Open Architecture in Access Control Systems

Why Open Systems Are Better Than Proprietary Systems

An RS2 Technologies White Paper

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

Open Architecture in Access Control Systems

Why Open Systems Are Better Than Proprietary Systems

Table of Contents

Executive Summary

In the initial paper of the RS2 White Paper series, which dealt with Total Cost of Ownership of Access Control Systems[1], we listed a series of questions that purchasers of Access Control Systems should ask prospective vendors. The first question on that list was "Does your system use 'open architecture' hardware?" The reason for that is that RS2 Technologies firmly believes that a good Access Control System is built on the cornerstone of open architecture hardware **and** software.

This White Paper endeavors to provide a useful definition of open architecture, discusses the pros and cons of open vs. closed systems, and briefly examines the history of the open architecture debate. Readers are then encouraged to apply the conclusions about the benefits of open architecture to their evaluations of access control systems.

What is Open Architecture?

What is open architecture as it relates to access control? Ten years ago, if you were to look up "open" and "architecture" in the print edition of the Merriam-Webster Dictionary, you would find "open" defined as "having no enclosing or defining barrier; accessible on nearly all sides" and "not restricted to a particular group or category of participants." The same edition defined "architecture" as "a style of construction." Today, if you look up the same words in Merriam-Webster's online edition, while you would still find those definitions among the several listed, you would also find (for "open") "not proprietary; available to third party developers" and (for "architecture") "the manner in which the components of a computer or computer system are organized and integrated."

The dictionary defines "open" as "not proprietary; available to third party developers."

What a difference a decade makes.

The concept of open architecture goes back more than twenty years, not necessarily starting with – but certainly popularized by – the IBM PC. In fact, in today's "PC compatible" world, only those among us with a few gray hairs can recall the days of closed-architecture computers. (Anybody remember the Amiga 500?) And yet, the days when companies that made "IBM compatible" peripherals had to actually go to court and sue for the right to sell these products are not so distant that they can't serve to provide lessons for today's purchasers of Access Control Systems.

[1] A copy of the RS2 White Paper "Total Cost of Ownership of 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.

For the purposes of this White Paper, we will use the term "open architecture" in the broadest sense, where it applies not only to hardware, but also to software and general interoperability, i.e., to the ability of Access Control Systems to integrate with a wide range of other security devices **manufactured by several different manufacturers**. This should not be confused with a discussion of "open source" software or "open systems" computing with all their various ramifications.

Open Architecture Hardware

Quite simply, open architecture hardware is the first critical step in an open Access Control System – it drives the rest of the system. Open architecture systems use widely available hardware platforms that allow end users to utilize equipment from a variety of different manufacturers. RS2 Technologies uses hardware manufactured by Mercury Security Systems. Mercury was an early pioneer of open architecture hardware. A February, 1999 article[2] in *Access Control and Security Systems* magazine stated, "On the hardware side, Mercury Security is one of the few manufacturers developing open technology components." The article went on to list Siemens Technologies and Hirsch Electronics as additional examples of open architecture hardware manufacturers. Since that time, other hardware manufacturers (e.g., Northern Computers, NCS, ITI) have adopted the open architecture concept.

Quite simply, open architecture hardware is the first critical step in an open Access Control System – it drives the rest of the system.

At one time, RS2 did, in fact, work with other hardware manufacturers, but after working with Mercury, decided to standardize on that platform because of the advantages it offered to end users. Today, Mercury Security is the largest manufacturer of open architecture hardware in the United States.

As pointed out in the White Paper on Total Cost of Ownership, it is important for end users to be aware that, while many Access Control System manufacturers use Mercury hardware, not all of them write software that is compatible with all three Mercury platforms. Some companies "code" only to Mercury's older SCP family, while others code only to the second-generation AP family or to Mercury's new EP series. RS2 Technologies codes to the SCP, AP, **and** EP families in order to make systems available at all price points and in a wider variety of sizes and configurations. (Note: At RS2, the AP series is referred to as the 2g – for 2nd generation.)

[2] "The Debate About Open Architecture", *Access Control and Security Systems*, February 1, 1999, Tina D'Aversa-Williams. © 1999.

