Appendix V

Overview of Punch Card & Card Reader Systems

APRIL 2007

Card Access System ... pg 2

Explains on the components of card reader system
- Access Cards
- Card Readers
- Control Units
- Control Unit Software

Technologies of Card Reader Systems..... pg 3

Evaluates a few card reader system technologies
- Proximity Card System
- Smartcard System
- Magnetic Stripe Technology
- Bar Code Technology
- Mixed Technology

Choosing and Implementing a Card System ..... pg 5

Important features to consider when selecting a card reader system include technological sophistication, security level, security needs, the frequency of usage, life cycle, conditions in which the system will be used and the system costs.

Estimated Costs..... pg 5

Discusses on the costs for card reader system

Comparison of Card Technologies ..... pg 5

Summarizes on card technologies comparisons

TIME AND ATTENDANCE SYSTEM TRENDS FOR 2005 ..... pg 6

Discusses the latest time and attendance system trend which highlights the tendency towards fingerprint biometrics system

One of the most valuable commodities in business is time. To better manage time while reducing expenses is the issue that most businesses need to pay attention to, in order to maximize efficiency which leads to increased productivity. There are some issues to address when it comes to choosing time and attendance system to work for you such as reduction of payroll-processing time, improved of payroll accuracy and improved of labor management through increased control and information. This article will review on conventional time and attendance systems which include of punch card system and various other types of card systems.

Manual Punch Card System

Manual punch card system is a system where employees punched time clocks, and at the end of the pay-period, supervisors manually totaled the hourly shifts. The organization tracked payroll totals through the manual punch card system. Total working hours and overtime hours were manually added by administration on a master time sheet. Master calculations were called into a payroll processing company. While this arrangement met the organization's basic needs, management was concerned with the amount of time supervisors and administrators spent manually keeping records. The payroll specialist spent more than two days a month pouring over punch cards, verifying totals and manually transcribing them into the summary journal.

Acroprint ATR120 Electronic Cross-Shift Time Recorder

Acroprint BP-125

It was virtually impossible to check employee time cards each day. Consequently, supervisors relied on their memories when completing missing in/out punches at the end of a two-week pay period. This often led to incorrect employee hours. Each supervisor had to round up or round down punch times when calculating pay period totals. It was difficult to ensure that rounding was consistently applied throughout the organisation. Duplicate data-entry was another concern. The same information was might be rewritten at least two times when totals were compiled at the end of a pay period. An incorrect figure entered on a calculator could easily throw off totals.

While the system is cheaper than many other time and attendance systems available in the market, the system cause inconvenience to a business particularly in this information technology era where information is needed almost immediately most of the time.

Lathem Time 6000E Series

Manual Punch Card System

Several brands of manual punch card system available in the market within price range from USD189 and USD750 are *Acroprint, Amano, Detex, Lathem, Isgus, Icon* and *Pyramid*.

Amano MRX35
ACI MRX35

Pyramid PTR4000

Isgus 2005

Amano BX-6000

Card Reader System

A card reader system is a type of electronic identification system that is used to identify a card and then perform an action associated with that card. Depending on the system, the card may identify where a person is or where they were at a certain time; or it may authorize another action, such as disengaging a lock. The reader will store the information and/or send it to a central location, where it can be checked later to ensure that the guard has patrolled the area. Other card reader systems can be associated with a lock, so that the card holder must have their card read and accepted by the reader before the lock disengages.

A complete card reader system typically consists of the following components:

