted $1,000. Conversely, if the plan is to *eventually* monitor a particular door, the customer should go ahead and have the installer put in the necessary cabling at the same time he’s “dragging cable” to the door for the lock and card reader.

You Paid For It – Why Not Use It?

A third sub-category of purchased feature underutilization is the largest and – for manufacturers of access control software – probably the most frustrating. This involves the underutilization or, more accurately, the non-utilization of some access control system features that manufacturers consider among the most useful. These are features that, in the case of access control manufacturers such as RS2 Technologies, are resident in the software and are included in the purchase price (i.e., at no additional cost), but are frequently not utilized by end users.

While there are several such examples of underutilized features, we will look at just a few, of which access control system users would be well advised to take advantage. This is not an exhaustive “how to” explanation of each feature, but is intended to pique the interest of readers and encourage them to learn more about these features by contacting the dealer or integrator who installed their system.

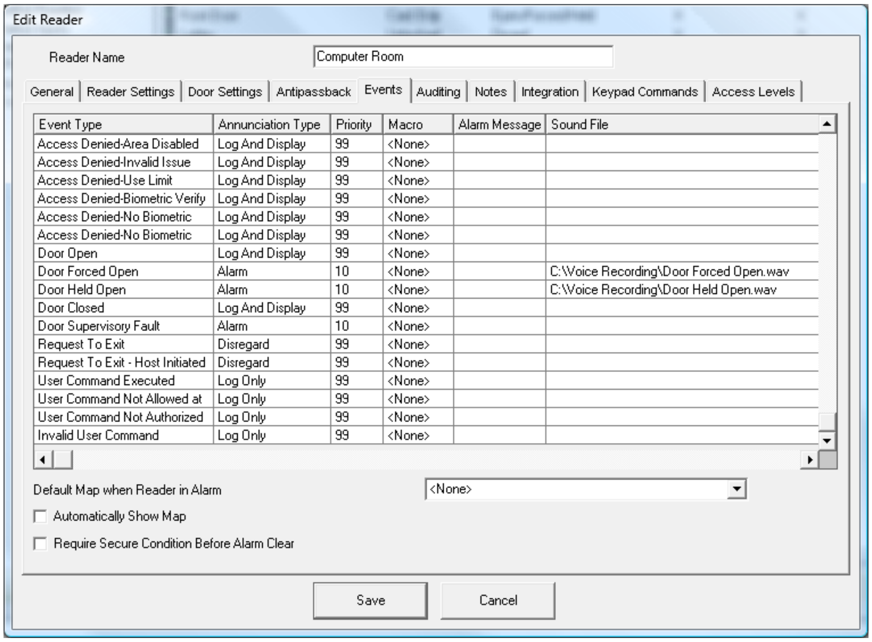
Underutilized & Unutilized Features

The most commonly underutilized access control features include:

- Sound Files
- Graphical Maps
- Definable Event/Alarm Colors
- System Management and Reporting Features

Sound Files

The ability to incorporate sound (.wav) files into an access control system is a feature that is common to higher-end systems such as such as RS2 Technologies' Access It!® Universal. One reason for incorporating sound files is that system operators and guards will – over time – become de-sensitized to alarm indicators on their screens. If the alarm indicator is a common one such as "Door Held Open", this might not be cause for undue concern. However, if the indicator is "Door Forced Open", this is more serious. Rather than have the system default to a standard Windows® tone, users can change these alarms (or *any* alarms in the system) to a more distinctive or custom tone, or to an actual voice message. For high-priority alarms, such as when someone has pushed a "duress" or hold-up button, system users can place a recorded audio file with a message such as "Call 911 immediately."