A trend driving the continued evolution of open architecture access control hardware is network connectivity. According to *SDM* Magazine's September *2007 Technician's Field Guide to Access Control*, "The widespread enterprise deployment of LAN/WAN TCP/IP connectivity through client buildings has created a standardized platform for connection of all types of security devices, including surveillance cameras, access control panels, intrusion alarm panels, intercoms, and other related building sensors and controls. Using 'relay magic', any device can be connected to the LAN." [3]

Open Architecture Software

While hardware is the initial driver of an open architecture Access Control System, software is the other key link. A technical explanation of what makes open architecture software "open" is not the province of this White Paper. A layman's explanation would be that open Access Control software acts as a system manager that coordinates the interaction between the various sub-systems that are attached to the Access Control System. The system communicates with the sub-systems via dial-up, serial (e.g., RS-232 and RS-485) or network (TCP/IP, LAN, etc.) communications.

Access Control software acts as a system manager that coordinates the interaction between the sub-systems attached to the Access Control System.

A key element of coordinating that interaction is the sharing of information from the different "silos of information" which reside in the various systems and their databases. Sharing that information is accomplished through various methods, including the use of Application Programming Interfaces (APIs), Software Development Kits (SDKs), and other programming tools and protocols that help programmers connect various elements of the Access Control System. Whatever means are employed, the ultimate goal is to ensure interoperability between applications in an integrated security system.

As an ISV/Software Solutions Microsoft® Certified Partner, RS2 Technologies, along with many other Access Control System manufacturers, bases its software on Microsoft's open technology standards. For end users, this means that they can look forward to seeing the familiar Outlook® style interface when using RS2's Access It!® software, and that it will run on the widely used Microsoft SQL Server™ relational database engine.

[3] Technician's Field Guide to Access Control, SDM Magazine, September, 2007, David J. Engebretson. © 2007 SDM Magazine.

The Benefits of Open Architecture

Any list of the benefits of an open architecture approach to Access Control Systems will be incomplete, as end users are constantly finding new reasons to purchase systems based on open architecture. However, a **basic** list of benefits would include the following:

- Ease of installation
- Lower TCO (Total Cost of Ownership)
- Ease of scalability and multinational application
- Elimination of "vendor lock-in"
- Ease of integration

More expansive lists include benefits such as "ease of communication on networks" and "streamlined network/systems management," but these are largely derivative of the above.

Ease of installation: Open architecture systems are easier for security systems dealers and integrators to install because, usually, they are being paired up with some existing system components such as card readers and electronic locks. And, generally, open systems do not require new cabling (or, when required, it is minimal).

Lower TCO (Total Cost of Ownership): Lower TCO is a combination of several factors, such as lower cost of integration and lower cost of upgrades. In terms of integration, true open architecture systems will integrate with the peripherals of almost any reputable security industry OEM (see below and also in the section on "Open Architecture as the Cornerstone of Integration."). Generally, upgrades are easier and much less expensive with open architecture systems because it is not necessary for end users to scrap their previous investment when attempting to "graft" new technology onto their systems. This allows users to practice what one IP video manufacturer calls "future proofing" in their White Paper on IP Video Surveillance [4], in which they state that open platforms "make additions and replacements easier and less expensive down the line." They also say, "More future proofing comes with the potential to add new applications that become available in the future."

Ease of scalability and multinational application: Scalability is a companion concept to upgrading (above), but does not necessarily involve the adoption of new technology. Growing companies frequently find that the two-door or three-door "starter" system that they purchased from ABC Company is not compatible with the enterprise-level system that they now plan to purchase from XYZ

[4] "Keeping Watch on the City", a Milestone White Paper, by Eric Fullerton and Søren E. Kannov. © 2008 Milestone Systems, Inc.

Company. With open architecture Access Control Systems, this concern is largely eliminated, although end users still need to pay attention to whether their vendor offers Software Upgrade programs. (RS2 offers a Software Upgrade (SU) program that allows customers to move up from one software level to the next as their Access Control System grows, and to receive **full credit** for their previous investment.)

