

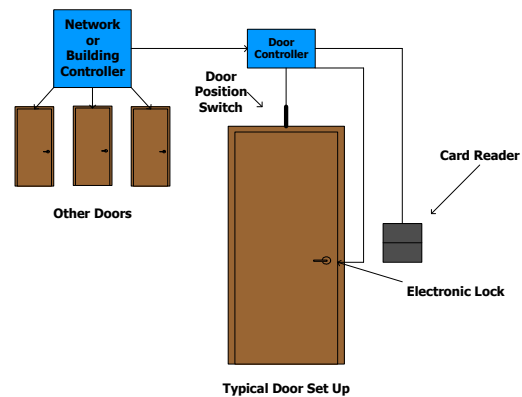
Opening the Door to IP POE-Powered Access Control Systems

Jim Sinopoli, PE, LEED AP, RCDD
Managing Principal, Smart Buildings LLC

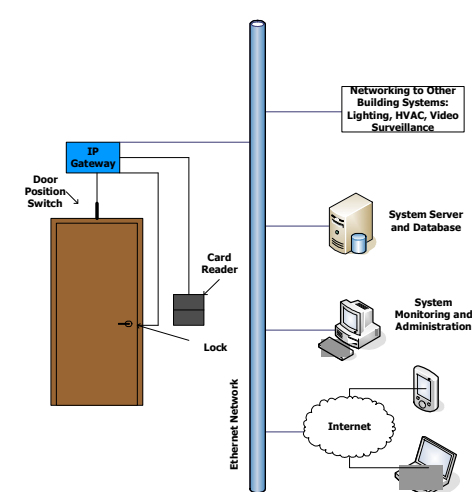
Access control systems that incorporate IP and Power-Over-Ethernet (POE) components were introduced to the marketplace almost two years ago. The evolution of access control systems to structured cabling, IP protocols and POE was inevitable; look what happen to telephone and video surveillance systems. The transformation leverages the existing IT infrastructure, eliminates the need for local power, consolidates and saves labor costs for cable installation, reduces the time to install system devices, is more scalable and provides a large base of management tools and support. The move is subtly but surely changing the design and deployment of access control systems.

Overview

In a traditional deployment of an access control system to a door, there is a door controller connected back to a network (non-IP) or building controller. (different manufacturers use different names for these devices). The door controller typically handles two card readers so it can handle one or two doors depending on whether one door is using a card reader for both entrance and exit. It controls essentially three devices, a door contact (which lets the system know if the door is open or closed), the door lock and a card reader. Above the door frame is a junction box with power that powers each of the devices. The power supply for the controller is typically providing DC power and is provided with a battery back-up.

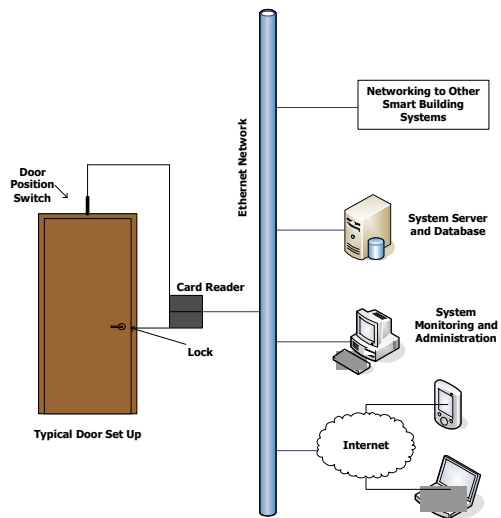


issues.



In the IP-based systems there is a direct network connection to either the door controller or the card reader, with the network connection providing low-voltage power. If the network connection is to the door controller, POE powers the door contact, the lock and the card reader. The door controller is really a gateway at the edge of the IP network, converting the data and protocols from the door devices to an IP format. For example Cisco's base entry into this market is a gateway door controller that can handle two doors. It has characteristics of typical door controllers such as the capability to buffer events or cache access credentials; features that address reliability and network performance

If the IP access control system doesn't use a door controller, the network connection is directly to the card reader, and the card reader powers the door contact and the lock. This approach not only eliminates the separate power supplies but also the door controller. An example is HID has the Edge product series, spanning not only IP door controllers but IP door controller/card readers.