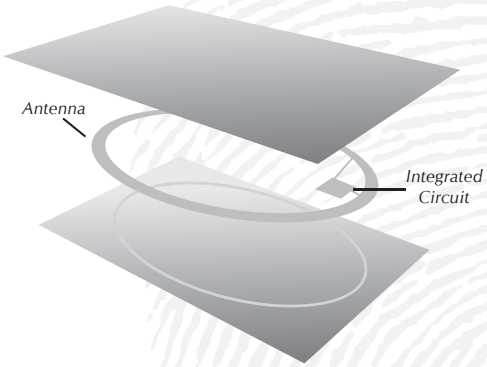
- **Access cards that are carried by the user** - A "card" may be a typical card or another type of device, such as a key fob or wand. These cards store electronic information, which can range from a simple code (i.e., the alphanumeric code on a Proximity card) to individualized personal data (i.e., biometric data on a Smartcard). The card reader reads the information stored on the card and sends it to the control unit, which determines the appropriate action to take when a card is presented.
- **Card readers**, which read the card signals and send the information to control units - The main function of the card reader is to read the code from the card and send that information on to the control unit. Some card reader systems require that the card be physically inserted into the card reader, while others, such as the Proximity system, only require that the card be in the general proximity of the reader. The specific methods by which data is transferred from the card to the reader are discussed under each card technology below.
- **Control units**, which control the response of the card reader to the card - A control unit is typically composed of both hardware and software. This unit is the main connection point for the card readers, locks, location monitoring points, and other wired inputs and outputs of the system. The primary function of the control unit is to record the information on the card, and respond, as appropriate. Depending on the needs and complexity of the system (i.e., the number of card holders, the number of card readers, the number of different permission levels, the types of transaction data tracked, etc.), a control unit can range from a localized control panel to a basic stand-alone PC to a more complex network, such as a Windows NT server or a UNIX-based RISC platform. For some simple systems that do not require the storage of large amounts of data, a localized control panel may be sufficient.
- **Control Unit Software** - The control unit is the main data storage and control center for the system. The control unit functions through a combination of hardware and software. The software is used to execute decision logic based on the interaction of the data stored on the card and its permissions stored in the system database, and the hardware then carries out this logic by powering locks, turning on switches, etc. The majority of card reader systems use software packages (usually Windows-based) to control the system. This software is the decision-making "brain" of a card reader system. It is used to develop and populate the card user database, to establish user "permissions," and to execute the decision logic (such as disengaging locks or recording a card location) when the card is read by the card reader. Card reading software is also used to assign different "permissions" to each card holder. Permissions are defined as the authorization levels given to users specifying the different things they can do within the system. It should be noted that the control of a location through a card reader system is limited only by what can be programmed into the system. Once data from a card has been read by the card reader, it can be used for any purpose that was written into the software.

Technologies of Card Reader Systems

While card readers are similar in the way that the card reader and control unit interact to control access, they are very different in the way data is encoded on the cards and in the way these data are transferred between the card and the card reader.

There are several types of technologies available for card reader systems. These include:

- **Proximity Card System**



Components in a Proximity Card

Proximity card is embedded with radio frequency circuits encoded with unique alphanumeric codes. The card is also embedded with a small coil of wire that acts as an antenna. When the card comes near tion on the card is then transmitted to the card reader, which then sends the information on to the control panel. Based on the information received from the card, the control panel either accepts the information and communicates with the reader to disengage the lock, or rejects the information and does not disengage the lock.

Proximity cards typically do not include any personalized information, and thus any person using the proper Proximity card can use it access the protected asset. Therefore, Proximity card systems cannot be used to track individuals (such as what individual accessed a doorway), and they may be most appropriate in applications where it is important that only authorized persons access the asset, but it does not matter which particular individual access the asset.

Icon Proximity Badge
100 Employee Time Clock

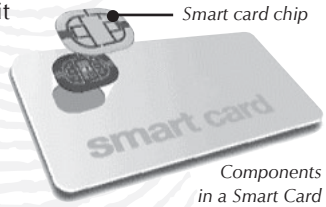
- **Smartcard System**

There are two general categories of smart cards: contact and contactless smart cards. A contact smart card requires insertion into a smart card reader with a direct connection to a conductive micromodule on the surface of the card (typically gold plated). It is via these physical contact points, that transmission of commands, data, and card status takes place.

CardMan® 5121 Contactless / Contact Smart Card Reader

A. **Contact Smart Card**

Contact smart cards are the size of a conventional credit or debit card with a single embedded integrated circuit chip that contains just memory or memory plus a microprocessor.

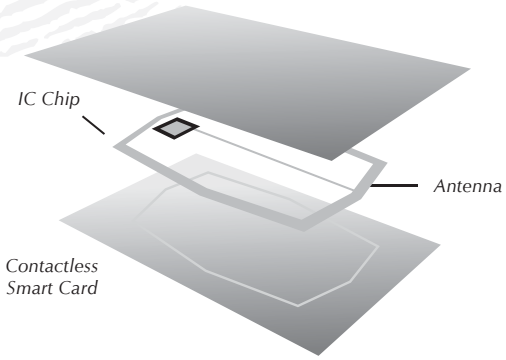


Components in a Smart Card

Memory-only chips are functionally similar to a small floppy disk. They are less expensive than microprocessor chips, but they also offer less security so they should not be used to store sensitive or valuable information.

Contact smart cards must be inserted into a card acceptor device where pins attached to the reader make "contact" with pads on the surface of the card to read and store information in the chip. This type of e-card is used in a wide variety of applications including network security, vending, meal plans, loyalty, electronic cash, government IDs, campus IDs, e-commerce, health cards, and many more.

