Keyless Electronic Systems

Overview & Design Considerations
for the manufacturer, designer, & engineer
August 3, 2007

Overview:

This white paper describes hardware considerations for designing keyless electronic products. The target audience is anyone who manufactures, distributes, or implements such systems. Keyless electronics are growing in popularity and are finding their way into a wide number of applications including security systems, access control, home automation, automotive systems, safes, apartment mailboxes, rental lockers, and more. These systems are suitable for a number of venues including schools, homes, hotels, airports, hospitals, health clubs, and theme parks. Two specific types of keyless system control are described in this document:

- Host control
- Standalone

A host control system features the use of a PC or laptop computer, one or more remote controllers, and reader(s). The systems are all networked on a single cable - RS-485 or Ethernet (TCP/IP). The host computer functions as the network server and provides the primary point of access for communication with the remote controllers. Software on the host provides functions for adding users, configuring controllers, and monitoring access. Host control systems provide special features including the ability to log individual access attempts.
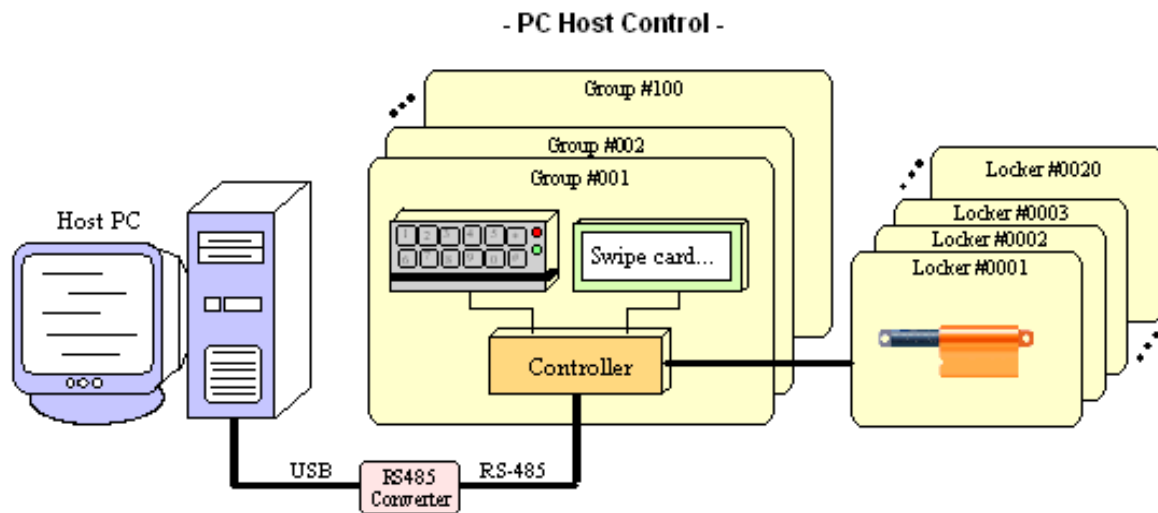
Host-control system including Windows PC

A standalone control system consists primarily of remote controllers and readers. Controllers operate independently and do not communicate with a host PC.

- Standalone Control -
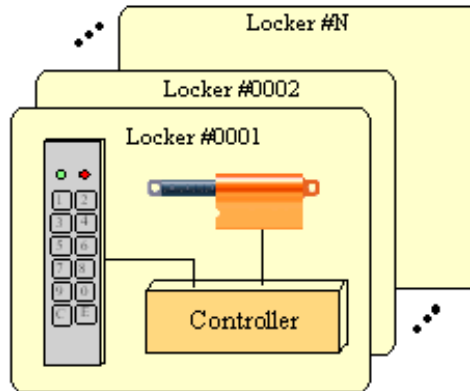
Standalone control system

Controllers:

Remote embedded controllers provide digital intelligence and device interfacing. Considered the "brains" of the system, they contain a microprocessor or microcontroller, non-volatile memory for program storage, serial communications ports, and general purpose digital I/O for LEDs, beepers, etc. Controllers interface external devices including readers, displays, and keypads. And, when used in networked systems, they provide RS-485 and Ethernet (TCP/IP) interfacing.

