



HK-II

Terminal User's Guide



This equipment has been tested and found to comply with the limits for a Class B 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 2011 Schlage Biometrics, Inc. – ALL RIGHTS RESERVED

Document Part Number: 70100-6001 – Revision 3.3 – July, 2011

HandKey and HandNet are trademarks of Schlage Biometrics, 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.

Schlage Biometrics, 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 Schlage Biometrics, Inc.

Table of Contents

Introduction	3
HandKey II	3
Biometrics	3
Principle of Operation	3
The HandKey II	3
Specifications	5
Options	6
UL Compliance	6
Planning an Installation	7
Site Preparation	7
HandReader Placement	7
Wiring	8
Power Input	8
Battery Backup	8
Earth Ground and Shielding	9
Earth Ground All Units	10
Carry a Ground Line to Each Unit	11
Door Control Output	12
Lock Output Mode	12
Card Reader Emulation Mode	12
Inputs and Outputs	12
Networking and Communications	15
Stand-alone HandReader	15
Master or Remote HandReader in a HandReader Network	15
Remote HandReader in a HandReader Network Connected to a Host PC	15
Remote HandReader Connected to a Host PC via Optional Modem	16
Remote HandReader Connected to a Host PC via Optional Ethernet	16
Printer	16
Mechanical Installation	17
Wall Plate Installation	18
Mounting the Wall Plate	18
Routing the Wiring	18
Closing the HandReader	20

Wiring Connections	21
Wiring Examples	21
Erasing the Memory	31
Erasing HandReader Memory	31
Enter a Command Menu	33
If No One is Enrolled in the HandReader	33
If Users are Enrolled in the HandReader	34
Navigating Command Menus	34
Programming the HandReader	35
Authority Level	36
Programming Order	36
System Management and Maintenance	37
Design an ID Numbering System	37
Service Menu	39
Navigating the Service Menu	39
Service Commands	39
Calibrate	40
Status Display	40
Network Status	40
Setup Menu	41
Navigating the Setup Menu	41
Setup Commands	41
Set Language	43
Set Date Format	43
Set Time and Date	43
Set Address	43
Set ID Length	43
Set Facility	44
Aux Out Control	44
Set Reader Mode	44
Set Serial	45
Set Duress Code	45
Set Beeper	45
Upgrade	45
Management Menu	47
Navigating the Management Menu	47
Management Commands	47
List Users	47

Data From Network	48
Data To Network	48
Enrollment Menu	49
Preparation	49
User Education	50
Proper Hand Placement	50
Left Hand Enrollment	50
Read Score	51
Navigating the Enrollment Menu	51
Enrollment Commands	51
Add User	51
Remove User	51
Security Menu	53
Navigating the Security Menu	53
Security Commands	53
Set User Data	55
Set TZ Table	55
Reject Threshold	56
Set Passwords	56
Clear Memory	56
Special Enroll	56
HandReader Maintenance	57
Cleaning the Hand Reader	57
User Score	57
Appendix A: Tips for a Successful Installation	59
Location and Installation	59
HandReader	59
Enrollment	60
Communication	60
Appendix B: Noted Board Configuration Differences	61
Terminal Block Labeling	62
Terminal Block Layout	63
Memory Reset	64
Appendix C: Old Board Configuration Information	65
Attaching the HandReader	65
Grounding	66
Wiring Examples	67
End of Line Termination	76
Erasing the HandReader Setup	77

Erasing the HandReader Setup and User Database 77

Appendix D: Troubleshooting Guide 79

Display Messages During Verification 79

Beeper and LED Status During Verification 80

Glossary 81

Limited Warranty 83

Introduction

HandKey II

The HandKey II is Schlage Biometrics' fourth generation biometric access control HandReader¹. The HandReader records and stores the three-dimensional shape of the human hand for comparison and identity verification. Upon verification, the HandReader produces an output that can unlock a door, send card format data to an access control panel, or communicate with a host computer. The HandReader also has auxiliary inputs and outputs that can be used to control other systems such as CCTV cameras and alarms.

Biometrics

Biometric 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. Schlage Biometrics Inc., founded in 1986, built the first mass-produced hand geometry readers and made biometric technology affordable for the commercial market. Today, Schlage Biometrics' products are in use in every imaginable application from protecting cash vaults to verifying parents in obstetric wards.

Principle of Operation

The HandReader uses low-level infrared light, and a CMOS camera to capture a three-dimensional image of the hand. The HandReader then converts the image to a 9 byte electronic template, and stores the template in a database with the user's information.

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

The HandKey II

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

¹ For the sake of using a consistent name throughout the manual, the HandKey II is referred to as the HandReader for the remainder of this manual.

² The platen is the flat surface at the base of the HandReader (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.

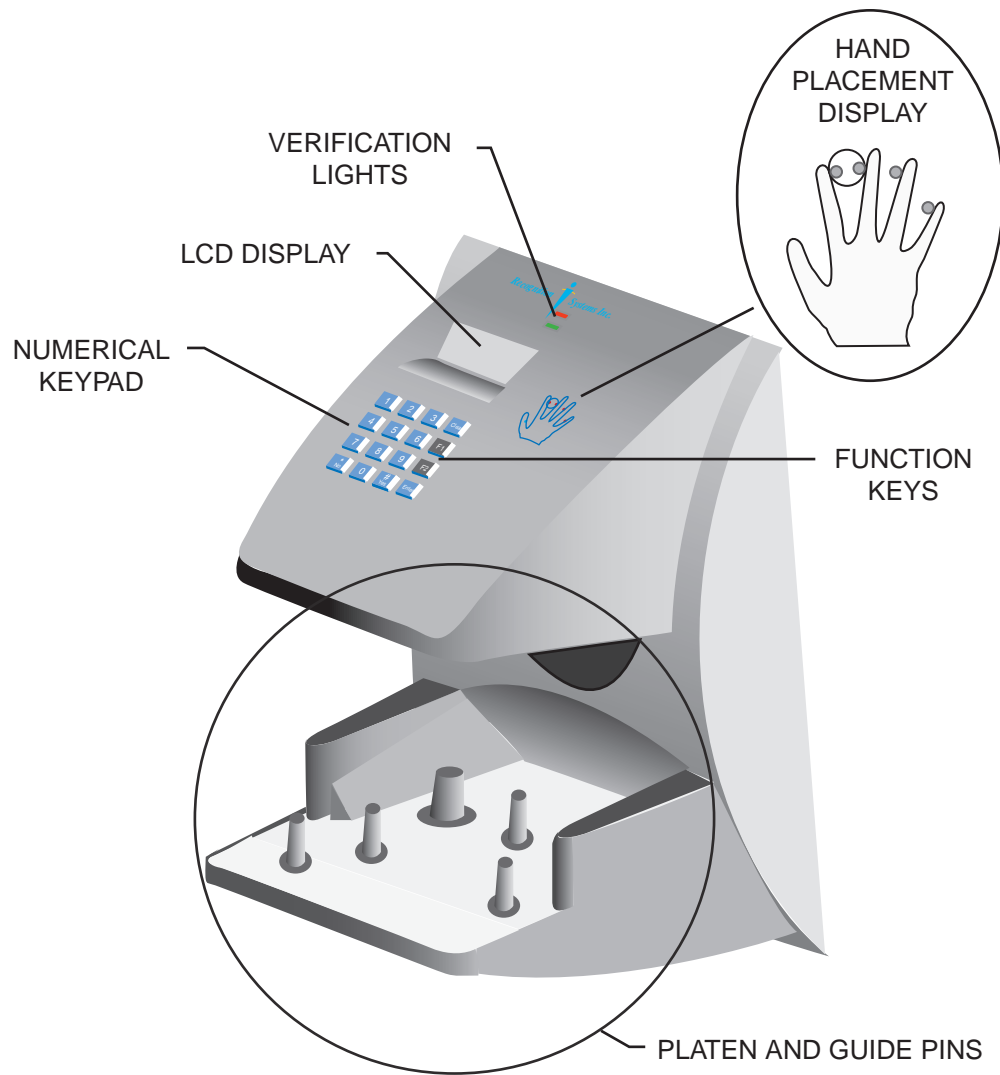


Figure 3-1: The HandKey II

The HandReader 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 and keys assist in data entry and programming.

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

A light emitting diode (LED) hand placement display on the HandReader's top panel assists users with hand placement on the platen.

A liquid crystal display (LCD) shows operational data and programming menus.

"Red light/green light" verification LEDs quickly inform users if their verification attempts were accepted or rejected.

An internal beeper provides audible feedback during keypad data entry and user verification.

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 259,072
Card Reader Input:	Proximity, Wiegand, Magnetic Stripe, Bar Code (5 VDC provided by HandReader)
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
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)

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 H

UL Compliance

Hand Readers are UL Listed as stand alone units only (i.e. the card reader function has not been evaluated by UL).

The HandKey II has not been tested for UL 294 in an Outdoor configuration.

Planning an Installation

Site Preparation

Before you begin installation, check the site blueprints, riser diagrams, and specifications for important information about the HandReader's location and other systems that will connect to the HandReader. Look for any existing wall preparations and wiring that other contractors may have installed for the HandReaders.

HandReader Placement

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

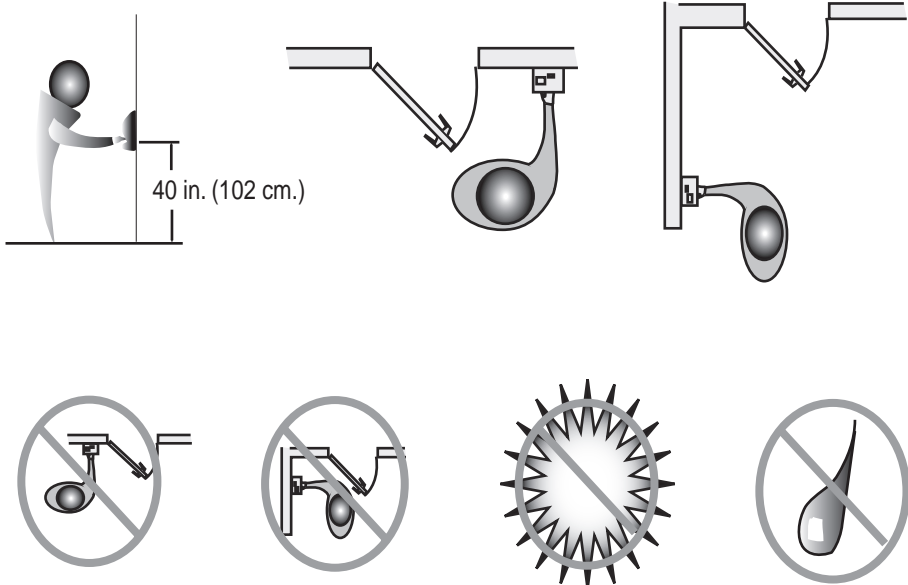


Figure 4-1: HandKey Placement Rules

!NOTE For the following sections, Schlage Biometrics 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 Schlage Biometrics to power the HandReader).

Wiring

Four basic circuits typically connect to the HandReader:

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

Power Input

The HandReader requires 12 to 24 volts DC (600 mA) or 12 to 24 volts AC (7 watts). Power can be connected either to the power terminal pins 1 and 2 or through barrel jack J12.

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

A full-wave bridge rectifier input structure is used in the power supply of the HandReader, making the polarity of terminals 1 and 2 irrelevant. Schlage Biometrics recommends using terminal 1 for positive (+) voltage and terminal 2 for common (-) for consistency. If J12 is used to attach power with the optional Schlage Biometrics 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 HandReader 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.*

Battery Backup

The HandReader 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 HandReader 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 HandReader 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 HandReader 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 HandReader 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 5-1 on page 21) enables or disables battery operation on those HandReaders equipped with optional battery backup. If a HandReader does not have the optional battery backup package installed, J7 is not used. On HandReaders 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 HandReader 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 HandReader will fully shut down. Once the HandReader 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 HandReader will shut down.

The HandReader 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 HandReader and plugs into jack J4 on the keypad control circuit board located in the top of the chassis.

Earth Ground and Shielding

Schlage Biometrics recommends that all HandReaders 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. Schlage Biometrics 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. Schlage Biometrics 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: 4, 10, or 13. Do NOT use terminal 2 to establish the earth ground connection; terminal 2 is not directly connected to ground.*

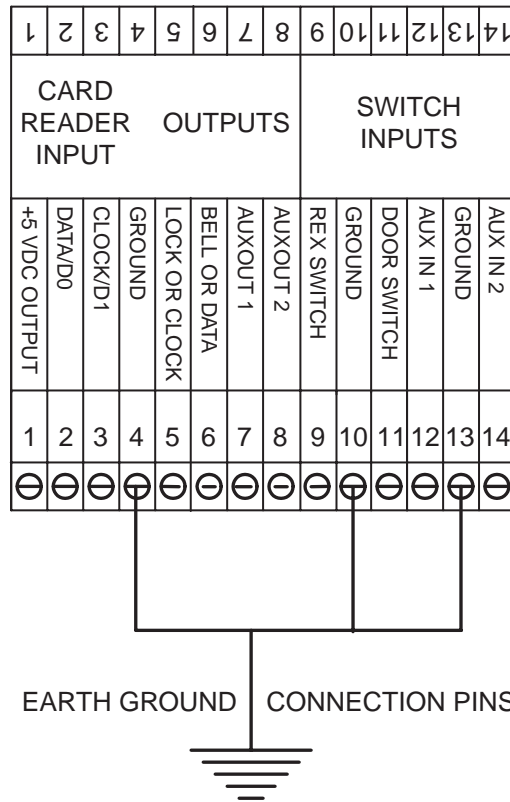


Figure 4-2: Earth Ground Connection Terminals

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

- earth grounding all units (see figure 4-3 on page 11)
- carrying an earth ground to each unit (see figure 4-4 on page 11)

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.

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.

