

A More Perfect Union: Video and Access Control

By Ed Thompson

In this increasingly integrated, converged security world, the next step is inevitably greater unification of systems and capabilities—seamless operation back and forth between, for example, access control and IP video. When these systems are unified into one application, the benefits can be unique and far-reaching.

Integration vs. Unification

Integration means that two products work together. Unification means that a single, multi-functional application provides unified security, administration, and response. Unification goes beyond integration to foster a solutions mindset, and unified systems will have a major impact in terms of cost, efficiency, overall capabilities, and level of security.

Integrated systems require a designer or integrator to log into the separate systems to program coordinated responses to system events. Failure to program either system properly can cause inconsistent or failed responses, and because integrated systems remain separate, neither can detect the programming inconsistency and warn the user. Technical support

teams may not be able to resolve the problems efficiently because they are not aware of the inconsistencies, thus increasing the total cost of ownership and system downtime.

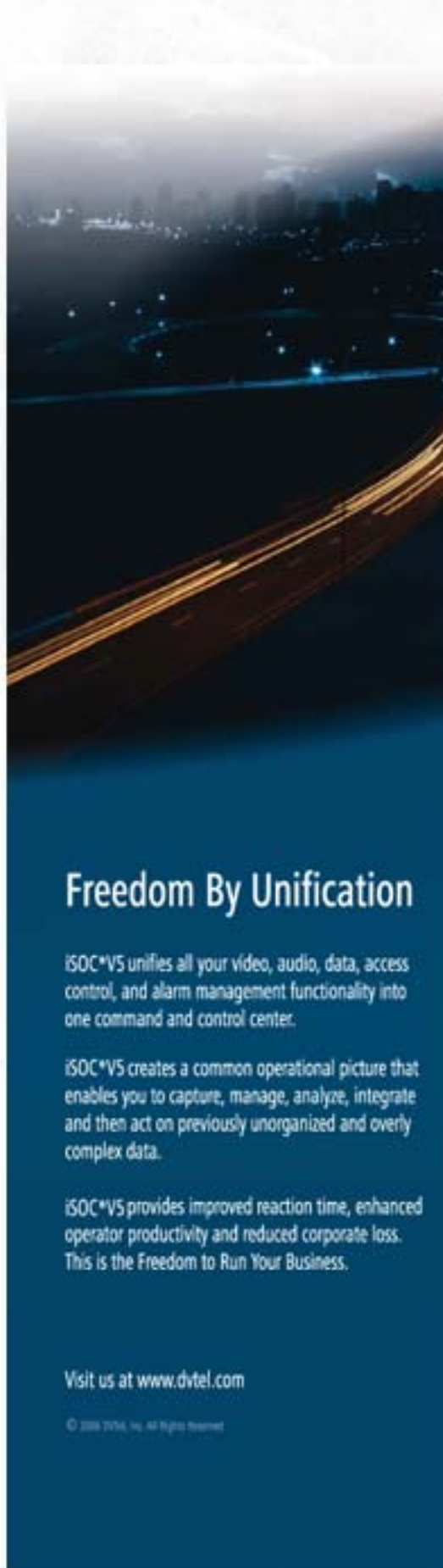
Unity brings about a higher level of availability to physical security due to access/video server consolidation and more efficient use of standard hardware, IT tools, and a shared knowledge base. In the past, cameras were hard-wired to DVRs or matrix systems, and card readers were hard-wired to access control panels and servers with serial communications. When the host failed, these hard-wired connections prevented automated failovers to standby services. In modern IP systems, failovers are automated because the underlying IP infrastructure permits hot standby services to immediately assume responsibilities for the failed components. But if communications were lost between the host and a remote site with cameras and card readers, the unified system's advantage is that the access control panel can control the cameras based on alarm events, and it can buffer video until communication has been restored.

A Smarter System

A unified system provides highly intelligent security. Because unified access control and video share a single database, they can correlate information between them. Access control anomalies can trigger video, and video anomalies—including alarms raised by intelligent video—can be used to control access. For example, if a threat is detected by video intelligence, the system can automatically secure facility entrances. A shared database also provides a single point of service and auditing for both access control and video alarms.

On a broader scale, unified systems can automatically coordinate the reaction to changing threat levels. For example, during a period of heightened facility security, the system can automatically suspend card entry and display live video of personnel requesting access. Or when an employee presents his access card, that person's personnel photo can be pulled from the database and displayed so that the guard can manually allow or deny access.

The intelligence gleaned from a unified security solution also provides



Freedom By Unification

iSOC*V5 unifies all your video, audio, data, access control, and alarm management functionality into one command and control center.

iSOC*V5 creates a common operational picture that enables you to capture, manage, analyze, integrate and then act on previously unorganized and overly complex data.

iSOC*V5 provides improved reaction time, enhanced operator productivity and reduced corporate loss. This is the Freedom to Run Your Business.

Visit us at www.dvtel.com

© 2006 DVTel, Inc. All rights reserved.

a wealth of statistics that can be used to illuminate and solve security challenges. For instance, you find that a particular door tends to remain open for an average of five seconds after a valid card read. However, a check of that door's summary activity on a given day shows three events longer than five seconds. You can click on each event to see video of what happened, or program the system to display video whenever the behavior for a door is outside the specified norm.

An IP-based, unified system also allows users to identify the whereabouts of personnel and access their identity verification data when they log into an enterprise application.

A Smooth Path for Growth

A unified system can still support integration as a means of migration from legacy systems. Such support defines a true open system for access control: a single platform from one vendor that can communicate directly with access control panels from multiple brands. In addition, IP-based distributed processing allows for modular and economical system expansion.

The unified system manufacturer ensures compatibility with consistent product versions as well as a consistent upgrade path. The video and access control versions will not fall out of sync or lose features as they might in an integrated system. Training and product support also take on a more holistic approach without requiring the end user to act as a middleman between various vendors.

Saving Trouble and Cost

When evaluating overall system design for an integrated system, one must ask, "What's missing?" or "Will component A be compatible with system B?" A unified system eliminates the research required to determine compatibility and how many functions are available in an integrated, bolted-together system. In a unified system, all functions between access and video are compatible, eliminating the need for the end user to manage version compatibility.

A unified system means one user interface. A single interface simplifies installation and is easier to learn and use. There is no more duplication of

The video and access control versions will not fall out of sync or lose features as they might in an integrated system.

system administration and other tasks. A user learns to set up a card reader using the same skills required to set up a camera. What's more, a single user login provides simple and secure access to all security functions.

Unified IP systems also provide higher availability and reduced maintenance costs by consolidating access and video, and networking issues are handled by the IT department using standard tools and practices.

The system's use of existing IP infrastructure eliminates significant wiring and installation costs. IP network nodes, including cameras and card/biometric readers, can all be managed by a corporate network management tool.

Unified system manufacturers will also have unified hardware. For example, DVTel's access panels can store video and control PTZ cameras. The system is no longer reliant on the host computers for control. This adds a level of survivability and greater efficiency, since edge devices can control both aspects of the system. Because of this architecture, IP-based distributed processing allows for modular, unlimited expansion of both access control and video based on the end user's needs and budget.

More Than Integration

Unified systems offer more than the "advanced" integrations of bolted-together components we've seen to date. They offer system openness and flexibility, enhanced efficiency, lower costs, higher functionality and improved overall security. **ST&D**



Ed Thompson is chief technical officer of DVTel.