Each controller handles access to one or more end-user items (i.e., doors, lockers, mailboxes, or safes) and exist in one of the following hardware configurations:

- Networked (standard & extended)
- Standalone

Networked controllers are required for use with host control systems. In the standard configuration, a controller can control up to 20 individual end-user items. In the extended configuration, up to 40 items can be controlled. The following hardware is required for host control:

- Host computer (and applicable software)
- Electronic controllers (standard or extended)
- Readers (biometric, proximity, barcode, iButton, or magnetic stripe)

Each electronic controller can function in one of two access modes, depending on the application and venue:

- Pay-per-use
- Long-term access

Pay-per-use means units are rented for a limited period of time, usually less than 24 hours. A pre-specified payment amount is required by the patron, typically by cash or credit card. Once payment has been made, the patron is granted access to a specified end-user item. Pay-per-use can be applied in either host control or standalone systems.

Long-term access allows longer use of end-user items, typically more than 24 hours. If a host control system is used, patron information can be maintained in a local database including name, address, phone, and/or e-mail. Long-term access can be applied in either host control or standalone systems.
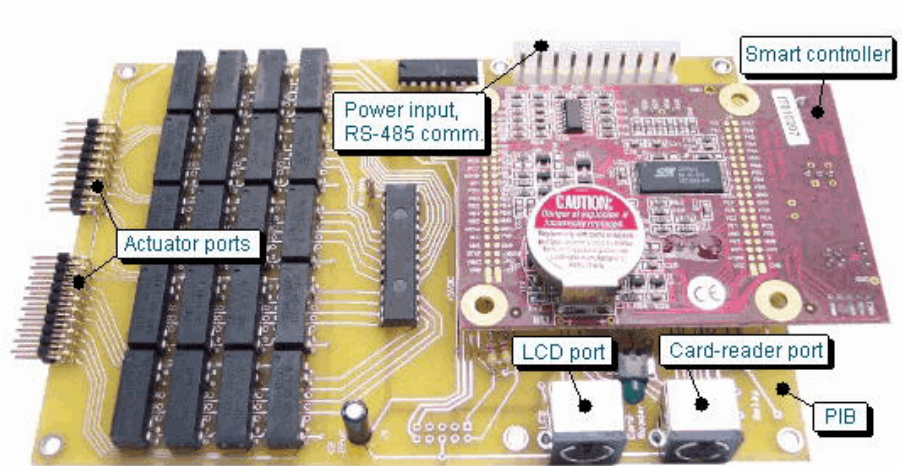
Embedded controller with card-reader & LCD ports, and RS-485 comm.

Readers:

Reader devices provide the means of validating and identifying users. They can also be used to accept cash and credit card payments in point-of-sale (POS) transactions. There is a variety of available readers including the following:

- Biometric (fingerprint, facial recognition)
- Magnetic stripe
- Proximity (RFID)
- Barcode
- iButton
- Keypad

Proximity card-readers

Reader selection must be made based on the application requirements. Cost is always a major consideration. Simple keypads provide a convenient compromise between cost and security without the need for physical card credentials. Magnetic stripe, barcode, proximity, and iButton readers are relatively inexpensive, but require the use of credentials. Biometric readers use fingerprints or facial recognition. While generally more expensive, they provide better security and have the distinct advantage of requiring no physical credentials.

The user environment will also play a role in the selection process. Considerations include exposure to the elements and possible vandalism. In some cases, a ruggedized device may be needed.

