



HandKey II

Installation and Operation Manual

Recognition Systems Inc.
1520 Dell Ave.
Campbell, CA 95008

Customer Care: Tel: 408-341-4110
RSI Main Tel: 408-341-4100
RSI Main Fax: 408-341-4101
Web: www.handreader.com

P/N: 70100-6001

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the Installation Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

© 1998 through 2001 Recognition Systems, Inc. – ALL RIGHTS RESERVED
Document Part Number: 70100-6001 – Revision 2.4 – September, 2001

HandKey and *HandNet* are trademarks of Recognition Systems, Inc.

Windows is a trademark of Microsoft Corporation.

The trademarks used in this Manual are the property of the trademark holders. The use of these trademarks in this Manual should not be regarded as infringing upon or affecting the validity of any of these trademarks.

Recognition Systems, Inc. reserves the right to change, without notice, product offerings or specifications.

No part of this publication may be reproduced in any form without the express written permission from Recognition Systems, Inc.

Table of Contents

Introduction	5
HandKey II	5
Biometrics	5
Principle of Operation	5
The HandKey II Reader	6
Specifications	8
Options	9
UL Compliance	9
Planning an Installation	11
Site Preparation	11
Hand Reader Placement	11
Wiring	12
Power Input	12
Battery Backup Operation	12
Earth Ground and Shielding	13
Door Control Output	17
Lock Output Mode	17
Card Reader Emulation Mode	17
Inputs and Outputs	17
Networking and Communications	19
Stand-alone Hand Reader	19
Master or Remote Hand Reader in a Hand Reader Network	19
Remote Hand Reader in a Hand Reader Network Connected to a Host PC	20
Remote Hand Reader Connected to a Host PC via Optional Modem	20
Remote Hand Reader Connected to a Host PC via Optional Ethernet	21
Printer	21
Mechanical Installation	23
Wall Plate Installation	23
Wall Preparation	23
Mounting the Wall Plate	24
Routing the Wiring	24
Attaching the Hand Reader	24
Wiring Connections	26
Wiring Examples	26
Setting the DIP Switches	35
End of Line Termination	36
Communication Method	37

Erasing Hand Reader Memory	37
Erasing the Hand Reader Setup	37
Erasing the Hand Reader Setup and User Database	37
Closing the Hand Reader	38
Powering the Hand Reader	38
Programming the Hand Reader	39
Authority Level	40
Programming Order	40
System Management and Maintenance	41
Design an ID Numbering System	41
Enter a Command Menu	42
If No One is Enrolled in the Hand Reader	42
If Users are Enrolled in the Hand Reader	43
Navigating Command Menus	44
System Maintenance	45
Cleaning the Hand Reader	45
User Score	46
Service Menu	47
Navigating the Service Menu	47
Service Commands	47
Setup Menu	51
Navigating the Setup Menu	51
Setup Commands	51
Set Beeper	59
Management Menu	61
Navigating the Management Menu	61
Management Commands	61
Enrollment Menu	63
Preparation	63
User Education	63
Proper Hand Placement	64
Left Hand Enrollment	64
Read Score	65
Navigating the Enrollment Menu	65
Enrollment Commands	65
Security Menu	67
Navigating the Security Menu	67
Security Commands	67
Limited Warranty	73
Glossary	75

1.0 Introduction

1.1 HandKey II

The HandKey II is Recognition Systems' fourth generation biometric access control Hand Reader¹. The Hand Reader records and stores the three-dimensional shape of the human hand for comparison and identity verification. Upon verification, the Hand Reader produces an output that can unlock a door, send card format data to an access control panel, or communicate with a host computer. The Hand Reader also has auxiliary inputs and outputs that can be used to control other systems such as CCTV cameras and alarms.

1.2 Biometrics

Biometrics is a term describing the automatic measurement and comparison of human characteristics. While its origins are ancient, the evolution of advanced scanning and microprocessor technology brought biometrics into everyday life. Electronic hand geometry technology first appeared in the 1970s. Recognition Systems Inc., founded in 1986, built the first mass-produced hand geometry readers and made biometric technology affordable for the commercial market. Today, Recognition Systems' products are in use in every imaginable application from protecting cash vaults to verifying parents in obstetric wards.

1.3 Principle of Operation

The Hand Reader uses low-level infrared light, optics, and a CCD (IC chip) camera to capture a three-dimensional image of the hand. Using advanced microprocessor technology, the Hand Reader converts the image to an electronic template. It stores the template in a database with the user's ID number.

To gain access, the user enters his or her ID number at the Hand Reader's keypad or uses an external card reader. The Hand Reader prompts the user to place his or her hand on the reader's platen². The Hand Reader compares the hand on the platen with the user's unique template. If the images match, the Hand Reader unlocks the door or sends the user's ID number to a third-party access control panel for processing.

-
1. For the sake of using a consistent name throughout the manual, the HandKey II is referred to as the Hand Reader for the remainder of this manual.
 2. The Platen is the flat surface at the base of the Hand Reader (see Figure 1-1). This is where users place their hands for enrollment and verification. It has guide pins to position the fingers during use.

1.4 The HandKey II Reader

The Hand Reader is an intelligent access control system that can operate as a stand-alone unit, in a network with other Hand Readers, or in a network with a host computer. Refer to Figure 1-1 when reviewing the information in this section.

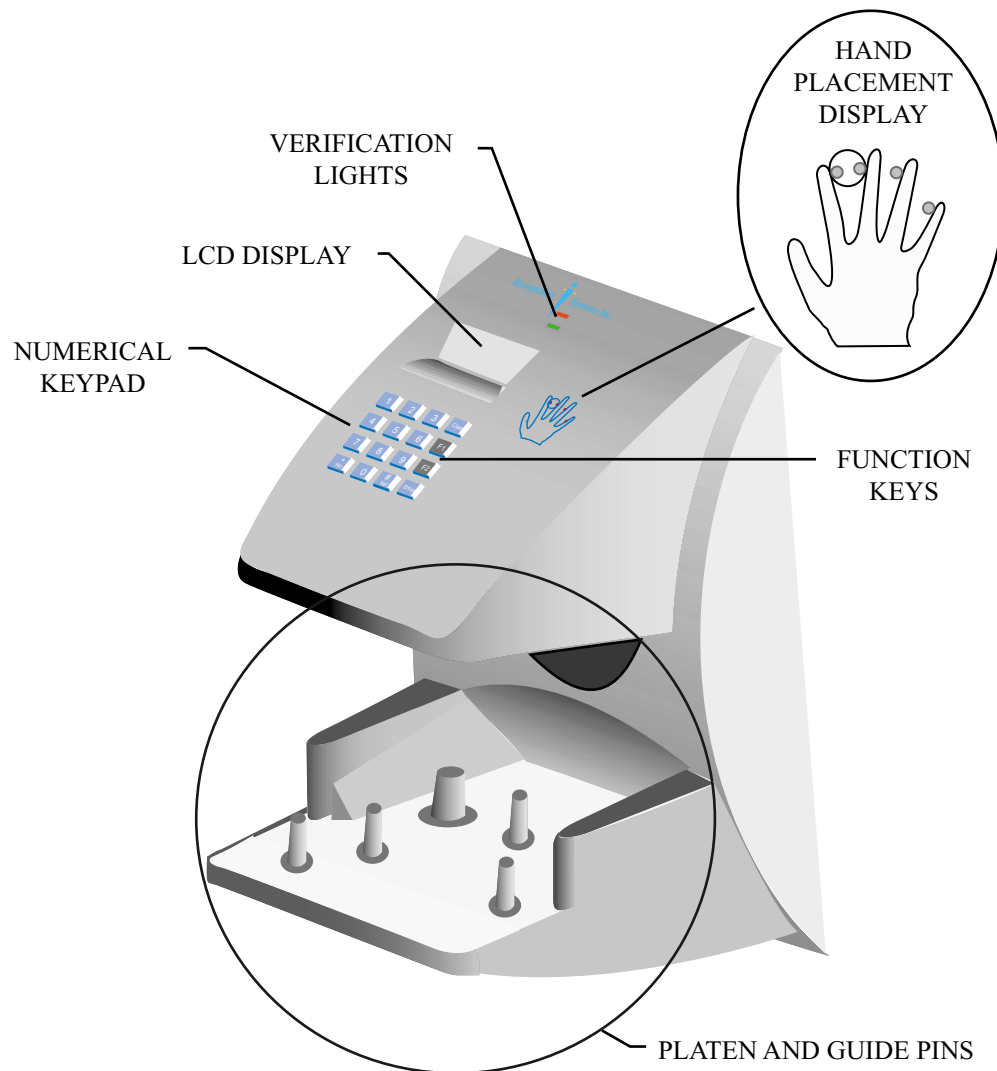


Figure 1-1: The HandKey II

The Hand Reader has an integrated keypad for ID entry and reader programming. It has two function keys (F1 and F2) that can be set to activate external devices such as a doorbell or an automatic door. The **CLEAR** and **ENTER** in data entry and programming.

Four different features assist the user with hand placement and read verification.

1. A light emitting diode (LED) hand placement display on the hand reader's top panel assists users with hand placement on the platen.
2. A liquid crystal display (LCD) shows operational data and programming menus.
3. "Red light/green light" verification LEDs quickly inform users if their verification attempts were accepted or rejected.
4. An internal beeper provides audible feedback during keypad data entry and user verification.

1.5 Specifications

Table 1: Specifications

Size:	8.85 inches wide by 11.65 inches high by 8.55 inches deep (22.3 cm)
	22.3 cm wide by 29.6 cm high by 21.7 cm deep
Power:	12 to 24 VDC or 12 to 24 VAC 50-60 Hz, 7 watts
Weight:	6 lbs (2.7 kg)
Wiring:	2 twisted-pair, shielded, AWG 22 or larger (such as Belden 82732)
Temperature:	-10C to +60C – non-operating/storage (14F to 140F)
	0C to 45C – operating (32F to 113F)
Relative Humidity Non-Condensing:	5% to 85% – non-operating/storage 20% to 80% – operating
Verification Time:	1 second or less
Memory Retention:	5 years using a standard internal lithium battery
Transaction Buffer:	5120 transactions
ID Number Length:	1 to 10 digits
Baud Rate:	300 to 28.8 K bps
Communications:	RS-232, RS-422, RS-485 2-wire, optional Ethernet, optional Modem
User Capacity:	512 users expandable to 32,512
Card Reader Input:	Proximity, Wiegand, Magnetic Stripe, Bar Code (5 VDC provided by Hand Reader)
Card Reader Output:	Wiegand, Magnetic Stripe, Bar Code
Duress Code:	1 leading digit, user definable
Door Controls:	Request to Exit input, Door Switch input, Lock output (open collector, 5 VDC present, sinks to ground, 100 mA max)
Alarm Monitoring:	Tamper, Door Forced, Duress
Event Monitoring:	There is a variety of monitoring options including events such as: Invalid ID, Time Zone Violation, ID Refused, Try Again, Power Failure
Time Zones:	62 total – 2 fixed, 60 programmable

Table 1: Specifications

Auxiliary Outputs	3 user definable (open collector, 5 VDC present, sinks to ground, 100 mA max)
Auxiliary Inputs	Auxiliary Input 1 and 2 (open collector, 5 VDC present, sinks to ground, 100 mA max)

1.6 Options


HandKey units have the following options available.

- Backup Battery Support See Technical Note 70200-0012 – Rev. C
- Modem Communication See Technical Note 70200-0013 – Rev. C
- Ethernet Communication See Technical Note 70200-0014 – Rev. C

Recommend European Power Supply¹:

Ault, Inc.
7300 Boone Ave. North
Minneapolis, MN 55428 USA
PH: 612-493-1900
E-mail: info@ault.com

Part number: D48-121000-A040G
230 VAC Input, 12 VDC @ 1Amp output (unregulated)
Ault style #41 connector (barrel plug)

 approved.



1. Not evaluated by UL for UL 294 installations.

1.7 UL Compliance

The HandKey II meets UL compliance requirements for UL294 Access Control Systems under the following conditions:

1. The HandKey II is configured at the factory with a Wiegand output that enables the HandKey II to communicate with an access control panel. The access control panel controls the locking and unlocking of the door. The panel must reside on the secure side of the facility.

2.0 Planning an Installation

2.1 Site Preparation

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about hand reader location and other systems that connect to the Hand Reader. Look for any existing wall preparations and wiring that other contractors may have installed for the Hand Readers.

2.2 Hand Reader Placement

The recommended height for the Hand Reader platen is 40 inches (102 cm) from the finished floor. The Hand Reader should be out of the path of pedestrian and vehicular traffic, and convenient to, but not behind the door it is controlling. Avoid placing the Hand Reader where users must cross the swing path of the door. The Hand Reader should be in an area where it is not exposed to excessive airborne dust, direct sunlight, water, or chemicals.

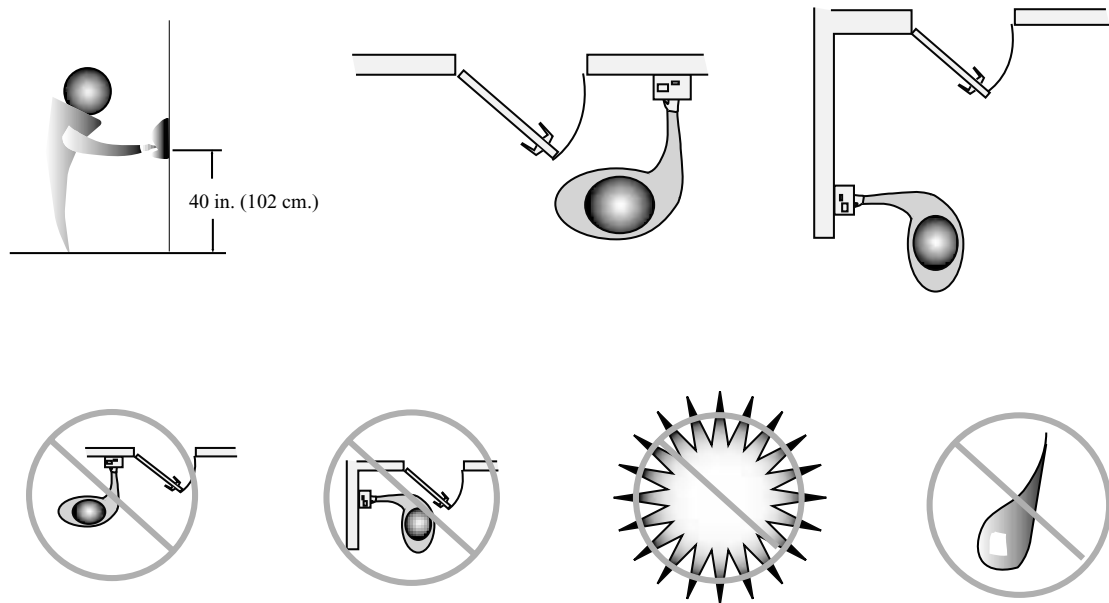


Figure 2-1: Hand Reader Placement Rules

NOTE For the following sections, Recognition Systems does not supply hardware items such as door control relays, door locks, switches, relays, communications or power wiring, or power supplies (a PS-110 or PS-220 power supply can be purchased from Recognition Systems to power the Hand Reader).


2.3 Wiring

Four basic circuits typically connect to the Hand Reader:


- Power Input
- Door Control Inputs and Outputs
- Networking and Communications
- Card Reader Input and Emulation Output


2.4 Power Input

The Hand Reader requires 12 to 24 volts DC (600 mA) or 12 to 24 volts AC (7 watts). Power can be connected either to terminals 1 and 2 on the terminal strip or through barrel jack J12.