B) **Contactless Smart Card**



Components in a Contactless Smart Card

In addition to the features and functions found in contact smart cards, contactless smart cards contain an embedded antenna instead of contact

Card Reader Systems Technologies

pads attached to the chip for reading and writing information contained in the chip's memory. Contactless cards do not have to be inserted into a card acceptor device. Instead, they need only be passed within range of a radio frequency acceptor to read and store information in the chip. The range of operation is typically from about 2.5" to 3.9" (63.5mm to 99.06mm) depending on the acceptor.

- **Magnetic Stripe Technology**

Magnetic Stripe Card

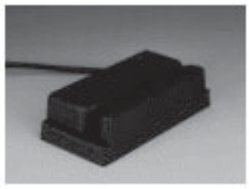
Magnetic Stripe technology is one of the most widely used card technologies, especially in the banking sector, where it is used for credit and automatic teller machine cards. Magnetic stripe technology uses electromagnetic charges to encode information on an oxide-coated piece of tape, which is attached to the back of a card. Typically, the oxide stripe contains three magnetic tracks of alphanumeric data bit strings of varying lengths. The card is placed in a magnetic stripe reader, which uses magnetic heads to read the information on one or more of the three magnetic tracks. This technology can store a large amount of personalized information (such as personal account numbers for use in credit transactions), and thus these card systems are ideal for tracking individuals.

Magnetic stripe technology is efficient because the configuration of the three magnetic tracks of alphanumeric data bit strings make it easy to access the data. However, there are several potential drawbacks to this type of technology. First, this type of technology has a limited lifetime because the magnetic stripe can become worn due to the frequency with which it must be swiped by the read head. Additionally, magnetic stripe cards are sensitive to magnetic fields, which can erase encoded information. Finally, the cards are also subject to duplication using computerized track readers and a magnetic stripe encoder. Based on these characteristics, magnetic stripe technology is considered to offer a low to moderate level of security.

Tysso MSE-630A Hi-Co. Magnetic Stripe Card Encoder / Reader

- **Bar Code Technology**

Bar Code Card



Opticon SR-110 Bar Code Slot Reader

Bar Code technology consists of information printed in a pattern or series of narrow and wide bars and spaces. Certain types of bar code readers use fixed infrared LED light sources to read the symbol. Bar code technology typically contains personalized data. For example, this technology is used extensively on driver's licenses in many states.

As with magnetic stripe technology, there are potential security problems with this technology. For example, bar codes are susceptible to reproduction by using a computer scanner or photocopier. Bar code technology is considered to offer a relatively low level of security due to the ease with which they can be counterfeited.

- **Mixed Technology**

Mixed technologies combine a variety of technologies on one card and provide different functions by combining these different technologies.

Combination of Fingerprint & Smart Card Technology

For example, Proximity technology can be combined with bar code, magnetic stripe, Wiegand, or Smart card technologies. One of the most popular combinations is magnetic stripe technology combined with Wiegand technology. Magnetic stripe technology is efficient at accessing data and Wiegand technology provides a high degree of security for gaining entry to designated areas. The two technologies together therefore provide quick, secure access. Another very common combination is magnetic stripe technology used in conjunction with Proximity technology. For this particular technology combination, the readers themselves are able to read both types of cards. This is very useful to businesses that are transitioning from older magnetic stripe technology to a more reliable, high functionality Proximity card technology.

Choosing and Implementing a Card System

Each of these technologies can be implemented for facilities of any size and with any number of users. However, because individual systems vary in the complexity of their technology and in the level of security they can provide to a facility, individual users must determine the appropriate system for their needs. Some important features to consider when selecting a card reader system include:

- The technological sophistication and security level of the card system;
- The size and security needs of the facility;
- The frequency with which the card system will be used. For systems that will experience a high frequency of use it is important to consider a system that has a longer life cycle and lower vulnerability rating, thus making it more cost effective to implement;
- The conditions in which the system will be used (i.e., will it be used on the interior or exterior of buildings, does it require light or humidity controls, etc.). Most card reader systems can operate under normal environmental conditions, and therefore this would be a mitigating factor only in extreme conditions; and
- System costs.

Estimated Costs

Costs for card reader systems can vary greatly depending on the level of system sophistication, including the size and level of security needed for a given facility. The cost for a card reader, which is required at every door that is part of the system, ranges from USD85 to USD250 per unit. Access cards, which must be issued to all personnel that will be accessing the facility, can range from USD0.75 to USD7 per card. As shown in Table 1, magnetic stripe and bar code systems would be on the low end of this cost scale, and Wiegand and smart card systems would be on the higher end. The higher costs for these technologies would be reflected in higher costs per unit for both the cards and the readers. Control panels start at around USD500 and can reach up to USD3,200. Software necessary to control the system is usually included with the package for basic-type systems, while software for more complex systems may be an additional cost and may range from USD200 to USD1,000. Optional card encoders or read/writers usually range from USD500 to USD1,500 each.