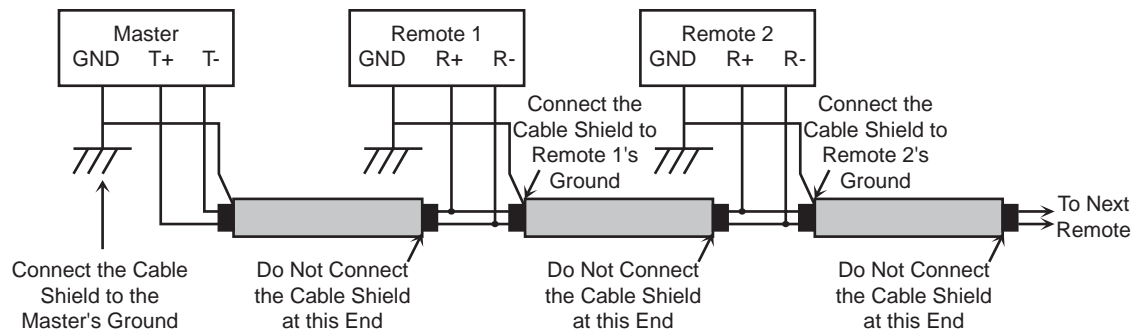


Figure 4-3: Communication Shielding With All Units Earth Grounded

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.

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.

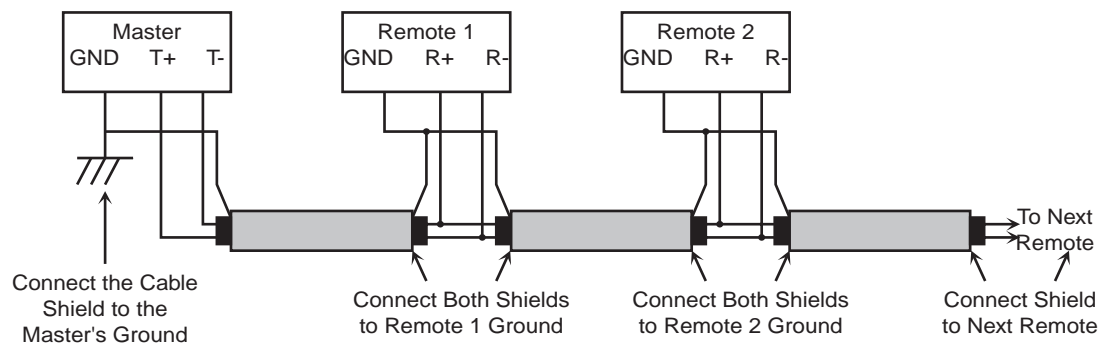


Figure 4-4: Communication Shielding Carrying a Single Ground to Each Unit

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.

Door Control Output

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

Lock Output Mode

In the lock output mode, the HandReader 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 HandReader after a valid verification. Users may be assigned time restrictions to limit access during specified hours or days.

Card Reader Emulation Mode

In card reader emulation mode, the HandReader outputs Wiegand (by default), 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 HandReader to the panel if it has AWG 22 or larger conductors and is in good condition.

The standard HandReader 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 HandReader 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 HandReader stores the card data and then sends the data, unmodified, to the access panel when the user successfully verifies.

Inputs and Outputs

In addition to the Lock and Auxiliary Output and the Card Reader Emulation Output, the HandReader 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.

HandReader 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 HandReader. 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 HandReader, 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 HandReader 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 HandReader ground to make a complete circuit path.

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

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

Networking and Communications

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

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

Stand-alone HandReader

When installed as a stand-alone access control system there is no communication wiring to other HandReaders 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 16). Schlage Biometrics highly recommends using Backhand™ software to backup template information stored in the HandReader.

Master or Remote HandReader in a HandReader Network

Multiple HandReaders can be linked together in a HandReader network.

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

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

Remote HandReader in a HandReader Network Connected to a Host PC

Multiple HandReaders 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 Schlage Biometrics’ HandNet for Windows™ (Schlage Biometrics 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 HandReaders simultaneously.
- An unlimited number of sites can be created with up to 32 HandReaders per site.
- The HandReaders 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 HandReader in the system. The PC collects the data and distributes it to other HandReaders in the network.
- Access may be restricted by time and by HandReader via HandNet’s access profiles and by the use of time zones.

Typically, HandReader 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 (Schlage Biometrics recommends Belden No. 82723 or equivalent cable).
- HandReaders must be wired together in a “daisy chain” network from HandReader to HandReader 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 (Schlage Biometrics P/N DC-102) at the PC.

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

Remote HandReader Connected to a Host PC via Optional Modem

An optional, internal “answer only” 14.4 bps modem is available for HandReaders. This modem is designed for operation with United States phone systems. Site wiring should conform to standard telephone wiring standards and terminate at the HandReader with a standard RJ-11 modular phone jack. Each HandReader with a modem includes a 6’ modem cable for the final connection between the phone jack and the HandReader modem. Modem HandReaders may be networked with up to 31 non-modem HandReaders using RS-422 wiring. Refer to the Modem Application Note (available from Schlage Biometrics) for detailed information.

Remote HandReader Connected to a Host PC via Optional Ethernet

The HandReader 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 HandReader with a standard RJ-45 modular jack. The cable from the jack to the HandReader is not provided with the Ethernet option. The IP address, Gateway, and Host Bits are entered at the HandReader in the SET SERIAL menu. Ethernet HandReaders may be networked with up to 31 non-Ethernet HandReaders using RS-422 twisted pair cable. Refer to the Ethernet Application Note (available from Schlage Biometrics) for detailed information.

Printer

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

Mechanical Installation

Select an installation location based on the guidelines provided in the Planning an Installation section beginning on page 7.

Wall Plate Installation

!NOTE For the following instructions protect the HandReader from the dust and debris generated during the wall plate installation process.

1. Remove the wall plate from the packing carton. Refer to Figure 4-1 for all wall plate references in the following section.

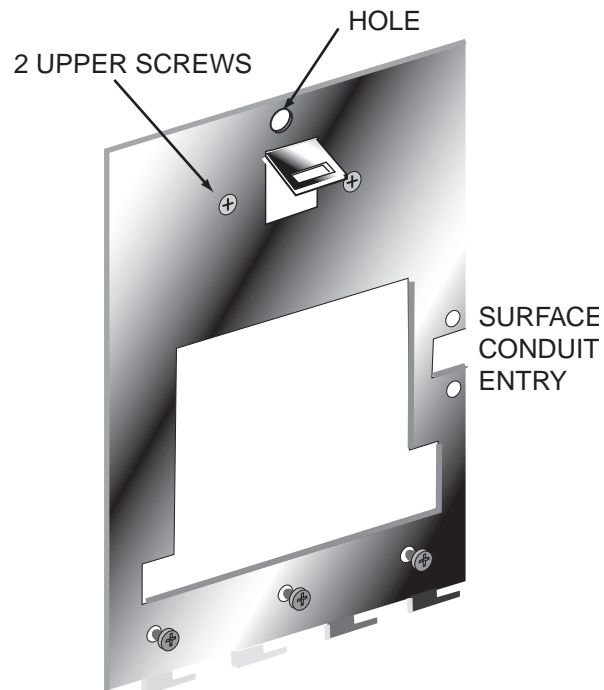


Figure 6-2: Wall Plate

3. 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 HandReader should be mounted.
4. 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.

5. For a solid wall, hold the wall plate against the wall, centering the leveling hole over the mark in the wall.
6. 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.
7. Secure the plate to the wall using heavy masking tape.
8. Using the wall plate as a template, mark the locations of the two upper screw holes and the three lower screw holes.
9. 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 HandReader's wiring will be mounted.
10. For a surface conduit wiring connection, mark the two conduit clamp holes at the right side of the wall plate.
11. Remove the wall plate, masking tape, and the nail (if used).

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.

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 HandReader 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 HandReader, ending the conduit between the two conduit clamp holes. Pull the wiring to enter the HandReader through the conduit.

Attaching the HandReader

1. Remove the HandReader from its carton.
2. Align the sleeves of the back plate with the pins of the wall plate and slide the HandReader to the left as shown in figure 4-2.

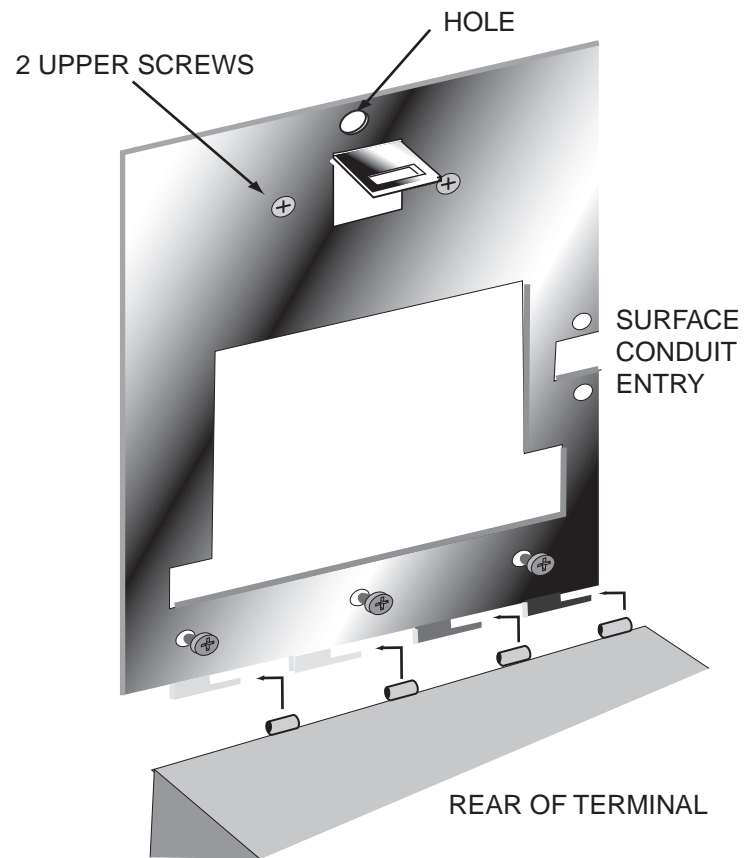


Figure 6-3: Attaching the HandReader to the Wall Plate

4. The HandReader is now ready for its wiring connections.

Closing the HandReader

With the wall mount latch in the unlocked position, swing the body of the HandReader up and rotate the key away from the wall. Hold the top of the HandReader firmly against the wall and rotate key towards wall, locking the latch into place (see Figure 4-3).

!NOTE Do not force the HandReader onto the wall mount latch when the latch is in the locked (down) position.

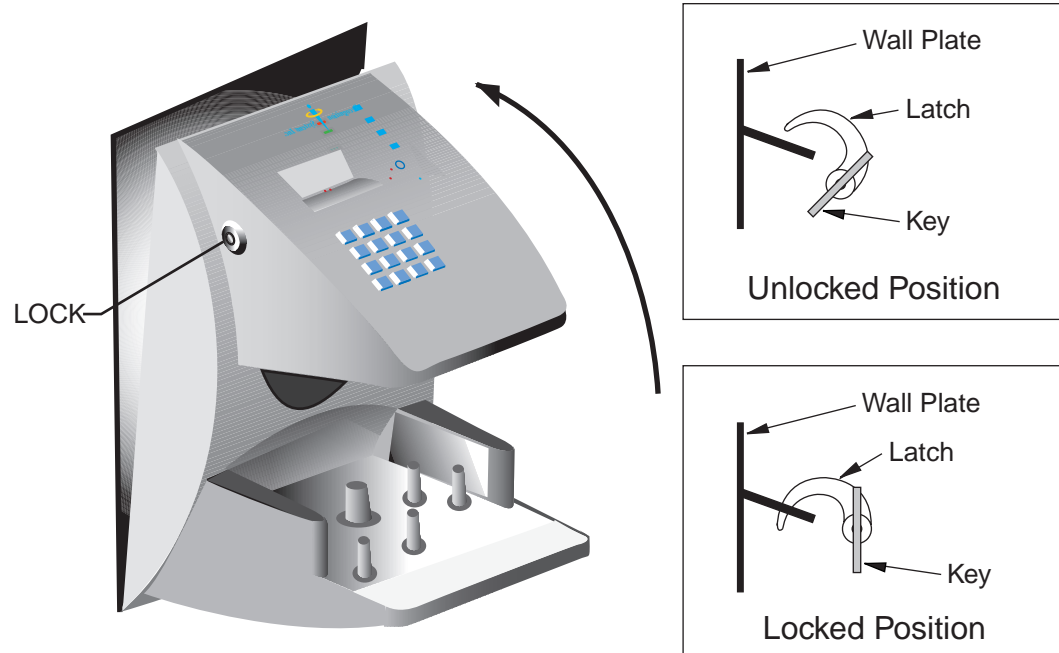


Figure 6-5: Closing the HandReader

Wiring Connections

Once the HandReader is attached to the wall plate the wiring connections to the HandReader can be made (see Figure 5-1).

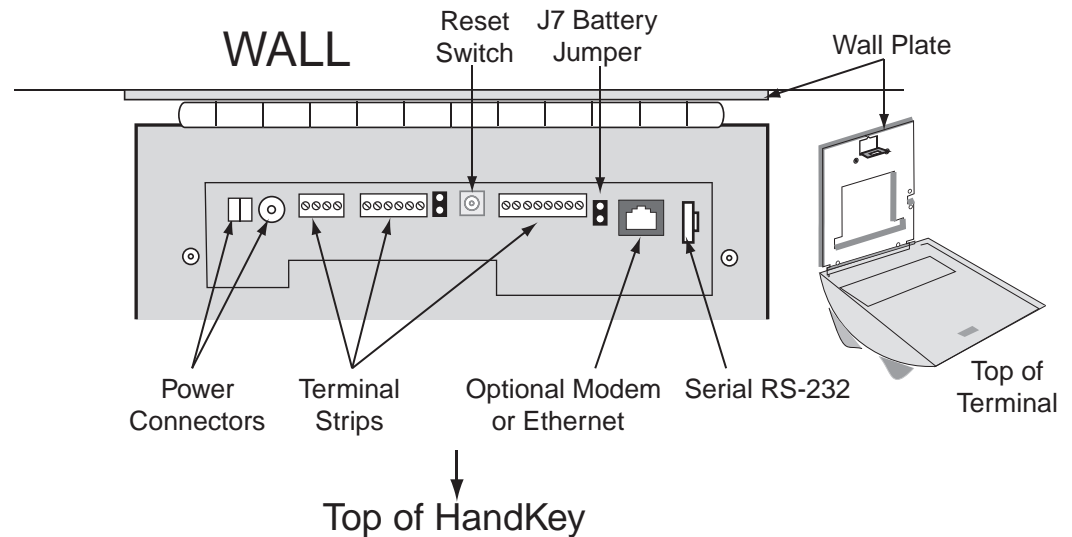


Figure 7-1: Wiring Connections

Wiring Examples

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

- Table 5-1 on page 22 provides the pin outs for TS-1: Communication Connections.
- Table 5-2 on page 22 provides the pin outs for TS-2: Input Connections.
- Table 5-3 on page 22 provides the pin outs for TS-3: Output Connections.
- Table 5-4 on page 22 provides the pin outs for the Serial RS-232 Connection.

