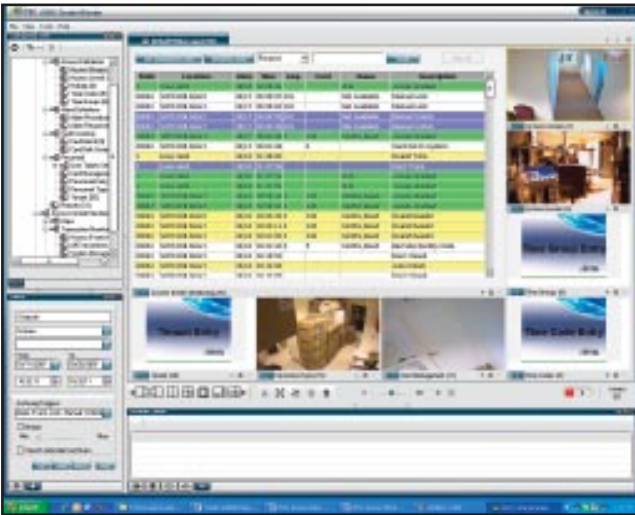


7 Myths about IP Access Control to the Door

Why IP to the door? There are considerable differences between today's legacy access control and the emerging technology of IP directly to the door. What follows are seven commonly heard myths when Security asked two industry experts what they feel is really happening in the market with respect to IP access control to the door.

MYTH 1. There is no difference between IP access control and traditional access control.

De-myth: There is a huge difference between IP and traditional or RS485 (multi-drop) in the access control world. Access control, as we have known it to date, can be compared to the video world using digital video recorders. Even though DVRs, as well as access control panels, can sit on a network, all cable to the actual edge device is traditional copper cable, proprietary to that system. Edge IP does for access control what IP cameras did for video. Software can now talk directly to the edge device with nothing but network in between. The control panel concept goes away for access control just as the



IP access can integrate with video to provide more functions and effectiveness than traditional methods.

DVR goes away for IP video. As a result, both video and access control can now be truly scalable in increments of one access point, with predictability of cost. This also results in a significant reduction in infrastructure cost as well.

IP-based distributed processing allows for modular and economical system expansion. An IP-based system supports integration as a means of migration from legacy systems and provides a cost-effective bridge to the future. The IP-to-the door system manufacturer ensures a consistent product version and consistent upgrade path.

Training and product support also take on a more holistic approach without requiring the end user to act as a middleman between various

vendors. What's more, an IP-based system ensures the latest standards-based software, networking, and hardware technology.

An IP-based system means one user interface. A single user interface simplifies installation and is easier to learn and use. With one common interface, there is no more duplication of system administration and other tasks. For example, a user learns to set up a card reader using the same skills required to set up a camera. In addition, a single user login provides simple and secure access to all security functions. 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.

Another difference between IP access control and traditional access control is the issue of power over Ethernet or PoE, which can be argued as a positive or a negative. On the positive side, most network closets already have emergency power to the network devices and they will continue to operate even when power to the building is lost, while traditional power requires battery back-up. PoE provides the same advantage to the IP access approach. The bigger issue is power to the locking device that may be required to unlock at loss of power to the building in order to meet fire code. It is more likely that installers will use PoE for the reader, but traditional power to the locking device.

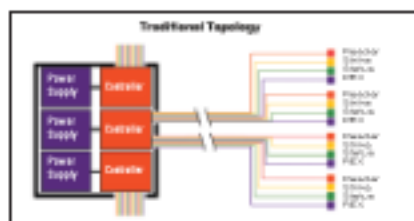
MYTH 2. IP access control is untested and unproven when compared to a traditional, hard-wired solution.

De-myth Depending on the configuration of the hardware a chief security officer selects, IP access control is as reliable, or even more reliable than the traditional topology of multi-reader controllers. With multi-door controllers, a single point of failure could cause multiple doors to become inoperable. With IP access control, each door is independent of other doors, so a single point of failure will only cause one door to be inoperable. Today's networks allow for layers of redundancy, so even if a network component fails, there are backup communications paths that can reroute the event transmissions around the problem component.

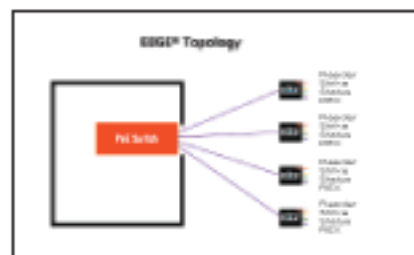
MYTH 3: IP access control is more susceptible to failure or "What happens when my network goes down?"

De-myth: In today's corporate environment, the network gets more attention and care than it used to simply because the network is carrying the information that keeps the company in business. As long as IP access still has power, the only impact of network communications failure is that the events will not be transmitted to the host application when the event occurs. The door still works and employees can still enter, with all the events being buffered. Once the network communication path is re-established, all events that took place during failure will be transmitted to the host. Communications loss is a universal problem that affects Ethernet and serially connected devices in the same way.

Keep in mind that the network rarely goes down, because it is the backbone of the entire business. One of the beauties of networked-based information is the fact that information can be rerouted in less



Traditional topology means that even though DVRs, as well as access control panels, can sit on a network, all cable to the actual edge device is traditional copper cable, proprietary to that system.



