Application Note 004

HID CORPORATION

Introduction to HID Radio Frequency Identification (RF ID)

HID is the future of Access Control

Access Control Systems are used to allow authorized people to enter a controlled area by unlocking the door.
When we think of Access Control Systems, thoughts of secret Government projects and ultra high security might come to mind. But today, Access Control systems with HID proximity products protect Bank Vaults, Airports, and children in Day Care. In fact, diverse facilities from exclusive social clubs and hospitals to parking lots and prisons use Access Control Systems to protect people and property. Industry uses Access Control with HID components to organize information, record employee attendance, payroll, tool distribution, and cafeteria billing. New uses are being added every day, and System Integrators are linking HID Access Control Products to Building Controls, Process Controls, Accounting, and other existing control systems.

HID makes a special type of identification card called a “Proximity” card. It is used with a HID “Proximity Reader”. The technology is called proximity because the information on the card can be transmitted without touching the reader. HID proximity cards can transmit data through common building materials like: concrete, brick, stone, drywall, plaster, glass, wood, plastic…in fact, through anything but metal. As a result, HID Readers can be hidden behind wood paneling, Plexiglas plates, tinted windows, and inside brick walls.

In a typical Access Control application the ID number is transmitted from the card to the reader using a radio frequency code. That ID number is then sent to the Access Control Panel. The computerized panel associates the ID number with a person and determines whether he is authorized to enter. If not, the entry will remain locked. If the card number is valid, then the panel commands the electric locking mechanism to open.

HID Readers can communicate with many different system types by using a variety of well established, industry standard interfaces including Wiegand, serial (RS232\422\485), and Clock-and-Data Magnetic Stripe Track/2.
With so many well-established reader output types it is easy to add HID Readers to existing systems.

Multiple technologies can also be combined on HID Cards. Proximity can be included with bar code (and any other dye sublimation printable ID), magnetic stripe, Wiegand strip, Debitek, and contact programmable Smart Chips.

HID Has the Advantage Over Other Technologies

HID cards use “Passive Technology”. The electronic components within the card get their power from the HID Reader. An unlimited number of reads can be performed. There is no battery that can wear out or fail, as with “Active Technology” cards. Passive proximity cards, unless they are physically abused, will last virtually forever since they never need to rub or touch the reader.

HID proximity cards are more convenient to use than other card technologies. They do not need to be aligned with slots, slid at a certain speed, placed into a narrow opening, or cleverly handled. Simply hold a proximity card in front of the reader to activate the system.

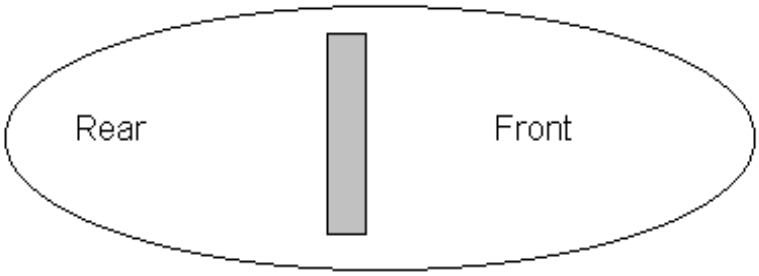
HID readers are also maintenance free, with no parts to wear out or adjust. They also can be secured from vandalism inside a building, behind glass, or inside walls and still read HID cards.

How HID Proximity Cards and Readers Work

The Proximity Card Reader is wired to an Access Control System Panel. The wires carry power to the Reader, and Data from the Reader to the Panel.

The Reader emits an electromagnetic field called the “excite field”. This field has an elliptical shape.

Figure 1



Side View of a Reader in its Field

As Figure 1 shows, the field extends behind the Reader almost as much as in front.

When a proximity card is brought within the reader field, the card absorbs some of the energy from the field. The card converts this field energy to

electricity. This causes the electronic circuits in the card “turn on”, and transmit its number to the reader. The reader then sends the card number to the Access Control System Computer, which then identifies the cardholder.

The card data transmission distance varies with card type and reader type. Larger, more powerful readers can energize some cards up to two feet away. The distance at which a card will successfully transmit data to the reader is called the “Read Range”. Read Range is not a single absolute distance. It can vary due to installation dependent variables. Maximum range is achieved when the reader is mounted away from metal and cards are presented parallel to the reader face. This allows the reader field to power up the card transponder at a farther distance.

HID Reader Family

A variety of HID readers are available for differing aesthetic tastes, mounting preferences, and interface requirements. But they all utilize passive card technology. In addition, all HID readers have a NEMA-4x rating and are suitable for outdoor use.

The Wiegand Data Interface is a widely used Access Control industry standard. All HID Readers are available with Wiegand output. The Wiegand interface consists of data lines called “Data 0”, “Data 1”, and “Data Return”. Toggling the respective line to ground (or Data Return) for a specified period of time sends data. The host sees these low signals as data bits. The data is a series of ones and zeros that can be partitioned to suit the needs of the system.