The following Figures provide typical HandReader wiring diagrams.

- Figure 5-2 on page 23 provides a typical Lock Output wiring diagram.
- Figure 5-3 on page 24 provides a typical Auxiliary Output wiring diagram.
- Figure 5-4 on page 25 provides a typical Card Reader Emulation Mode wiring diagram.
- Figure 5-5 on page 26 provides a typical RS-422 Master/Remote Network System wiring diagram.
- Figure 5-6 on page 27 provides a typical RS-485 2-Wire Master/Remote Network System wiring diagram.
- Figure 5-7 on page 28 provides a typical Host PC Network System wiring diagram.
- Figure 5-8 on page 29 provides a typical Printer to HandReader wiring diagram.

Table 7-1: TS-1 - Power and Communication Connections

Terminal	Connection
15	RS-422 Rx- or RS-485 Rx-/Tx-
16	RS-422 Tx- or RS-485 Rx+/Tx+
17	RS-422 Rx+
18	RS-422 Tx+

Table 7-2: TS-2 - Input Connections

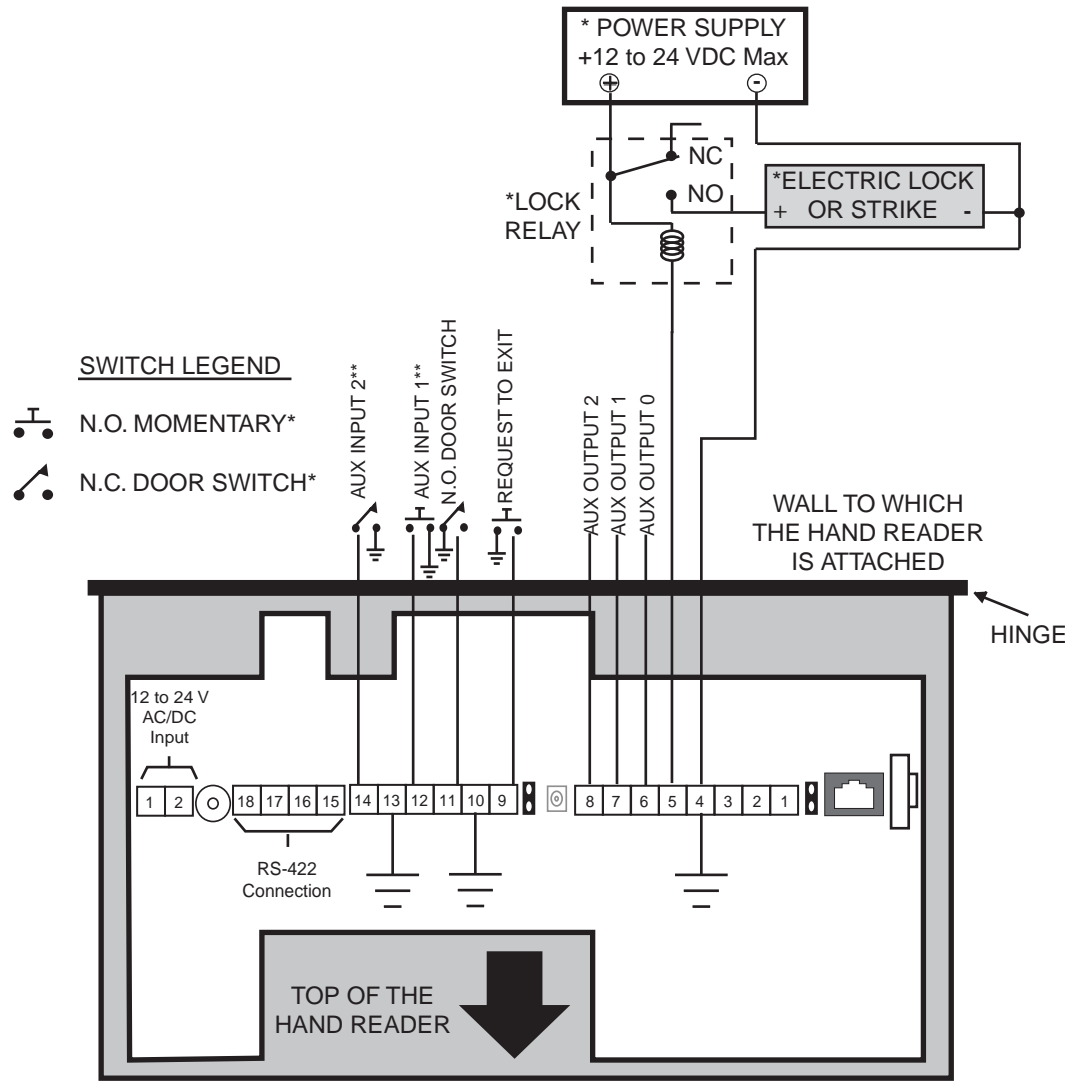
Terminal	Connection
9	Request to Exit Input
10	Ground
11	Door Monitor Switch Input (NC Standby)
12	Auxiliary Input 1
13	Ground
14	Auxiliary Input 2

Table 7-3: TS-3 - Output Connections

Terminal	Connection
1	+5 VDC @ 400mA Max. Output for External Card Reader
2	Card Reader: Wiegand D0 or Magnetic Stripe Data Input
3	Card Reader: Wiegand D1 or Magnetic Stripe Clock Input
4	Ground
5	Lock Output or Wiegand D1 or Magnetic Stripe Clock Output
6	Auxiliary Output 0 or Wiegand Data 0 or Magnetic Stripe Data Output
7	Auxiliary Output 1
8	Auxiliary Output 2

Table 7-4: RS-232 Connection

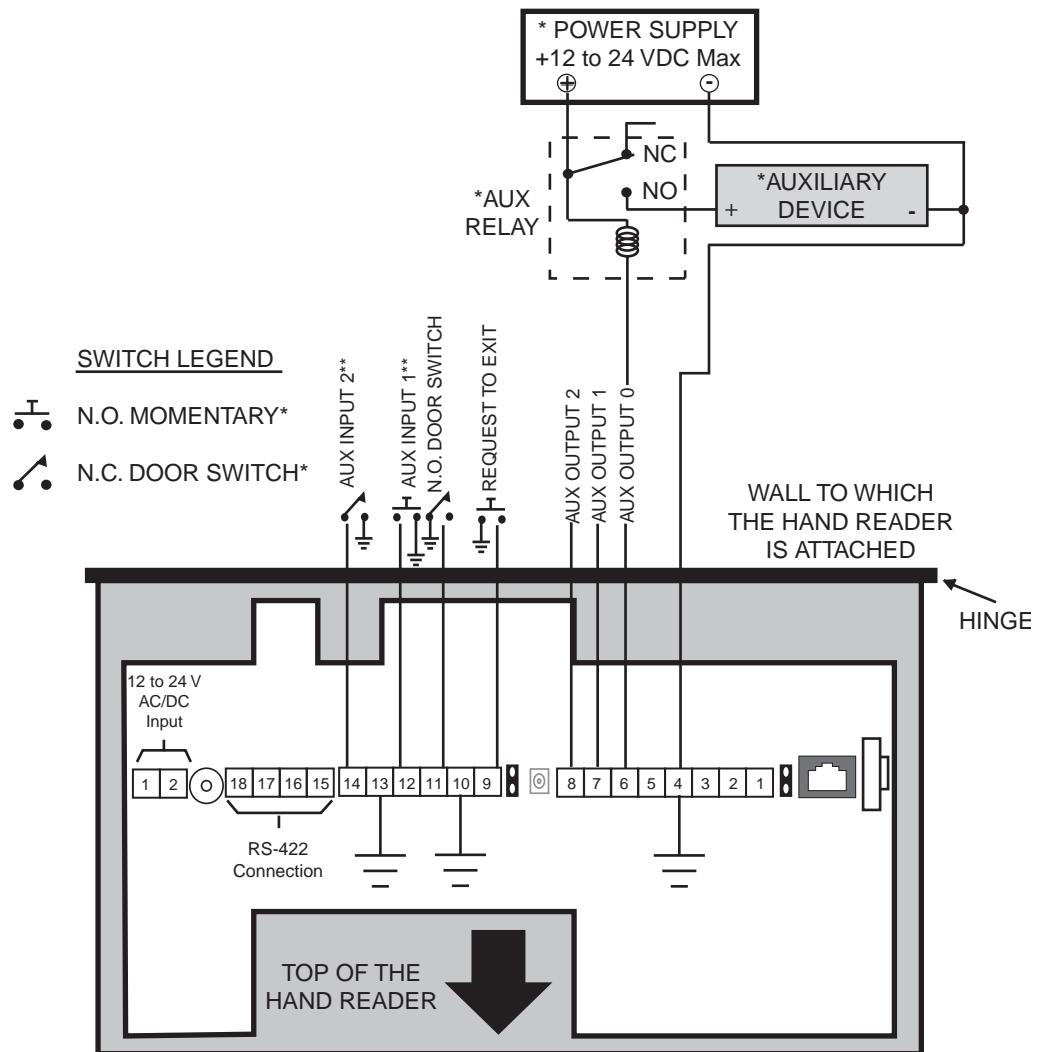
Pin	Signal	Connection
1	GND	Ground
2	RXD	Receive Data Input (from external device)
3	TXD	Transmit Data Output (to external device)
4	RTS	Ready to Send Output (to external device)



* These components are not supplied by Schlage Biometrics, Inc.

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

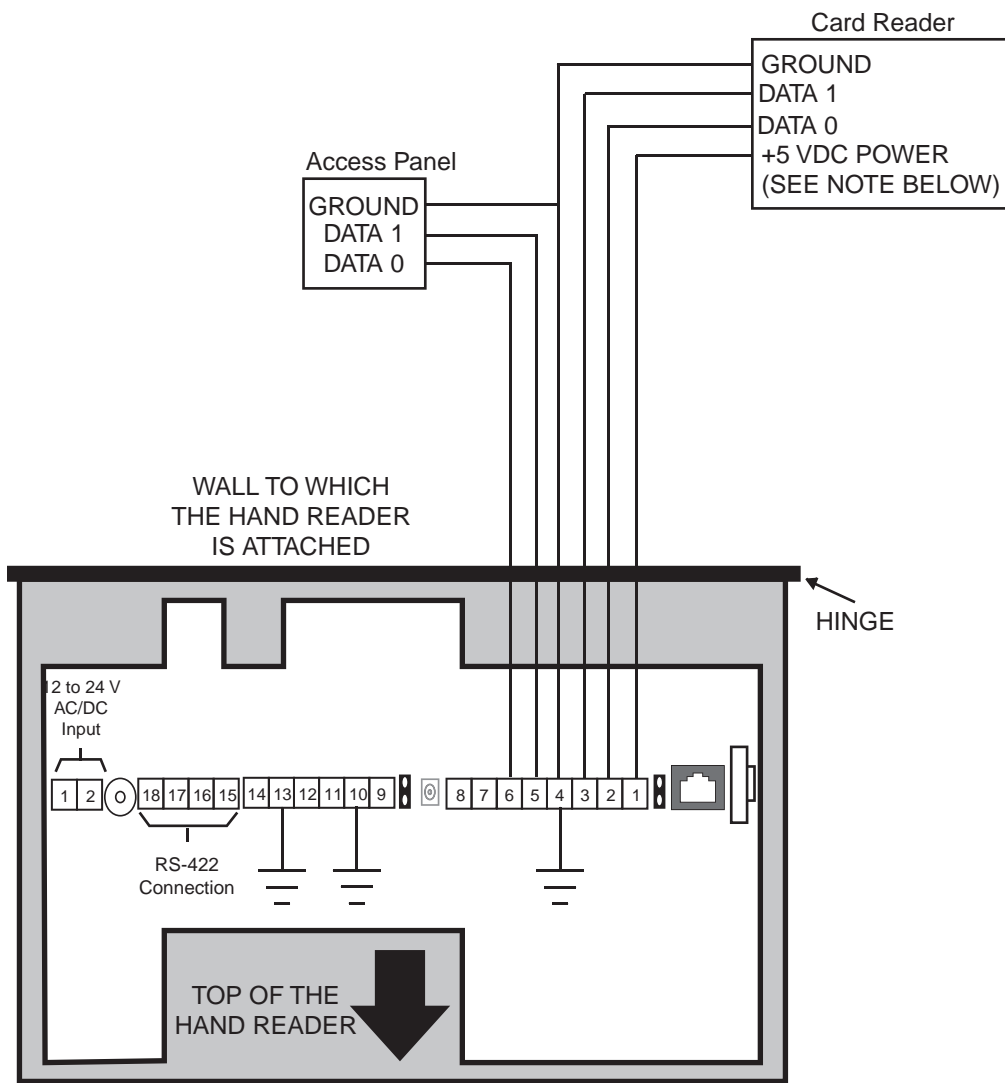
Figure 7-2: Lock Output Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