Open architecture also facilitates the multinational application of access control systems, which is increasingly important in today's global business environment. Multinational companies have found that open architecture has allowed them to utilize existing hardware (such as card readers) when installing systems in their branches and offices from Chicago to China.[5]

Elimination of "vendor lock-in": ("Vendor lock-in" is discussed in detail in the following section, "The Problem(s) with Proprietary Systems.") In a June, 2008 article in SDM Magazine[6], RS2 National Sales Director Gary Staley points out that open-architecture systems protect end users against the ultimate vendor lock-in, which would occur if the manufacturer of their Access Control System goes out of business. "If I am a building owner looking to put in access control, knowing what I know about the industry, I would only select a product that is based on open architecture – not lock into one supplier. Our systems code to a platform that 20 other U.S. companies use. If we were to go away tomorrow, 19 other companies could talk to our systems." Staley's point is a key one and gives a whole new meaning to "redundant back-up."

End users are constantly finding new reasons to purchase systems based on open architecture.

Ease of integration: (Integration is discussed in detail in the section on "Open Architecture as the Cornerstone of Integration.") In the same *SDM* article referenced above, Brent Franklin, president of Systems Integrator Unlimited Technology, makes the point that open architecture systems can be very beneficial when companies merge and two or three systems need to be "brought together." Franklin observes that, "One of the things that has happened in these days of mergers and acquisitions is that you have all these different platforms. What you end up doing is looking for a command-and-control product that can bring these together so that they look synonymous with each other, without having to replace the whole system."

[5] "RS2 Technologies Expands Global Presence with Installations and Dealers in Europe, India, and South America", press release, December 2007.

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

The Problem(s) with Proprietary Systems

The antonym of "open" is "closed," and in Access Control, closed systems are usually referred to as "proprietary systems." Loosely defined, proprietary Access Control Systems are systems in which the manufacturer has restricted compatibility with other hardware, software, peripherals, and "downstream" third-party systems such as video, intercom, CCTV, intrusion detection, etc. This is done by making the hardware or software – and usually both – incompatible with other manufacturers' products. The "how" is pretty simple. The bigger issue is "why." If open architecture systems make so much sense, why isn't **everybody** on board? i.e., why do some Access Control System manufacturers insist on making their products proprietary?

The answer lies in an explanation of what is known primarily as **"vendor lock-in,"** sometimes also referred to as "customer for life" (which ultimately – and ironically – seldom happens). Another term for the concept is "the razor & blade" model, although that has limited application in the Access Control market. The classic "vendor lock-in" business model makes a customer dependent on a vendor for products and services, unable to use another vendor without substantial switching costs. Vendor lock-in is referred to as "customer for life" when the vendor that is using lock-in techniques calculates that a customer's switching costs are so prohibitive that they will **never** switch to another vendor. In earlier years, this was particularly true in the Access Control industry, as switching costs could include not only the basic system hardware and operating software, but also card readers (and cards), cabling, and in some particularly egregious examples, even the computers that house the system.

Why do some manufacturers still make their products proprietary? To make their customers completely dependent on them for all other Access Control products.

The "razor & blade" model, while not particularly widespread in the Access Control industry, does come into play in some instances. "Razor & blade" is aptly named after the practice used by many razor blade companies, in which the initial razor is relatively inexpensive (even, in some cases, free), but the replacement blades – which are **proprietary** to the razor – are expensive. In the Access Control industry, this happens when manufacturers design **their** systems around proprietary card readers which will only read their cards, which can sell for several dollars more per card than the equivalent card used in an open architecture system. (And, as bad as that sounds for a single card, multiply that difference by the 35,000 - 40,000 cards that are used in the Access Control System of a major company or university and you will see how quickly the costs of proprietary systems add up.)[7]

[7] At the University of Pittsburgh, which uses an RS2 system, there are more than 36,000 cards in use (25,000 students and over 11,000 employees). To read more about how Pitt used the open architecture concept to preserve their existing investment in hardware and cards, call 877- 682-3532 and ask for a copy of the July, 2007 *Security Management* article "Campus Access Controlled."

RS2 systems are compatible with the entire spectrum of card technologies (magnetic stripe, proximity, smart card and multi-technology cards, etc.) manufactured by firms such as HID, AWID, Integral Engineering, Farpointe Data, XceedID, and others. Additionally, RS2 and other vendors who embrace the open architecture concept support wireless and biometric recognition solutions.