In an edge approach, IP-based distributed processing allows for modular and economical system expansion dependent on power over the Ethernet.

than 100 milliseconds by finding an alternative path. No legacy access control solution has this level of reliability.

MYTH 4: IP access control is more vulnerable to security breaches or hackers that can open doors.

De-myth: IP access control is no different than any other device on the network. Network security measures that block unauthorized access to the network (and devices) should be employed, whether it is through a local connection or virtual private network (VPN). With any Ethernet connection, care must be taken not to expose the connection in unprotected environments (like on the outside of a perimeter door). This is just good common sense. With IP access control, you have the option of separating the reader from the controller without losing any functionality, and gaining the ability to keep the network connection within the protected space.

IP access control benefits from the \$5 billion network security market which provides a powerful, secured environment that is not available to the traditional access control world.

MYTH 5: IP access control costs more and upgrading to IP access control requires a "fork lift" upgrade.

De-myth: In most cases IP access control costs less than traditional access control topologies. Cost savings occur not only in the cost of the devices themselves, but also in the cost to run and maintain the associ-

ated wiring. With traditional topologies, a bundle of cables is run from a closet out to the door. This wiring is run separately from the other communications wiring in a building and is singular in purpose. With IP access control, the wiring to the door is the same wiring used for the computers, phones, and IP cameras. Being able to combine the access control communications cable installation into a larger wiring contract leads to a lower cost per door.

In the instances where an existing access control system is in place, IP access control can be layered on top of it for new doors, which means a forklift upgrade is not always necessary.

MYTH 6: Customers sacrifice functionality when they move to an IP-based access control system.

De-myth: On the contrary, IP access control has more benefits and functionality



DVTel: IP-Based Unified Video and Access Control System

...Our Innovation.
Your Freedom.

ISOC® V5 unifies all your video, audio, data, access control, and alarm management into one IP-based 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.

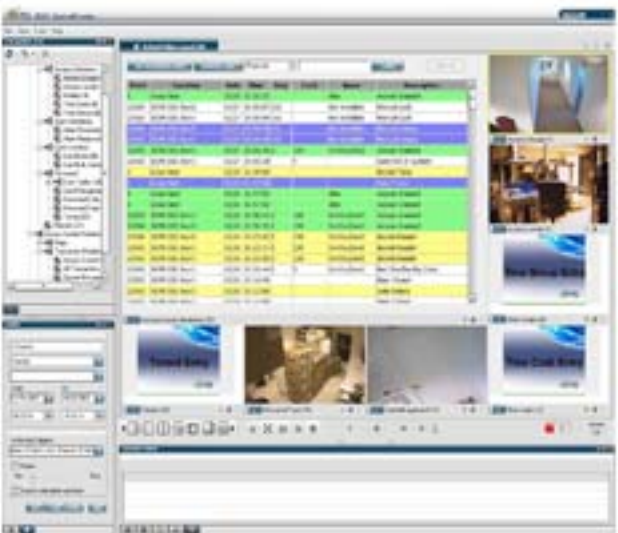
ISOC V5 provides improved reaction time, enhanced operator productivity, and reduced corporate loss.

This is the Freedom to Run Your Business.

Ranked #1 In IP Video

visit our website at www.dvtel.com





than traditional access control. Both systems use a server as a host computer and all of your features and functionality will generally be the same. However, while most traditional access control does not allow for bi-directional communications to the door, TCP/IP does such communications. Functionality like writing to smart cards and driving LCD displays is not possible with Wiegand wiring.

Predictable cost per door is another benefit of IP access control. With traditional access control using multi-door controllers, the first door is always more expensive than the second because the controller is part of the cost of the first door. With IP access control, each door gets the same components so the cost is fixed for each door. Budgeting is a simple matter of math rather than an exercise in determining where there is a spare part in a multi-door controller.

MYTH 7: Integrated systems are fine; unified systems (access control and video surveillance) are over-rated, unproven.

De-myth: Integration means only that two products work together. "Unification," on the other hand, means a single, multi-functional application with unified security, administration, log-ins, and unified responses to events along with fully coordinated failover capabilities.

In this increasingly integrated, converged security world, the next evolutionary step is inevitably greater unification of systems and capabilities – seamless operation back and forth between, for example, access control and video. If both systems are unified into one application the overall benefits to the end-user are even greater and more far-reaching than anything simple integration has provided up until now.

Unification solves many shortcomings that exist with integration: Integrated systems require logging into the separate systems to program coordinated responses to system events. Failure to program either system properly can result in unpredictable results and neither system can detect the programming inconsistency and warn the user. Technical support teams are often not able to resolve the problems efficiently because they are not aware of the inconsistencies, thus increasing the total cost of ownership and system downtime.

As long as these systems are kept separate and joined only by integration, there will always be two different road maps with two different agendas. Only when you start to think about these two applications as unified do we create true value to the end-user and the installer.

IT'S AN IP-TO-THE-DOOR FUTURE

Following a similar path or evolution as IP video, IP access control is now gaining wider market acceptance and is being implemented in some of the largest new installations worldwide as well as in retrofit installations.

In the future, unified platforms will grow into powerful solutions when combined with information security, business continuity planning and data/content analysis. When the traditional data from access control becomes highly available, usable information on the network, we will see tremendous opportunity to make employees more efficient while making the business environment safer.

SECURITY

About the Sources

Security thanks Eli Gorovici of DVTel and Tom Heiser of HID Global for the information contained in this article.