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

Figure 7-3: Auxiliary Output Wiring Diagram



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

Figure 7-4: Card Reader Emulation Mode Wiring Diagram

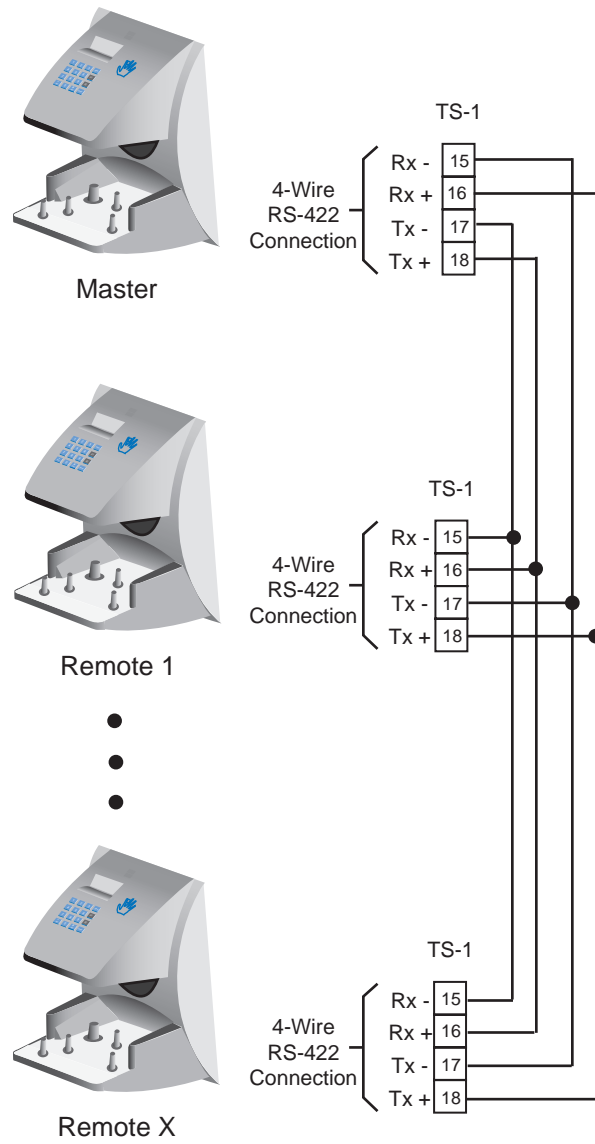


Figure 7-5: RS-422 4-Wire Master/Remote Network System Wiring Diagram

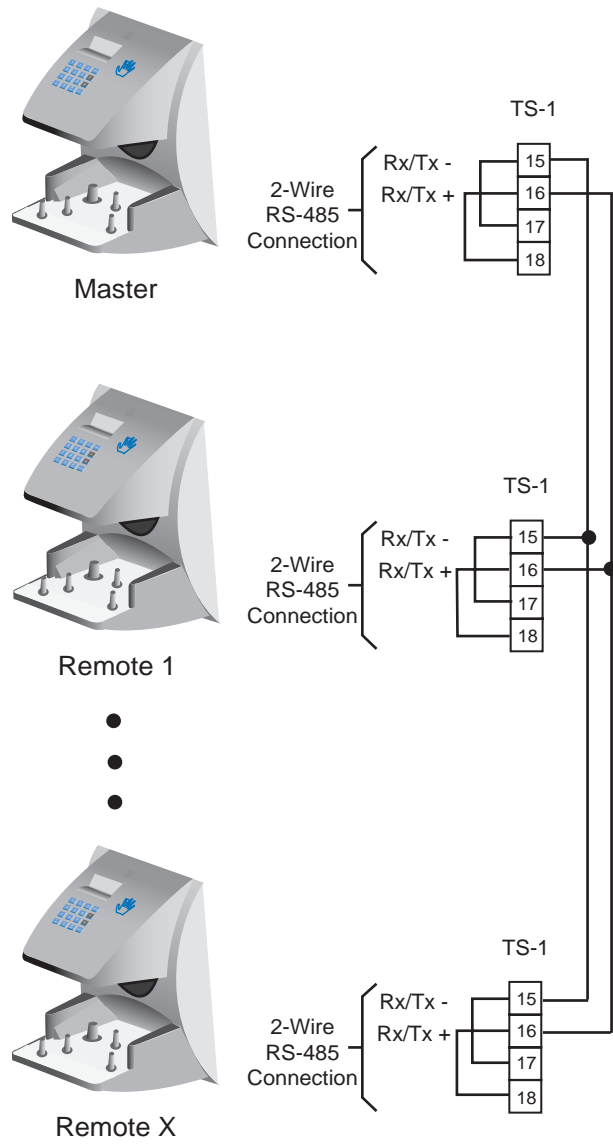


Figure 7-6: RS-485 2-Wire Master/Remote Network System Wiring Diagram

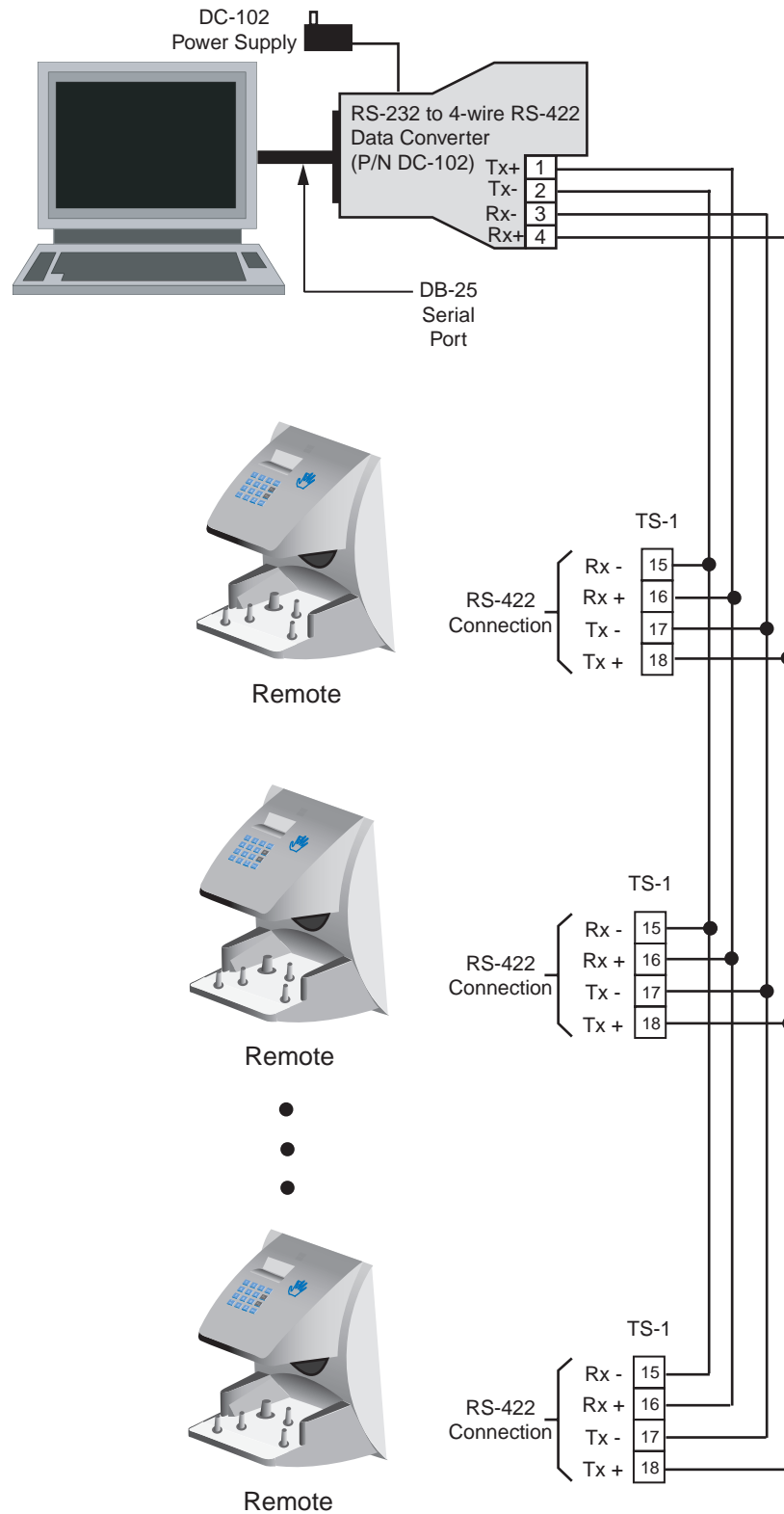
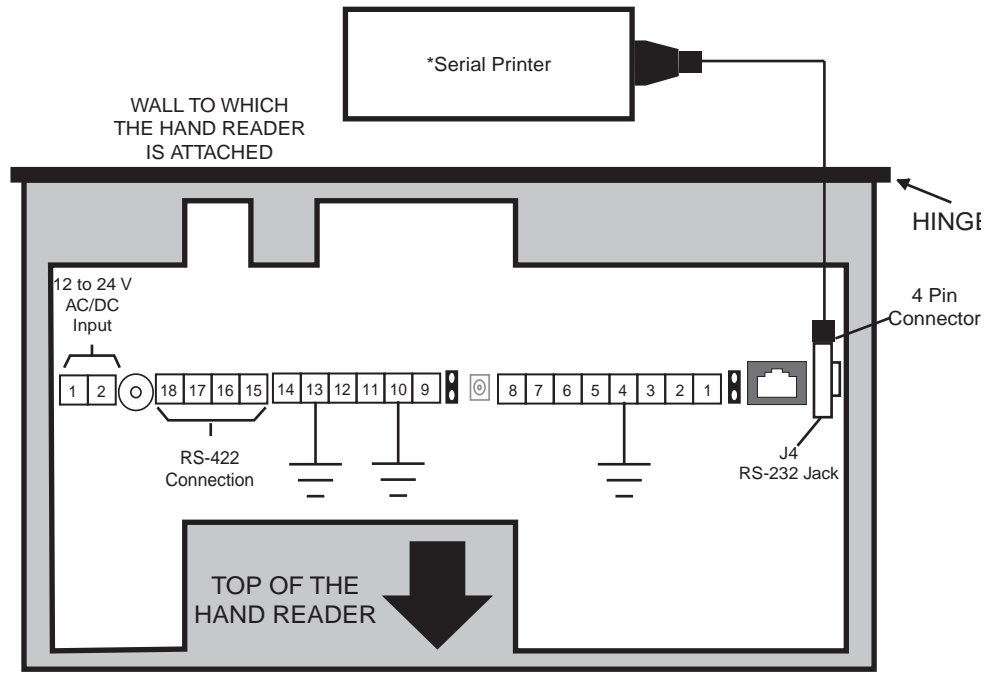


Figure 7-7: Host PC Network System Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

Figure 7-8: Printer to HandKey II Wiring Diagram

All HandReaders in a network must be set to the same communication method. Four-wire RS-422 cabling is required for HandNet for Windows™ network installations. Schlage Biometrics does not recommend two-wire RS-485 cabling for new network installations.

Erasing the Memory

There are two options when erasing the memory of the HandReader.

1. Setup
2. All

The erasing of the setup will set the HandReader's address, passwords, etc. back to factory defaults.

Choosing the All option will take the HandReader's setup back to factory defaults plus erase all user databases and datalogs. This action can not be undone. If there is a software that is managing the system then the users can be downloaded back to the HandReader if needed.

Erasing HandReader Memory

The erase memory function allows a HandReader's setup and/or user database to be erased.

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

1. With system power OFF, depress reset switch.
2. Turn system power ON and wait 5 seconds.
3. LCD screen will display

ERASE	:1 SETUP :2 ALL
--------------	----------------------------------

Enter a Command Menu

Press the and keys simultaneously to enter a command menu.

If No One is Enrolled in the HandReader

1. The display appears as follows.



ENTER PASSWORD

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

Press for the Service Menu.

Press for the Setup Menu.

Press for the Management Menu.

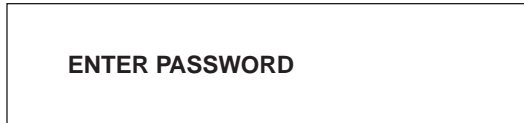
Press for the Enrollment Menu.

Press for the Security Menu.

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

If Users are Enrolled in the HandReader

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 for the Service Menu.

Press for the Setup Menu.

Press for the Management Menu.

Press for the Enrollment Menu.

Press for the Security Menu.

5. Press .
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.



!NOTE *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 HandReader'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 HandReader 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 Erasing HandReader Memory on page 31.*

Navigating Command Menus

Once an operator has 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 to exit the command menu (pressing any numeric key also exits the command menu). If the operator is in a command's sub-menu, the operator may have to press multiple times to completely exit the command menu.

Programming the HandReader

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

Table 10-5: 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			
	Upgrade			

* These menu options only appear in HandReaders 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 HandReader, Schlage Biometrics 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.

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 HandReader 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 HandReader. Once a user has been assigned to Authority Level 5, all other user authority levels are applied as per the list above.

!NOTE *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. Schlage Biometrics 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.*

Programming Order

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

1. Design an ID Numbering System – Define the format for user ID assignments. A properly designed ID numbering system makes the HandReader easier and faster to use.
2. Enter a Command Menu – Enter a Command Menu and begin HandReader programming per the commands in that menu.
3. Enroll all Supervisory Staff – Enroll yourself and the supervisors who will have responsibility for HandReader management. This is done through the Enrollment Menu.
4. Set Supervisory Staff Authority Levels – Assign Authority Levels to the supervisors with specific HandReader management responsibilities. This is done through the Security Menu.
5. Set Reader Site Parameters – Set the reader's Operating Parameters to meet site specific needs and usage. This is done through the Setup Menu.
6. Train and Enroll Users – Train each user regarding HandReader usage and then Enroll each user. This is done through the Enrollment Menu.

System Management and Maintenance

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

1. Set Reader Operating Thresholds – Set the Reject and Number-of-Tries HandReader operating thresholds to meet the site's security requirements. This is done through the Security Menu.
2. System Management – Backup or Restore HandReader data and List the Users authorized to use a HandReader. This is done through the Management Menu.
3. System Maintenance – Calibrate the HandReader, display HandReader Status, and display Network Status. This is done through the Service Menu.

!NOTE *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.*

Design an ID Numbering System

The ID numbering system helps identify the user about to use the HandReader. 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.

!NOTE *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.

Calibrate

The Calibrate command verify that the HandReader's exposure values are within normal operating parameters. The normal operating parameters are shown in Table 2.

Table 11-7: Normal Operating Parameters

Parameter	Normal Range
Row "r"	0 +/- 2
Column "c"	0 +/- 2
Exposure	100 +/- 20

Status Display

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

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

Figure 11-1 on page 40 identifies each status display field value.

