

SECURITY SYSTEMS NEWS

THE BUSINESS NEWSPAPER FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER

A United Publication

Reprinted with permission from Security Systems News, copyright February 2005.

Access control on the enterprise: The new frontier

By Douglas Karp

The computer industry has been touting the benefits of the enterprise ever since LAN/WAN technology came onto the scene several years ago. The ability to tie together all the various software applications required to run a company was and remains a highly desirable IT objective. In fact, there are many organizations running enterprise-wide applications today—although I have reservations that they are doing so on a true enterprise platform. It's not that reports of the enterprise-wide systems are false; it's just that the definition of what constitutes the enterprise continues to change as new technologies evolve. A perfect example: the security industry's focus on IP-based systems integration over the past few years.

Depending on your perspective – building systems operations, information technology or security – the definition of the enterprise differs dramatically based on the applications it encompasses. In the security market for example, there is a great deal of discussion on how access control, video surveillance, intrusion and fire alarm systems can work together seamlessly and are being deployed today with a high degree of efficiency. Although a significant step in the right direction, a higher level of interaction between these systems and previously unrelated systems needs to be accomplished to achieve enterprise level performance.

WHAT IS THE ENTERPRISE?

It's important that we define the "enterprise" relative to the microcosm we

call the security industry. Our definition needs to be somewhat more limited incorporating just those security technologies most commonly deployed in large-scale facilities. They include: video surveillance systems, access control systems, intrusion alarm and fire alarm systems, as well as any primary building management systems. The key component in our definition is the ability to integrate the operations of these systems so that they truly function together.

There is a significant difference between interfacing and integrating systems. Interfacing is merely the ability to connect one system to another so that they interact with each other to perform a predetermined function. Let's look at a relatively simple example: An access control system sends a signal to a video surveillance system to reposition dome cameras and begin recording in real time, while a series of doors lock and lights are turned on in the affected areas. This is easily accomplished with today's software driven controllers, but in reality I think you'll find most facilities do not even employ this level of systems interface.

Enterprise level integration calls for a much higher level of sophistication or "intelligence." With the relatively new ability to engage communications between systems with high level serial or TCP/IP connections, software driven system controllers can share programmed commands on a single platform via

multiplexed signals across the network. Once the controllers of previously unrelated systems are integrated on a single platform, these systems can function as a single entity and not as a series of systems simply reacting to external commands.

The most significant benefits of integrating security on the enterprise level include the ability to manage all of the systems from a centralized location, or any location on the network. In addition, enterprise security systems allow for systems architecture to be distributed along several network nodes with the ability to share data between multiple systems. This is a critical concern for multi-tenant systems or companies with branches in different regional or global locations.

Another significant benefit of operating security systems on the enterprise level is that they can be configured, operated and updated continuously given the nature of the system. Once the network connection is established on the designated open platform, the entire security system's operational parameters can be changed and/or restored at moment's notice. Unlike traditional hardware-driven systems, truly integrated enterprise level security systems are limited only by the processing capabilities of the control software.

Additionally, there are numerous systems already in place that can provide "data integration" to an enterprise level security system. Examples include point-of-sale systems, elevator/escalator sys-

tems, counting devices, ticketing/token machines, gaming and vending machines. By integrating shared data from these systems and providing a common interface capable of "mining" the database, specific events can be readily identified.

THE NEW FRONTIER

The question is: how do we as an industry achieve true enterprise level security systems operation? First, it is imperative to select the system technology that will serve as the platform for your enterprise level security system. The key selection criterion in making this decision should be the ability to provide the open architecture necessary to integrate all of the technologies that will comprise your specific system.

Now that video systems have joined access control systems on a digital platform, access control systems are the logical choice for system control and integration given the scalability and virtual unlimited expansion capabilities these systems offer. You'll also need to have a secure network in place with sufficient bandwidth to handle the signal capacities required for true enterprise-level integration. Fiber optics may hold the key given the virtual unlimited bandwidth they provide. Given the progression of technology over the past 20 years, the migration to enterprise level security systems may be a lot closer in our future than we thought.

Douglas Karp is general manager of the ID Products Group for Checkpoint Systems, Inc. He can be reached via email at douglas.karp@checkpt.com. SSN