Are there ever any instances where vendor lock-in is a good thing? Not really, but sometimes it is not vendor lock-in, but simply popularity and very large installed bases that make technologies "industry standards." Examples would be the Wiegand and clock/data standards for data signaling. While significantly different from each other, both are so widely used that each has become a standard. Similarly, a case could be made that the world of Microsoft software (starting initially with DOS and then with Windows and NT) is so broad, so deep, and so functional that, when combined with Microsoft's enormous market share, it has become "locked in" as the de facto industry standard, as evidenced by its almost universal acceptance by Independent Software Vendors. (As previously mentioned, RS2 Technologies is an ISV/ Software Solutions Microsoft Certified Partner.)

Open Architecture as the Cornerstone of Integration

Over the past several years, integration has become the buzzword of the Access Control industry – and justifiably so. Integration among the products of the ever-increasing number of vendors in the security industry has been one of the most positive developments in the industry. The subject of integration is broad enough that we will treat it in depth in a future RS2 White Paper, but for the purposes of this paper, we will deal only with its relationship to open architecture. In a nutshell, open architecture and integration go hand in hand. Integration is not possible without open architecture – the latter is an absolute prerequisite for a successfully integrated system.

Open architecture is an absolute prerequisite for a successfully integrated Access Control System.

End users who have purchased an Access Control System built around the open architecture concept can now build a completely integrated security system that incorporates access control, badging, visitor management, CCTV, digital or network video recording, intrusion detection, intercom, and other functions. This was not always the case. Let's look at intrusion detection as just one example of how open architecture has facilitated systems integration:

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 software such as RS2's Access It!® Universal with intrusion detection products via TCP/IP communication on the same network, end users can 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 1.)