Reader Name: Computer Room

Event Type	Annunciation Type	Priority	Macro	Alarm Message	Sound File
Access Denied-Area Disabled	Log And Display	99	<None>		
Access Denied-Invalid Issue	Log And Display	99	<None>		
Access Denied-Use Limit	Log And Display	99	<None>		
Access Denied-Biometric Verify	Log And Display	99	<None>		
Access Denied-No Biometric	Log And Display	99	<None>		
Access Denied-No Biometric	Log And Display	99	<None>		
Door Open	Log And Display	99	<None>		
Door Forced Open	Alarm	10	<None>		C:\Voice Recording\Door Forced Open.wav
Door Held Open	Alarm	10	<None>		C:\Voice Recording\Door Held Open.wav
Door Closed	Log And Display	99	<None>		
Door Supervisory Fault	Alarm	10	<None>		
Request To Exit	Disregard	99	<None>		
Request To Exit - Host Initiated	Disregard	99	<None>		
User Command Executed	Log Only	99	<None>		
User Command Not Allowed at	Log Only	99	<None>		
User Command Not Authorized	Log Only	99	<None>		
Invalid User Command	Log Only	99	<None>		

Default Map when Reader in Alarm: <None>

□ Automatically Show Map

□ Require Secure Condition Before Alarm Clear

Figure 1: As shown on this screen from RS2's Access It!®Universal software, users can substitute a .wav file of a voice recording in place of a standard Windows® tone.

Graphical Maps

Interactive graphical maps are quite possibly one of the most useful but most underutilized features in access control systems. While some access control manufacturers charge extra for maps, they are included in the base price of higher-end systems. Interactive maps give operators full functional control of the entire access control system through the use of dynamic device and alarm icons displayed on graphical map screens. The best systems use dynamic color graphics and fully scalable alarm presentation with automatic zoom. Operators use these maps to acknowledge and clear alarms in the exact same way that they would at the device or alarm level. The maps in such systems have full drill-down capabilities to allow precise location of alarms as well as full control of all the cameras shown on the map.

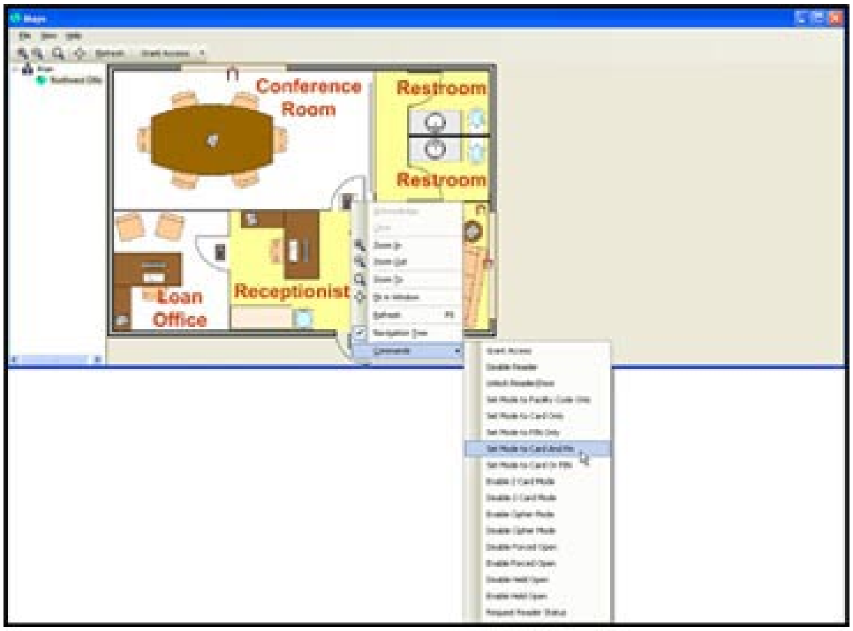
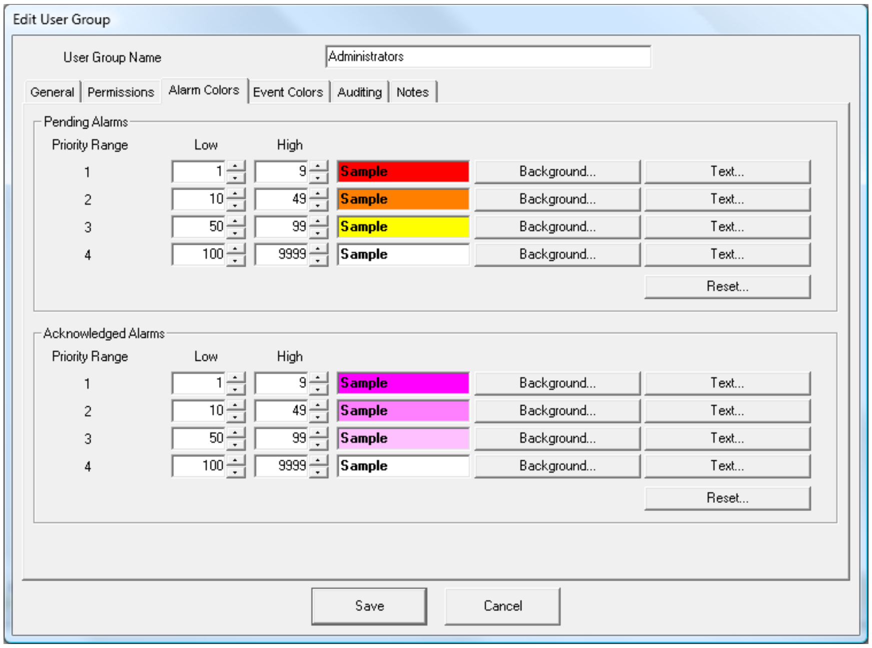