 **NOTE** *Terminal 1 and the center pin of jack J12 are connected together. Terminal 2 and the sleeve of jack J12 are connected together.*

A full-wave bridge rectifier input structure is used in the power supply of the Hand Reader, making the polarity of terminals 1 and 2 irrelevant. Recognition Systems recommends using terminal 1 for positive (+) voltage and terminal 2 for common (-) for consistency. If J12 is used to attach power with the optional Recognition Systems wall-mount power supply, terminal 1 will reflect +13.8 VDC (unregulated) and terminal 2 will be power supply common.

 **NOTE** *Neither terminal 1 or terminal 2 is connected to the Hand Reader ground.*

 **NOTE** *Do not connect a HandKey's power supply to a switched duplex outlet. The HandKey must have a constant source of power for proper operation.*

2.4.1 Battery Backup Operation

The Hand Reader uses an internal switching regulator to obtain internal operational power. It accepts input voltages from 12 to 24 VDC or 12 to 24 VAC at 50 to 60 Hz. An optional power-fail protection circuit board can be attached to the main circuit board to provide and control battery backup. The design of the internal power supply is such that any range of the above input voltages may be used and still provide proper battery charge voltage and battery backup operation. Switch-over to battery power is automatic and occurs when the input voltage falls to approximately 10.5 volts. At that time the internal battery charger is disabled to save power and uninterrupted operation continues on battery power.

When input power is restored, the Hand Reader switches off of battery operation and the battery charger is re-enabled to recharge the battery. Battery charge voltage is set at approximately 13.65 volts, and battery charge current is limited to approximately 50 mA. A fully discharged battery requires approximately 12 hours of charge to fully recover.

Additional options installed and specific configurations within the Hand Reader make it difficult to predict precisely how long battery support will last, but in general two hours of battery operation can be expected. While operating on battery backup due to loss of main input power, the battery output voltage is constantly monitored by internal circuitry. If the battery voltage reaches approximately 9.5 volts the Hand Reader automatically shuts down. This is done to prevent full exhaustion of the battery. A yellow indicator on the top panel illuminates to indicate that the Hand Reader is running off of battery power. This indicator extinguishes when main input power is restored.

Shunt J7 which is located immediately in front of the DIP switches on the main logic board (see Figure 3-3) enables or disables battery operation on those Hand Readers equipped with optional battery backup. If a Hand Reader does not have the optional battery backup package installed, J7 is not used. On Hand Readers equipped with the battery backup option, J7 allows service personnel a mechanism for disabling battery backup operation before removal of main input power. To fully power down a Hand Reader equipped with battery backup, remove or reposition shunt J7 so that the two pins protruding up from the main logic board are not connected to each other. This effectively opens the circuit, removing the battery from any internal circuitry. Main input power can then be removed and the Hand Reader will fully shut down. Once the Hand Reader has fully shut down, shunt J7 may be reinstalled. The design of the power supply is such that main input power must be reapplied to re-enable the battery protection mechanism. If shunt J7 is not properly installed, the internal backup battery will not be charged, and in the event of a main input power loss, the Hand Reader will shut down.

The Hand Reader with the battery backup option uses a 12 volt 800 ma/hour sealed lead acid battery to provide backup battery power. This battery is located immediately inside the rear panel of the Hand Reader and plugs into jack J4 on the keypad control circuit board located in the top of the chassis.

2.4.2 Earth Ground and Shielding

Recognition Systems recommends that all Hand Readers be grounded with a solid, reliable earth ground connection. This connection establishes a common ground return point used to protect internal semiconductor devices from ElectroStatic Discharge (ESD) and from external signal line transients. It also provides a common signal level reference point between externally networked HandPunches. Recognition Systems recommends that the earth ground source be identified by a qualified electrician familiar with electrical codes as well as wiring and grounding techniques.

This is an extremely important and often overlooked aspect of hard-wired serial communication systems. If the sending and receiving stations do not agree on the ground reference for the signal voltages, communication errors or a total inability to communicate may be observed. If the voltages are very different, it is even possible to damage the units.

The subject of grounding can be complicated, and the full circuit of a system, including power supplies and often even the building line power wiring, must be understood. It is strongly recommended that a qualified electrician or electrical engineer familiar with this subject be consulted when designing the wiring of an HGU network installation. Always adhere to any applicable electrical codes for your area. Recognition Systems is not responsible for damage done to units due to improper wiring.

NOTE Use any one of the following ground terminals to make the earth ground connection: 8, 10, 12, 14, 18, 20, 22, 24, or 26. Do **NOT** use terminal 2 to establish the earth ground connection; terminal 2 is not directly connected to ground.

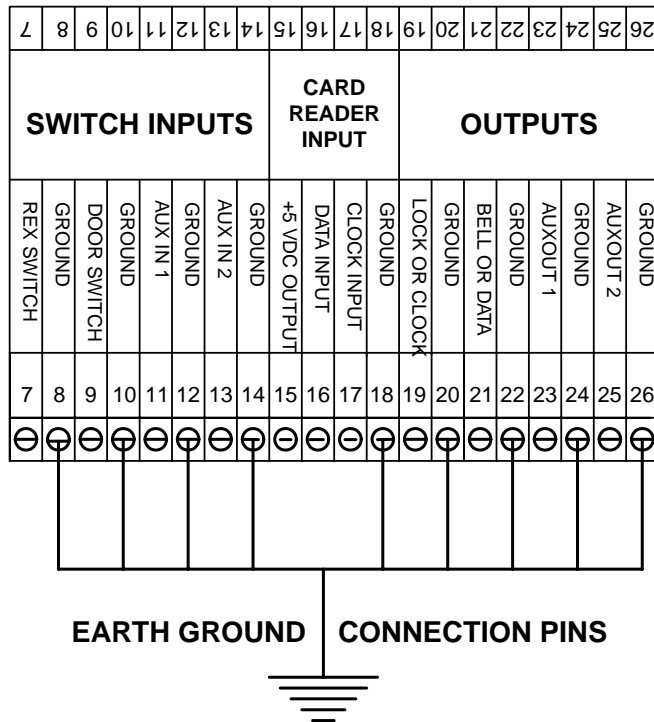


Figure 2-2: Earth Ground Connection Terminals

There are two standard methods for providing earth grounding to HandPunch units:

- earth grounding all units (see Section 2.4.2.1 on page15)
- carrying an earth ground to each unit (Section 2.4.2.2 on page15)

Earth ground all units when there is a good earth ground source near each unit and/or when there are very long cable runs between units.

Carry an earth ground to each unit when there are no earth grounds convenient to the unit and the unit’s power supply is floating.

2.4.2.1 Earth Ground All Units

One method of establishing a ground reference is to connect each unit's main board ground to earth ground. Earth ground is found on the third pin on standard AC line sockets (in the United States, this is the round one in the middle). If the building wiring is functioning correctly, this should be a low-impedance path to a true ground, which then serves as a common reference point for the units.

If this method of grounding the units is used, it is not necessary to connect the units in the network together with a ground line in the communication cable. Indeed, doing so could create ground loops—large-area loops which provide a good coupling to external magnetic fields—which may actually compound communication problems. If a magnetic field, such as that from a lightning strike, induces a voltage in the ground loop, it is possible for large currents to flow around the loop, which can raise the ground potential of some units relative to others. When the shield or the cable is connected to any ground in this configuration, it should be connected only at one end to prevent the formation of ground loops.

For systems with multiple units on a network, there will be a series of cables daisy-chained between the units, and the shield of each leg of the network should be connected to ground at only one end. It does not matter which end. An example of this method of grounding is shown in Figure 2-3.

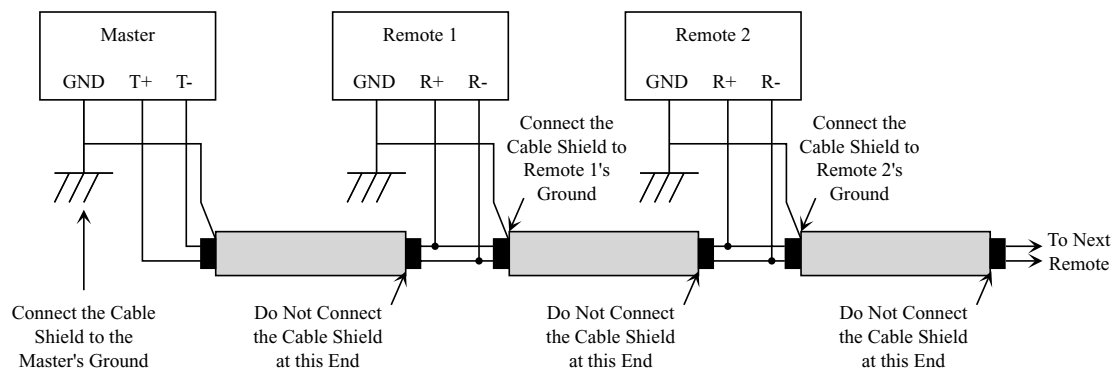


Figure 2-3: Communication Shielding With All Units Earth Grounded

All units are connected to the same earth ground. Each shield ground is connected to only one unit, then interrupted to prevent the formation of ground loops. Two sets of lines are wired as shown in Figure 2-3. It does not matter significantly which unit's GND is used for a particular shield, as long as the path is broken from unit to unit.

2.4.2.2 Carry a Ground Line to Each Unit

The second method of establishing a ground reference in a system with floating power supplies is to use the ground line in the RS-422 cable to establish a common reference voltage for the communication signals. This line should be connected to the negative power terminal on the data converter or the ground line in the RS-232 port from the host PC system. It should then be carried to one of the ground terminals on the back of

each unit in the network. An example of this method of grounding is shown in Figure 2-4.

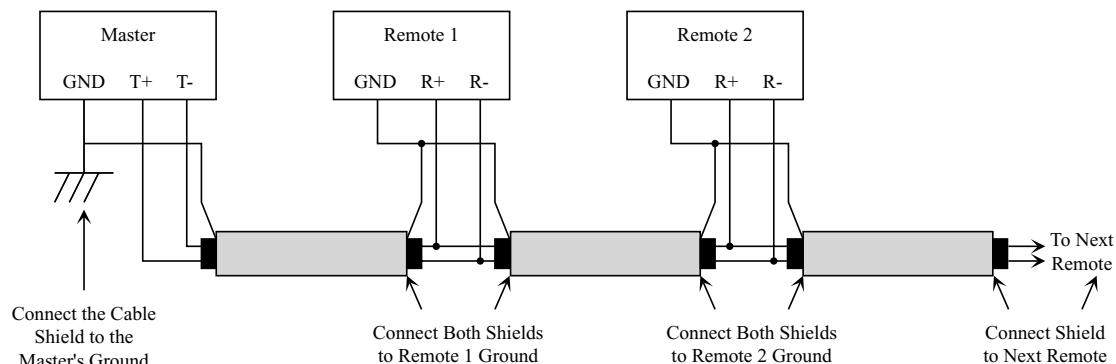


Figure 2-4: Communication Shielding Carrying a Single Ground to Each Unit

If no earth ground is available at the units, this is the only possible method of connecting the grounds. Even if an earth ground is available, depending on the building's power wiring and other environmental issues, this method may be superior to the previous one, since it establishes the ground of each unit independently of the building power lines. Local variations in grounds between buildings, or from one point to another in a very large building, (perhaps due to elevator motors or other large-current drawing machines) will have no effect on the communication network if this configuration is used.

However, the power supplies must be truly floating, with no hidden paths back to the high-voltage side of the transformers, or to earth ground. Since this is difficult to achieve (there is always some parasitic capacitance between the primary and secondary in any transformer), this method may be more susceptible to high-frequency transients in the high-voltage side of the power lines than the earth-grounded method.

The master unit's ground establishes the ground for the entire system. The main board ground points are connected to the shield ground at each unit, but are not connected to earth ground. The ground point on the master can be the data converter power supply negative terminal, or the GND pin on the RS-232 cable. If the master is an HGU, its main board ground can be used. This configuration should only be used if the power supplies to the units are truly floating, otherwise ground loops will be created, and differences in local grounds may cause large currents to flow through the cable shield.

2.5 Door Control Output

The Hand Reader can operate a door in two different modes: lock output and card reader emulation. The wiring for each mode is significantly different.

2.5.1 Lock Output Mode

In the lock output mode, the Hand Reader acts as an intelligent access reader signaling a lock relay or controller to unlock the door. It also monitors the status of the door. The decision to unlock the door is made by the Hand Reader after a valid verification. Users may be assigned time restrictions to limit access during specified hours or days.

2.5.2 Card Reader Emulation Mode

In card reader emulation mode, the Hand Reader outputs Wiegand, magnetic stripe, or some other card reader signal, typically to an access control panel when a user successfully verifies. This mode makes integrating with existing access control systems fast and simple. On retrofit applications, the existing card reader wiring can be used to connect the Hand Reader to the panel if it has AWG 22 or larger conductors and is in good condition.



The standard Hand Reader emulation format is for a 26-bit Wiegand card using an 8-bit facility code. Other formats and card reader technology emulations are available. Consult the factory for formats other than 26-bit Wiegand.

The ID number may be entered via the integrated keypad or an external card reader.

- If the user enters the ID number from the keypad, the Hand Reader sends the ID number to the access panel in the specified card format with a pre-programmed facility code.
- If the ID number is entered via the card reader, the Hand Reader stores the card data and then sends the data, unmodified, to the access panel when the user successfully verifies.

2.5.3 Inputs and Outputs

In addition to the Lock and Auxiliary Output and the Card Reader Emulation Output, the Hand Reader has additional inputs and outputs for use with alarms and other controllers.

- Three Programmable Auxiliary Outputs
- Door Monitor Switch Input
- Request to Exit Input
- Card Reader Input for Wiegand or Magnetic Stripe
- Two Auxiliary Inputs

An open collector transistor driver drives each one of these outputs. Open collector refers to a transistor configuration capable of sinking current (by “pulling down” one side of a load to ground) but not able to source current – e.g. the transistor output is incapable of supplying current to drive up the output voltage and must rely on an external voltage source to accomplish this.

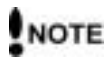
Hand Reader outputs, when measured to ground, generally show around 4.5 volts when they are inactive and no load is attached. This voltage is developed by a combination diode and series resistor pull up to the internal +5 volt supply of the Hand Reader. These outputs are pulled up internally to insure that they remain in a known condition if used to output Wiegand or magnetic stripe data to some external device.

If one of the outputs is shorted to ground, there will be approximately 5 mA of current flowing through the short, but no damage will occur. Because of the open collector structure of the outputs, each output is free to float to whatever external voltage is applied (when inactive). For example, if one side of a relay coil is connected to an external +12 volt power source and the other side of the relay coil is measured with respect to the ground of the external power source, the measurement will be +12 volts.

If the ground of the external power source (+12 volt return) is tied to the ground of the Hand Reader, and the free relay coil wire connected to the LOCK output, the LOCK output pin will read +12 volts also (when inactive). This is because the LOCK output is not active and free to “float” to whatever external voltage is applied. When a hand is verified, the LOCK output becomes active and essentially looks like a short to the Hand Reader ground. This “short” causes the full +12 volts of the external power source to be placed across the relay coil, energizing the relay. The ground of the external +12 volt source must be tied to the Hand Reader ground to make a complete circuit path.

All Hand Reader outputs are rated at +24 volts DC maximum with a maximum current draw of 100 mA. This means that it is acceptable to use up to a +24 volt DC external power supply to energize external devices. Whatever external relay is used should be chosen to match the external power supply voltage. For example, if the external relay coil is rated at 15 volts, a 15 volt external power supply should be used. In no case should the external voltage be higher than +24 VDC.

