



## Bridging IT and Security

Many physical security systems, including video surveillance and electronic access control, are being managed by a company's Information Services department. With physical security becoming more IT centric, many administrators are requiring these systems to work off the facility's existing IP infrastructure rather than using a separate RS-485 (serial) network that is difficult to manage and even harder to troubleshoot when it goes down. They want to have their physical security systems running on a platform that they understand and can easily manage.

## Network Configurations

An RS-485 network is an independent network that is deployed to each controller in the access control system. Power to the access control panels is provided by a hard-wired boxed power supply. In many cases, the power supply contains batteries as backup power in case of a primary power failure. Even in traditional analog access control systems with multidoor controllers that require all wiring to be home ran back to the panel or use a distributed architecture, communication is provided by RS485 cabling.

In response to the IP platform requirement, manufacturers have developed IP-based access control systems that integrate into the facility's

existing IP infrastructure. With a distributed architecture, single-door access control panels can be located above each door as edge controllers. These controllers make all of the access control decisions just as their analog predecessors.

Although these controllers are using the LAN to communicate with the access control server, they were still relying on traditional hardwired power supplies for power.

## Access Control with Power over Ethernet

With Power over Ethernet (PoE) powering most network appliances, many single-door access control panels now have the option to be PoE powered as well. They are using either a midspan PoE power injector or a PoE switch to provide reliable power. The infrastructure's uninterruptable power supply (UPS) is supplying backup power to the controllers.

Most PoE access control panels also supply output power to ancillary devices such as card readers, fail-secure electric strikes, electrified leversets and motion request to exit (REX) devices. However, because the controllers are being powered by PoE, the amount of amperage is limited. Most PoE controllers will publish two voltage limits: lock output power and the total power output. In most cases, the total power output for all ancillary components, including the lock power, is approximately 600 mA. This requires that every

component that is connected to a PoE controller be prescreened to determine the amperage draw so the total amperage for all components is less than the total output limits of the controller.

## Powering Access Control in Practice

For a PoE controller that has a lock output power of 500 mA and a total output power of 625 mA, an electric strike draws 450 mA, which is less than the lock output power of 500 mA. However, a reader draws 170 mA and a REX draws 50 mA. The total of all three components is 670 mA, which exceeds the total output amperage of 625 mA for the PoE controller.

Powering access control with PoE has great advantages when deploying a system; however, careful consideration needs to be taken when choosing each component in the system to make sure that it is power compatible with the PoE controller.

## Anixter Solutions

Even though technologies shift and standards change, Anixter keeps you up to date with the latest products and best practices. Anixter partners with best-in-class manufacturers to bring you the right access control products for your solutions.



**For more information, contact your local Anixter representative or visit [anixter.com](http://anixter.com)**

**About Anixter:** [anixter.com/aboutus](http://anixter.com/aboutus)  
**Legal Statement:** [anixter.com/legalstatement](http://anixter.com/legalstatement)  
13T2677X00 © 2014 Anixter Inc. · 04/14

1.800.ANIXTER | [anixter.com](http://anixter.com)