An Integrated Access Control & Intrusion Detection System

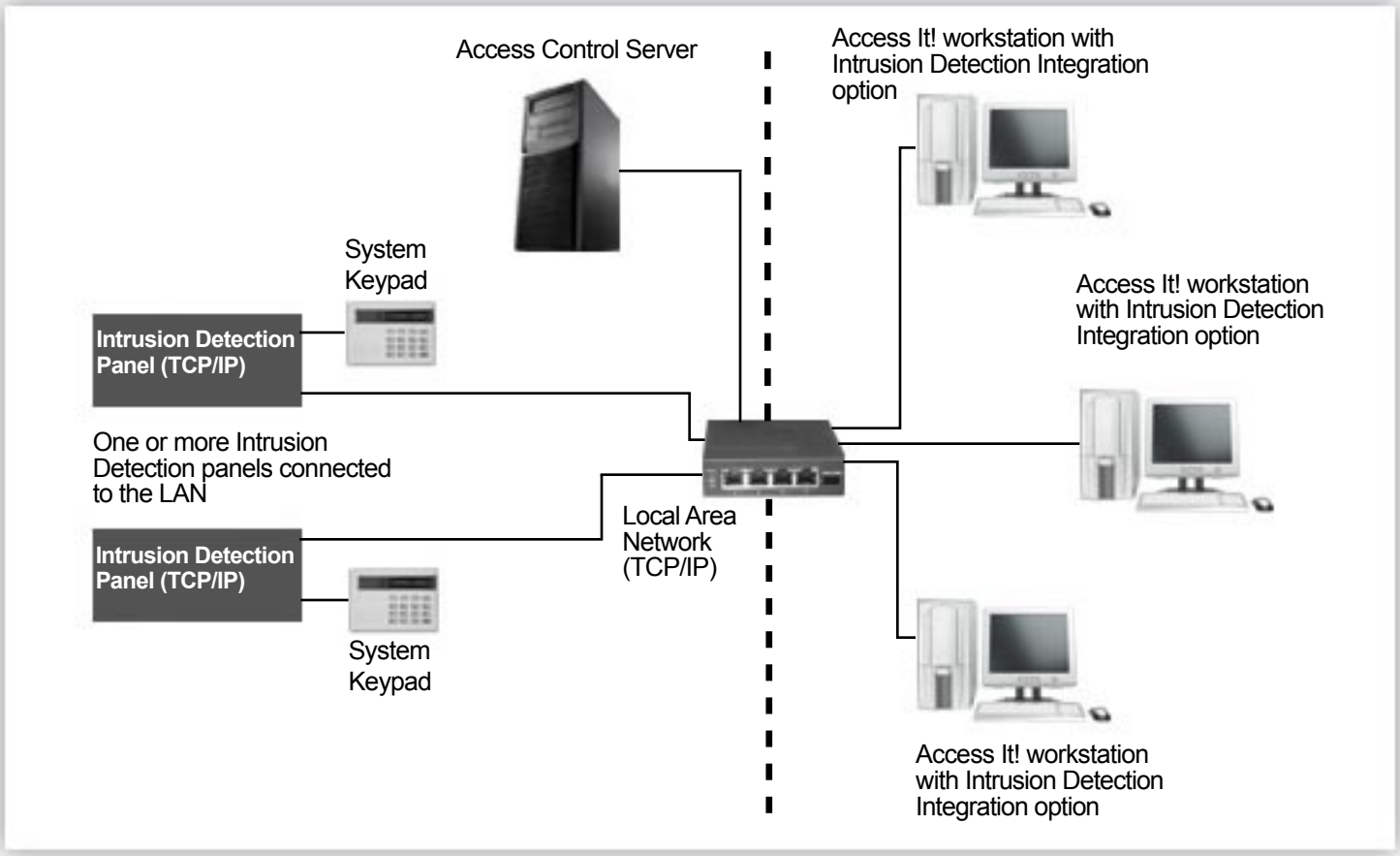

Figure 1: This diagram shows the network setup for an RS2 Access Control System that has been integrated with an intrusion detection system.

Similar examples could be given for CCTV, DVR/NVR, intercom, etc., in which functions such as camera control and connection to intercom stations are now possible using a completely integrated Access Control System. And, these are all possible only because of open architecture. (See Figure 2.)