Each Hand Reader has a protection mechanism built in to protect against voltage transients (spikes) coming back into the Hand Reader from an external relay coil. Transients from an “opening” or de-energizing relay coil can reach several hundred volts. This protection is on all Hand Reader outputs and will limit reverse spikes to approximately 28 volts to protect the open collector transistor driver. Hand Reader outputs are NOT designed to switch AC voltages. DC voltages MUST be used and the correct polarities MUST be maintained.



Relays or devices connected to the lock and auxiliary outputs must not exceed 0.1 A current draw.

3.0 Networking and Communications

Hand Reader networking and communications can be configured in one of five ways:

- as a stand-alone Hand Reader
- as a master or remote Hand Reader in a Hand Reader network
- as a remote Hand Reader in a Hand Reader network connected to a host PC
- as a remote network connected via optional Modem to host PC
- remote network connected via optional Ethernet to host PC

3.1 Stand-alone Hand Reader

When installed as a stand-alone access control system there is no communication wiring to other Hand Readers or to a host computer. Power input and control output wiring are all that are required. An RS-232 serial printer output is available for event logging (refer to the [Printer](#) section on page 11). Recognition Systems highly recommends using Backhand™ software to backup template information stored in the Hand Reader.

3.2 Master or Remote Hand Reader in a Hand Reader Network

Multiple Hand Readers can be linked together in a Hand Reader network.

- Up to 32 Hand Readers can be linked together on a 2-wire RS-485 or 4-wire RS-422 network (see Figure 3-1).
- Two twisted-pair, shielded, AWG 22 (or larger) wire should be used (Recognition Systems recommends Belden 82732 or its equivalent).
- The wiring must be a “daisy chain” network from Hand Reader to Hand Reader and must not exceed 4,000 feet (1220 meters) in total length.

The master/remote network requires user enrollment at the “master” Hand Reader. The master Hand Reader distributes hand template data with ID numbers and time restrictions (if any) to the other Hand Readers in the network. Users removed at the master Hand Reader are automatically removed from the remote readers. A printer connected to the master Hand Reader will report transactions from all Hand Readers on the network.

The master/remote network is highly effective with systems using card reader emulation mode for user populations smaller than 500 people since it does not require a host computer to manage the Hand Reader template database. Recognition Systems highly recommends using Backhand™ software to backup template information stored in the Hand Reader.

3.3 Remote Hand Reader in a Hand Reader Network Connected to a Host PC

Multiple Hand Readers can be linked to a personal computer (PC) for an integrated access control network. Real time monitoring of door status and a variety of alarm types can be done with Recognition Systems' HandNet for Windows™ (Recognition Systems model number HN-300) software. To run HandNet for Windows™ the computer must be PC compatible, using a Pentium™-166 or faster microprocessor and it must have a CD-ROM.

- The HandNet software can monitor over 1,000 Hand Readers simultaneously.
- An unlimited number of sites can be created with up to 32 Hand Readers per site.
- The Hand Readers report all transactions to the PC. The HandNet software records all transactions and displays a variety of reports generated from this information.
- Template management is handled automatically.
- Users may enroll at any Hand Reader in the system. The PC collects the data and distributes it to other Hand Readers in the network.
- Access may be restricted by time and by Hand Reader via HandNet's access profiles and by the use of time zones.

Typically, Hand Reader networks link to a PC using an RS-422 connection. These networks have the following requirements.

- Two twisted pair, shielded, AWG 22 wire or larger should be used (Recognition Systems recommends Belden No. 82723 or equivalent cable).
- Hand Readers must be wired together in a "daisy chain" network from Hand Reader to Hand Reader and then to the host PC. The total length of the wiring must not exceed 4,000 feet per network.
- The network requires an RS-422 to RS-232 converter (Recognition Systems P/N DC-102) at the PC.

Recognition Systems' optional HandNet for Windows™ software allows programming of most of the remote Hand Reader setups from the computer. However, each Hand Reader on the network requires the setting of an address. Hand Reader addresses may be repeated, but **only** on different sites. Display language, date format changes, and the communication mode must also be set at the Hand Reader.

3.4 Remote Hand Reader Connected to a Host PC via Optional Modem

An optional, internal "answer only" 14.4 bps modem is available for Hand Readers. This modem is designed for operation with United States phone systems. Site wiring should conform to standard telephone wiring standards and terminate at the Hand Reader with a standard RJ-11 modular phone jack. Each Hand Reader with a modem includes a 12-inch (30 cm) cable for the final connection between the phone jack and

the Hand Reader modem. Modem Hand Readers may be networked with up to 31 non-modem Hand Readers using RS-422 wiring. Refer to the [Using a Modem in a HandKey Network](#) Application Note (available from Recognition Systems) for detailed information.

3.5 Remote Hand Reader Connected to a Host PC via Optional Ethernet

The Hand Reader is available with an optional, internal Ethernet communications module for TCP/IP communications. The wiring must conform to 10BaseT standards. Typically, network wiring terminates at the Hand Reader with a standard RJ-45 modular jack. The cable from the jack to the Hand Reader is not provided with the Ethernet option. The IP address, Gateway, and Host Bits are entered at the Hand Reader in the SET SERIAL menu. Ethernet Hand Readers may be networked with up to 31 non-Ethernet Hand Readers using RS-422 twisted pair cable. Refer to the [Using an Ethernet HandKey Network](#) Application Note (available from Recognition Systems) for detailed information.

4.0 Printer

You can connect a serial printer to a Hand Reader. A printer connected to the master Hand Reader (in a master-remote application) will print every event as it occurs. A printer connected to a remote Hand Reader will print only the events that occur at that Hand Reader. Recognition Systems Inc. does not supply serial printers. Refer to the [Printer String Information](#) Application Note (available from Recognition Systems) for detailed information.

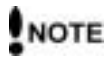
This page is intentionally left blank.

5.0 Mechanical Installation

Select an installation location based on the guidelines provided in the [Planning an Installation](#) section beginning on page 11.

5.1 Wall Plate Installation

5.1.1 Wall Preparation



For the following instructions protect the Hand Reader from the dust and debris generated during the wall plate installation process.

1. Remove the wall plate from the packing carton. Refer to Figure 5-1 for all wall plate references in the following section.

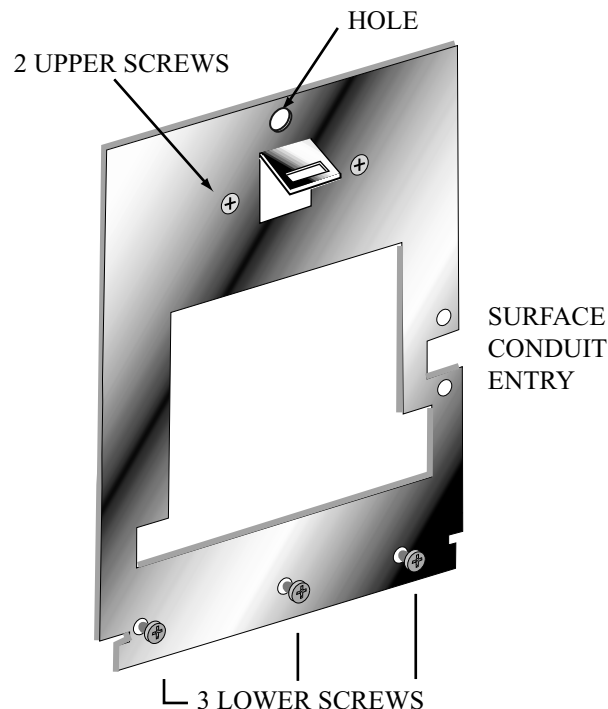


Figure 5-1: Wall Plate

2. Measure and mark a point 48 1/2 inches (123 cm) from the surface of the finished floor. This point will correspond to where the top-center point of the Hand Reader should be mounted.
3. For a hollow wall, drive a small nail into the wall at the mark and hang the wall plate from the leveling hole located near the top of the wall plate.
4. For a solid wall, hold the wall plate against the wall, centering the leveling hole over the mark in the wall.

5. Align a bubble level with the top edge of the wall plate and gently rotate the wall plate until the bubble level shows that the top edge of the wall plate is level.
6. Secure the plate to the wall using heavy masking tape.
7. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
8. For a concealed wiring connection, trace the outline of the open area in the center of the wall plate. Identify and mark a 1/2 inch hole through which the Hand Reader's wiring will be mounted.
9. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
10. Remove the wall plate, masking tape, and the nail (if used).

5.1.2 Mounting the Wall Plate

1. For a hollow wall, use the provided hardware to mount the wall plate. Use the two auger style fasteners for the upper two mounting holes. Use the toggle bolts for the three lower mounting holes.
2. For a solid wall, use expansion bolts to mount the wall plate. For all five mounting holes, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor.

5.1.3 Routing the Wiring

1. For a concealed wiring connection, drill a 1/2 inch hole in a convenient location within the open area of the wall plate. Pull the wiring to enter the Hand Reader through this hole in the open area.
2. For a surface conduit wiring connection, drill a 1/4 inch diameter hole, 1/4 of an inch deeper than the length of the expansion anchor for each of the two conduit clamp holes. Route 1/2 inch conduit to the Hand Reader, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the Hand Reader through the conduit.

5.1.4 Attaching the Hand Reader

1. Loosen the three bottom mounting screws until there is approximately 1/8 inch (3 mm) clearance between the screw head and the wall plate.
2. Remove the Hand Reader from its carton.
3. At the base of the Hand Reader is a piano hinge with three keyhole shaped slots that correspond with the three lower mounting screws. Align and hang the Hand Reader from the three lower mounting screws (see Figure 5-2 on page 25).

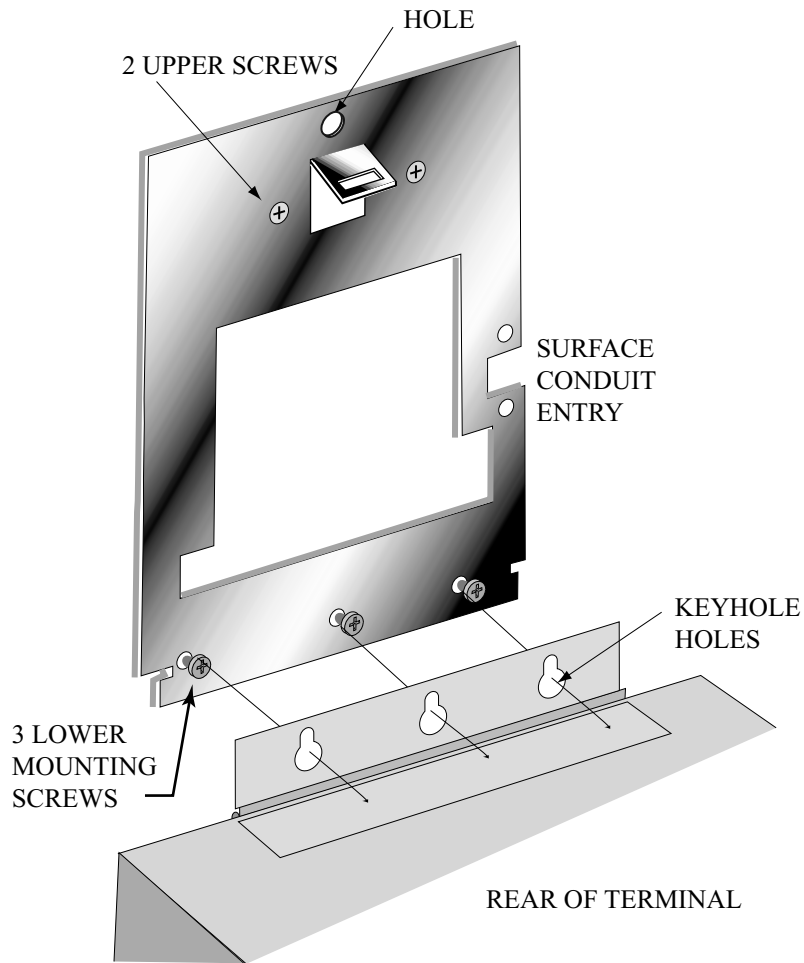


Figure 5-2: Attaching the Hand Reader to the Wall Plate

4. Tighten all three lower mounting screws.
5. The Hand Reader is now ready for its wiring connections.

6.0 Wiring Connections

Once the Hand Reader is attached to the wall plate the wiring connections to the Hand Reader can be made (see Figure 5-3).

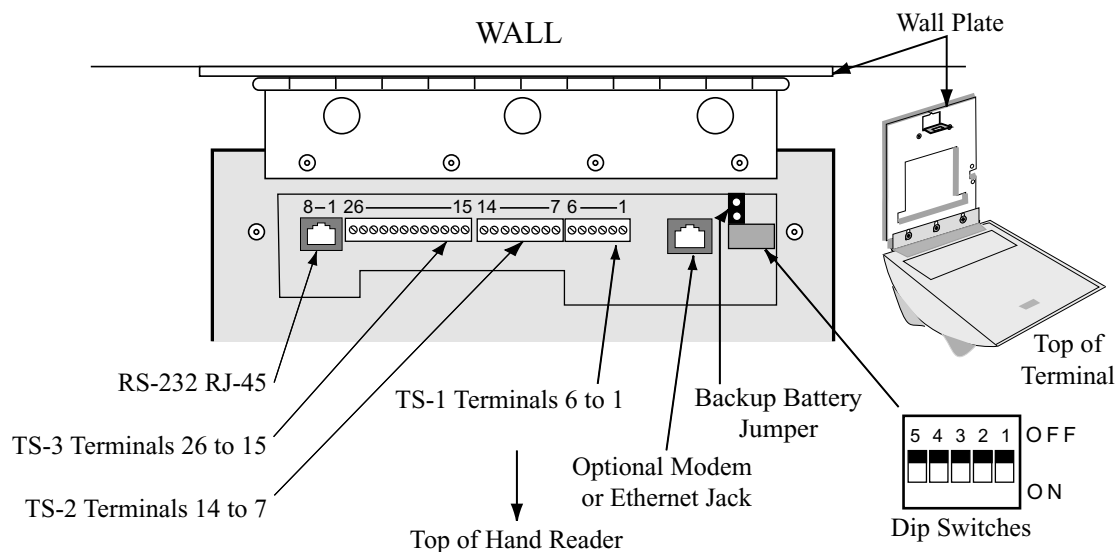


Figure 5-3: Wiring Connections and Dip Switches

6.1 Wiring Examples

The following Tables provide the pin outs for the terminal strips on the Hand Reader.

- Table 2 on page 27 provides the pin outs for TS-1: Power and Communication Connections.
- Table 3 on page 27 provides the pin outs for TS-2: Input Connections.
- Table 4 on page 28 provides the pin outs for TS-3: Card Reader and Output Connections.
- Table 5 on page 28 provides the pin outs for the RJ-45 Serial RS-232 Connection.

The following Figures provide typical Hand Reader wiring diagrams.

- Figure 5-4 on page 29 provides a typical Lock Output wiring diagram.
- Figure 5-5 on page 30 provides a typical Auxiliary Output wiring diagram.
- Figure 5-6 on page 31 provides a typical Card Reader Emulation Mode wiring diagram.
- Figure 5-7 on page 32 provides a typical RS-422 Master/Remote Network System wiring diagram.
- Figure 5-8 on page 33 provides a typical RS-485 2-Wire Master/Remote Network System wiring diagram.