Figure 2: Interactive graphical maps are among the most useful underutilized tools in access control systems.

Conversely, users who have no intention of ever monitoring and managing the alarms in their system should think twice before paying for this feature if they are buying systems sold by manufacturers who offer it only as an option – at an added cost. Similarly, they should not let the SI (Systems Integrator) spec it into the system if they're not going to use it. Some SIs will do this because they also charge fees for doing the set-up that is required to tie the maps into the system.

Definable Event/Alarm Colors

This requires little, if any, explanation; it's just a nifty little feature that, as illustrated in Figure 3 below, makes the identification of events and alarms easier and more manageable.



Edit User Group

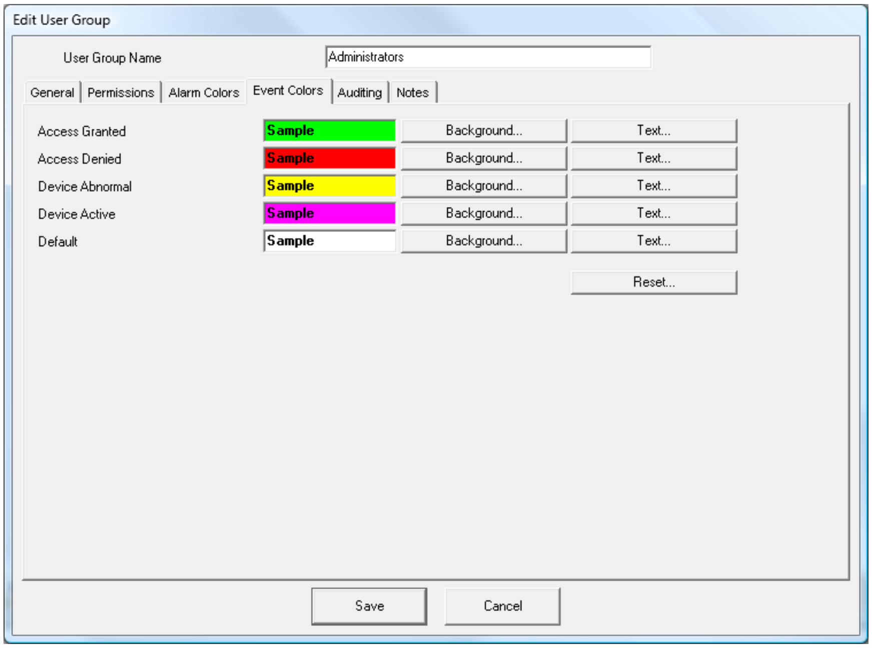
User Group Name: Administrators

Pending Alarms

Priority Range	Low	High	
1	1	9	Sample
2	10	49	Sample
3	50	99	Sample
4	100	9999	Sample

Acknowledged Alarms

Priority Range	Low	High	
1	1	9	Sample
2	10	49	Sample
3	50	99	Sample
4	100	9999	Sample