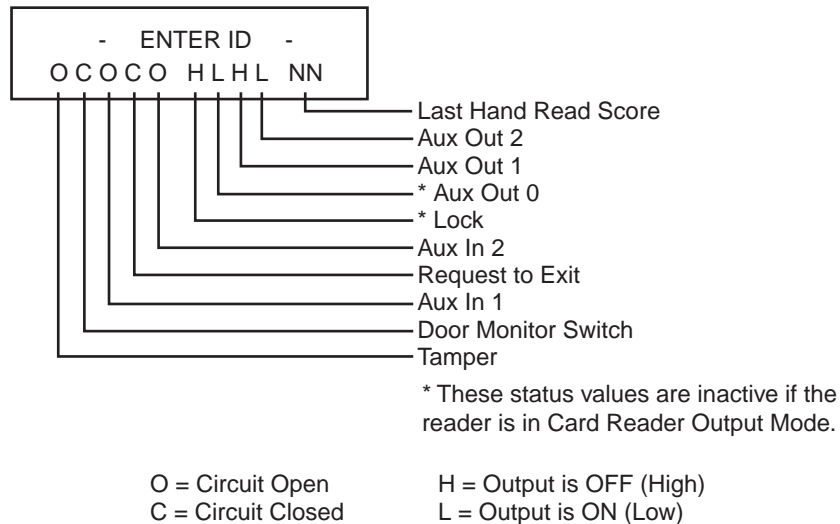


Figure 11-1: Status Display Chart

Network Status

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

!NOTE You can check network status only from the Master HandReader in a master/remote HandReader network.

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



Each "O" and "." represents a HandReader address in the network. An "O" indicates that the HandReader corresponding to that address is communicating on the network. A "." indicates that the HandReader with that address is not communicating on the network.

Setup Menu

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

!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.*

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 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 multiple times to completely exit the command menu.

Setup Commands

There are 12 commands available from the Setup command menu.

- Set Language
- Set Date Format
- Set Time and Date
- Set Address
- Set ID Length
- Set Facility
- Aux Out Control
- Set Reader Mode
- Set Serial
- Set Duress Code
- Set Beeper
- Upgrade

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

Table 12-8: 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 Facility	
Auxiliary Output Control	Select Auxiliary Output 1/2
	Aux 1 Out Control
	Aux 2 Out Control
	Output Set by Tamper
	Output Set by ID Refused
	Output Set by Duress
	Output Set by Try Again
	Output Set by F1 Key
	Output Set by F2 Key
	Output Set on Battery Backup
	Auxiliary Output Cleared by Timer
	Aux Output Cleared by Valid Access
Set Reader Mode	To Master/Remote
Set Serial	RS-422 (Y/N)
	Select Baud Rate
	RS-232 (Y/N)
	Select Baud Rate
	Use RS-232 for Printer or Host
Set Seriala	Verify/Enter IP Address
	Verify/Enter Gateway
	Verify/Enter Host Bit
Set Duress Code	Enter Duress Code
Set Beeper	Turn Beeper On/Off (Y/N)
Upgrade	Enter Code

Set Language

The Set Language command allows the language shown on the HandReader'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

Set Date Format

The Set Date Format command allows the date format shown on the HandReader'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	

Set Time and Date

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

!NOTE *Stand-alone HandReaders and HandReaders on a master/remote HandReader network require adjustment for the daylight savings time changes. HandReaders 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)

Set Address

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

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 `key` to complete an ID number entry. Once the ID Length is set, when a user enters an ID number the HandReader 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 49). The default value for ID Length is 10.

!NOTE *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.*

Set Facility

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

!NOTE *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.*

Aux Out Control

The Aux Out Control command allows the Auxiliary Outputs in the HandReader 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.

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

Table 12-9: Auxiliary Output Choices

Auxiliary Output	Function
Auxiliary Output 1	Auxiliary 1 switched to ground
Auxiliary Output 2	Auxiliary 2 switched to ground
Tamper	HandReader opened, shaken, or removed.
ID Refused	User not verified after allowed number of tries.
Duress	User entered the duress code digit.
Try Again	User rejected.
F1 Key	F1 key pressed.
F2 Key	F2 key pressed.
On Battery Backup	AC power failure, HandReader switched to battery power.

Set Reader Mode

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

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

!NOTE *All remote HandReaders on a HandReader network must have a unique address. Refer to the Set Reader Address section on page 43.*