- Figure 5-9 on page 34 provides a typical Host PC Network System wiring diagram.
- Figure 5-10 on page35 provides a typical Printer to Hand Reader wiring diagram.

Table 2: TS-1 - Power and Communication Connections

Terminal	Connection
1	Power Input 12 to 24 VDC/VAC
2	Power Return
3	RS-422 Rx- or RS-485 Rx-/Tx-
4	RS-422 Tx- or RS-485 Rx+/Tx+
5	RS-422 Rx+
6	RS-422 Tx+

Table 3: TS-2 - Input Connections

Terminal	Connection
7	Request to Exit Input
8	Ground
9	Door Monitor Switch Input (NC Standby)
10	Ground
11	Auxiliary Input 1
12	Ground
13	Auxiliary Input 2
14	Ground

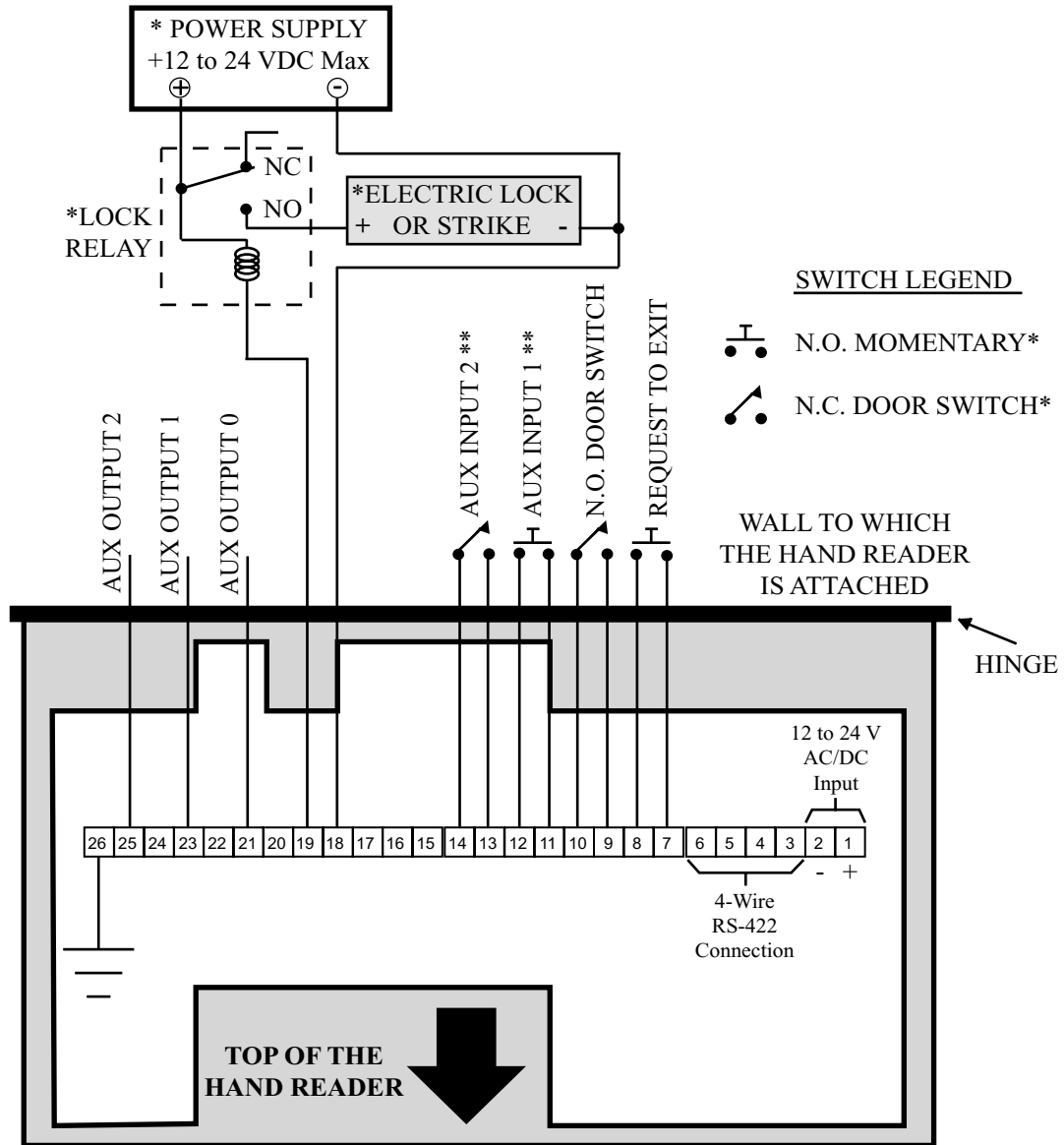
Table 4: TS-3 - Card Reader and Output Connections

Terminal	Connection
15	+5 VDC @ 400 mA Max. Output for External Card Reader
16	Card Reader: Wiegand D0 or Magnetic Stripe Data Input
17	Card Reader: Wiegand D1 or Magnetic Stripe Clock Input
18	Card Reader Ground
19	Lock Output or Wiegand D1 or Magnetic Stripe Clock Output
20	Ground
21	Auxiliary Output 0 or Wiegand Data 0 or Magnetic Stripe Data Output
22	Ground
23	Auxiliary Output 1
24	Ground
25	Auxiliary Output 2
26	Ground

Table 5: RJ-45 Serial RS-232 Connection

Pin	Signal	Connection
1	RI	* Ring Indicator Input (from external device)
2	CD	* Carrier Detect Input (from external device)
3	DTR	* Data Terminal Ready Output (to external device)
4	GND	Ground
5	Rx Data	Receive Data Input (from external device)
6	Tx Data	Transmit Data Output (to external device)
7	CTS	* Clear to Send Input (from external device)
8	RTS	* Ready to Send Output (to external device)

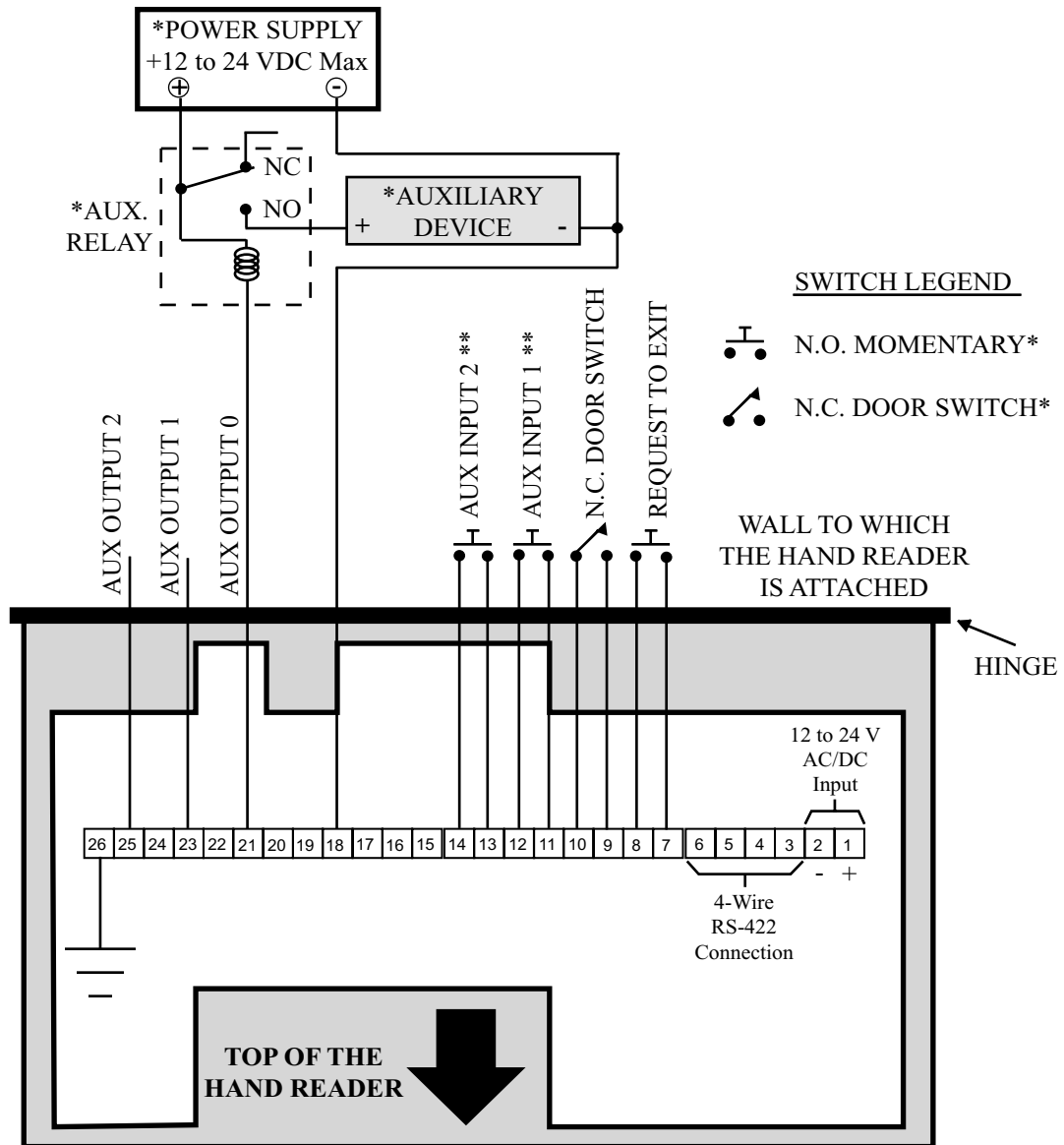
* These signals are not currently supported.



* These components are not supplied by Recognition Systems, Inc.

** The operation of the Auxiliary Inputs depend upon how the inputs have been configured.

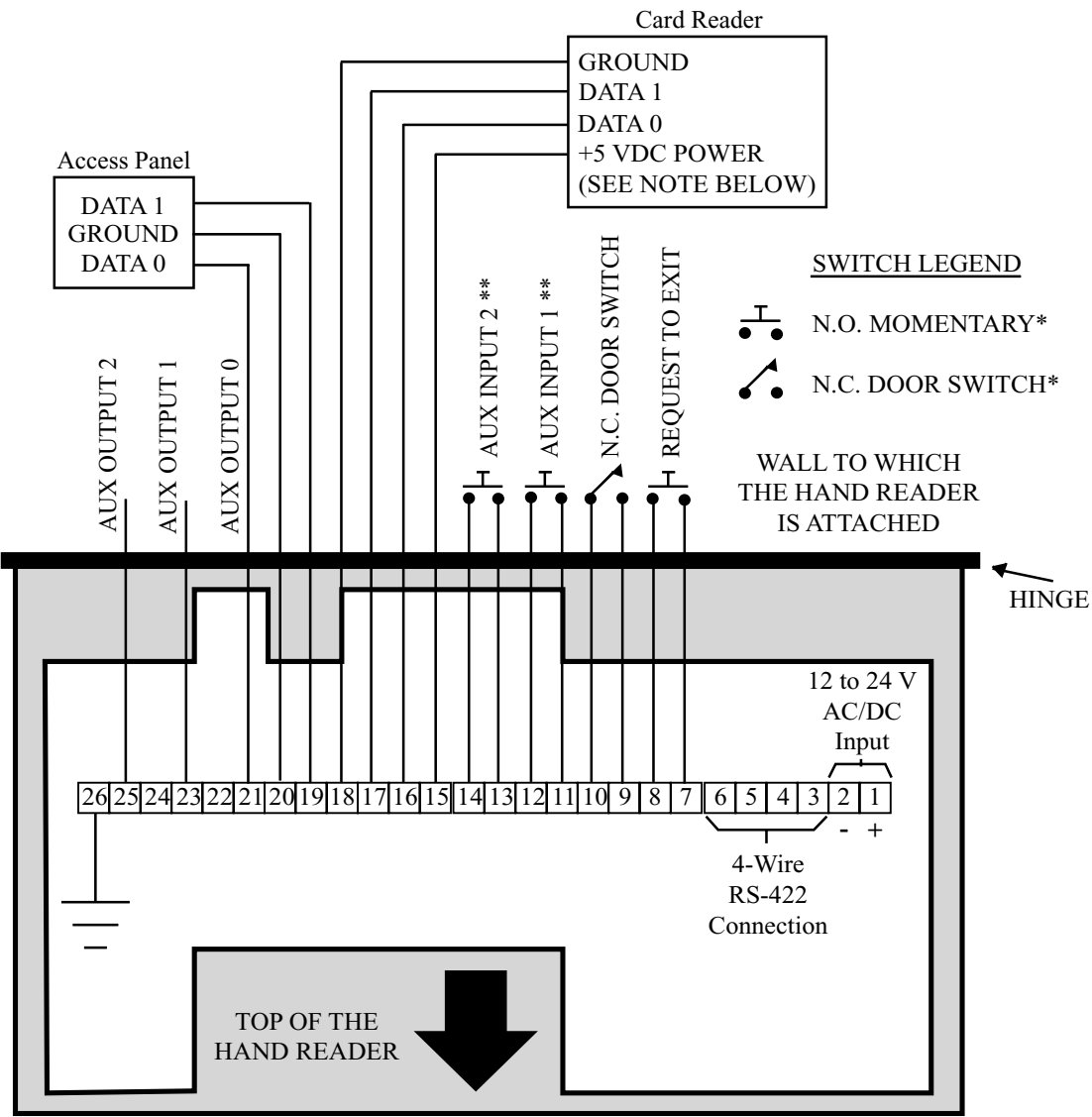
Figure 5-4: Lock Output Wiring Diagram



* These components are not supplied by Recognition Systems, Inc.

** The operation of the Auxiliary Inputs depends upon how the inputs have been configured.

Figure 5-5: Auxiliary Output Wiring Diagram



* These components are not supplied by Recognition Systems, Inc.

** The operation of the Auxiliary Inputs depends upon how the inputs have been configured.

NOTE: For +12 VDC readers, connect power supply +12 VDC to card reader.