Edit User Group

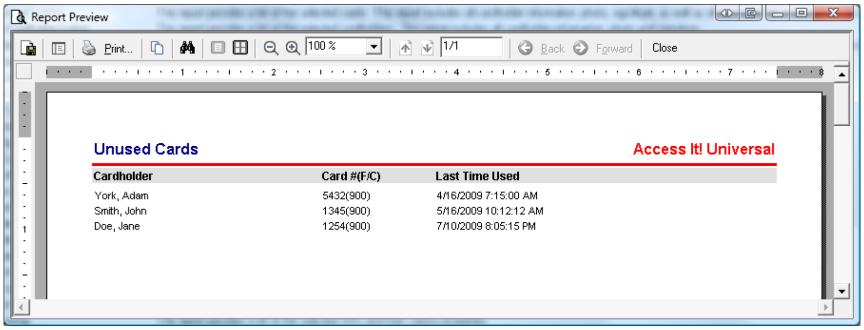
User Group Name: Administrators

Access Granted	Sample
Access Denied	Sample
Device Abnormal	Sample
Device Active	Sample
Default	Sample

Figure 3: As shown on these screen from RS2's Access It!® Universal software, users can color code alarms or events to indicate priority, importance, or some other criterion.

System Management and Reporting Features

The best access control systems typically have a very powerful array of system management and reporting features. Unfortunately, many of these features go unused. A typical example, says Dave Barnard, RS2 Technologies' Director of Dealer Development, is the Inactive/Unused Cards Report, a very simple report (see Figure 4 below) to set up and run, but one that many users never run unless they are in a business (banking, health care, etc.) where they are required by statute or Federal regulation (Sarbanes-Oxley, HIPAA, FIPS, etc.) to do so. "Everybody should run it at least once a year," says Barnard, "and quarterly would be better."



Unused Cards

Access It! Universal

Cardholder	Card #(F/C)	Last Time Used
York, Adam	5432(900)	4/16/2009 7:15:00 AM
Smith, John	1345(900)	5/16/2009 10:12:12 AM
Doe, Jane	1254(900)	7/10/2009 8:05:15 PM

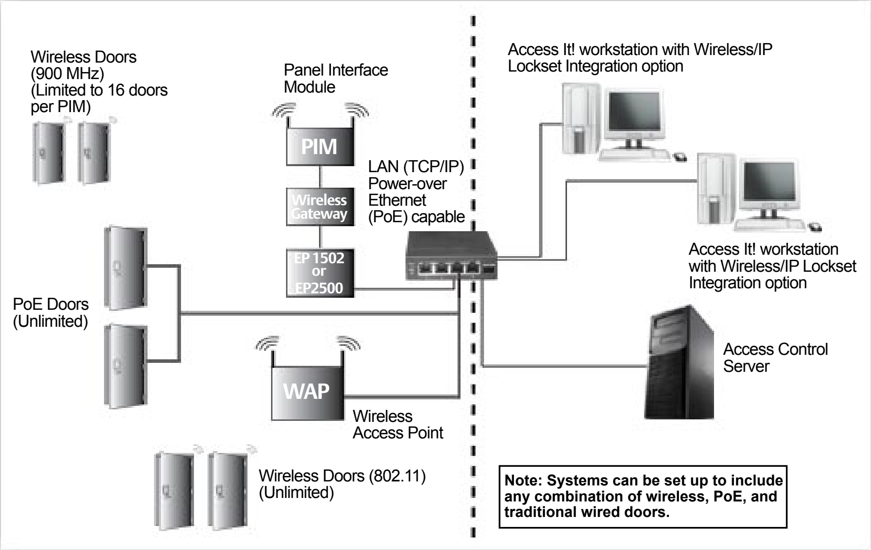
Figure 4: Inactive/Unused Cards Report.

Another underutilized management/reporting feature is the use of e-mail to automatically notify users when certain alarms occur (for example, security managers might want to be notified whenever a "Door Forced Open" alarm occurs anywhere in the system) and also to set up scheduled reports to be automatically e-mailed to certain users. Scheduled reports can be e-mailed monthly, weekly, or even daily. This feature is one that many users are originally excited about, but then never implement. This happens because it requires that someone be assigned to the initial set-up responsibility, which frequently doesn't happen. However, users that have taken the time to implement the feature are generally glad that they did.

