

WHAT IS ACCESS CONTROL?

Access control is the process of providing access to those who are authorized and denying access to those who are not.

Over the years, this definition has resolved itself into one that implies the use of a centralized database of cardholders with their associated access permissions, and the equipment and electric locks that control the entry points. That was not always the case. The process can be as simple as a person with a list who is stationed at a portal. This person can let in the people on the list and keep out the ones who are not on the list. Keys are still the primary security control mechanism in the world. But keys and lists are difficult and costly to manage. So, electronic access control systems have developed to fill the need for managed control.

The great advantage of an access control system over a keying system is that all of the changes to the permissions as to who can access what space are made to the host computer. There is no need to go to each door and change the biting of the cylinder in the lock. Typical re-keying charges run from \$10.00 to \$20.00 per cylinder. If security is to be maintained, whenever a key is lost, all of the cylinders for which that key worked should be re-keyed. New keys need to be issued for all of the re-keyed doors. For a large campus of buildings, these charges are often in the hundreds of thousands of dollars per year. In fact, the costs are so high that, more often than not, the vulnerability is ignored, leaving a big hole in the security program. With access control, a lost card can be removed from the system in less than a minute, and the only loss is the actual card, and possibly the badge printing cost associated with a combined credential.

An access control system is typically composed of:

- **Host Computer** - holds the database of cardholders and their permissions
- **SRBs (Smart Remote Boxes)** - make the access decisions electronically
- **Card Readers** - read the card signals and send the information to the SRBs
- **Access Cards** - that are carried by the users of the system

There are many options and standard features that can be implemented, even for the simplest of systems. As the systems grow in functionality, these choices grow exponentially. In most cases, there is no "right" way to implement a system, just options that are more or less applicable to the site. Therefore, there are always decisions to be made. This site offers a way to gather information on the features and functions that are available.

Specifically not addressed here are unwired hotel locking systems. Historically, these systems have used inexpensive Hollerith or magnetic stripe cards, which are not part of any other larger system. However, one of the proximity card manufacturers is now marketing a product that can be integrated with a battery powered locking system that will allow for possible combinations of typical access control and unwired style access control. As this becomes a usable possibility, this site will address this potential.

Host computers used by access control manufacturers vary from small PCs to large NT servers and Unix based RISC platforms. Several different operating systems are used, usually a network server style, but the functionality of the application code for all systems is similar. Most systems today also utilize a separate commercial relational database engine. This allows development of the application independent of the integration and reporting tools that come as part of the database. Virtually all of these database engines support SQL (Structured Query Language) queries.

SRBs are the connection points for the card readers, locks, door monitoring points, and all other wired inputs and outputs of the system. The primary job of the SRB is to make the access decision when a card is presented to a connected reader. The SRB will handle all of the supervision of the transaction when a person enters or exits a building through a card reader door. Supervision includes making sure that the door is normally closed, that it only opens when it gets an appropriate signal such as a valid card read, and that the door closes at the end of a transaction.

SRBs communicate with the host to send any alarms as well as all historical card transactions. The host will communicate with the SRBs if a card is added or deleted from the list of those that are authorized to access one of the doors that the SRB serves.

The general structure of today's access control systems that use SRBs creates system reliability. While there is typically only one host, there are usually several SRBs, sometimes hundreds. Each SRB serves just the doors that are connected to it. If it breaks, only the doors that it serves are affected. If the host breaks, then all of the day-to-day access decisions continue to be made. All of the people that need to get in a door can continue get in. The SRBs will store the transactions in a history buffer until they can once again talk to the host.

Card readers are designed to take the code from the card and send it to an SRB. The SRB then determines if the card is valid for the particular door and time. If it is, then the SRB will send out a command to unlock the door. Once a door is unlocked, a timer is started that will re-lock the door if it is not opened. A common setting for this timer is 5 seconds. Some doors need longer unlock times because the card reader is farther from the door. If the card reader is designed to work a motorized portal such as a gate, then the unlock time is usually set to 1 second.

Once the door is opened, a held timer is started. Access doors must self close so that they are secure. If the held timer expires before the door is closed, then a door held alarm would be sent to the host. A typical setting for a held timer for a door is 30 seconds for a low traffic door and up to 120 seconds for a high traffic door. People will usually get through a typical hinged door in a few seconds, and the door closer will then get the door closed in about 10 seconds. If all of that transaction works as expected, the SRB will send a completed transaction record to the host.

A door contact is used to sense when the door is open. It is this contact that allows the system to sense when some form of security violation has occurred. If the door opens without a valid card or REX transaction preceding it, the SRB will send a door forced

alarm to the host. The term REX stands for Request to Exit. The device that senses a person walking up to the door from the inside of the space is usually a PIR (passive infrared) sensor. It is possible to use a switch in the inside handle of a mortise lockset to send a REX signal as well.

Access Cards are the most common form of credential used for access control. Proximity cards are very popular, with magnetic stripe cards also prevalent. Weigand cards are not as prevalent now as they were in the early 1990s. Each of these cards has the common purpose of holding a unique number that can be used by the SRB and host to define a set of permissions for allowing access.

The early proximity cards were patented by Schlage Electronics and were tuned coil/capacitor sets that absorbed certain frequencies. Today, electronic cards usually contain a coil that absorbs the energy from the reader to charge a chip. The chip, in turn, transmits a code number that is the card number. No batteries are used in this configuration. A few of these electronic proximity cards do have batteries that cannot be replaced. The projected life of the batteries is commonly 5 years. By using a battery in the card, the range can be increased.

Magnetic stripe cards have been on the market for many years. Because the card user is required to insert the card in a slot to get the card read, people have gravitated to the easier use of proximity cards. The ability to put badge information right on the access card has also contributed to the trend toward proximity. With a magnetic stripe card, the read head needs to be right on the magnetic stripe. To accomplish this, pressure is applied to the opposite (badge) side of the card. Over time, the rubbing of the card reader on the badge creates lines, streaks, and sometimes holes in the image and/or data of the badge. With proximity, there is no physical contact, and therefore, a longer badge life.

Access cards are designed to be used with specific readers. From the system standpoint, cards and readers are a pair. This is especially true for proximity readers. When an access system is being designed, the decision as to the brand of access card and reader is generally an independent decision from the Host software and SRB decision. The host software is designed to work with a specific set of SRBs. Generally, any host-SRB system can use any of the common card-reader combinations.

So if the system has:

- access cards assigned to the user population,
- card readers on doors that communicate with SRBs that make the access decisions,
- and finally a host that is used for programming and reviewing the historical activity,

then the system is a complete, modern, access control system.