



SECURITY SYSTEMS NEWS

THE NEWSPAPER OF RECORD FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER

Search GO

General News

Markets

- Commercial & Systems integrators
- Fire systems Installation
- Monitoring
- Residential Systems
- Suppliers

Blogs

Editorial / Opinions

Resources

- 20 under 40
- New products
- Source Books
- SSN Digital Edition

Editorial Calendar

Media Kit

Back Issues

Subscribe

Manage my Account

Editorial / Commentary

The near-term future of access control

By Mark Isaacson - 08.2008 [email](#)

Where is access control heading in the next five years? A major trend today that will continue into the future is the convergence of access control and other security systems as network devices: components on a network. Access-control technology products will become more and more compatible with networking and other technology, taking on elements of infrastructure organizations and systems.

With that as accepted fact, here are trends you should be monitoring:

STORY CONTINUES BELOW

Advertisement

The value of standards

An important continuing trend is toward "standards-based" products. Products conforming to standards are essentially commodities. This benefits end users by providing interchangeability of parts, and the resulting competition tends to keep a cap on costs. The card and reader industry has already gone the standards route, and the market reflects these benefits to the consumer.

Access control panels are still proprietary to their specific manufacturers, but the standards-based trend is expected to apply here, too. Panels for software applications will more consistently conform to standards so a user or integrator can buy panels from one supplier and access control hardware from another supplier, and they will work together.

Networking for productivity

Networking is another productivity trend. Access control panels enabled with network productivity become part of the real devices on the network.

As a result, access control is no longer a separate system installed with separate wiring. It's a fully integrated solution that can be managed by the IT department.

ALSO IN THIS SECTION

[What ESX did right](#)

[The near-term future of access control](#)



That group is already becoming more often involved in specifications, purchase decisions and support of access control, as it is with other security systems within the organization.

The result is greater value to the end user. With security as a network component there will be no worry about separate infrastructure, wiring and service. The IT department provides the infrastructure for the security system, just as it does for the organization's communication systems.

Intelligent network devices

Separation between devices is blurring. Readers now have functionality that used to be assigned to panels, and panels may include integrated readers. Physical security devices are becoming intelligent network devices. They communicate better with each other, and they're essentially "plug-and-play" on the network. No special interfaces or special know-how are needed to make connections, resulting in a worthwhile saving of time and money and extra convenience for the end user.

Tremendous expansion of remote capability

As long as the infrastructure is in place, a WAN (wide area network) can cover the entire world. With IP connectivity, the concept of "remote" becomes a thing of the past in many applications. The security system is part of the network, and as long as the network is there, the physical security unit is there as well.

But beyond networking there is still some need to provide connectivity for remote applications where appropriate infrastructure does not exist. Manufacturers still need to provide for a true remote location, with a dial-up connection, for example. Wireless is another solution for near-distance remote capability.

Troubleshooting the network

It's important for integrators to have networking skills for the service aspect of their work as well as for system design. As the trend toward network-based connectivity continues, integrator service professionals need to work with customer IT departments, or do stand-alone troubleshooting of communication on the network.

In a parallel scenario, remote access to trusted vendors will allow the troubleshooting to be done from the integrator's or manufacturer's office, reducing service cost tremendously.

Merging and converging

In the future, access control and CCTV technology will increasingly be merged into a single solution where any event triggers real-time recording and logs the occurrence. The converging technologies provide more security from a recording point of view; the information will be more available and event management is improved. Converging cell phone/PDA technology will be used by integrators and administrators to manage the access system.

Mark Isaacson is vice president of engineering at access control manufacturer Sielox and can be reached at mark.isaacson@sielox.com.

Related

mark.isaacson@sielox.com

SECURITY SYSTEMS NEWS INFO CENTER

SOURCE BOOKS

December 2007 Biometrics & Access Control

Access as a service: Centrals see RMR potential in managing card systems for their clients...p3. Privacy and biometric The industry needs to be involved now with local, state and federal governments...p5. The growing SMB market: Enterprise systems may get the hype, but "don't go elephant hunting"...p11. Product guide...p12

The new technology of campus security

In the weeks following the Virginia Tech shooting, Security Systems News polled our readers about what might improve campus security going forward, and what hinders security, if any such obstacle exists, on U.S. campuses today. Here are the results.