The HandReader'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

```

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 HandReader uses the Ethernet communication option, the TCP/IP address, gateway, and host bit parameters are set instead of the baud rate.

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.*

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.

Upgrade

For instructions on how to upgrade the memory of the HandReader please refer to the Memory Upgrade Note.

Management Menu

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

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 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 multiple times to completely exit the command menu.

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 HandReader.
- Data From Network – upload data from the network to the master HandReader.
- Data To Network – download data from a master HandReader to the network.

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

Table 13-10: Management Command Menu

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

List Users

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

**Data From
Network**

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

**Data To
Network**

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

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 HandReader 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 time.¹

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 HandReader before you enroll them.

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 advance.²
- The HandReader 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 digit.³
- 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 Schlage Biometrics dealer.

1. Refer to the Set User Data > Set Authority Level command in the Security command menu on page 55.

2. Refer to the Design an ID Numbering System section on page 37.

3. Refer to the Set Duress Code command in the Setup command menu on page 45.

User Education

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

- The HandReader 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.
- 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.

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 12-1). 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 14-1: Placing Your Hand on the Platen

Left Hand Enrollment

Some right hands are not suitable for use in the HandReader 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.

Read Score

When a user uses the HandReader 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.

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 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 multiple times to completely exit the command menu.

Enrollment Commands

There are two commands available from the enrollment command menu.

- Add User
- Remove User

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

Table 14-11: Enrollment Command Menu

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

Add User

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

Remove User

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

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

Security Menu

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

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 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 multiple times to completely exit the command menu.

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

Table 15-12: 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 #
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 #

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.

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 HandReader. Once a user is assigned a Time Zone, access attempts outside of that time/date period are rejected by the HandReader.

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 HandReader.

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

!NOTE *All time entries made for time zones are entered in 24-hour format. For example, 8 A.M. is entered as 08:00, 5 P.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.

!NOTE *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 HandReader 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).

Reject Threshold

Use the Reject Threshold command to set the HandReader'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 HandReader.

The reject sensitivity level and number of tries are global values. This means that these values are applied to all users on all HandReaders 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 page 54).

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

- Raising the threshold level makes the HandReader 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 HandReader will refuse all subsequent attempts with that user ID number. This means the user will be locked out until another user is verified successfully.

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 HandReader, 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 54) and must enter the correct password.

Clear Memory

Use the Clear Memory command to clear the user data from the HandReader, but retain the setup data. This allows you to clear the HandReader's user database of all templates and ID numbers, but retain all HandReader setup information. Typically, this is done when moving the HandReader 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 HandReader's memory the user data is not recoverable.*

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 HandReader 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 55).*

HandReader Maintenance

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

!NOTE *There are NO user serviceable parts inside the HandReader.*

Once a HandKey system is in operation there are three HandReader commands that can assist with system maintenance. These commands are performed through the Service Menu. The instructions for these commands begin on page 39.

- 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.
- Network Status – Display the network communication status of Hand Readers in the HandKey system (master Hand Reader only).

Cleaning the Hand Reader

Inspect and clean the HandReader 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 14-1). 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.*

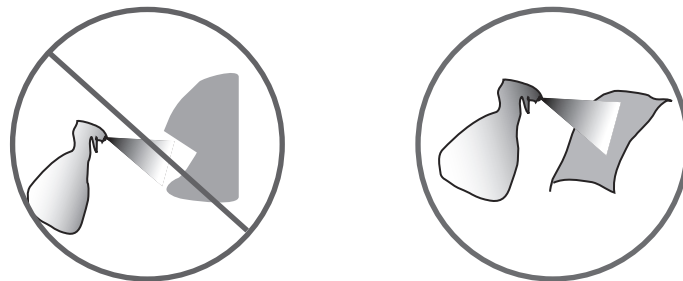


Figure 16-1: HandReader Cleaning

User Score

Periodically check users' scores (refer to the Read Score section on page 51). 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 HandReader and check scores again. If scores remain high, or if users are experiencing frequent rejections, run the Calibration command (see page 40).

Appendix A: Tips for a Successful Installation

Unless the following tips are followed, the installation runs the risk of having some level of difficulties. These tips come from years of experience with thousands of sites installed around the world. By far the biggest problem tends to be that the HandReader is allowed to get dirty. Think of the HandReader as a camera, because that is exactly what it is. If a user takes a picture with a dirty camera, then what you get is a dirty picture.

Location and Installation