Power Issues

Some of the benefits and design issues with IP access control involve the elimination of high voltage power and the use of Power-Over-Ethernet. These include:

- Power Backup** – In a traditional system backup power to door devices involves batteries and/or high voltage circuits above each door on emergency power. With the IP-access control system, if the network switches in the telecom rooms powering the IP access control system are on UPS and emergency power, which they generally are, backup power is provided in a more centralized, less costly, more manageable way. With several companies now having software application residing on a network that can monitor and manage POE devices the deployment of an IP access control systems provides more data, information and manageability of the power than a traditional access control.
- Power Sharing** - One of the critical design issues for the systems is selecting the right “power source equipment” which is either a network switch with POE capabilities or a device called a midspan, that is used with a non-POE network switch to inject power into the communication connection. The issue is really with POE network switches that “power share”, a characteristic of older POE network switches. These are switches that do not have the power capacity to supply full POE power to every port on the switch, so they “share” the power among the switch ports. The switch manufacturers figure that not every port will be needed to have POE capabilities. Here’s an example. You have a 24-port POE network switch, with a 200-watt power supply. The switch uses 50 watts to power itself and has 150 watts to provide POE to ports. With POE (IEEE802.3af) at 15.4 watts of power, only 9 of the 24 ports on the switch could be provided POE. The potential risk is that connecting an access control device to a network switch using power sharing could be the access control devices having no power. It is important to make sure the networking equipment for an access control system will provide maximum POE power to every port.

- **Power for Locks** - Although each of the devices at a door (lock, card reader, request to exit sensor, door contact, etc.) has different power requirements, the lock is typically the most demanding. A lock requiring 600mA at 12vdc or 7.2W essentially uses half the POE power. Locks are dumb devices; there are no POE or even IP locks. A mag lock for example, simply gets a power feed and locks the door when there is power and stops locking when the power is cut off. The issue is really providing the power requirements for all the door devices within the current POE standard of 15.4 watts. The yet to be ratified POE Plus standard will resolve this power “budgeting” and provide 30 watts of power. Keep in mind that “mag” locks are inherently “fail-safe” devices (if they lose power they unlock). As such, having a PoE powered reader feeding a “mag” lock could create a security issue since anyone that knows the lock is feed by the card reader and wants to get through the door can just destroy the reader to gain access. (In some cases it might be a better idea to use a fail-secure “mag” strike in order to prevent this, but that also has life safety considerations.)

Benefits

The IP and POE access control system approach has several advantages:

- **Scalability** - Instead of dealing with network or building controllers that may scale at 4 or 8 doors at a time, the IP solution scales per door.
- **Reliability** - The loss of one traditional network or building controller may take out 4-8 doors; the loss of a network connection will take out one door in the IP approach.
- **Cost** – There is considerable savings in infrastructure cost with IP systems. You eliminate the junction box above the door and the high voltage power to it, network or building controllers, and the local battery packs. The cable contractor handling the IT network or video surveillance system can now also cable for access control, thus providing less contractors to coordinate and potential savings on cabling, labor and cable pathways.
- **Integration** – The IP solution is standards-based; standards-based cable, standards-based communication protocols, and hopefully specified to have a standards-based database, all of which are integration foundations at the physical, networking and application level.
- **International Applications** - PoE is an international standard being marketed and deployed worldwide, allowing manufacturers to avoid supplying different power supply for different countries and eliminating the need for installers POE to worry about different equipment and power cords.

For more information about smart buildings, technology design or to schedule a Continuing Education program for your office write us at info@smart-buildings.com