

In Enterprise Environments

By Douglas Karp, Contributing Writer

Depending on the end user's perspective – building systems operations, IT or security – the definition of “enterprise” differs dramatically based on the applications it encompasses. In the security market, for example, there is a great deal of emphasis 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 true enterprise-level performance.

It is important that “enterprise” be defined relative to the microcosm of the security industry. Its definition needs to be somewhat limited, incorporating just those event management systems most commonly deployed in large-scale facilities. They include: video surveillance, access control, intrusion alarm and fire alarm systems, as well as any primary building management systems (elevator alarms, HVAC, lighting, etc.). The key component in this definition is the ability

to integrate the operations of these systems so that they truly function as one.

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 most facilities do not even

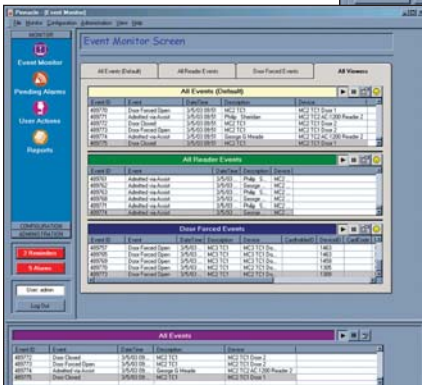
tem controllers can share programmed commands on a single platform via multiplexed signals across the network. Once the controllers of previously unrelated systems are integrated on a single platform, these systems can function as a single entity and not as a series of systems simply reacting to external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

Continuous upgrading

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 a moment's notice. Unlike traditional hardware-driven systems, truly integrated enterprise 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 systems, counting devices, ticketing/token machines, gaming and vending machines. By integrating shared data from these systems and providing a common interface



Above, enterprise integration calls for a more sophisticated level, including more data in cardholder screens. Left, enterprises want to track a diversity of events across a variety of buildings and locations.

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 sys-



Record Keeping...

Does yours reflect your efforts to keep your facility Safe & Secure?

It will with...

TOUR TRAX
PATROL & INCIDENT REPORTING SOLUTIONS

Guard Tour Verification & Reporting Systems

Fully networkable, multi-location solutions customized for Contract Security Providers

Rhino Rugged Hardware features the **New GUARDUS** from...

CONTRONICS

Digital Security Concepts Inc.

Toll Free...800-366-0662

www.GuardTourSystems.com

For free information circle 206 or visit www.secmag.com/webcard

Enterprise Asset Tracking, Guard Tours

When Herold Amandi, director of public safety for the Mall of the Americas in Miami, Fla, wanted to make sure security officers were making their rounds, he decided to shop for a guard tour system. He picked a system from Miami-based ProxiGuard.



Data collectors play a security officer role at enterprises.

The device holds 28,000 records in its 4Mb flash memory and is water and shock resistance.

Such data collectors come in all shapes, sizes and colors; some have bells, some have whistles, some read unique hexadecimal ID numbers, some read barcodes and some even read RFID tags. Most have a downloader and/or transfer station, a serial or USB interconnect cable and a software program.

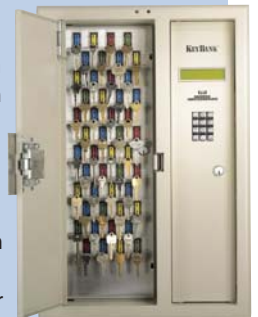
From R.E.B. Software Technology of Deming, N.M., its guard tour software uses the Videx (Corvallis, Ore.) products and iButton technology from Maxim Dallas Semiconductor (Dallas). Included with the software: activity group reports as well as lists, exception, time management and missed hits.

One data collection unit for security officers at enterprises is the DuraTrax from Videx. It has a laser barcode scanner as well as touch memory reader.

From Digital Security Concepts of Kingston, Ontario, Canada, there is TourTrax. It is designed to exceed demanding needs for accurate, timely reports and documentation of security patrols. TourTrax is a comprehensive solution for any busy security department or agency.

Some security operations seek guard tour systems that can handle harsh environments. One example: the ProxiPen from Detex of New Braunfels, Texas. ProxiPen is a proximity reader with an integral read head and a user-replaceable battery. No matter if a checkpoint is wet, frosty, dirty or painted over, the device reads RFID tags, which are available in a variety of shapes and sizes. Detex software can create tours, produce evaluation reports as well as incident reporting and guard identification.

Beyond guard tour, there are key management systems for asset tracking by officers. Oxford, Conn.-based Morse Watchmans, for example, has KeyBank III key management system for high-volume key users. It features an updated storage system with individually illuminated Smart-Key locations, allowing for instant visual identification of checked-out keys and keys available for individual user checkout. Designed as a replacement system for manual key storage and tracking, KeyBank III key management system eliminates outdated key lock boxes, hand-written checkout logs and key identification tags.



Key management systems can eliminate paper logs.

capable of "mining" the database, specific events can be readily identified.

The question is: how can the security industry achieve true enterprise-level security systems operation? First, it is imperative to select a system that will serve as the platform for the application's security and other event management needs. 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 each specific system, today and in the future.

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 virtually unlimited expansion capabilities these systems offer. The introduction of an access control system, with an embedded

software development kit, new IP capabilities and database partitioning, exemplifies the versatile programming capabilities available to systems integrators for enterprise. End users 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. With 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 previously thought. ❖

About the Author

Douglas Karp is general manager of the Access Control Products Group for Checkpoint Systems Inc., Thorofare, N.J.