Figure 5-6: Card Reader Emulation Mode Wiring Diagram

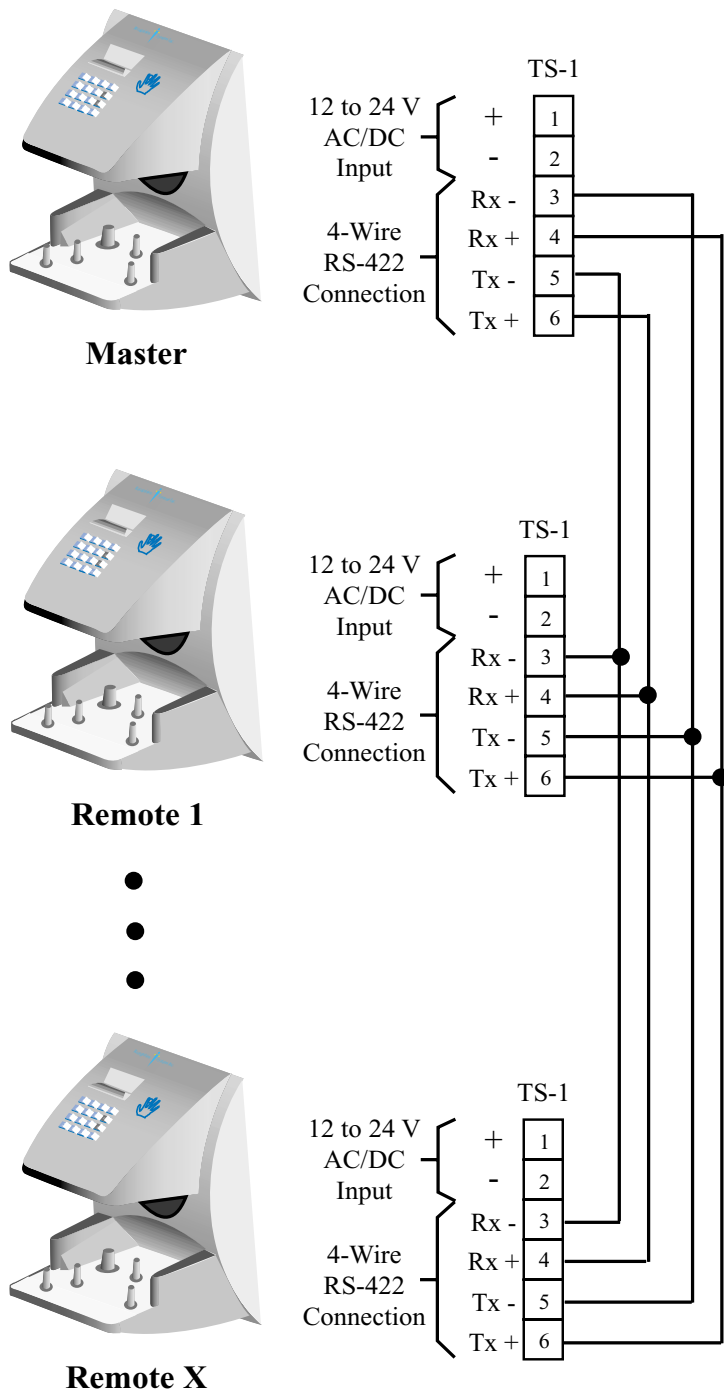


Figure 5-7: RS-422 4-Wire Master/Remote Network System Wiring Diagram

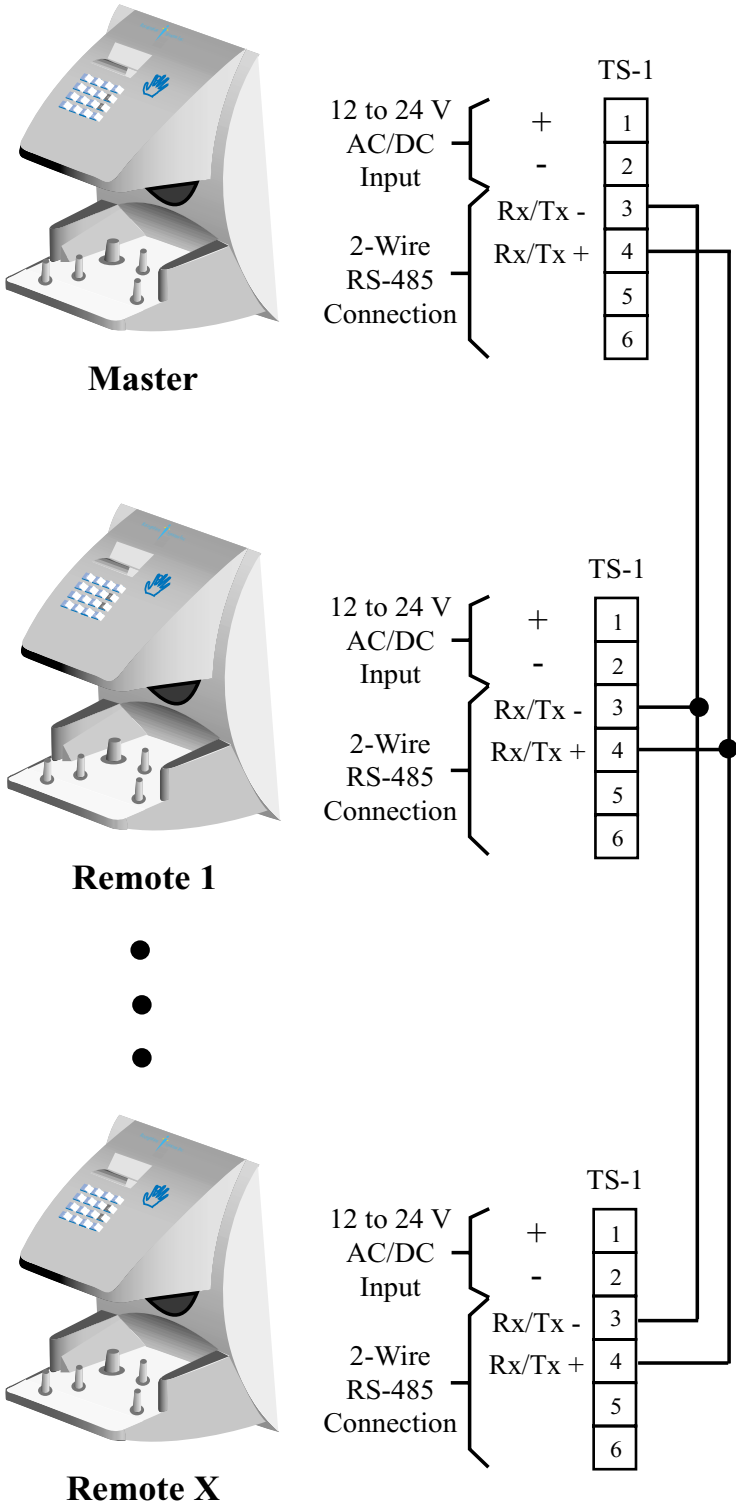


Figure 5-8: RS-485 2-Wire Master/Remote Network System Wiring Diagram

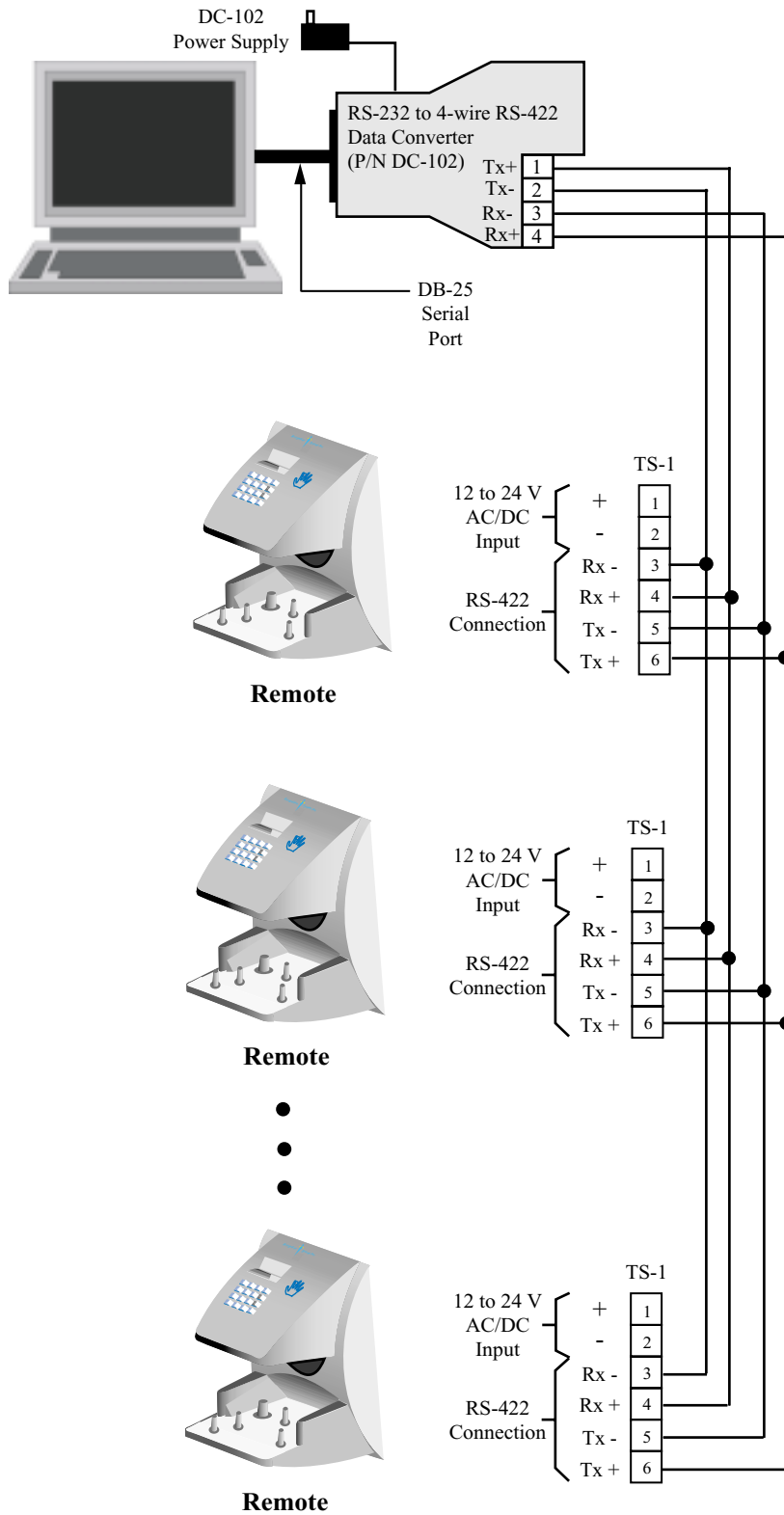
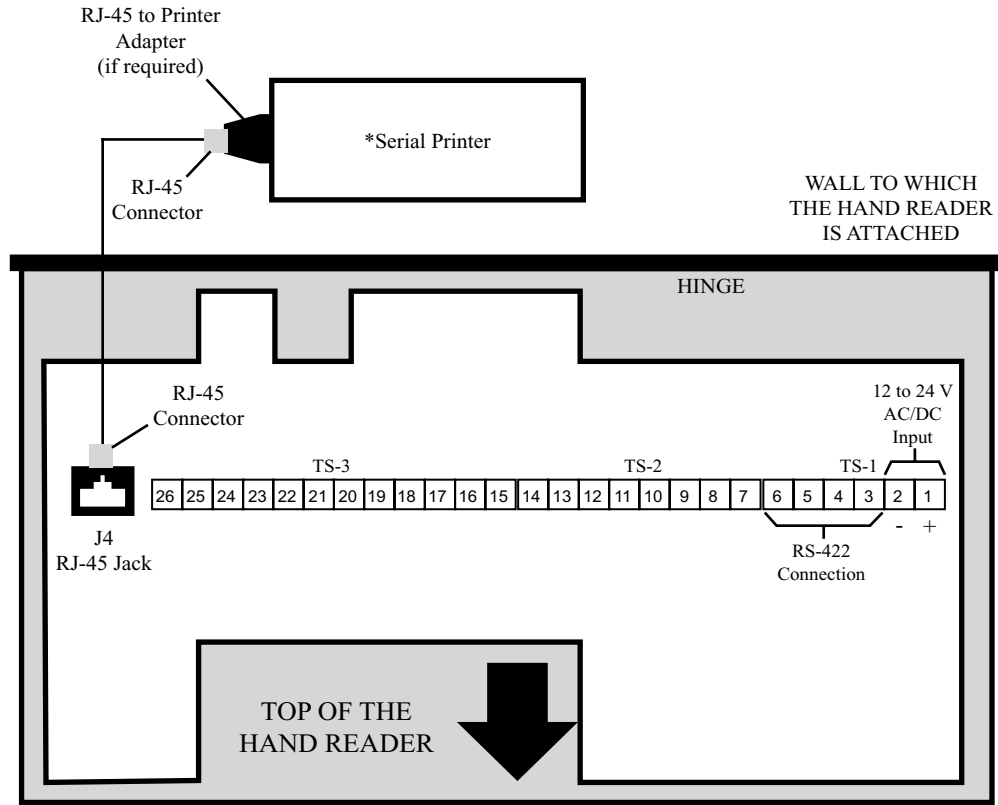


Figure 5-9: Host PC Network System Wiring Diagram



* These components are not supplied by Recognition Systems, Inc.

Figure 5-10: Printer to HandKey II Wiring Diagram

7.0 Setting the DIP Switches

DIP Switch settings perform three tasks for the Hand Reader (see Figure 5-11).

- Set End of Line (EOL) Termination to match the type of termination the network being used needs.
- Set the Communication Method to match the type of network used.
- Erase Memory to clear Hand Reader memory to all factory default values and also clear all user memory.

Refer to Figure 5-11 on pag e36 for the location of all DIP switches described in this section.



If a Hand Reader is used as a stand-alone Hand Reader, the End of Line (EOL) Termination and Communication Method dip switches are not used and should be left in their default positions.

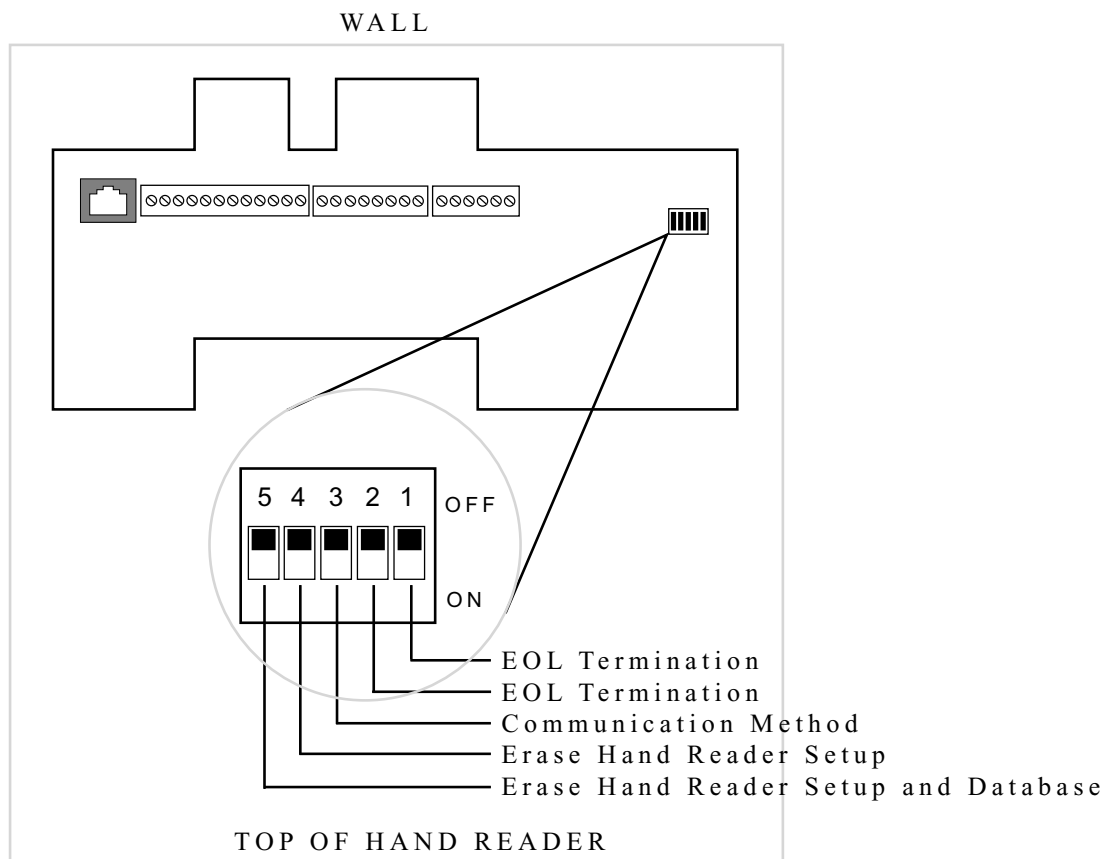


Figure 5-11: Hand Reader Dip Switches

7.1 End of Line Termination

The factory default setting is for EOL termination to be disabled – switches 1 and 2 OFF. Refer to Figure 5-11 for switch ON/OFF positioning.