New/Changing Technologies

The examples of underutilized features on the preceding pages generally fall into the category of features that have been available for at least a few years. However, new feature sets are constantly being added as a result of continuing development by access control manufacturers. One of the more interesting –and useful– features to come along in recent years has been the ability of access control systems to integrate with wireless, IP, and PoE (Power-over-Ethernet) locksets. This feature allows 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. The cost reduction is a result of 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


Wireless Doors (900 MHz) (Limited to 16 doors per PIM)
Panel Interface Module
PIM
Wireless Gateway
EP 1502 or EP2500
LAN (TCP/IP) Power-over Ethernet (PoE) capable
PoE Doors (Unlimited)
WAP
Wireless Access Point
Wireless Doors (802.11) (Unlimited)
Access It! workstation with Wireless/IP Lockset Integration option
Access It! workstation with Wireless/IP Lockset Integration option
Access Control Server

Note: Systems can be set up to include any combination of wireless, PoE, and traditional wired doors.

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.

Because of the relative newness of this feature, it would not be fair to characterize this as a "typically underutilized" feature, but it illuminates an important point. Users who have access control system needs that are not being met –such as controlling hard-to-reach doors– should check with the systems integrator that installed their system. In fact, top-notch SIs will proactively keep their customers abreast of changing technologies that could benefit them. (For a detailed treatment of wireless/IP and other integration, see our May 2009 White Paper entitled "Integration in Access Control Systems." See footnote number 1 on page 3 for details on how to obtain this White Paper.)

Top-notch SIs will proactively keep their customers abreast of changing technologies that could benefit them.

Bill Zalud, writing in the September 2009 issue of *SDM Magazine*, makes this very point. "For some system integrators and security dealers, innovation and new technology coming over the horizon may seem like a threatening gang to avoid." Zalud goes on to quote John Centofanti of Panasonic Systems Solutions: "In an age of corporate downsizing and budget tightening, it is much less likely that a security client, whether existing or new, will be able to keep up with technology innovation. Therefore, they will be depending more than ever on the dealer and integrator community to educate them on the new technologies and how they can be integrated into a business solution." Zalud closes his extensive article by again quoting Centofanti: "The customer relationship needs to evolve beyond that of buyer and seller to a higher level of trust and cooperation. By necessity, users will look to integrators for technology information, and smart integrators will provide it in a way to add value in a crowded marketplace."[5]

In summary, there is a tremendous amount of capability in today's access control software, including the ability to automate processes such as turning on/off alarm systems, auto-generating reports, e-mailing reports, etc., and that capability is expanding every year. Even the most qualified installers and systems integrators sometimes can't or don't get around to making their customers aware of this capability, so savvy customers need to just ask.

[5] "Game Changers", SDM Magazine, September 2009, Bill Zalud. © 2009 SDM Magazine.

Maximizing System Value Through Integration

The second major type of underutilization occurs when an end user makes a considerable investment in installing an access control system and also spends money on a sub-system, but does not spend the comparatively few extra dollars required to integrate the two systems. While this can occur with any sub-system (intrusion detection, intercom, visitor management, etc.), the most striking example is when end users invest in an access control system and a DVR- or NVR-based video system, and then opt not to make the small extra investment to integrate the two systems – and reap the considerable benefits of doing so.

What are those benefits? In a nutshell, integration of the access control and video systems allows the user to manage both systems through a single GUI (Graphical User Interface). When the access control and DVR/NVR systems are integrated, users are able to perform many of the same functions as with the CCTV system (i.e., PTZ camera control, live camera view on demand, etc.) (see Figure 6), 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 (see Figure 7), simple GUI 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.