Another communications protocol called “Clock and Data” is also quite popular. HID produces reader models with Clock and Data interfaces. HID Clock and Data emulates a magnetic stripe reader (M/S Track 2). This reader can be used to replace existing magnetic stripe readers while keeping the existing host system. This reader outputs “Card Present”, “Clock”, and “Data” signals. The Card Present signal goes low before the start of data transmission, remaining there while card data is transferred and returns to high after transmission is complete. The Clock signal synchronizes the host system with the reader to ensure reliable data transfer. The Data signal sends the Card Number to the Host. Low signals are interpreted as 1’s and high signals as 0’s.

Serial communication interfaces are also rather common. In fact, almost all Personal Computers have at least one of them. The HID ProxPro is available with an RS232 and RS422 serial interface. RS485 connections are there too, but as of this writing, no standard protocol has been established.

The serial message sent contains HID card data in ASCII encoded hexadecimal digits followed by a checksum carriage return and line feed.

A transponder is the electronic circuit that is energized by, and sends data to the reader. HID builds transponders into several different packages.

HID Card and Transponder Family

HID Cards are available in a number of styles and programming formats. The ProxCard II and PhotoProx cards are the same size as credit cards and a little thicker. The ISOProx II, DuoProx II, and SmartProx are the same size and thickness as a credit card. For those who prefer not to carry a card, the ProxKey II is a small plastic key fob that fits nicely on a key chain. The Vehicle ID Tag is built to adhere to the inside of windshields for vehicle entry control.

ISOProx II and DuoProx II cards offer direct print capability and include options to combine other card technologies with proximity in a thin, easy to carry access control card.

The format in which a card is programmed determines the data pattern. All HID transponders can be programmed with the standard 26-bit card format. That format is compatible with most access control systems.
Exclusive “proprietary” formats are also available through system manufacturers.

HID Makes it Simple

The word that best summarizes the HID concept is “convenience”.

Convenience for an employee who can use the same HID card to open the gate of a secured parking lot, enter the building, clock in for payroll and attendance, document the checkout of tools and equipment, enable controls for restricted machinery, and record how much he spent for lunch at the company snack bar.

Convenience for system integrators who need to interface to a wide variety of systems.

Convenience for building management who need maintenance free equipment.

Convenience for security personnel who need to know that the people they protect are safe.

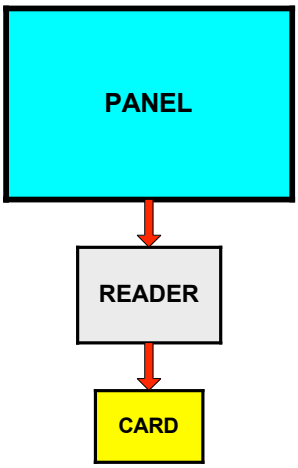
Tech Tip #8
The Roles of Panels, Readers, and Cards

When HID proximity cards, proximity readers, and panels are linked together in a system, the jobs they perform are co-operative, yet distinct. The differences in their roles are not always intuitively understood. Even people with years of experience in controls may have difficulty getting a clear picture of how these components work together. This is due to advances in reader and card engineering design, and the "security" environment in which these technologies were born. We want integrators and installers to have a solid grasp of the concepts. But we also want to avoid compromising security.

HID has taken a design approach that allows flexibility in the exchange of technical information during system setup, while making it very difficult to forge, or reverse-engineer the security product.

How can a complex security system be planned, and implemented without the exchange of sensitive information? *It can't.* But detailed information can be communicated and remain secure *if the information is dictated by the panel.*

It all starts at the panel…



The panel determines two fundamental features of readers and cards. First is the instrumentality of reader to panel data transmission. This is called the "protocol", or the "interface". Second is the conformation the data must have to be accepted and understood. This is called a "format".

1. Panel Communications Protocol

The panel dictates what components can be connected to it. In the case of the reader, ***the reader interface must match that of the panel***. It is a hardware reality. If the panel only accepts Wiegand data, then only readers that can output Wiegand data can be used. Common panel interfaces include Wiegand, Clock-and-Data, and Serial RS232, RS422, RS485*.
*A standard RS485 protocol has not been established as of this writing, 1998 A.D.

Some panels can connect to a variety of interfaces via signal conditioning modules, or "personality" daughter boards. After-market data converters are also available that convert one interface type to another.

2. Panel Format Settings

Panels are built to accept data in specific formats. Most use the 26-bit standard format, in addition to others. Simple panels might use only one or two formats, but sophisticated panels are software configurable and accept hundreds of different formats. Some can even create customized formats.

Once a format is decided upon, the panel is configured for it. Then proximity cards can be ordered for use with that format. The ***card must be programmed to conform to the panel's format*** in order to function.

This "One Way" flow of setup information from panel to card is intentional. It makes it difficult for an unauthorized person who finds a proximity card to know where and how to use it. Even a person with the technical knowledge and equipment cannot positively identify the card format. That is because ***the complete format information is not on the card***, it's in the panel. The card data merely conforms to the panel format.