- To enable EOL termination at a Hand Reader, both switches 1 and 2 must be ON.
- To disable EOL termination at a Hand Reader, both switches 1 and 2 must be OFF.
- In a Master/Remote Hand Reader network, the Master reader and the last Remote reader in the daisy-chain must have EOL termination turned ON. All other readers in the network must have EOL termination turned OFF.
- In a Hand Reader/host PC network, a modem/host PC network, and a Ethernet/host PC network, the last Remote reader in the daisy-chain must have EOL termination turned ON.

7.2 Communication Method

Communication can be done via an RS-232 direct connection, a 4-wire RS-422 network configuration. The factory default setting is for network communication via 4-wire RS-422 cabling – switch 3 OFF. Refer to Figure 5-11 for switch ON/OFF positioning.

- For network communication via RS-422 cabling, switch 3 must be OFF.
- For network communication via 2-wire RS-485 cabling, switch 3 must be ON.
- For network communication via RS-232, the switch 3 position does not apply. Leave switch 3 in the default OFF position.

NOTE *All Hand Readers in a network must be set to the same communication method. Four-wire RS-422 cabling is required for HandNet for Windows™ network installations. Recognition Systems does not recommend two-wire RS-485 cabling for new network installations.*

7.3 Erasing Hand Reader Memory

The erase memory function allows a Hand Reader's setup and/or user database to be erased. The factory default setting (and normal operation setting) is for switches 4 and 5 to be OFF, retaining memory.

7.3.1 Erasing the Hand Reader Setup

Perform the following steps to erase the setup programs but retain the user database.

1. With system power OFF, set switch 4 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn switch 4 OFF.

7.3.2 Erasing the Hand Reader Setup and User Database

Perform the following steps to erase both the setup programs and the user database.

1. With system power OFF, set both switches 4 and 5 ON.
2. Turn system power ON and wait 5 seconds.
3. Turn both switches 4 and 5 OFF.

NOTE *Before putting the hand reader into service ensure DIP switches 4 and 5 are both OFF. If switches 4 and 5 are not off, the next time the Hand Reader's power is cycled the Hand Reader's memory will be erased.*

8.0 Closing the Hand Reader

Before closing the Hand Reader, ensure dip switches 4 and 5 are OFF (refer to Figure 5-11 on page 36). With the wall mount latch in the unlocked position, swing the body of the Hand Reader up and lock the latch into place with the key provided with the Hand Reader (see Figure 5-12).

NOTE Do not force the Hand Reader onto the wall mount latch when the latch is in the locked position.

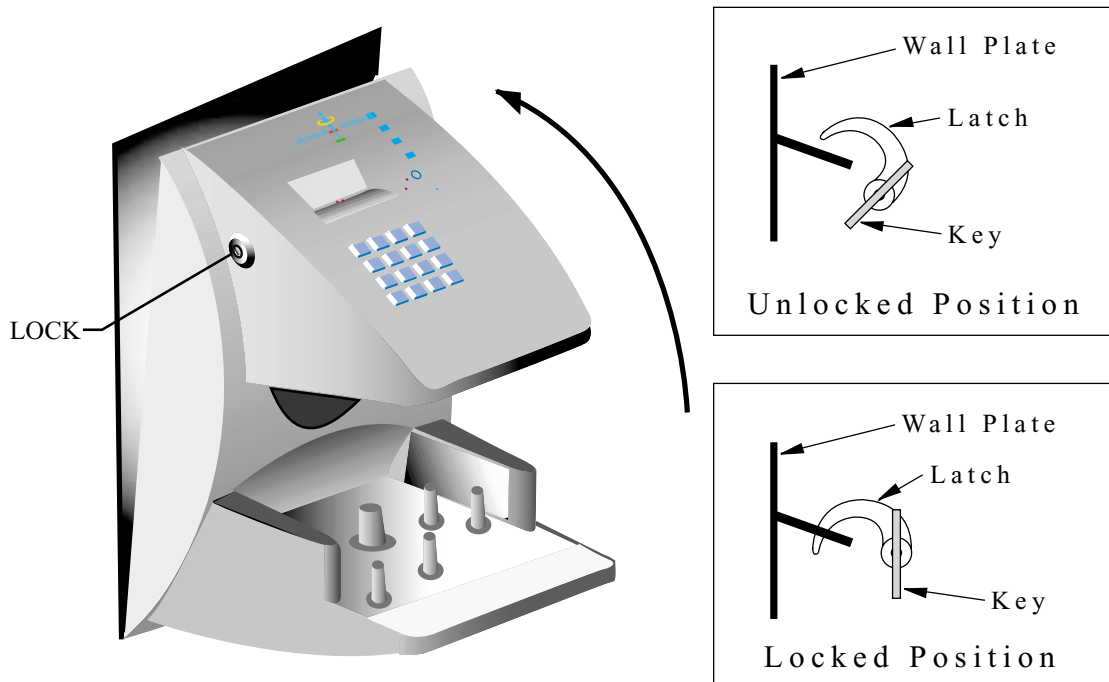


Figure 5-12: Closing the Hand Reader

9.0 Powering the Hand Reader

The Hand Reader is powered through the cabling run to the Hand Reader. Apply power via this cabling. The Hand Reader's display lights up. After a several second delay the Hand Reader's display shows the following information.



If the display remains blank, verify the power connections made to the Hand Reader.

10.0 Programming the Hand Reader

The Hand Reader is programmed via a series of command menus. A summary of the menus and commands is given in Table 6.

Table 6: Basic Command Mode Structure

Service Menu	Setup Menu	Management Menu	Enrollment Menu	Security Menu
Password 1	Password 2	Password 3	Password 4	Password 5
Calibrate	Set Language	List Users	Add User	Set User Data
Status Display	Set Date Format	Data From Network*	Add/Remove User	Set TZ Table
Network Status*	Set Time and Date	Data to Network*		Reject Threshold
	Set Address			Set Passwords
	Set ID Length			Clear Memory
	Set Output Mode			Special Enroll
	Set Facility			
	Lock/Shunt Time			
	Aux Out Control			
	Set Reader Mode			
	Set Serial			
	Set Duress Code			
	Print Options			
	Set Beeper			

* These menu options only appear in Hand Readers configured as a “Master” unit.

To control access to the command menus, each menu has a unique password. This password is requested as a part of the process for accessing each menu. A supervisor must enter the correct password for that menu to access that menu. The default menu passwords are given in Table 6.

To increase the security of the Hand Reader, Recognition Systems recommends changing the passwords for the command menus to new numbers. These password numbers can be up to 10 digits long. This is done with the Set Passwords command described on page 71.

10.1 Authority Level

A second method for controlling access to the command menus is through the use of Authority Levels. Authority Levels control which command menus a user is allowed to access; the higher the authority level a user is granted, the greater the number of menus the user may access. Assign Authority Levels to users according to the types of tasks to which they are assigned.

- Level 0 is for a user who does not need access to any of the command menus.
- Level 1 provides access to the Service command menu.
- Level 2 adds access to the Setup command menu to all previous access levels.
- Level 3 adds access to the Management command menu to all previous access levels.
- Level 4 adds access to the Enrollment command menu to all previous access levels.
- Level 5 adds access to the Security command menu to all previous access levels.

The Hand Reader automatically assigns Authority Level 0 to each ID number enrolled. Until a user has been assigned to Authority Level 5, every user with Authority Level 0 can access every menu. This is done to ensure that the first person enrolled is able to access all the menus to perform all the programming required to support the Hand Reader. Once a user has been assigned to Authority Level 5, all other user authority levels are applied as per the list above.



The first person enrolled should be designated the System Administrator and should change his/her Authority Level to 5. This protects the integrity of the system by enacting the Authority Level rules described in the list above. Recognition Systems strongly recommends assigning at least two users to Authority Level 5 to ensure that more than one person has the authority to access all menus and all commands.

10.2 Programming Order

When setting up Hand Reader operations there is a general programming/operations order that should be followed.

Design an ID Numbering System – Define the format for user ID assignments. A properly designed ID numbering system makes the Hand Reader easier and faster to use.

Enter a Command Menu – Enter a Command Menu and begin Hand Reader programming per the commands in that menu.

Enroll all Supervisory Staff – Enroll yourself and the supervisors who will have responsibility for Hand Reader management. This is done through the Enrollment Menu.

Set Supervisory Staff Authority Levels – Assign Authority Levels to the supervisors with specific Hand Reader management responsibilities. This is done through the Security Menu.

Set Reader Site Parameters – Set the reader's Operating Parameters to meet site specific needs and usage. This is done through the Setup Menu.

Train and Enroll Users – Train each user regarding Hand Reader usage and then Enroll each user. This is done through the Enrollment Menu.

10.3 System Management and Maintenance

Once a Hand Reader network is in operation the following commands are used to manage and maintain the Hand Reader network.

Set Reader Operating Thresholds – Set the Reject and Number-of-Tries Hand Reader operating thresholds to meet the site's security requirements. This is done through the Security Menu.

System Management – Backup or Restore Hand Reader data and List the Users authorized to use a Hand Reader. This is done through the Management Menu.

System Maintenance – Calibrate the Hand Reader, display Hand Reader Status, and display Network Status. This is done through the Service Menu.



For documentation clarity, instructions for operating each of the menu commands are presented in menu order, which is not necessarily programming order. Please keep this in mind as you review the commands for all of the menu options.

10.4 Design an ID Numbering System

The ID numbering system helps identify the user about to use the Hand Reader. ID numbers are used when enrolling users. A properly designed ID numbering system allows for quicker user recognition (through the use of the Set ID Length command) and allows the assigning of a Duress code. A Duress code sends a silent alarm to a pre-defined location when entered by a user. Use the following guidelines when designing an ID numbering system.



Designing an ID numbering system is not necessary when using an external card reader to enter the ID number. All ID information is provided by the card.

- Each user must have a unique ID number.
- ID numbers can be up to 10 digits long.
- For ease of memorization, make each number as short as possible. Generally speaking, 4 digit or fewer ID numbers are easy to remember.

- Make all ID numbers the same length. This allows the Set ID Length command to be used, automatically reading an ID number when the proper number of digits have been entered. If different ID number lengths are used, a user must press the **#** key to identify when the complete ID number has been entered.
- To use the Duress feature, ID numbers must begin with one specific digit that has been identified as the Duress code and this digit cannot be used as the first digit in any of the user ID numbers. This means that in normal use a user enters his/her ID number followed by the **#** key. To create a Duress alarm, the user enter the Duress code, the user's ID number, and the **#** key. The Set ID Length command cannot be used if the Duress feature is used.

10.5 Enter a Command Menu

Press the **CLEAR** and **ENTER** taneously to enter a command menu.

10.5.1 If No One is Enrolled in the Hand Reader

1. The display appears as follows.



2. Press the default password for the menu you wish to enter.

Press **1** for the Service Menu.

Press **2** for the Setup Menu.

Press **3** for the Management Menu.

Press **4** for the Enrollment Menu.

Press **5** for the Security Menu.

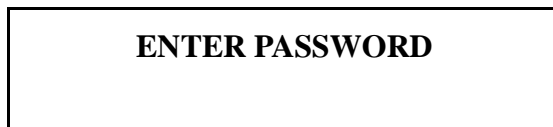
3. Press **ENTER** and the first command option in the selected menu appears.

10.5.2 If Users are Enrolled in the Hand Reader

1. The display appears as follows.



2. Enter your ID number on the keypad and place your hand on the platen for verification.
3. If verification is successful, the display appears as follows.



4. Enter the password for the menu you wish to enter. The default passwords are as follows.

Press **1** for the Service Menu.

Press **2** for the Setup Menu.

Press **3** for the Management Menu.

Press **4** for the Enrollment Menu.

Press **5** for the Security Menu.

5. Press **ENTER**.

6. If you are authorized to use this command the first command option in the selected menu appears.

7. If you are not authorized to enter this command the display appears as follows.





To access all five menus you must be the first person enrolled in a new system installation or you must have the highest authority level and the correct passwords for all five menus. If you are blocked from a menu to which you should have access, verify your access/password rights with management personnel. If authority levels or passwords have been incorrectly changed and you must have access to all menus, it is possible to reset the Hand Reader's memory. Resetting memory allows access to all five menus by the first person enrolled (as if it is a new system installation), but this means that any user information programmed into the Hand Reader must be re-entered (manually or by using HandNet software to restore the user information). Be sure you need to reset memory before performing this function. To reset memory, refer to the Erasing Hand Reader Memory section on page 37.

10.5.3 Navigating Command Menus

Once you have entered a command menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press ***** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

10.6 System Maintenance

A minimum amount of system maintenance is required to keep Hand Readers fully functional. Hand Readers should be cleaned periodically to prevent an accumulation of dust from affecting the Hand Reader's readability. User Scores should be reviewed periodically to ensure the Hand Reader is performing properly.

NOTE *There are **NO** user servicable parts inside the Hand Reader.*

Once a HandKey system is in operation there are three Hand Reader commands that can assist with system maintenance. These commands are performed through the Service Menu. The instructions for these commands begin on page 47.

- Calibrate – View Hand Reader exposure values.
- Status Display – Display Hand Reader input/output status, the hand read score of the last user to verify on the system, and the master/remote status of the Hand Reader.
- Network Status – Display the network communication status of Hand Readers in the HandKey system (master Hand Reader only).

10.6.1 Cleaning the Hand Reader

Inspect and clean the Hand Reader regularly to maintain optimum performance. Clean the platen, side mirror, reflector, and the window above the platen using a clean cloth dampened with ordinary, non-abrasive window cleaner (see Figure 10-1). Start at the rear corners of the platen and work your way forward.

NOTE *DO NOT SPRAY CLEANING FLUID DIRECTLY INTO OR ON THE HAND READER.*

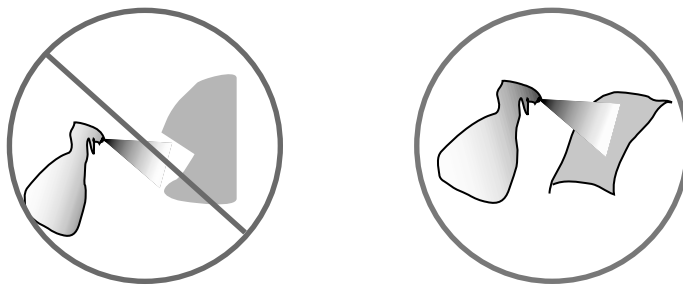


Figure 10-1: Hand Reader Cleaning

10.6.2 User Score

Periodically check users' scores (refer to the Read Score section on page 65). Scores should average under 30. Occasionally a user will score above 30. This is not necessarily an indication of poor performance. If a number of scores average over 30, clean the Hand Reader and check scores again. If scores remain high, or if users are experiencing frequent rejections, run the Calibration command (see page 48).

10.7 Service Menu

The Service Menu commands provide information that helps you determine if the Hand Reader is operating properly and within normal operating parameters.

10.7.1 Navigating the Service Menu

Once you have entered the Service menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press ***** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

10.7.2 Service Commands

There are three commands available from the Service command menu.

- Calibrate – Run a calibration test to check Hand Reader exposure values.
- Status Display – Check the status of Hand Reader inputs and outputs, the hand read score of the last user to verify on the system, and the master/remote status of the Hand Reader.
- Network Status – Check the network communication status of Hand Readers in the HandKey system (master Hand Reader only).

Refer to Table 7 on page48 and identify the command you need to perform. Step through all previous commands until you reach the desired command. All commands are listed in menu order.

