Analysis of Benefits and Technological Limitations

www.icdsecurity.com

ICD Security Solutions

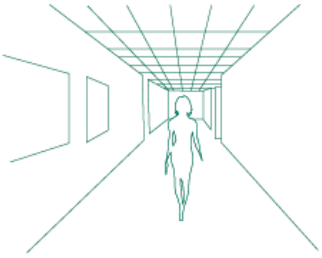
OVERVIEW

There is increasing awareness among security professionals about wireless access control systems, which offer a convenient way for companies to upgrade doors to use electronic card-based access control and never have to worry about keys ever again.

Wireless lock systems are certainly easier and quicker to install than traditional wired systems, and ICD calculates that companies can save more than 50% of initial installation costs compared with traditional wired systems. The cost of maintaining wireless systems is also lower in some ways, particularly because wireless locks consume less power than traditional wired security apparatus.

However, because of certain limitations, wireless systems will not meet the security requirements of every organization. Security managers need to be aware of what wireless lock systems can and can't do before they decide to incorporate them into their security system designs. That is why we have prepared this overview of how wireless lock systems work, when they should be used and who will benefit from adopting them.

Read on to find out more!



ICD Security Solutions

HOW ARE "WIRELESS" AND "OFFLINE" LOCKS DIFFERENT?

OFFLINE LOCKS:

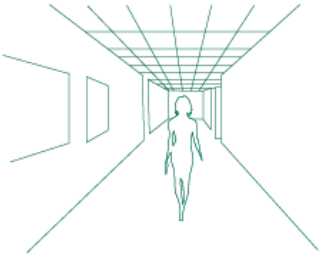
Offline locks are the simplest type of wireless electronic access control. Whereas traditional wired systems require a door lock, a card reader, electric strike, request to exit device an access controller, offline locks combine the functions of each of these into a single device. All access authorization information is programmed directly into the door lock itself, and card readers or keypads are built into the structure of the door handle.

Installing these locks is simple; users only need to replace the existing mechanical lock on their door with an electromechanical offline lock. Once the lock has been installed and programmed, it can operate independently without connecting to a central security management system until the battery needs replacing, which generally happens after 1-2 years of use, or after up to 70 000 door interactions.

WIRELESS LOCKS

Wireless locks add another level of functionality to offline locks by connecting wirelessly to a central security management system. Wireless access control systems share the advantages of offline lock systems such as easy installation and independent operation, even when a network is unavailable. They also allow end users to monitor intrusions and other system activity in real time, through a centralized security management software platform.

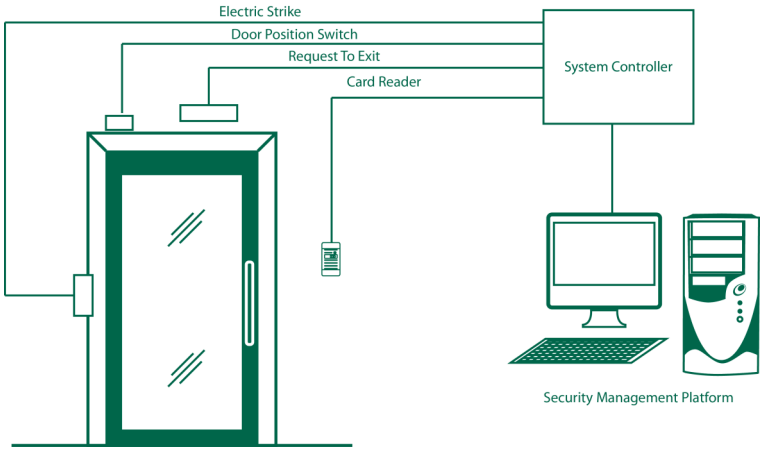
Similarly to traditional wired systems, wireless access control systems also allow users to perform other actions remotely from a central location, such as unlocking doors, deleting authorized cards from all doors simultaneously and configuring door open times. Wireless access control systems typically use "repeater" devices to connect a large number of wireless locks to a centralized security management system using just a few onsite Ethernet ports.



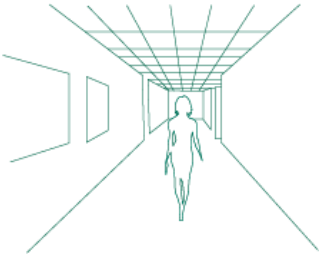
ICD Security Solutions

WIRED AND WIRELESS SYSTEMS COMPARED

WIRED ACCESS CONTROL



WIRELESS ACCESS CONTROL



ICD Security Solutions

WHO BENEFITS FROM WIRELESS ACCESS CONTROL SYSTEMS?