Installation of card reader systems can be complex, and therefore most, if not all, card reader systems are installed by a manufacturer's representative. This will be an added cost, and will depend on the number of card readers and control units in the system, as well as the type of data transmission system implemented.

Comparison of Card Technologies

The Table below summarizes various aspects of these card reader technologies. As discussed above, the determination for the level of security rating (low, moderate, or high) was based on the level of technology a given card reader system has and how simple it is to duplicate that technology, and thus bypass the security. Vulnerability ratings were based on whether the card reader can be damaged easily due to frequent use or difficult working conditions (i.e., weather conditions if the reader is located outside). Often this is influenced by the number of moving parts in the system - the more moving parts, then greater the system's potential susceptibility to damage. The life cycle rating is based on the durability of a given card reader system over its entire operational period. Systems requiring frequent physical contact between the reader and the card often have a shorter life cycle due to the wear and tear to which the equipment is exposed. For many card reader systems, the vulnerability rating and life cycle rating have a reciprocal relationship. For instance, if a given system has a high vulnerability rating it will almost always have a shorter life cycle.

Types of Card Readers	Technology	Life Cycle	Vulnerability	Level of Security	Cost
Proximity	Embedded radio frequency circuits encoded with unique information.	Long	Virtually none	Moderate-High	Expensive-Moderate
Magnetic Stripe	Electro-magnetic charges to encode information on a piece of tape attached to back of card.	Moderate	Moderately susceptible to damage due to frequency of use.	Low-Moderate	Inexpensive
Bar Code	Series of narrow and wide bars and spaces.	Short	High; easily damaged.	Low	Inexpensive
Smartcards	Patterns or series of narrow and wide bars and spaces.	Short	High susceptibility to damage, low durability.	Highest	Expensive

Table 1 : Comparison of Card Reader Technologies

TIME AND ATTENDANCE SYSTEM TRENDS FOR 2007

Automated time and attendance systems continue to make inroads in organizations of all sizes as employers discover the benefits of eliminating paper timesheets and old-fashioned punch cards.

Trends indicate that automated time and attendance systems are evolving as functionality moves from Punch time clocks and card time clock to fingerprint biometric systems. Despite the growing prevalence of fingerprint time and attendance system and the continuing popularity of traditional systems in some industry segments, biometric devices that combine time attendance and security in one unit as well as biometrics that considers with Card System, are emerging as the clear choice for many companies.

Booming of Fingerprint Time Attendance System

Biometrics - systems that verify a user's identity based on a physical characteristic - have been around for a number of years as security devices. Over the last few years, Fingerprint time and attendance systems have emerged as a means to streamline the typically labor-intensive, paper-heavy task of collecting and reporting employees' worked hours. Biometrics is readily adapted to time attendance because of the tasks they integrate.

Their original role as a security measure cannot be overstated. Security is a major issue for businesses of all sizes today, and biometrics is at the forefront of the movement toward better workplace protection. Because time collection terminals can be programmed for physical access control, time and attendance is a natural extension for biometrics. Biometrics allows management to be fully confident that the person entering time cannot falsify his or her identity, thereby eliminating fraud.

Likewise, biometrics alleviates the costly practice of "buddy punching" where one employee clocks in for another to credit the absent worker for time not worked. Traditional time clocks can only verify a card or badge, not the person using them. With biometrics, buddy punching is not an issue - a person's body is his or her "card." The elimination of buddy punching has prompted many larger companies to adopt biometric time and attendance solutions. It reduces the cost and effort of maintaining cards and eliminates any chance of buddy punching.

Besides employee buy-in, cost has been one of the biggest stumbling blocks to biometrics' acceptance. Prices have decreased to the point that fingerprint devices are becoming more widespread in businesses of all sizes. Significant growth is being seen, especially in the hospitality and food service industries." Aside from its application in businesses with large numbers of hourly workers, Fingerprint time attendance systems are finding their way into the white-collar world as well, as time and attendance with biometrics systems save lots of time and energy. The system has been able to reduce payroll-processing time as it is integrable to payroll software which solves the issue of payroll accuracy and improved labor management through increased control and information.

TA102
Fingerprint TA System

AC900
Time Attendance
& Door Access System

AC100-R
with RFID function

AC800 Plus MC
with Mifare Card