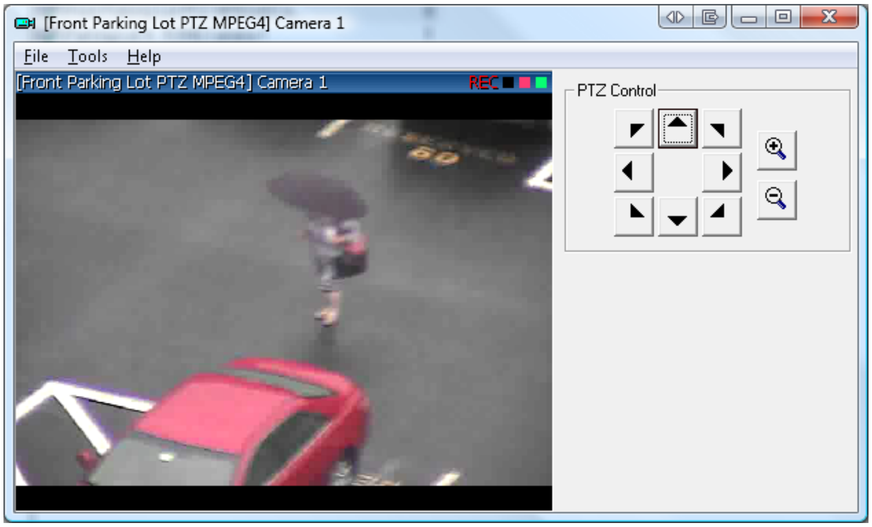
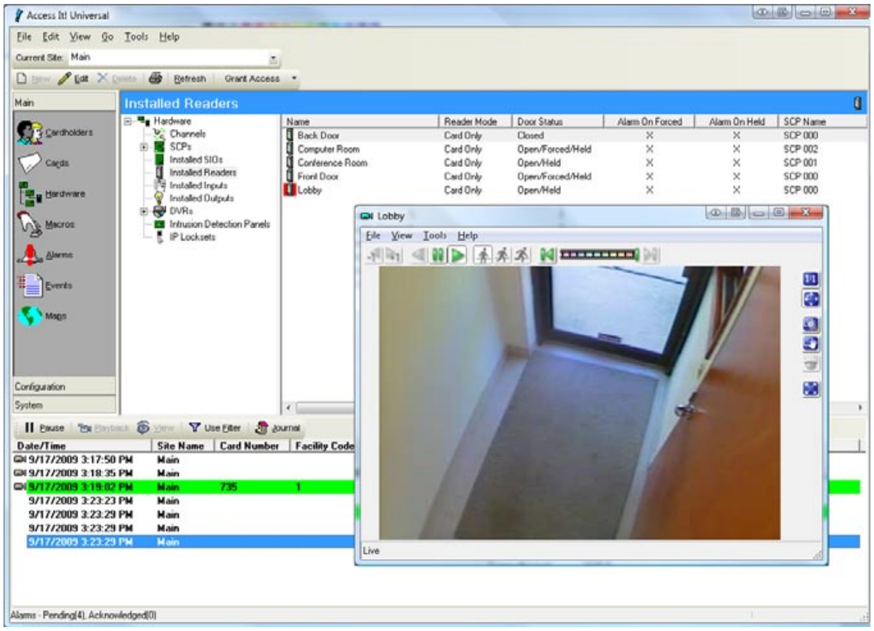

[Front Parking Lot PTZ MPEG4] Camera 1
File
Tools
Help
[Front Parking Lot PTZ MPEG4] Camera 1
REC
PTZ Control

Figure 6: By integrating access control and video, users are able to perform many of the same functions as with the CCTV system (i.e., PTZ camera control, live camera view on demand, etc.).

Let's take the example of a user who is trying to find the video recording of a particular event. Without integration, the security officer has to review the event report and cross-reference it to the video list by manually typing in the event time and camera number. Reviewing 40 or 50 events can take as much as 2 hours in an unintegrated system, even if no input mistakes are made. The chance for errors is substantial. Conversely, in an integrated system, the same review (40-50 events) will typically take 15-20 minutes. This is possible because, in a high-end system such as such as RS2's Access It!® Universal, when you run an event report, there is a hot link from the event to the corresponding point in the video recording.