RECORDS

HID must assume that authorized persons have access to panel format, facility code, and card range information for the purpose of ordering cards, and testing the system. If the format contains a facility code, it should be recorded and stored with format information. If panel particulars are filed and maintained by the security department, or system integrator, making new card orders is very easy. If these records have not been kept, the simplest transaction can become impossible.

3. Reader and Card Exclusivity

All current standard HID readers can read data from all current standard HID cards. Standard HID readers and cards are not cross compatible with other brands of card and reader. There is one exception to this, the HID MultiProx system. The MultiProx reads Schlage 1030, 1040, 1050 cards and standard HID cards. There are also a few custom HID cards and readers that are not compatible with standard HID products. These are very rare. If an HID reader does not read a card it is almost always because the card is not an HID card.

All standard HID readers operate independent of the format. The reader will read and transmit card data to the panel without regard for what format was used to program the data. But the panel will reject all data that does not match its format. Just because the reader sends the data does not mean the panel will accept it.

Summary

The panel requirements dictate protocol, format, and facility code. This information, in addition to card number range, is vital for placing accurate reader and card orders.

Tech Tip #2
Wiegand Data Description

Wiegand Data is a prominent communications protocol in the Access Control industry.

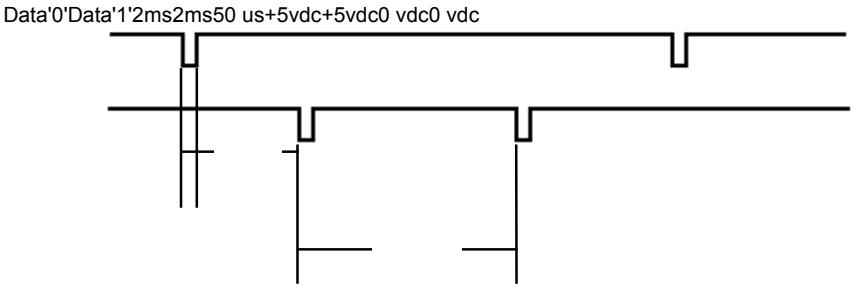
All current HID Reader Types (ProxPoint, MiniProx, Thinline, ProxPro, MultiProx Controller, and MaxiProx) are available with a Wiegand Interface.

The Wiegand Interface consists of three lines called “Data 1”, “Data 0”, and “Data Return” (Ground).

Both “Data 1” and “Data 0” lines normally sit at 5vdc. The “Data Return” line is normally tied to Ground. Data is considered to be present when either line goes low (0vdc) relative to Ground.

Switching “Data 1” to Ground (Data Return) for a period of 40 to 70 microseconds is interpreted as a logic “1”. Switching “Data 0” to Ground (Data Return) for a period of 40 to 70 microseconds will produce a logic “0”. There also must be a minimum 2 millisecond period between data hits, in which both “Data 1” and “Data 0” are high (+5vdc).

The presence of a two millisecond period between pulses between data bits results in a baud rate of 500 bits per second.



1001 (Binary 9) is represented in this drawing.

Tech Tip #5
Standard 26 bit Format

The Standard 26-bit Format is an open format. It is a widely used industry standard, and is available from many sources. Almost all access control systems accept the Standard 26-bit Format.

There are 256 possible facility codes. There can be up to 65,535 card ID numbers per facility code. The total number of cards that can use the entire range without duplication is 16,711,425. There are no restrictions on the use of this format. It is not tracked by HID, and there are duplicate cards in use.

Standard 26 Bit Format Structure

The standard 26 bit Wiegand format is H10301. It is binary encoded data. The format consists of 2 parity bits, 8 bit facility code and 16 bit card number fields. The format is shown below.

```
  ⇓   FC  ◊⇓    Card Number    ◊
PAAAAAAAABBBBBBBBBBBBBBBP
EXXXXXXXXXXXX
                XXXXXXXXXXXXO
```

P = Parity
A = Facility code, range = 0 to 255
B = Card Number, range = 0 to 65,535

O = Odd Parity
E = Even Parity
X = Parity mask

Tech Tip #7
Power Supply Recommendations

A ***LINEAR*** type power supply ensures maximum reader performance. Switching type supplies often interfere with optimum reader performance.

HID does not specify a single brand or model linear supply. It is recommended that you contact a power supply manufacturer of your choice. Ask them to specify a linear power supply that will meet the current and voltage requirements for your model of proximity reader.

REASONS FOR USING A LINEAR P.S.

1) When readers cycle through low, medium, and high power modes they need instantaneous current. Switching supplies monitor their output voltage and adjust their supply current by switching "on" and "off" rapidly (so they can't supply current on demand). This also causes fluctuations in the voltage of the power supply, compounding the problem. The result is seen as a reduction in read range.
In contrast, linear power supplies are always on, and ready to supply constant voltage and current.

2) Switching power supplies can radiate electrical "noise" that can interfere with card data transmission to the reader. This also reduces read range.