A Completely Integrated Security System

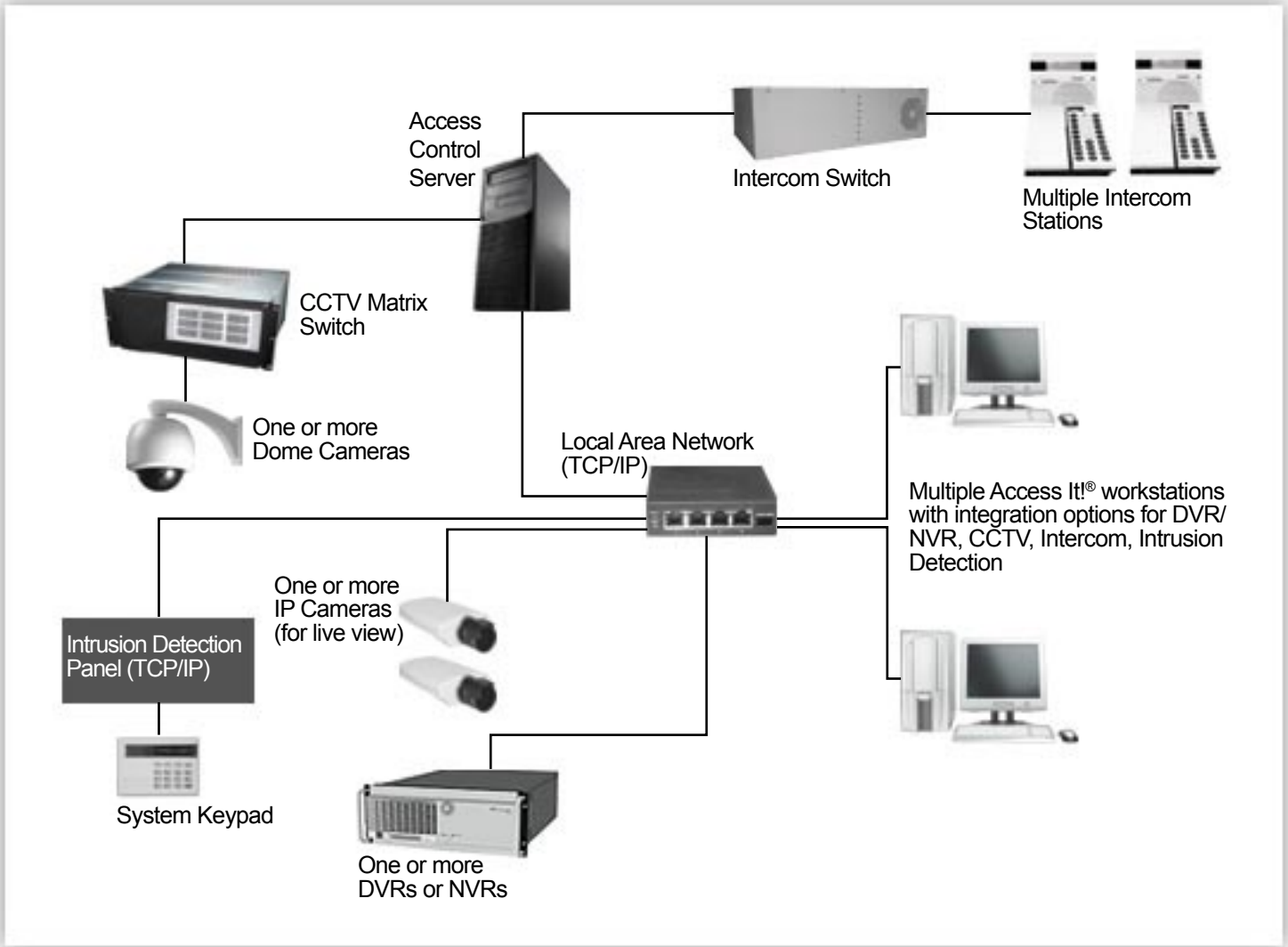

Figure 2: This diagram shows the network setup for an RS2 Access Control System that has been integrated with video surveillance, intercom, CCTV, and intrusion detection systems.

Questions to Ask Vendors

As in our first White Paper, we offer a list of questions that purchasers of Access Control Systems should ask vendors to determine if the system(s) that they are contemplating purchasing meet the "open architecture" test. Like all such lists, it is not all-inclusive, but a good basic list of questions would include:

- Does your system use "open architecture" hardware?
- If so, who is the manufacturer?
- Is your software written to support all generations of this manufacturer's hardware?
- Does your system use "open architecture" software?
- Does your system easily integrate with CCTV, digital or network video recording, intrusion detection, intercom, visitor management, and other security functions? (And, do you charge for these integrations?)
- Can you provide a list of the manufacturers with whom you integrate?
- Is your system compatible with the full spectrum of card technologies (i.e., magnetic stripe, proximity, smart card and multi-technology cards, etc.)?

Conclusions

Open architecture Access Control Systems have become the de facto standard by which all Access Control Systems should be judged. They reduce costs for buyers, they are easier to install and upgrade, and they facilitate multinational application and integration with other security systems and subsystems. Proprietary Access Control Systems do not. In our view, end users, dealers, System Integrators, and security consultants should insist on open architecture based systems. At the very least, they should ask Access Control System vendors the questions outlined in this White Paper, and they should also query the manufacturers of products that integrate with Access Control Systems.

When evaluated using the open architecture criteria outlined in this White Paper, RS2 Technologies Access Control Systems deliver the highest business value in the access control industry.

In March, 2008, *Electronic Engineering Times* published a special section entitled "35 People, Places and Things That Will Shape The Future."[8] One of the 35 items listed was "Open Source." After making the case for open source software, contributing writer Alexander Wolfe concludes by saying, "Clearly, open source will soon be less about discrete pieces of code and more about **a way of doing business**. . . . Further out, the technology will become so pervasive that it will no longer be referred to as 'open source'. It will simply be 'software'."

Borrowing Mr. Wolfe's thought and applying it to access control, RS2 Technologies firmly believes that, in a very few years, there will be no "open" or "proprietary" Access Control Systems. **All** Access Control Systems will be open systems.

[8] "35 People, Places and Things That Will Shape The Future", *Electronic Engineering Times Magazine*, March, 2008, Alexander Wolfe. © 2008 Electronic Engineering Times, CMP Media, LLC.

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