1. ORGANIZATIONS THAT WANT TO EXTEND SECURITY SYSTEMS TO COVER REMOTE LOCATIONS

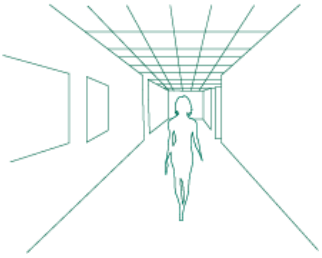
Securing entrances throughout sites with large areas is highly challenging when wired access control systems are used. Extending wired systems to cover remote locations on campus sites and similar facilities can be costly and difficult to install. Offline locks allow organizations to install electronic access control on doors in any area on their sites without having to worry about the logistics of cable installation.

As a result, offline locks give users much more flexibility when they want to extend the coverage of a security system within a large site.

2. ORGANIZATIONS THAT WANT TO UPGRADE SECURITY SYSTEMS WITH POORLY INSTALLED CABLING :

Some organizations who wish to upgrade their security system face a significant challenge if the existing cabling on a site was installed so poorly that it can not be used again. This becomes even more difficult if the building has already been decorated and it is impossible to rewire the system without damaging the decoration.

In this situation, wireless access control systems can help users to avoid significant disruptions and installation costs. These systems are therefore ideal for retrofitted security installation projects.



ICD Security Solutions

3. ORGANIZATIONS WITH SMALL, "LOW-TECH" SITES THAT WANT TO UPGRADE TO ELECTRONIC ACCESS CONTROL:

Small scale organizations with simple, key-based security are among the groups that would benefit most from offline locks. Card-based electronic access control based on a traditional wired system is often not a practical option for small scale security systems due to the high costs of hardware, wiring, servers, installation and software licenses.

Now, smaller organizations can adopt card-based access control and never again worry about changing a lock because of one lost key, as lost or stolen cards can be easily deleted from the system. Disruptions caused by upgrading are also minimal, as users can simply replace existing mechanical locks with electro-mechanical offline locks.

4. ORGANIZATIONS THAT WANT A SECURITY SOLUTION WITH BASIC FUNCTIONALITY THAT IS COST EFFECTIVE

Traditional access control systems often offer an overwhelming number of system functions that allow users to perform sophisticated security operations. However, the many security teams typically only require a small percentage of these functions to manage daily security operations, which reduces the value proposition of these complex systems for certain users.

Offline locks allow users to enjoy the convenience of card-based access management without making them pay for features that they will never use, making these systems a much more cost effective option for many organizations.

ICD Security Solutions

CURRENT CONCERNS ABOUT WIRELESS ACCESS CONTROL TECHNOLOGY

1. INTEGRATION CAPABILITIES ARE CURRENTLY MORE LIMITED THAN THOSE OF TRADITIONAL SYSTEMS

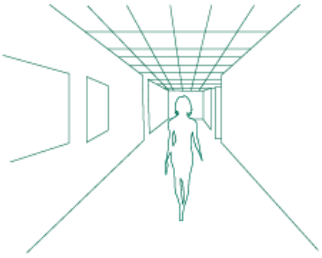
Whereas offline locks are a good solution for organizations with basic security requirements, many solutions are not able to integrate operations as deeply with surveillance and alarm systems as more established wired solutions. For this reason, many large organizations may find that wireless access control solutions do not necessarily meet their global security system requirements.

This could soon change, however, as the integration capabilities of wireless access control systems are growing every year

2. SYSTEMS MAY BE VULNERABLE TO HACKING

Because wireless access control systems use a radio signal to transmit information, it is theoretically possible for information to be intercepted and even controlled by a “middle man” hacker. Information is highly encrypted though, so breaching security in this way may be possible, but not easy.

Nevertheless, security managers of high level security sites may want to be cautious about incorporating wireless locks into their security systems.



ICD Security Solutions

3. REPLACING DOOR LOCK BATTERIES CAN INCREASE WORKLOAD

One major downside of wireless locks is that they can not be connected to a power source. This means that even though they consume less power overall than wired systems, minor disruptions are inevitable when the battery of each lock runs down and needs to be replaced.

This can often increase the workload of security teams when compared to traditional wired systems, so it is often not practical to design security systems with large numbers of wireless locks or for sites with large people flow volumes.

Battery life in for current locks ranges from 15000 to 70000 opening actions, so security end users should bear this in mind when comparing different product lines.

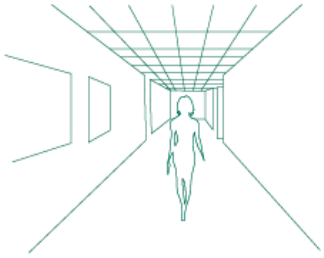
4. RADIO SIGNAL FREQUENCY ISSUES

Security managers need to pay attention to the signal frequency of each wireless system. Some product lines are not suitable for use in Mainland Chinese sites, for example, as they use the same wireless frequency as mobile phones in the region. ICD has had to advise several clients against adopting wireless access control technology for precisely this reason.

For this reason, security managers need to pay careful attention to the radio frequencies used by wireless access control brands, especially when they are considering which products to incorporate into global security design standards.

GOT ANY OTHER QUESTIONS?
CLICK HERE TO CONTACT US
THROUGH OUR WEBSITE!

www.icdsecurity.com



ICD Security Solutions