If a user would have to place their body in an awkward or dangerous position to use the HandReader then that probably is not the correct location for a HandReader.

- Mount all HandReaders in a network so that the top of the platen is 40" off of the floor
- If an enrollment HandReader is used make sure that it is placed with the top of the platen 40" off of the floor and not sitting directly on top of a desk, this will help to eliminate "bad enrollments"
- Mount the HandReader so that it is not difficult or dangerous to verify then open the door
- It is not recommended to mount the HandReader in an area where there is airborne dust, in the path of direct sunlight, or where the HandReader can be exposed to water or corrosive gasses
- Do not remove the foam backing from the wall mounting plate
- Seal any holes made in the wall for wire routing, so that dust will not blow into the HandReader. Walls act as billows as the pressure changes in a room (opening and closing a door can cause this).

HandReader

It is extremely important to keep the HandReader clean. If a HandReader is not kept clean verification issues will ensue. This is especially true in a networked environment, all HandReaders should be at the same level of cleanliness for optimum performance.

- Think of the HandReader as a camera
- Clean the HandReader before it gets dirty
- Use non-abrasive cleaners such as glass cleaners and non-abrasive cleaning cloths
- Make the cleaning of the HandReader part of the Janitorial program
- Never spray cleaner directly into the HandReader
- "Recalibrate" after cleaning the HandReader

Enrollment

Bad enrollments equal bad verification (meaning scores will be too high). The key to successful verification is education.

- Educate the Enrollee on Hand Geometry
- Explain enrollment process
- Train Enrollee on hand placement
 - Practice placing hand on platen
 - Rotate rings to be stone-up
 - Make sure hand is flat on platen
 - Close finger towards the center of hand
 - Fingers need only to gently touch finger pins
- Let the enrollee enter in their own ID number during the enrollment process, this forces the Enroller to step aside allowing the Enrollee to properly stand in front of the HandReader helping to eliminate “bad enrollments”
- If an enrollment HandReader is used make sure that it is placed with the top of the platen 40” off of the floor and not sitting directly on top of a desk, this will help to eliminate “bad enrollments”
- If an enrollment transaction fails:
 - Retrain the user on correct placement and ensure that rings are rotated to be stone-up then
 - Try again to enroll the same hand
 - Try to enroll the other hand (with the hand placed upside-down so the thumb still contacts the thumb-pin on the platen)
- After enrollment, it is a good idea to let the enrollee enter their ID number and practice a verification transaction to ensure that the enrollment was high-quality
- If a user consistently fails during verifications days/months/years later, re-enroll the user to ensure a high quality and up-to-date enrollment record

Communication

Direct

- Use shielded cable when installing direct networks. This will help reduce outside noise interference
- Do not lay cabling on top of fluorescent lighting. Make sure the Data Convertor is plugged in
- When starting a network for the first time bring one HandReader up at a time, this is a very easy way to find out where communication problems may exist

Modem

- Use default init string for modem first
- Do not set the baud rate of the HandReader down below 9600, unless communicating in a E series network (metal HandReaders), or risk over-running buffers
- In the init string set the line rate to 14400
- Use analog lines (POTS)
- Troubleshooting by plugging the HandReader on the fax machine’s phone line

Ethernet

- make sure network cable is plugged in to Ethernet card before powering up the HandReader
- Port 3001 must be set on all switches and routers in order to successfully communicate over WANs
- If the HandReader can be “pinged” but will not communicate with the software, power down the HandReader and run “ping” again

Appendix B: Noted Board Configuration Differences

Because of Schlage Biometrics' camera retrofit of the HandReader some changes have been made to the main PCB and they are listed as follows:

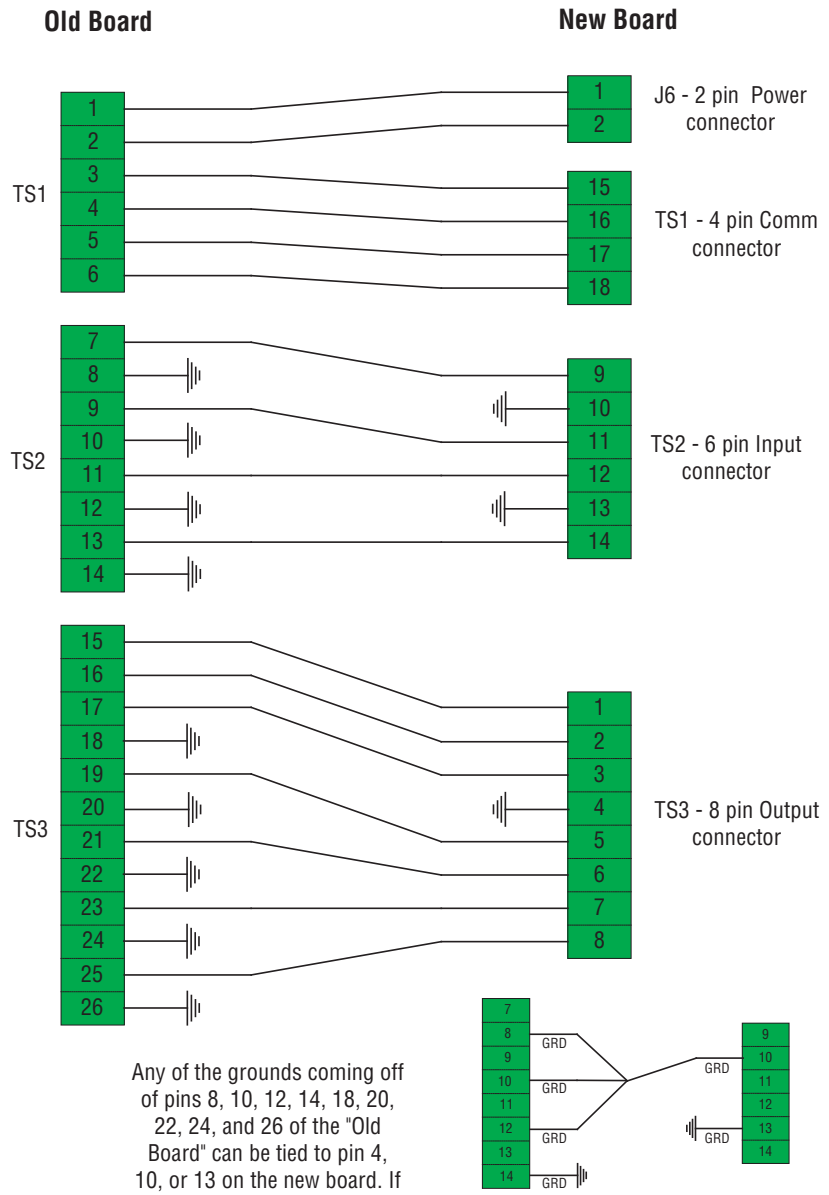
- Dipswitches have been removed
 - comm lines are terminated
 - RS-485 is set by wiring jumpers
 - memory is reset with a push-button reset and user interface with keypad and LCD
- The labeling of the terminal strips have changed. See Figure 16-1
- The configuration of the terminal strips have changed. See Figure 16-2
- Power has moved to the right side of the PCB
- The RSS-232 RJ-45 receptacle has been replaced with a 4 pin Molex connector on the left side of the PCB
- A 2 pin Molex connector (J5) has been added to the board, next to the reset button, to supply power for the LEDs. This connector should never be unplugged. unless a modem or Ethernet is added to the PCB
- The upgrading of the memory is now handled through software codes at the HandReader. Contact Order Entry for memory upgrades

Terminal Block Labeling

Number	OLD PCB	Number	NEW PCB
1	12-24 VDC (+) OR VAC	1	(+) 5 VDC OUTPUT
2	12-24 VDC (-) OR VAC	2	DATA/D0
3*	RX-	3	CLOCK/D1
4*	RX+	4	GROUND
5*	TX-	5	LOCK OR CLOCK OUTPUT
6*	TX+	6	BELL OR DATA OUTPUT
7	REX SWITCH	7	AUXOUT 1
8	GROUND	8	AUXOUT 2
9	DOOR SWITCH	9	REX SWITCH
10	GROUND	10	GROUND
11	AUX IN 1	11	DOOR SWITCH
12	GROUND	12	AUX IN 1
13	AUX IN 2	13	GROUND
14	GROUND	14	AUX IN 2
15	(+) 5 VDC OUTPUT	15	RX- *
16	DATA/D0	16	RX+ *
17	CLOCK/D1	17	TX- *
18	GROUND	18	TX+ *
19	LOCK OR CLOCK OUTPUT		
20	GROUND	1	12-24 VDC (+) OR VAC
21	BELL OR DATA OUTPUT	2	12-24 VDC (-) OR VAC
22	GROUND		
23	AUXOUT 1		
24	GROUND		
25	AUXOUT 2		
26	GROUND		

Figure 18-1: Terminal Block Labeling

Terminal Block Layout



Any of the grounds coming off of pins 8, 10, 12, 14, 18, 20, 22, 24, and 26 of the "Old Board" can be tied to pin 4, 10, or 13 on the new board. If there are multiple grounds create a pig tail so that there is only 1 wire going into the terminal block

Figure 18-2: Terminal Block Layout

Memory Reset

1. To reset the memory of the HandReader follow these steps-
2. Remove power and battery jumper, if a back up battery is installed
3. Press down on reset button and apply power
4. Release button
5. Reader will boot to
 - Press 1 to erase setup i.e. address, outputs, passwords, but retain user database and datalogs
 - Press 9 to erase everything i.e. HandReader goes back to factory defaults

Appendix C: Old Board Configuration Information

Wall Plate Installation

Attaching the HandReader

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 HandReader from its carton.
3. At the base of the HandReader is a piano hinge with three keyhole shaped slots that correspond with the three lower mounting screws. Align and hang the HandReader from the three lower mounting screws (see Figure 17-1).

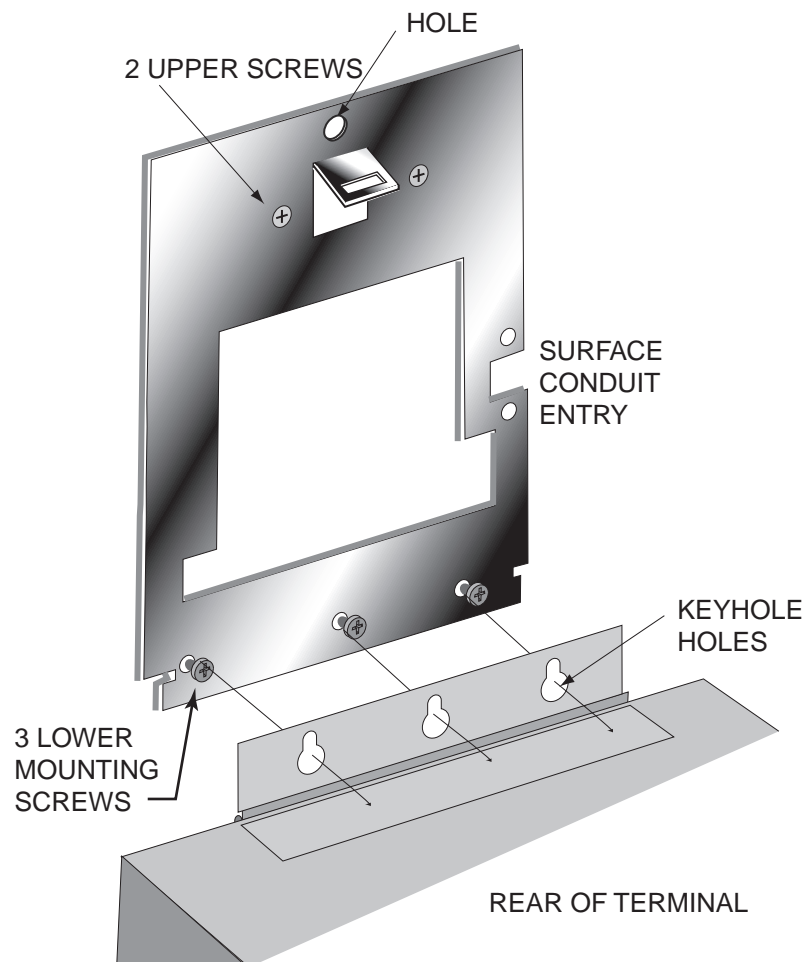


Figure 19-4: Attaching the Hand Reader to the Wall Plate

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

Wiring Connections

Once the Hand Reader is attached to the wall plate the wiring connections to the Hand Reader can be made (see Figure 17-2).

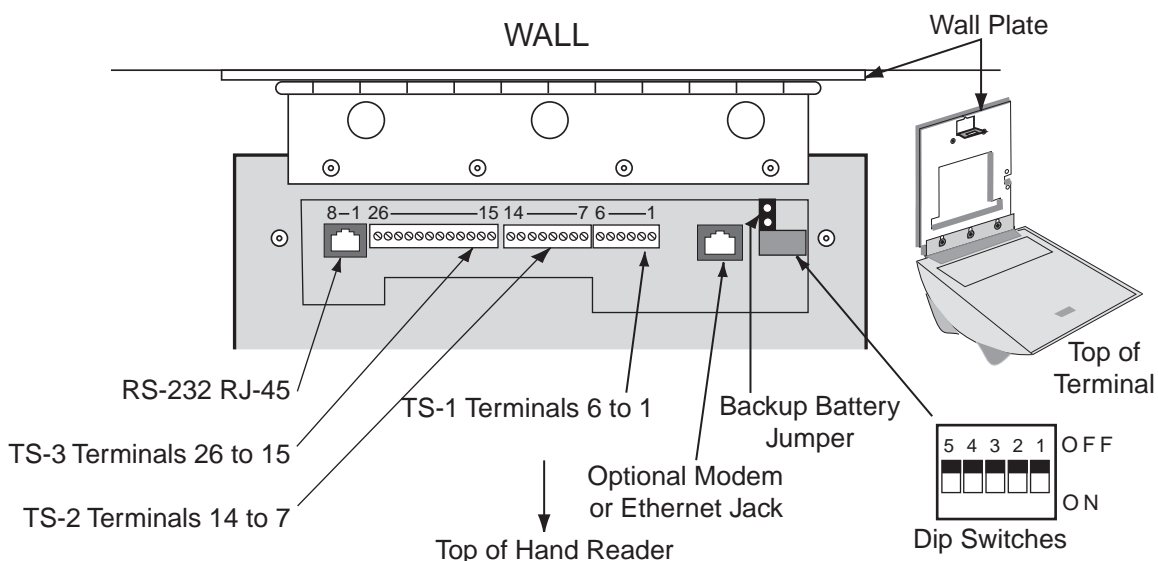