Locking Device:

An electronic or electro-mechanical device is required to release or unlock the end-user item or other mechanism. The choice of a suitable locking device will depend largely on the type of mechanical latching that is needed. Space constraints and voltage/current requirements will be important considerations as well. There are several basic choices, each with its advantages and disadvantages:

- Solenoids
- Magnetic locks
- Actuators

In general, magnetic locks are the simplest to implement, but must be continuously powered. Solenoids are generally inexpensive and widely available. Actuators allow the greatest flexibility but usually involve the highest cost. The following table summarizes the differences between device types:

| Locking Device Comparisons		
	Pros	**Cons**
Solenoid	Inexpensive; widely available in many different sizes	Low holding force, short arm travel
Magnetic Lock	Easy implementation; high holding force	Must be continuously powered
Actuator (linear, rotary)	Flexibility; range of available torques from low to high	More expensive
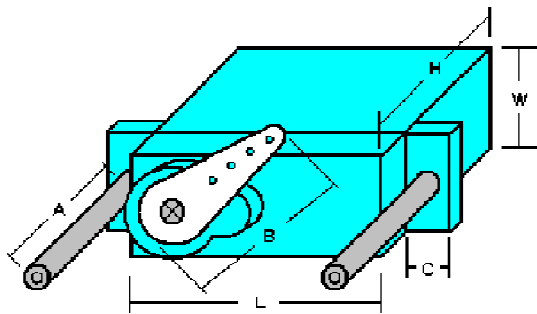
Rotary actuator

Linear actuator

Conclusion:

Keyless electronic products can be found in a number of markets around the world and are expected to become even more widespread over the next several years.   As these systems grow in popularity, their cost will decrease, making them even more attractive to OEMs and designers.

Applications:
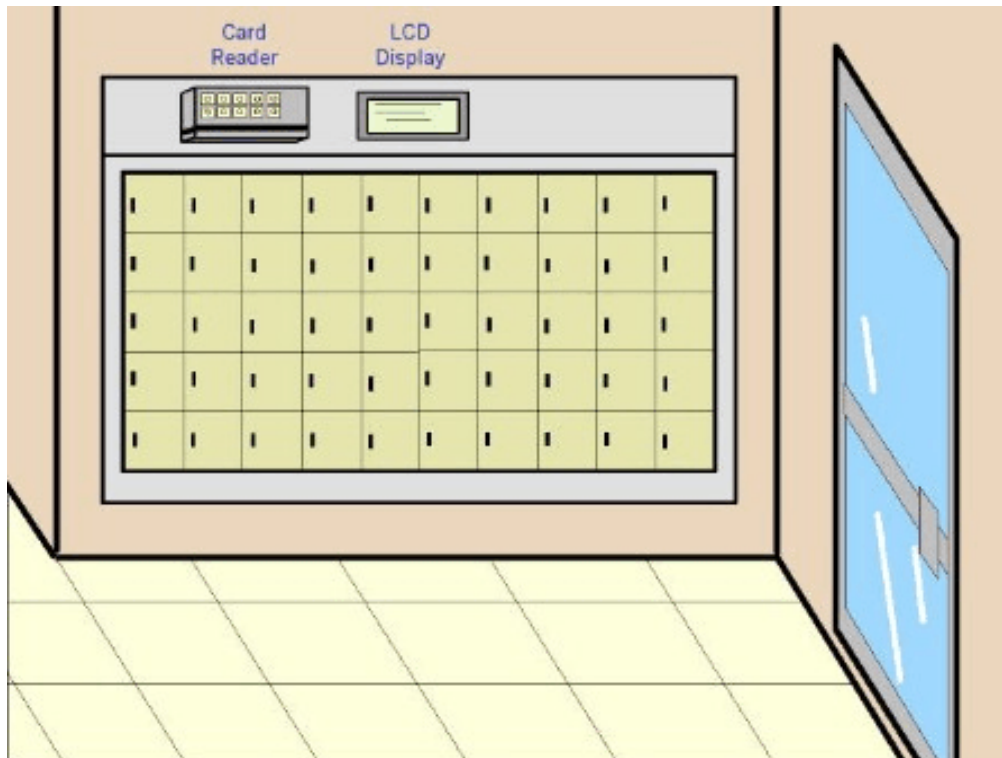
Typical application - Keyless mailboxes and lockers

About the author:

Kenneth Delahoussaye is a consultant and design engineer residing in Melbourne, FL. His background is electrical engineering and software development for embedded systems. He owns and operates Kadtronix, an online resource that specializes in automation and control.

Contact:

Kenneth A. Delahoussaye
Delahoussaye Consulting
http://www.kadtronix.com
kdelahou@kadtronix.com