Name	Reader Mode	Door Status	Alarm On Forced	Alarm On Held	SCP Name
Back Door	Card Only	Closed	X	X	SCP 000
Computer Room	Card Only	Open/Forced/Held	X	X	SCP 002
Conference Room	Card Only	Open/Held	X	X	SCP 001
Front Door	Card Only	Open/Forced/Held	X	X	SCP 000
Lobby	Card Only	Open/Held	X	X	SCP 000

Date/Time	Site Name	Card Number	Facility Code
9/17/2009 3:17:50 PM	Main		
9/17/2009 3:18:35 PM	Main		
9/17/2009 3:19:02 PM	Main	735	1
9/17/2009 3:23:23 PM	Main		
9/17/2009 3:23:29 PM	Main		
9/17/2009 3:23:29 PM	Main		
9/17/2009 3:23:29 PM	Main		

Alarms - Pending(4), Acknowledged(0)

Figure 7: This screen illustrates the hot link from the event in the event report to the corresponding point in the video recording.

The benefits are obvious, but what is the cost? In an access control system covering 30 doors with a CCTV and DVR/NVR system comprising 12-15 cameras, the access control system cost would be approximately $90,000, while the video system cost be approximate $25,000. The additional cost to integrate the two systems? Approximately $3,000, making the additional utilization exponential for the small added cost. In smaller systems, the integration cost as a percentage to the initial investment is similar – generally on the order of 3-4%.

In the paragraph on New/Changing Technologies, we emphasized that new feature sets are constantly being added as a result of continuing development by access control manufacturers. Video – and the analytics associated with it – is the best example of this development. It is certainly the fastest-developing area that is integrating with access control. New developments are allowing 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.

Questions to Ask Access Control Manufacturers and Systems Integrators

As in our previous White Papers, we offer a list of questions that purchasers and existing users of access control systems should ask the manufacturers of those systems – in relation to the underutilization of their systems. And, because this White Paper (similar to our White Paper on Integration) deals with the role of the systems integrator in helping customers achieve the best utilization of their access control systems, we have included a short list of questions that should be posed to systems integrators. Like all such lists, this list is not all-inclusive, but a good basic set of questions would include:

Questions for Access Control Manufacturers:

- **What is your policy on charging for "client seats"?**
- **Do you charge for Software Maintenance Agreements? If so, are they coupled to each client seat?**
- **Can you provide a list of all the features (such as use of sound files, graphical maps, etc.) that we are paying for in the base cost of the system?**
- **Will your system cost-effectively integrate with video and other sub-systems?**
- **Do your dealers have a good working knowledge of all the built-in features of your system?**
- **Can you provide a list of such dealers and integrators in our area?**
- **Can you provide references to customers who utilize all or most of the features in your system?**

Questions for Systems Integrators:

- **How many "client seats" do we really need? Can one or more be shared by some of our employees who only need occasional access to the system?**
- **Can/Will you make a recommendation on which doors in our facility should be wired (and have the applicable hardware) for true door monitoring? Can you provide separate cost estimates for cabling and door hardware such as door contacts and REX devices?**
- **Are you fully knowledgeable about all the features of the access control system that you are recommending?**
- **Can you provide training on all those features so that we can fully utilize the system?**
- **What is the additional cost to integrate my access control system with my video system?**
- **Can/Will you keep us fully apprised of new/changing technologies that might address any of my current or future access control needs?**
- **If applicable to the project: Do you have personnel who have Wireless/IP/PoE knowledge and installation experience?**

For a list of other general questions for systems integrators, see "The Integrator Relationship", in the April 2009 issue of *Security* Magazine.

Conclusions

Much too frequently, users of access control systems do not get full utilization of their systems – and therefore do not get their money's worth – for a variety of reasons, some of which have been detailed in this White Paper. The position of RS2 Technologies is that customers should be savvy consumers. They should practice due diligence, especially before, but also after, they purchase their systems. They should make every effort to acquaint themselves with the features of their access control system, and should use as many of these features as is feasible – if only on a trial basis – and then decide which features make sense to implement on a permanent basis. (Our Regional Sales Managers call this approach "What You Buy, What You Try, and What You Apply.")

End users who are contemplating the purchase and installation of new access control systems (or the expansion of their existing systems) should ask manufacturers and systems integrators – at a minimum – the questions outlined in this White Paper. They should make sure that their systems integrator is knowledgeable about every feature of the system(s) that the SI represents and, after installation, they should make sure that the SI is keeping them abreast of all new technological developments relating to access control systems.

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:

RS2 Technologies, LLC
877.682.3532
inquiry@rs2tech.com