Figure 19-7: Wiring Connections and Dip Switches

Grounding

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

!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.

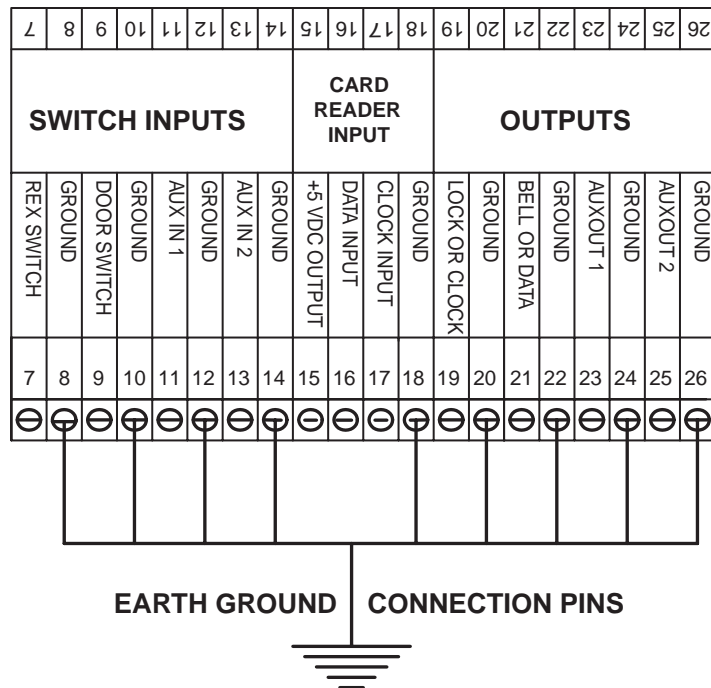


Figure 19-8: Earth Ground Connection Terminals

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

- earth grounding all units (see page 10)
- carrying an earth ground to each unit (see page 11)

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.

Wiring Examples

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

- Table 17-1 on page 68 provides the pin outs for TS-1: Power and Communication Connections.
- Table 17-2 on page 68 provides the pin outs for TS-2: Input Connections.
- Table 17-3 on page 68 provides the pin outs for TS-3: Card Reader and Output Connections.
- Table 17-4 on page 68 provides the pin outs for the RJ-45 Serial RS-232 Connection.

The following Figures provide typical Hand Reader wiring diagrams.

- Figure 17-3 on page 67 provides connection points for ground
- Figure 17-4 on page 69 provides a typical Lock Output wiring diagram.
- Figure 17-5 on page 70 provides a typical Auxiliary Output wiring diagram.
- Figure 17-6 on page 71 provides a typical Card Reader Emulation Mode wiring diagram.
- Figure 17-7 on page 72 provides a typical RS-422 Master/Remote Network System wiring diagram.
- Figure 17-8 on page 73 provides a typical RS-485 2-Wire Master/Remote Network System wiring diagram.
- Figure 17-9 on page 74 provides a typical Host PC Network System wiring diagram.
- Figure 17-10 on page 75 provides a typical Printer to Hand Reader wiring diagram.

Table 19-13: 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 19-14: 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

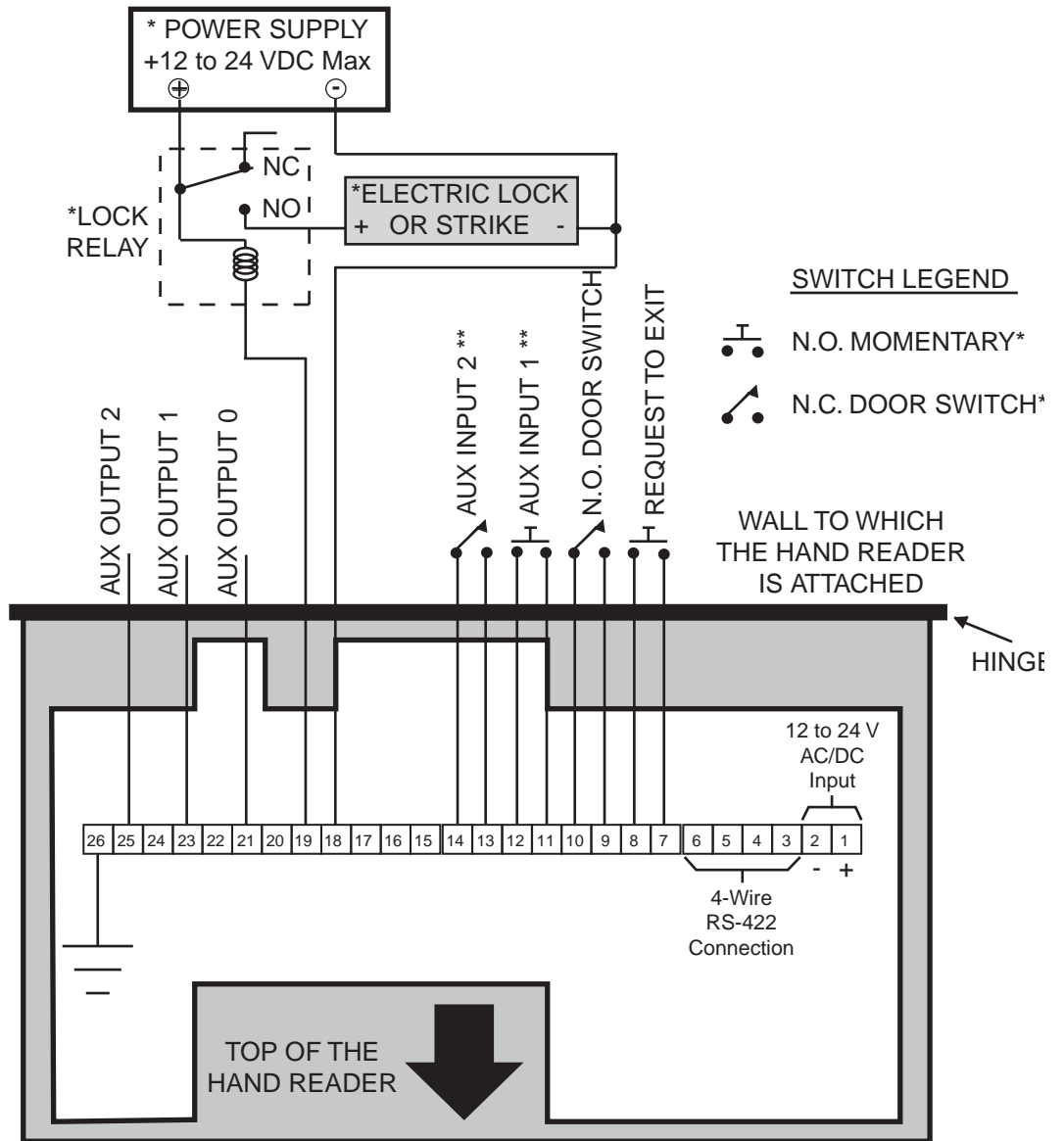
Table 19-15: TS-3 - Card Reader and Output Connections

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 19-16: 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)

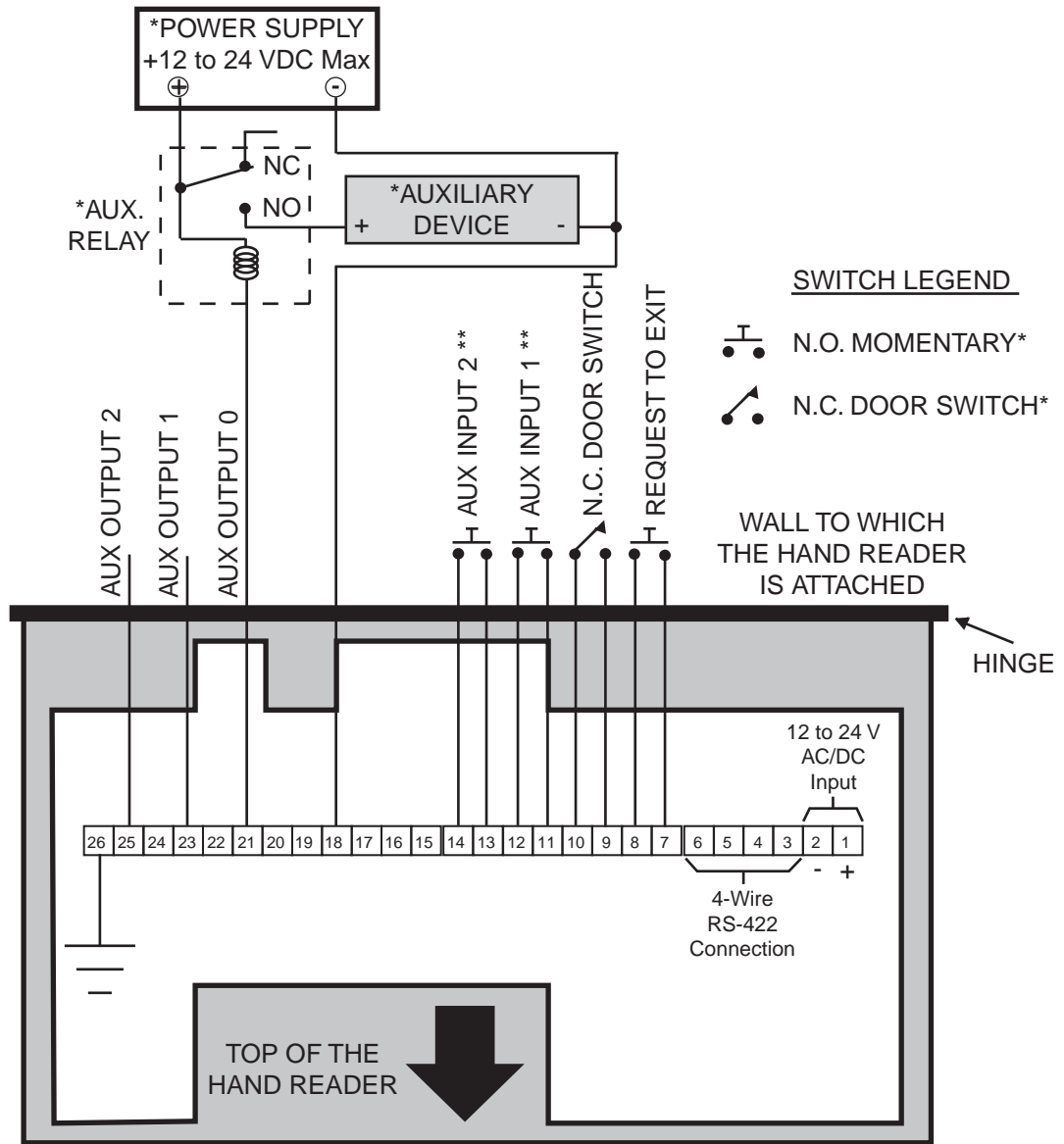
* These signals are not currently supported.



* These components are not supplied by Schlage Biometrics, Inc.

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

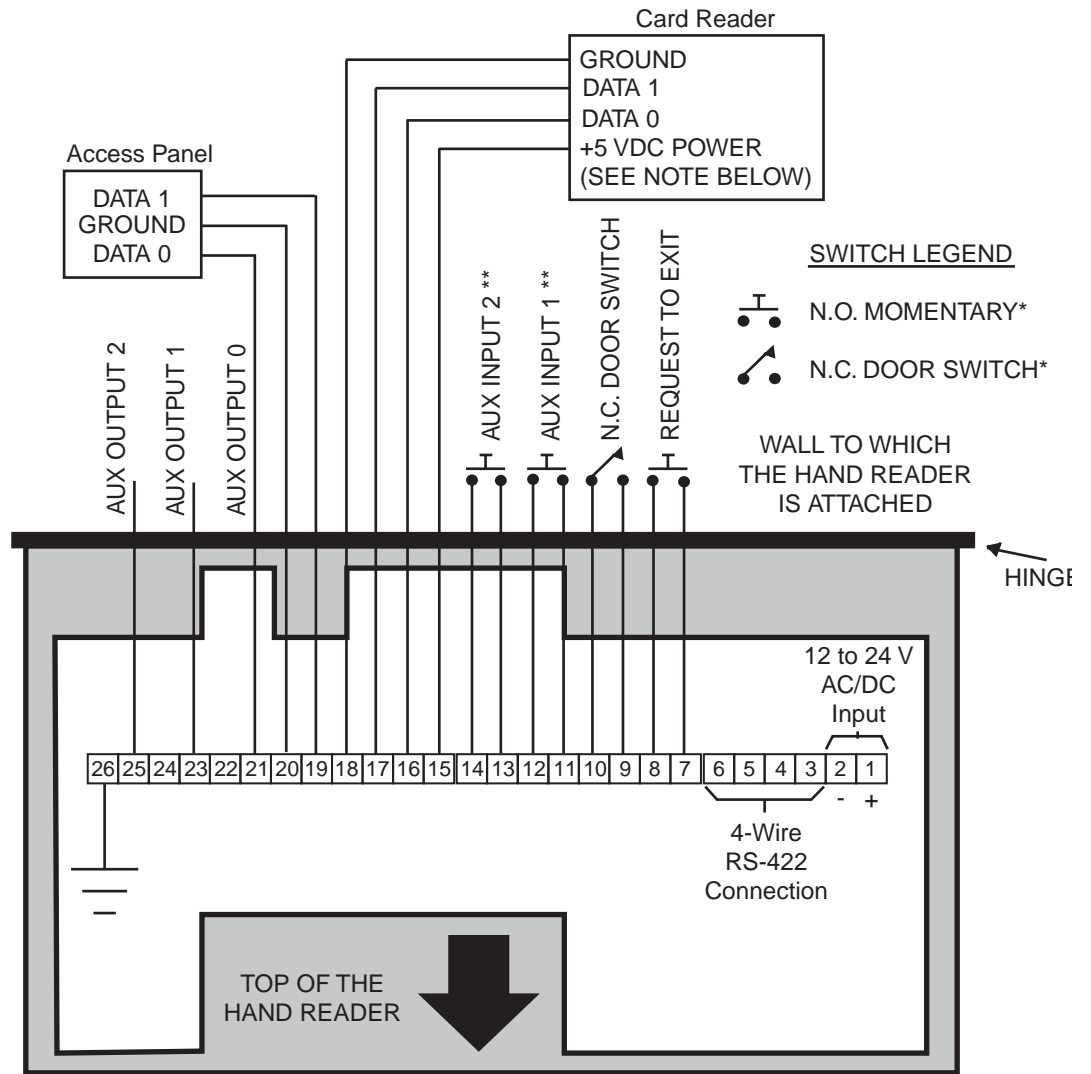
Figure 19-9: Lock Output Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

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

Figure 19-10: Auxiliary Output Wiring Diagram



* These components are not supplied by Schlage Biometrics, 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 19-11: Card Reader Emulation Mode Wiring Diagram

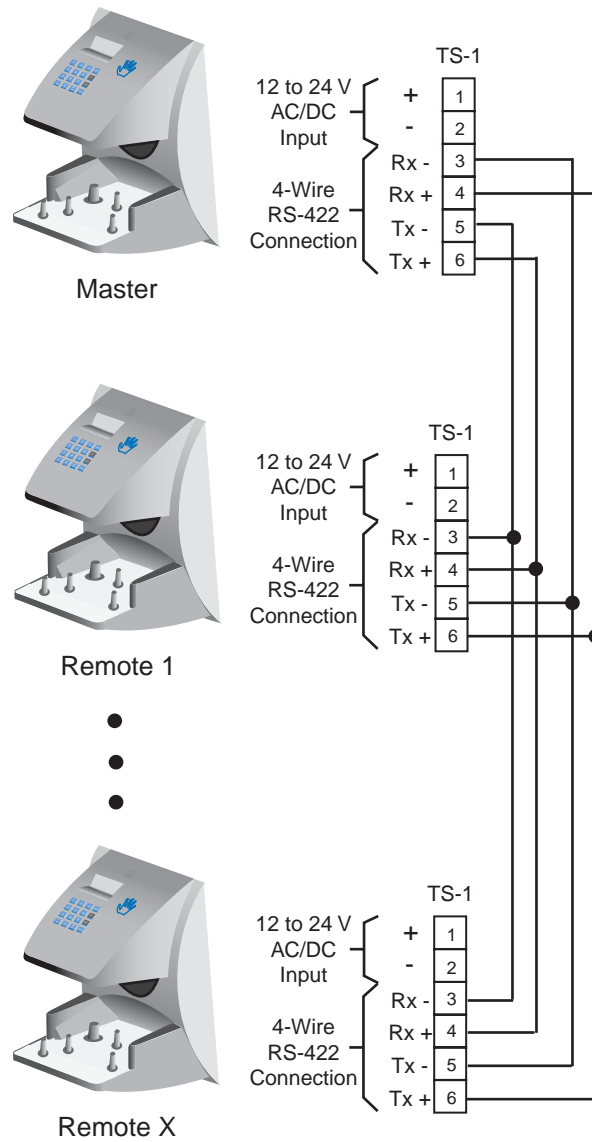


Figure 19-12: RS-422 4-Wire Master/Remote Network System Wiring Diagram

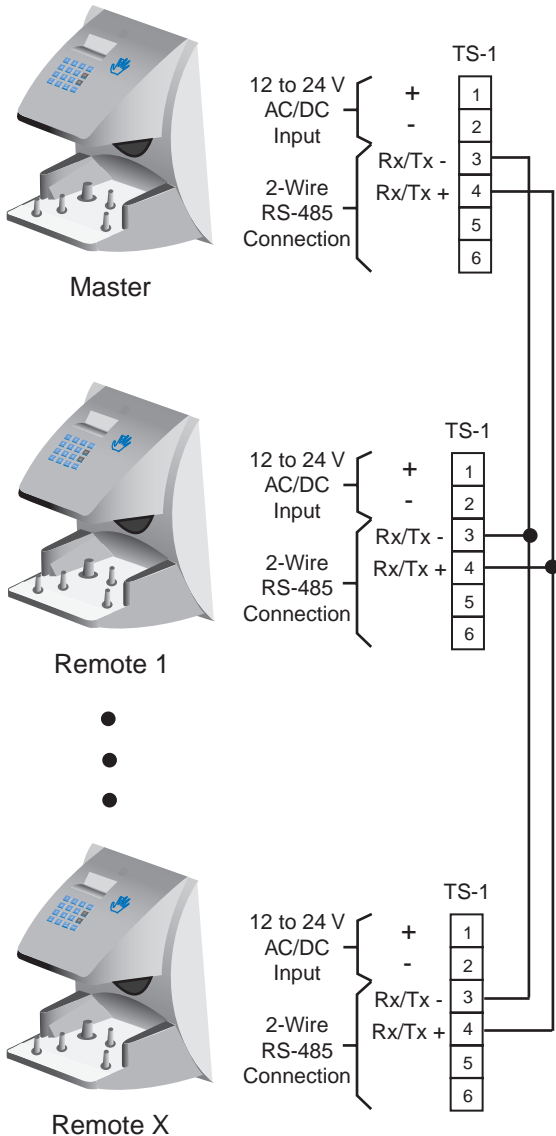


Figure 19-13: RS-485 2-Wire Master/Remote Network System Wiring Diagram

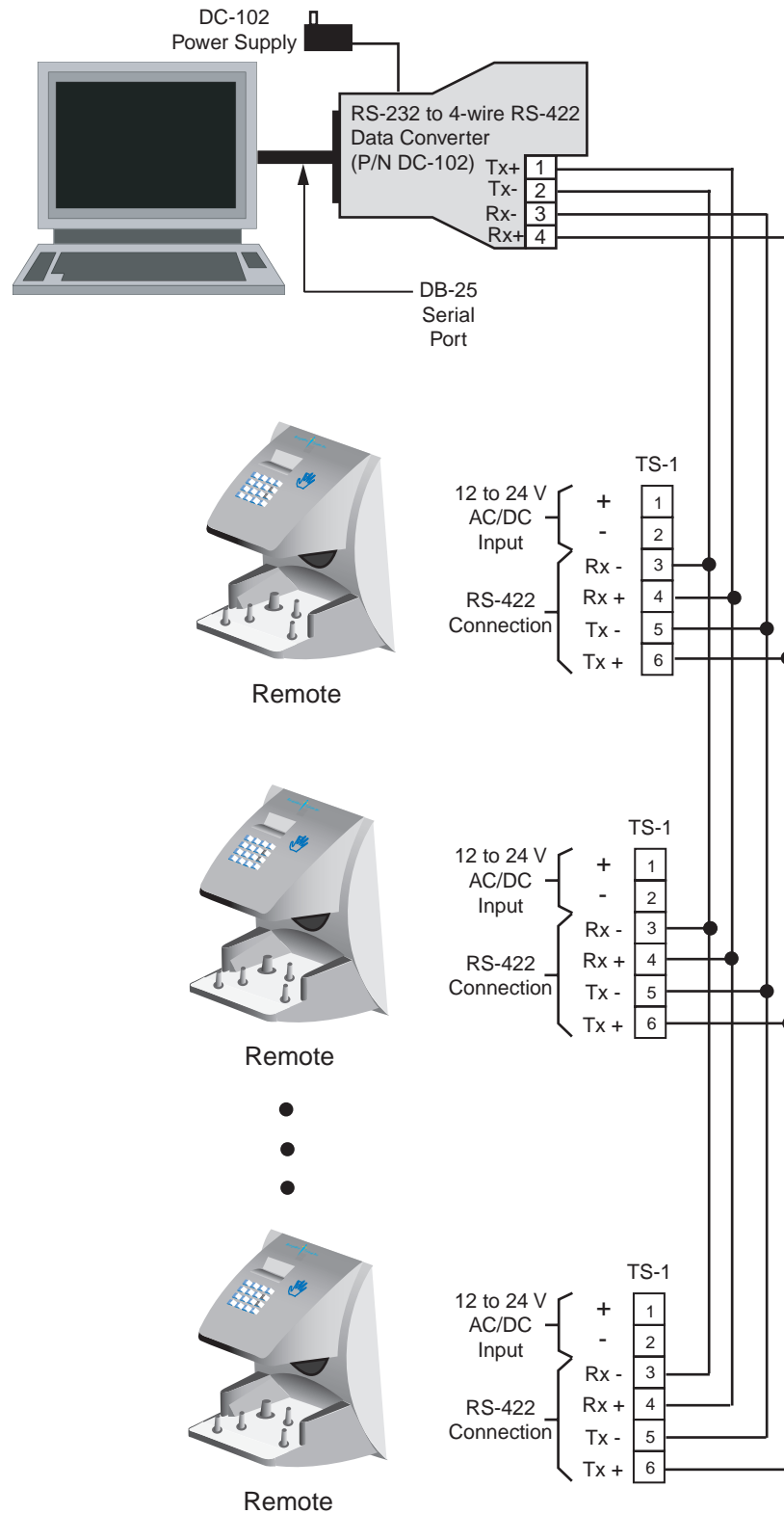
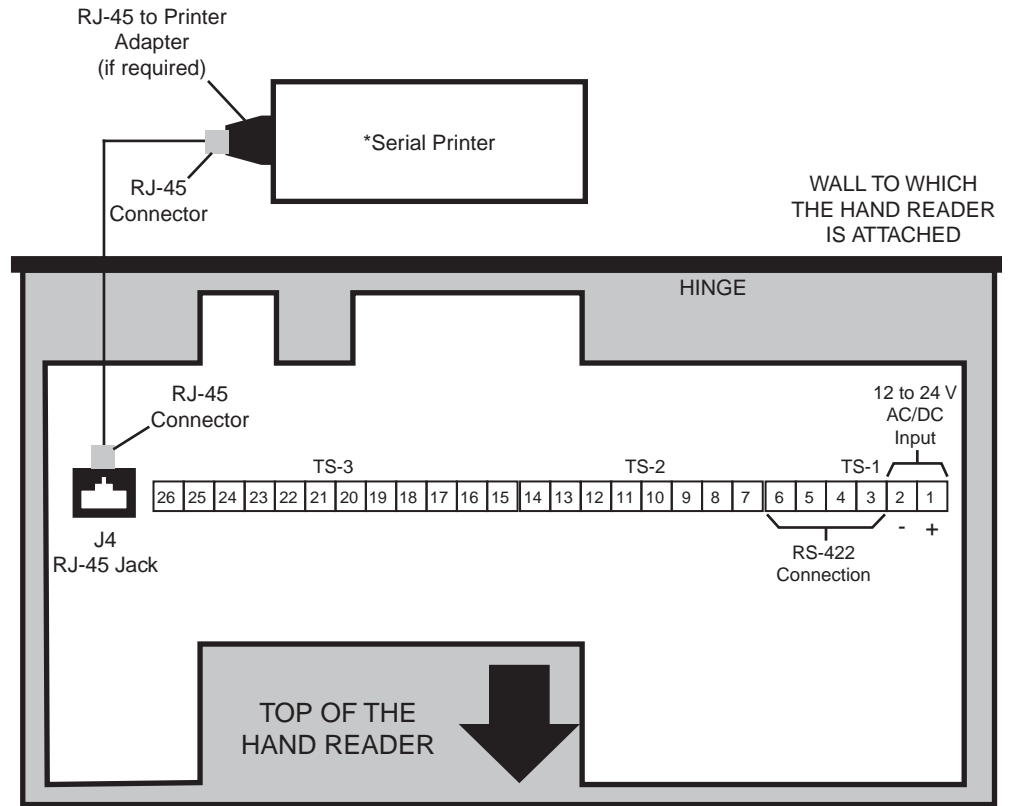


Figure 19-14: Host PC Network System Wiring Diagram



* These components are not supplied by Schlage Biometrics, Inc.

Figure 19-15: Printer to HandKey II Wiring Diagram

Setting the DIP Switches

DIP Switch settings perform three tasks for the Hand Reader (see Figure 17-11).

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 17-2 on page 66 for the location of all DIP switches described in this section.

!NOTE *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.*

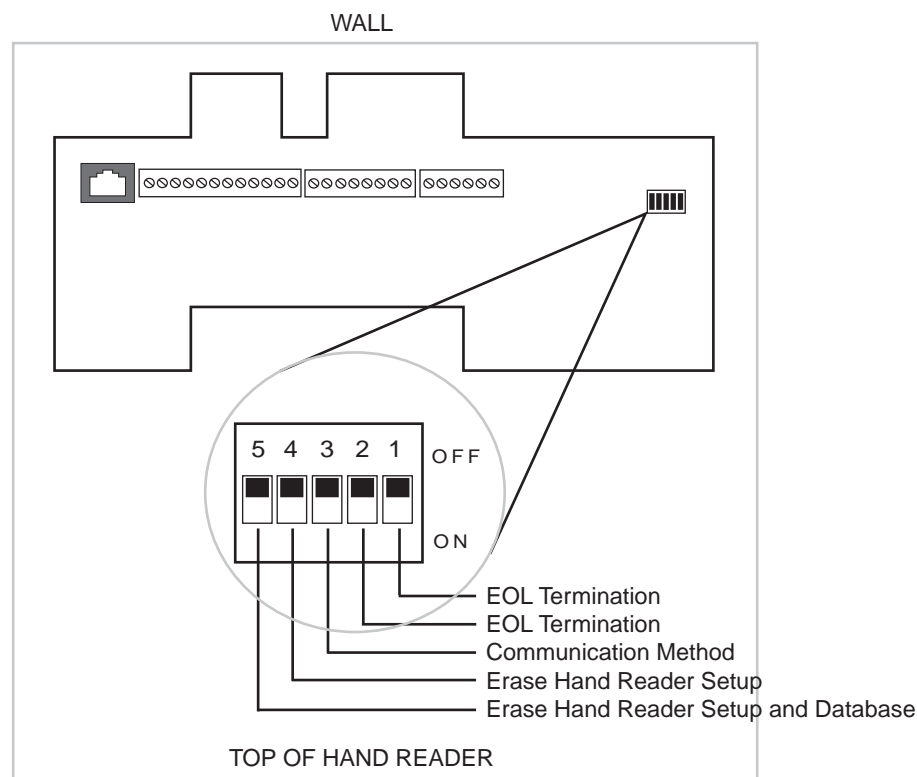


Figure 19-16: Hand Reader Dip Switches

End of Line Termination

The factory default setting is for EOL termination to be disabled – switches 1 and 2 OFF. Refer to Figure 17-11 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, the last Remote reader in the daisy-chain must have EOL termination turned ON.
- In an Ethernet / host PC network the EOLs must be turned OFF.

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 17-11 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. Schlage Biometrics does not recommend two-wire RS-485 cabling for new network installations.*

Erasing HandReader 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.

Erasing the HandReader 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.

Erasing the HandReader 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.*

Closing the HandReader

Before closing the Hand Reader, ensure dip switches 4 and 5 are OFF (refer to Figure 17-11). 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 17-12).

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

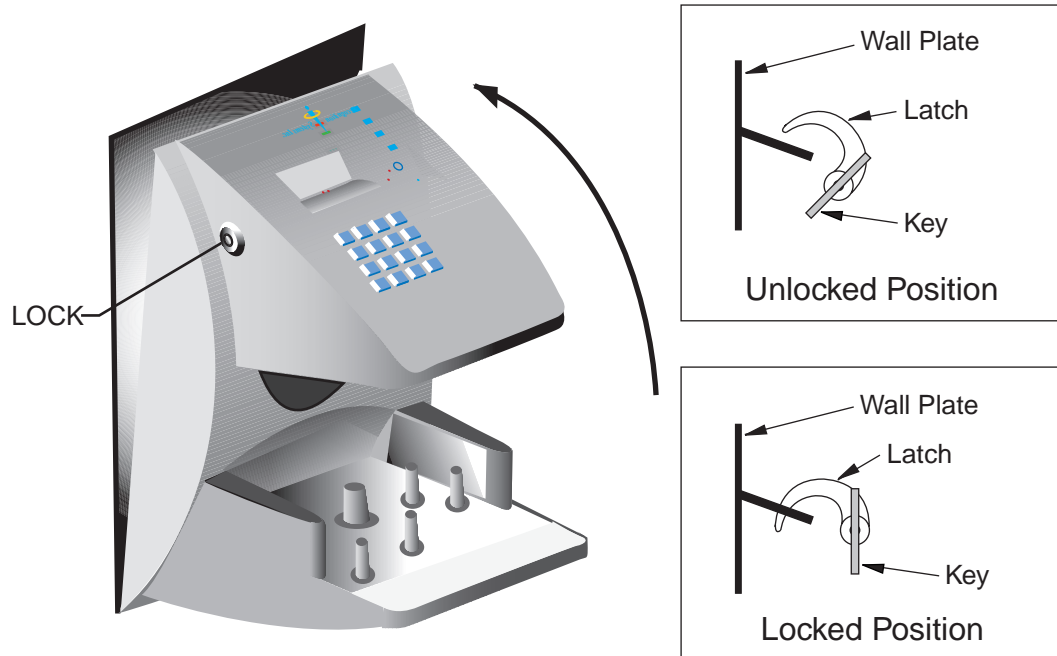


Figure 19-4: Closing the Hand Reader

Appendix D: Troubleshooting Guide

Display Messages During Verification

Various messages can appear on the HandPunch's display during hand verification. These messages are defined in.

Table 20-17: Display Messages During Verification

Message	Definition
PLACE HAND	The platen is ready to receive your hand for verification.
ID VERIFIED	You are verified, proceed.
REMOVE HAND	Remove your hand and place it on the platen again. Follow proper hand placement rules.
TRY AGAIN	Your attempt was rejected. Repeat verification following proper hand placement rules.
ID REFUSED	Your rejections exceeded the maximum number of tries allowed. Wait until another employee has verified and try again or call your supervisor.
ENTER ID	You entered your ID number incorrectly or your access time is restricted.

- If the display shows TRY AGAIN, you are not verified. You may have made an error in entering your ID number or in placing your hand on the platen. Re-enter your ID number and try again, taking care to follow proper hand placement rules (see page 50).
- If the display shows TIME RESTRICTION, you are not authorized to punch in at this time. If this seems to be in error, contact your supervisor about time restrictions.
- After a pre-programmed number of denied attempts, an ID number will no longer be accepted and the display will appear as follows.
- This is called a "lockout." Before the rejected ID number can be used again, another employee or a supervisor must successfully verify at the HandPunch.
- If you enter your ID number, but do not place your hand on the platen, the HandPunch will time-out in about 25 seconds. You can immediately end this time-out by pressing the key.

Beeper and LED Status During Verification

The HandPunch's beeper and LED status display also display hand verification information. This information is defined in.

Table 20-18: Beeper and LED Status During Verification

Operation	Beeps	LED	Meaning
During Keypad Entry	1 per Keystroke	–	Keystroke Accepted
After ID Entry	–	–	OK - Proceed
After ID Entry	2	–	ID Number Not in Database
After Hand Placement	1	Green	ID Verified
After Hand Placement	2	Red	ID Not Verified - Try Again
After Hand Placement	1 Long		
Continuous	Red	ID Refused	

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.

Limited Warranty

Schlage Biometrics, 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:

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

The Product has not been abused, misused, or improperly maintained and/or repaired during such period; and

Such defect has not been caused by ordinary wear and tear; and

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

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.

Schlage Biometrics 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.