Table 7: Service Command Menu

Service Menu
Password = 1
Calibrate
Recal (N/Y)
Status Display
On/Off (Y/N)
Network Status ^a
Status Information

a. Master controller only.

10.7.2.1 Calibrate

The Calibrate command verify that the Hand Reader’s exposure values are within normal operating parameters. The normal operating parameters are shown in Table8.

Table 8: Normal Operating Parameters

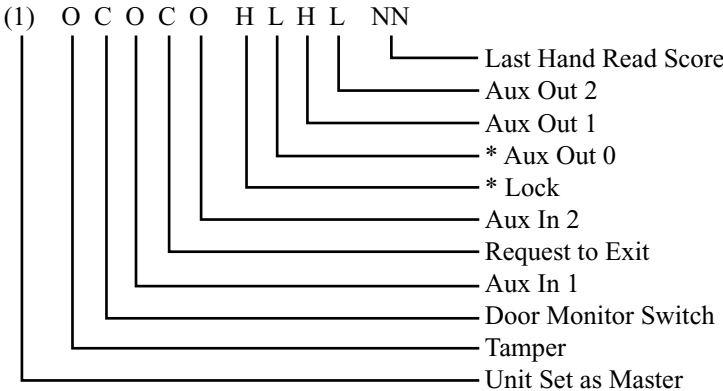
Parameter	Normal Range
Row “r”	0 +/- 2
Column “c”	0 +/- 2
Exposure	100 +/- 10

10.7.2.2 Status Display

The status display command allows you to enable or disable the displaying of the following information.

- the status values of Hand Reader inputs and outputs
- the hand read score of the last user to verify on the Hand Reader

Figure 10-2 on page 49 identifies each status display field value.



* These status values are inactive if the reader is in Card Reader Output Mode.

O = Circuit Open H = Output is OFF (High)
C = Circuit Closed L = Output is ON (Low)

Figure 10-2 Status Display Chart

10.7.2.3 Network Status

The network status command allows you to check the network communication status of the Hand Readers in the HandKey system.

NOTE *You can check network status only from the Master Hand Reader in a master/remote hand reader network.*

Network status is displayed by reader address, 16 units at a time.



Each “O” and “.” represents a Hand Reader address in the network. An “O” indicates that the Hand Reader corresponding to that address is communicating on the network. A “.” indicates that the Hand Reader with that address is not communicating on the network.

This page is intentionally left blank.

10.8 Setup Menu

The Setup menu commands allow you to set the basic operating parameters for the Hand Reader.

NOTE *Once in the Setup menu you can step through and set the parameters for each command sequentially. You do not have to exit command mode after setting any individual command.*

10.8.1 Navigating the Setup Menu

Once you have entered the Setup menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press ***** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

10.8.2 Setup Commands

There are 14 commands available from the Setup command menu.

- Set Language
- Set Date Format
- Set Time and Date
- Set Address
- Set ID Length
- Set Output Mode
- Set Facility
- Lock/Shunt Time
- Aux Out Control
- Set Reader Mode
- Set Serial
- Set Duress Code
- Print Options
- Set Beeper

Refer to Table 9 on page52 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 9: Setup Command Menu

Setup Menu
Password = 2
Set Language
Select Language
Set Date Format
Select Date Format
Set Time and Date
Month (MM)
Day (DD)
Year (YY)
Hour (HH)
Minute (MM)
Set Address
New Address
Set ID Length
New ID Length
Set Output Mode
For Door Lock and Aux Outputs
For Card Reader Emulation
Set Lock/Shunt Time
Set Lock Time
Set Shunt Time
Set Unlock on Auxiliary Keypad
Set Auxiliary Keypad Time Zone
Auxiliary Output Control
Select Auxiliary Output
Output Set by Time Zone

Table 9: Setup Command Menu

Setup Menu
Password = 2
Output Set by Tamper
Output Set by Time Zone Violation
Output Set by ID Refused
Output Set by Duress
Output Set by Auxiliary Input 1
Output Set by Auxiliary Input 2
Output Set by Door Alarm
Output Set by Try Again
Output Set by F1 Key
Output Set by F2 Key
Output Set on Battery Backup
Output Set by Unlock
Output Set by Auxiliary Keypad
Set Reader Mode
To Master/Remote
Set Serial ^a
RS-422 (Y/N)
Select Baud Rate
RS-232 (Y/N)
Select Baud Rate
Use RS-232 for Printer or Host
Set Serial ^a
Verify/Enter IP Address
Verify/Enter Gateway
Verify/Enter Host Bit

Table 9: Setup Command Menu

Setup Menu
Password = 2
Set Duress Code
Enter Duress Code
Print Options
Print "Valid Access" (Y/N)
Set Beeper
Turn Beeper On/Off (Y/N)

- a. The Set Serial command has different values based on whether the Hand Reader is configured for serial or modem communication versus Ethernet communication.

10.8.2.1 Set Language

The Set Language command allows the language shown on the Hand Reader’s display to be “localized” for a variety of countries. The default language is English. The following languages are available.

English	Japanese
French	Polish
German	Portuguese
Indonesian	Russian
Italian	Spanish

10.8.2.2 Set Date Format

The Set Date Format command allows the date format shown on the Hand Reader’s display to be “localized” for a variety of countries. The default date format is the U.S. standard date format – MM/DD/YY. The following date formats are available.

mm/dd/yy	mm-dd-yy
dd-MMM-yy	MMM dd,yy
dd-mm-yy	ddMMMyyyy
dd/mm/yy	

10.8.2.3 Set Time and Date

The Set Time and Date command allows the Hand Reader’s time and date to be set. If the Hand Reader is networked to a PC, this step is not necessary as the Hand Reader’s time and date will be set by the host computer.



Stand-alone Hand Readers and Hand Readers on a master/remote Hand Reader network require adjustment for the daylight savings time changes. Hand Readers networked to a host PC do not require adjustment as the host PC automatically makes the adjustment.

Time is kept using a 24-hour clock. The time is set in the following format.

Hour: two digits – 00 to 23

Minute: two digits – 00 to 59

The date is set in the following format.

Month: two digits – January = 01, incrementing to December = 12

Day: two digits – 01 through 31

Year: two digits – enter the last two digits of the current year (i.e. 2001 = 01)

10.8.2.4 Set Address

The Set Address command allows a unique address to be set for each Hand Reader in a network. For proper operation, each Hand Reader in the network must have a unique address. Addresses 0 to 254 are available – address 255 is reserved for the master Hand Reader in a network. The default address is 0. An address does not need to be set for stand-alone Hand Readers.

10.8.2.5 Set ID Length

The Set ID Length command allows you to reduce the number of keystrokes required to enter the ID number by eliminating the use of the **ENTER** key to complete an ID number entry. Once the ID Length is set, when a user enters an ID number the Hand Reader will automatically accept that number once the correct number of characters have been entered. Set ID Length does not apply when ID entry is made from a card reader. Set ID Length cannot be used if a Duress Code has been assigned.

Set the ID Length to the number of digits in the longest ID number. This command is unnecessary (and should be left at its default value) if ID entry is made from a card reader. The ID Length should not be set if a Duress Code is being assigned (see page 58). The default value for ID Length is 10.



*Users assigned ID numbers shorter than the number of digits in the longest ID number must press **#** following their ID entry to indicate the complete entry has been made.*

10.8.2.6 Set Output Mode

The Set Output Mode command allows either of two output modes to be set.

- Lock/Aux for Hand Readers acting as door controllers
- Card Reader Emulation for Hand Readers outputting to an access control panel

Outputs are pulled to ground when activated. The selected mode is applied to Output 0. Lock and Auxiliary Output mode is the default setting.

10.8.2.7 Set Facility

The Set Facility command allows the facility code to be entered in Hand Readers configured for card reader emulation output mode. A facility code is not valid or required for Hand Readers configured in Lock/Aux output mode.

Set the Facility Code to match the code expected by the access control panel. This command is unnecessary (and should be left at its default value) if the output mode is set to Lock and Auxiliary Output Mode. The default facility code value is 50.



When using a HandKey II on a Wiegand format access control panel and a keypad is used for ID entry, you must set the site code to the access control panel's facility code. Without a matching code the access control panel will deny access to HandKey users.

10.8.2.8 Set Lock and Shunt

The Set Lock and Shunt command allows you to set the time-of-day that the door lock output is activated and the door alarm is shunted. It also allows the auxiliary keypad to be used for user ID entry.

- The Lock time is the number of seconds the lock output is active (door is unlocked) following user verification. The Lock time is only valid when the Hand Reader is set to the Lock & Aux output mode.
- The Shunt time is the number of seconds the door may be held open before an alarm is generated. Lock and Shunt times are not required for Hand Readers configured in Card Reader Emulation output mode.

This command is unnecessary (and should be left at its default values) if the output mode is set to Card Reader Output Mode. The default Lock time is 5 seconds. The default Shunt time is 10 seconds. The default Auxiliary Keypad value is set to **not** allow entry when the user's ID number is entered.

10.8.2.9 Aux Out Control

The Aux Out Control command allows the Auxiliary Outputs in the Hand Reader to be set to trigger based on selected events. Alarms can be mapped to appropriate Auxiliary Outputs. Outputs are also cleared in this menu option. In the Lock and Shunt mode, all three Auxiliary Outputs are available. In the Card Reader Emulation mode, Auxiliary Outputs 1 and 2 are available.

There are three outputs that can be set: 0, 1, 2. Output 0 can only be set when the Hand Reader is in Lock and Auxiliary Output mode; Outputs 1 and 2 can be set regardless of the mode the Hand Reader is in.

Outputs 0, 1, and 2 can be connected to a variety of peripheral devices such as audible or silent alarms, door locks, or lighting systems. Verify Hand Reader/peripheral wiring is correct and that the peripheral meets Hand Reader/system specifications before changing the output settings. Table 10 on page 57 describes the Auxiliary Output choices.

Table 10: Auxiliary Output Choices

Auxiliary Output	Function
Aux Set by Time Zone	Activated by a time zone.
Tamper	Hand Reader opened, shaken, or removed.
TZ Violation	User attempted entry during a restricted time period.
ID Refused	User not verified after allowed number of tries.
Duress	User entered the duress code digit.
Auxiliary Input 1	Auxiliary Input 1 switched to ground.
Auxiliary Input 2	Auxiliary Input 2 switched to ground.
Door Alarm	Door forced open or held open beyond shunt time.
Try Again	User rejected.
F1 Key	F1 key pressed.
F2 Key	F2 key pressed.
On Battery Backup	AC power failure, Hand Reader switched to battery power.
Unlock	Door unlocked.
Auxiliary Keypad	Auxiliary keypad is used.

10.8.2.10 Set Reader Mode

The Set Reader Mode command allows a Hand Reader to be set as the Master Hand Reader in a Hand Reader network. All user enrollment is done through the Master Hand Reader. The Master Hand Reader automatically downloads user data to all remote Hand Readers on the network. The Reader Mode does not need to be set for stand-alone Hand Readers and PC networks.

In Hand Reader networks, one Hand Reader must be set as a Master Hand Reader and all remaining Hand Readers must be set as Remote Hand Readers. The default Reader Mode is Remote mode. Reader Mode does not apply to stand-alone Hand Readers or Hand Readers in a PC network (the Hand Reader should be left in its default value).

NOTE *All remote Hand Readers on a Hand Reader network **must** have a unique address. Refer to the Set Reader Address section on page55.*

The Hand Reader’s display can tell you if a reader has been configured as a Master Reader or a Remote Reader.

A Master Reader has double-dashes surrounding the “READY” text.

= READY = TIME DATE

A Remote Reader has single-dashes surrounding the “READY” text.

- READY - TIME DATE

10.8.2.11 Set Serial

The Set Serial command allows you to select either the RS-485, RS-422 or RS-232 communication mode and to set the baud rate for the selected communication mode. The default baud rate is 9600 bps which is suitable for most network communication applications. If the Hand Reader uses the Ethernet communication option, the TCP/IP address, gateway, and host bit parameters are set instead of the baud rate.

10.8.2.12 Set Duress Code

The Set Duress Code command allows a special digit code to be defined that, when entered before a user’s PIN entry, sends a silent alarm to security personnel using an auxiliary output. This function only works with keypad ID number entry systems – it does not work with Card Reader entry systems. If a Duress Code is set, an ID Length cannot be set by the Set ID Length command.

NOTE *For this function to work properly the following must be true: an auxiliary output must be defined to activate on DURESS and assigned ID numbers cannot begin with the duress code number.*

10.8.2.13 Set Print Options

The Set Printer Options command disables the printing of the “Valid Access” event message. The Valid Access event message is the most frequently printed event. If a printer is connected to the RS-232 serial port, it prints all events in real-time. This means the printer will print a message for every Valid Access event unless disabled here.

10.8.3 Set Beeper

The Set Beeper command allows the beeper to be enabled or disabled. When enabled, the beeper sounds an audible response to key strokes and events.

This page is intentionally left blank.

10.9 Management Menu

The Management menu commands allow you to manage employee data stored in a Hand Reader.

10.9.1 Navigating the Management Menu

Once you have entered the Management menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press ***** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

10.9.2 Management Commands

There are three commands available from the Management command menu.

- List Users – display or print a list of all the users enrolled in a Hand Reader.
- Data From Network – upload data from the network to the master Hand Reader.
- Data To Network – download data from a master Hand Reader to the network.

Refer to Table 11 on page 62 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 11: Management Command Menu

Management Menu
Password = 3
List Users
Display or Print
Data from Network ^a
Select Reader
Data to Network ^a
All Readers (Y/N)
Select Reader

a. Master controller only.

10.9.2.1 List Users

The List Users command displays or prints a list of all the users enrolled in a Hand Reader. The list is shown, one user at a time, on the Hand Reader’s display, or it is printed by a serial printer attached to the Hand Reader being polled or to a printer attached to the Master Hand Reader in a Hand Reader network. Before displaying the user list, the amount of memory available for enrolling more users is displayed.

10.9.2.2 Data From Network

The Data from Network command allows the master Hand Reader to receive information from a Hand Reader on the network. This is used to transmit user enrollment and system configuration information from an existing Hand Reader to the master Hand Reader.

10.9.2.3 Data To Network

The Data to Network command transmits all data held by the master Hand Reader to all Hand Readers connected to the network. This is used to transmit user enrollment and system configuration information to all Hand Readers on the network.

10.10 Enrollment Menu

Enrollment is the process of recording a hand image and associating it with an ID number. The first person to enroll in the Hand Reader has access to all command menus. This person should be considered the System Administrator and should retain the highest authority level to access all five menus at any time¹.

As other users are enrolled they can be left as basic access users or they can be assigned varying degrees of authority depending upon the tasks for which they will be responsible.

Advance planning and training make enrollment fast and easy. Users should be informed on what to expect and how to place their hands on the Hand Reader before you enroll them.

10.10.1 Preparation

Here are a few guidelines to help you prepare for an enrollment session.

- You can enroll one person or a group of people during an enrollment session.
- Each user must have a unique personal identification (ID) number. It will save you considerable time if you assign the ID numbers in advance²
- The Hand Reader will not accept two people with the same ID number.
- If you enroll people using the last four digits of their phone numbers or social security numbers, you may get duplicate numbers.
- If you plan to use the Duress function, do not enroll ID numbers that begin with the Duress code digit³.
- If you are enrolling large groups of people you may consider using an enrollment trainer. It is a replica of a platen that is available through your Recognition Systems dealer.

10.10.2 User Education

The Hand Reader is easy to use and non-threatening. However, most people have never used a biometric Hand Reader. Training users on how the Hand Reader works and how to use it will eliminate most fears and concerns before they occur. Inform the users of these facts.

- The Hand Reader reads the shape of the hand, not the fingerprints or palmprints.
- It does not identify people. It confirms people's identity.
- It scans with an invisible light of the type used in TV remote controls.
- It does not transfer germs any more than a doorknob or money.

1. Refer to the [Set User Data > Set Authority Level](#) command in the Security command menu on page 69.
2. Refer to the [Design an ID Numbering System](#) section on page 41.
3. Refer to the [Set Duress Code](#) command in the Setup command menu on page 58.

- It does not invade privacy; it guarantees it.
- The enrollment process requires three or more reads to collect enough information to verify the user's identity.

10.10.3 Proper Hand Placement

For correct, consistent hand reads it is very important that your hand is placed on the platen in the same manner every time (see Figure 10-3). The following rules apply for proper hand placement on the platen.

- If you are wearing a ring, rotate the ring so the stone faces up in its normal position.
- Slide your right hand onto the platen rather like an airplane landing at the airport.
- Slide your hand forward until the web between your index and middle finger stops against the Web Pin.
- Keep your hand flat. You should feel the surface of the platen on your palm and the underside of your fingers.
- Close your fingers together until they touch the Finger Pins and watch the hand diagram light display on the top panel.
- The lights go out when you have properly placed your fingers. If a light remains on, a finger is not in proper contact with its Finger Pin.



Figure 10-3: Placing Your Hand on the Platen

10.10.4 Left Hand Enrollment

Some right hands are not suitable for use in the Hand Reader due to disabilities such as missing fingers. You can enroll a user with the left hand facing palm side up. The techniques for left hand enrollment are the same as for standard enrollment. The user should keep the back of the hand flat against the platen and move the fingers against the web pin and the finger pins in the same manner as in standard enrollment. Users enrolled with the left hand must always verify with the left hand. Extra practice on placing the hand on the platen may be required to ensure correct, consistent hand reads.

10.10.5 Read Score

When a user uses the Hand Reader a number appears in the display.



The number on the display reflects how accurately the user is placing his/her hand on the platen. Scores that vary greatly between low and high numbers are indicative of inconsistent hand placement. Scores above 50 are indicative of improper hand placement or of a drastic change in the physical appearance of the hand.

When this occurs, emphasize the importance of sliding the hand onto the platen and keeping the hand flat. Re-training and practice should lower a user's score. It might be necessary to change a user's sensitivity if the user has a mild disability. Re-enrollment might be necessary to create a new user template.

10.10.6 Navigating the Enrollment Menu

Once you have entered the Enrollment menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press ***** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

10.10.7 Enrollment Commands

There are two commands available from the enrollment command menu.

- Add User
- Remove User

Refer to Table 12 on page 66 and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 12: Enrollment Command Menu

Enrollment Menu
Password = 4
Add User
ID #
Remove User
ID #

10.10.7.1 Add User

The Add User command allows you to enroll a new employee into the Hand Reader.

10.10.7.2 Remove User

The Remove User command allows you to remove an employee from the Hand Reader.



Once a user has been removed from the Hand Reader, that user no longer has access through the door controlled by that Hand Reader. To be granted access again, that user must be re-enrolled.

10.11 Security Menu

The commands in the Security menu control the security of the information within the Hand Reader and the sensitivity of the Hand Reader when reading hands.

10.11.1 Navigating the Security Menu

Once you have entered the Security menu, there are three options available for navigating the command menu system.

- Press **#** to enter the command shown on the display.
- Press ***** to step to the next command in the menu.
- Press **CLEAR** to exit the command menu (pressing any numeric key also exits the command menu). If you are in a command's sub-menu, you may have to press **CLEAR** multiple times to completely exit the command menu.

10.11.2 Security Commands

The Security menu has six primary commands.

- Set User Data
- Set TZ Table
- Reject Threshold
- Set Passwords
- Clear Memory
- Special Enroll

Refer to table and identify the command you need to perform. Step through all previous commands until you reach the desired command.

Table 13: Security Command Menu

Security Menu
Password = 5
Set User Data
Set User Authority Level (Y/N)
ID #
Authority Level
Set User Reject Level
ID #
Reject at #
Set User Time Zone
ID #
New Time Zone?
Edit Time Zone
Time Zone #
Time Zone Data
Print Time Zone
Clear Time Zone
Time Zone #
Edit Holidays
Enter Month and Day
Print Holidays
Clear Holidays
Holiday Month
Set Unlock Time Zone
Time Zone #

Table 13: Security Command Menu

Security Menu
Password = 5
Set Reject Threshold
Reject Threshold #
of Tries
Set Passwords
Security Password
Enroll Password
Management Password
Setup Password
Service Password
Clear Memory
Special Enroll
ID #
Time Zone#

10.11.2.1 Set User Data

The Set User Data command allows you to set the User Authority level, the User Reject Level, and the User Time Zone.

- The Authority Level controls which command menus a user is allowed to access; the higher the authority level, the greater the number of menus the user may access.
- The User Reject level allows you to set the number of failed hand read attempts for a user before rejecting further attempts by that user.
- The User Time Zone allows you to assign a time zone to a user, restricting the time-of-day that a user may be granted access.

10.11.2.2 Set TZ Table

The Set TZ Table command allows you to create or edit Time Zone and Holiday tables. A time zone is an identified period-of-time and days-of-the-week, during which a user is allowed access to an area secured by a Hand Reader. Once a user is assigned a Time Zone (refer to the Set User Time Zone command on page 69), access attempts outside of that time/date period are rejected by the Hand Reader.

A time zone may be “split.” This means that a time zone may identify more than one set of period-of-time and days-of-the-week – up to four sets in one time zone. This provides a great deal of flexibility in providing secured access through a Hand Reader.

Time Zone information can also be printed for review or cleared if a time zone becomes unnecessary.



All time entries made for time zones are entered in 24-hour format. For example, 8 A.M. is entered as 08:00, 5P.M. is entered as 17:00, and 11 P.M is entered as 23:00.

The Holiday schedule for a calendar year can be entered. Once a holiday schedule is set, holidays are applied to time zones just like another day of the week (1 to 7 for the days of the week, 8 for holidays). Once entered, the holiday schedule can be printed for review and cleared.



Certain holidays, such as Easter and Thanksgiving, change their days from year to year. You must review and edit your holiday schedule each year to ensure the correct days are counted as holidays.

An Unlock Time Zone can also be set. The unlock time zone is a special time zone that automatically unlocks the door associated with a Hand Reader when the time zone is active, and then automatically locks that door when the time zone becomes inactive. This can be used on doors where general access is allowed during specific times of the day (such as business hours).

10.11.2.3 Reject Threshold

Use the Reject Threshold command to set the Hand Reader’s reject sensitivity level applied when reading hand data and to set the number of tries a user is allowed before being rejected by a Hand Reader.

The reject sensitivity level and number of tries are global values. This means that these values are applied to all users on all Hand Readers on the network – except for those users who have been assigned an individual user reject level (refer to the Set User Reject Level command on page69).

The default reject threshold is 100. This is the best threshold value for most applications.

- Raising the threshold level makes the Hand Reader less sensitive to variations in user hand placement on the platen.
- Lowering the threshold level might result in a greater number of rejected attempts, but also results in a more secure system.

The default number of tries is 3. If a user exceeds the number of tries without a valid hand read, the Hand Reader will refuse all subsequent attempts with that user ID number. This means the user will be locked out until another user is verified successfully.

10.11.2.4 Set Passwords

Use the Set Passwords command to change the passwords assigned to each of the five command menus. To increase the security of the Hand Reader, the password for any or all menus can be changed to a new number, up to 10 digits long. This means that to enter a command menu, a user must have the correct Authority Level (refer to page 69) and must enter the correct password.

10.11.2.5 Clear Memory

Use the Clear Memory command to clear the user data from the Hand Reader, but retain the setup data. This allows you to clear the Hand Reader's user database of all templates and ID numbers, but retain all Hand Reader setup information. Typically, this is done when moving the Hand Reader to a new location with different users but the same setup requirements.

NOTE *Use this command with caution. Once user data is cleared from the Hand Reader's memory the user data is not recoverable.*

10.11.2.6 Special Enroll

Allows a user to be enrolled such that the ID number is the primary criteria for determining access. A hand read is required, but is not verified against any stored identification data. A time zone value can also be applied to the Special Enrollment ID number to increase access limits. The default is for no time zone to be applied.

NOTE *Special Enrollment affects the integrity of the Hand Reader network and should only be used as a last resort. Anyone who knows a Special Enroll ID number is granted access when the ID number is used. Before specially enrolling a user, try to alleviate verification problems by adjusting the individual user's reject threshold (see page 70).*

This page is intentionally left blank.

11.0 Limited Warranty

Recognition Systems, Inc. (the “Company”) warrants to the original user the products manufactured by the Company (the “Product”) to be free of defects in material and workmanship for a period of one year from the date of purchase by such user or 15 months from the date of shipment from the factory, whichever is sooner, provided:

1. The Company has been notified within such period by return of any alleged defective product, free and clear of all liens and encumbrances, to the Company or its authorized dealer, transportation prepaid; and
2. The Product has not been abused, misused, or improperly maintained and/or repaired during such period; and
3. Such defect has not been caused by ordinary wear and tear; and
4. Such defect is not the result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war, or similar phenomenon; and
5. Accessories used as integral to the Product have been approved by the Company.

The Company shall, at its option, either repair or replace, free of charge, the Product found, upon the Company’s inspection, to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Product.

THE COMPANY MAKES NO OTHER WARRANTY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

THE COMPANY’S MAXIMUM LIABILITY THEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT. IN NO EVENT SHALL THE COMPANY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SAME OR THE USE OF THE PRODUCT.

Recognition Systems Inc. reserves the right to make changes in the design of any of its products without incurring any obligation to make the same change on units previously purchased.

This page is intentionally left blank.

12.0 Glossary

Address, IP – An Internet Protocol address is a unique address assigned to a computer for communicating over the Internet. It is made up of 4 sets of numbers, separated by periods (for example, 123.245.78.901).

Address, Reader – A Hand Reader Address is a unique identification number assigned to a Hand Reader. Each Hand Reader on a network must be assigned a unique address.

AWG – American Wire Gauge is a U.S. standard set of wire conductor sizes. The “gauge” refers to the diameter of the wire. The higher the gauge number, the smaller the diameter, the thinner the wire, and the greater the electrical resistance. Thicker, smaller gauge wire carries more current because it has less electrical resistance over a given length. Thicker wire is better for long wire distances.

Card Reader Emulation Mode – In Card Reader Emulation Mode, the Hand Reader outputs hand read data in a card reader format, typically to an access control panel. The data is outputted when user’s hand is successfully read. This mode is commonly used when a Hand Reader is being added to an existing access control network. By configuring the Hand Reader in card emulation mode, it can easily replace an existing access control reader in the network. The Hand Reader can be configured to output data in a variety of card reader formats – such as Wiegand, ABA Track-II magnetic stripe, or bar code.

Daisy-Chain – A Daisy-Chain is a method of wiring together Hand Readers on a network, where the first Hand Reader is connected to the second Hand Reader, which is connected to the third Hand Reader, and so on until the last Hand Reader is reached.

End-of-Line (EOL) Termination – EOL Termination is a set of resistors attached to the data lines at the last Hand Reader physically connected to a network. These resistors prevent data signal distortion and reflection back across the data lines, improving the integrity of the network connection.

IP Address – see Address, IP

Platen – The Platen is the flat surface at the base of the HandKey, on which a user places his/her hand for enrollment and verification. The platen has guide pins to ensure the user’s fingers are consistently positioned correctly.

Reader Address – see Address, Reader

Template – A Template is a set of data generated for a user. It is made up of the user’s enrollment information and any system configuration parameters that are assigned to the user. The template is stored at each Hand Reader and can be stored at a host computer when the HandNet™ for Windows™ software is used.

Time Zone – A Time Zone is an identified period of time, during which a user is allowed access to an area secured by a Hand Reader. Access attempts outside of that time period are rejected by the Hand Reader.

Transaction – A Transaction is any kind of event recorded at a Hand Reader. Transactions may include actions such as accepted or denied hand reads, input and output events, and doors opening and closing.

Wiegand™ Reader – The term “Wiegand Reader” has two meanings depending upon its application. A true Wiegand reader reads a specially constructed card made up of small pieces of magnetic wire. As the card is swiped through the reader, the individual bits of wire generate a unique data signal. This data signal is made up of a Facility Code field (typically 8 bits), an ID Number field (typically 16 bits), and parity bits (typically 2 bits) for a total of 26 bits of data. Now this 26-bit Wiegand data format has been adopted by a variety of access reader devices and access control panels for transferring user access data.

Index

- B
 - Biometrics, 5
- C
 - Cleaning, 45
 - Command Menu
 - Entering, 42
 - Navigation, 44
 - Communications - See Networking and Communications
- D
 - Dip Switches
 - Communication Method, 37
 - End of Line Termination, 36
 - Erasing Hand Reader Memory, 37
 - Setting, 35
- E
 - Enrollment
 - Command Menu, 63, 65
 - Add User, 66
 - Remove User, 66
 - Education, 63
 - Hand Placement, 64
 - Left Hand, 64
 - Preparation, 63
 - Read Score, 65
- G
 - Glossary, 75
- H
 - HandKey
 - Principle of Operation, 5
 - Specifications, 8
- I
 - ID Numbering
 - System Design, 41
- M
 - Management
 - Command Menu, 61
 - Data from Network, 62
 - Data to Network, 62
 - List Users, 62
 - Mechanical Installation, 23
 - Wall Plate, 23

N

- Networking - See Networking and Communications
- Networking and Communications, 19
 - Ethernet, 21
 - Hand Reader Networks, 19
 - Modems, 20
 - PC Networks, 20
 - Stand-alone Units, 19

P

- Printer, 21
- Programming, 39
 - Authority Level, 40
 - Order of, 40
 - Security Menu, 67

R

- Reader
 - Closing the Hand Reader, 38
 - Powering On, 38

S

- Security
 - Command Menu, 67
 - Clear Memory, 71
 - Reject Threshold, 70
 - Set Passwords, 71
 - Set Time Zone Table, 69
 - Set User Data, 69
 - Special Enroll, 71
- Service
 - Cleaning the Hand Reader, 45
 - Command Menu, 47
 - Calibrate, 48
 - Network Status, 49
 - Status Display, 48
 - User Score, 46
- Setup
 - Command Menu, 51
 - Auxiliary Keypad, 56
 - Auxiliary Output Control, 56
 - Lock Time, 56
 - Set Beeper Options, 59
 - Set Date Format, 54
 - Set Date, 55
 - Set Duress Code, 58
 - Set Facility Code, 56
 - Set ID Length, 55

Command Menu (continued)

- Set Language, 54
- Set Output Mode, 55
- Set Print Options, 58
- Set Reader Address, 55
- Set Reader Mode, 57
- Set Serial Port Parameters, 58
- Set Time, 54
- Shunt Time, 56

Site Preparation, 11

- Door Controls, 17
 - Card Reader Emulation Mode, 17
 - Inputs, 17
 - Lock and Auxiliary Output Mode, 17
 - Outputs, 17
- Earth Ground, 13
- Grounding, 13
- Power, 12
 - Battery Backup, 12
- Reader Placement, 11
- Shielding, 13
- Wiring, 12

Specifications, 8

System Maintenance, 41, 45

System Management, 41

U

User Score, 46

W

Warranty, 73

Wiring Connections, 26

This page is intentionally left blank.