

SecureLINX Wireless

Wiegand Access Control Interface Product

Operations Manual



August 2011

www.AscendanceWireless.com



1 August 2011

© 2011 Ascendance Wireless, LLC

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and does not represent a commitment on the part of Ascendance Wireless, LLC

Ascendance Wireless, LLC shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.

Ver: 1.0

Table of Contents

Overview:	4
Contact Information:.....	4
Typical SecureLINX Wiegand Central Unit Wiring Diagram (Head End)	5
Typical SecureLINX Wiegand Remote Unit Wiring Diagram (Reader End)	6
External connections and DIP Switch Settings.....	7
Quick Reference For Typical Connections.....	8
Central Unit.....	8
Remote Unit.....	8
Setup and Pre-installation.....	9
Note:	9
Features:	9
Electrical Specifications:.....	Error! Bookmark not defined.
Environmental Specifications:	Error! Bookmark not defined.
Indicators and Operating Modes	10
LED Diagnostic Indicator:	10
DIAGNOSTIC LED NOT ILLUMINATED:.....	10
CENTRAL UNIT FLASHING BETWEEN RED/GREEN:	10
REMOTE UNIT ILLUMINATED RED:	10
REMOTE AND CENTRAL UNITS FLASHING BETWEEN RED/GREEN:	10
Operating Modes:	10
Bench Testing:.....	11
Network Addressing:.....	11
Changing the IP Address	12
Changing the Net mask	12
Door Strike and LED I/O Wiring Example.....	18
Door Strike and LED I/O	19
Relay 1 Controls	20
Relay 2 Controls	21
Relay 3 Controls	22
Relay 4 Controls	23
Expansion Modules.....	24
Using the Expansion Modules.....	25
Setup Process:.....	25
Operation with Expansion Modules:	25
Central Unit Configuration Mode Settings.....	25
Expansion Module - Panel “Central” Interface	26
Expansion Module Reader/Door “Remote” interface	27

Overview:

The SecureLINX Wireless Wiegand Access Control system is designed to connect Access Control Card Readers, Door Locks, Gates and other remote devices which support the Wiegand protocol to a Panel or other Host computer at another location when it is not feasible to run cable.

This is accomplished by connecting the Card Reader or other remote device to the SecureLINX Remote unit. The SecureLINX Remote unit is then connected to a SecureLINX Wireless Access Point/Client device where it is converted from a proprietary Wiegand data stream to a TCP/IP packet delivery protocol. It is then transmitted wirelessly to the intended destination. At that destination the SecureLINX Wireless Access Point/Client is connected to the SecureLINX Central unit. The data is then converted back to the proprietary Wiegand protocol and connected to the Panel or Host computer.

The SecureLINX Wiegand Access Control system must connect to a SL-IAP-X-2E, SL-IAP-X-5E (Integrated Access Point) or SL-WPLT-X-2E, SL-WPLT-X-5E (Wireless Platform) SecureLINX Wireless Access Point/Client system with an available Ethernet PoE Switch port.

Contact Ascendance Wireless for pre-sale configuration questions to ensure the correct components are incorporated into the design.

Contact Information:

Ascendance Wireless, LLC

www.ascendancewireless.com

International +1 (530) 887-8300
US/Canada (888) 415-9633

sales@ascendancewireless.com

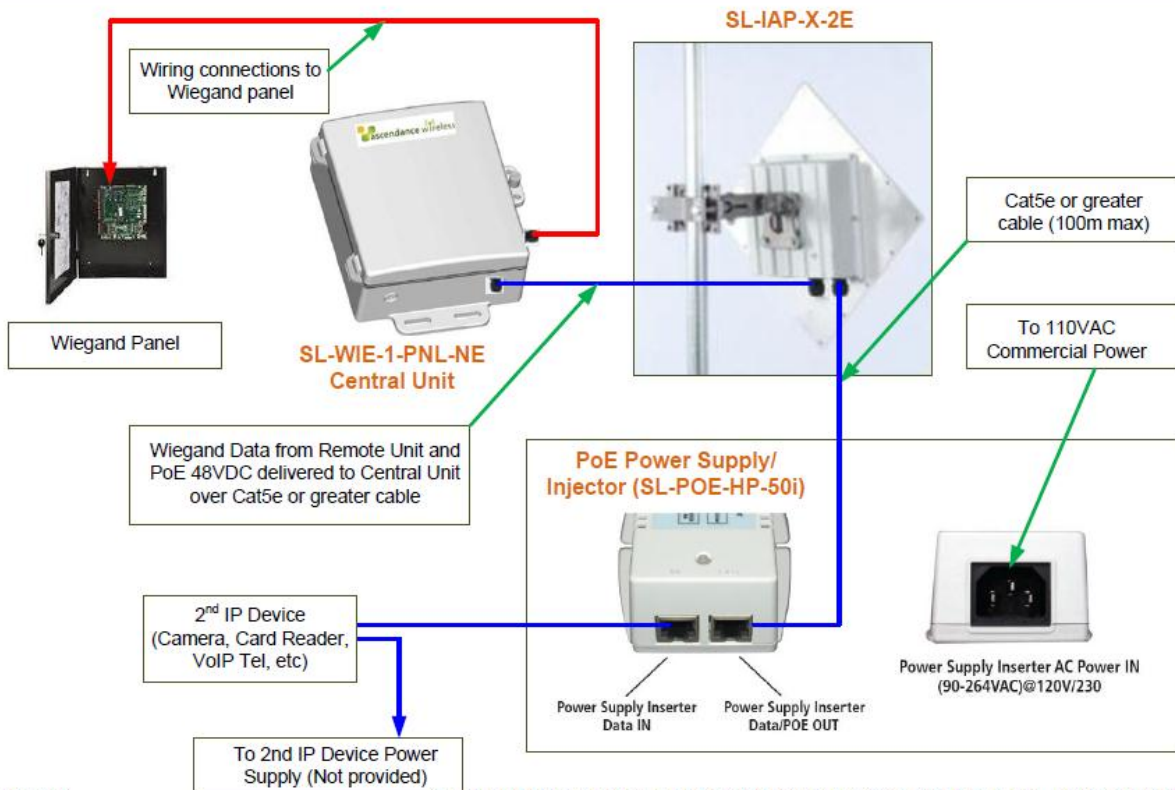
support@ascendancewireless.com

Typical SecureLINX Wiegand Central Unit Wiring Diagram (Head End)

The following drawing shows connection to a SL-IAP-X-2E (2 Port Ethernet system). If you are connecting to a SL-IAP-X-5E, SL-WPLT-X-2E or SL-WPLT-X-5E system, your system will look different, however the concept is the same. You will want to connect to an available PoE Ethernet port.



SecureLINX Wiring Diagram
Typical Wiegand Central Unit (2 Ethernet)
Integrated Access Point (IAP)

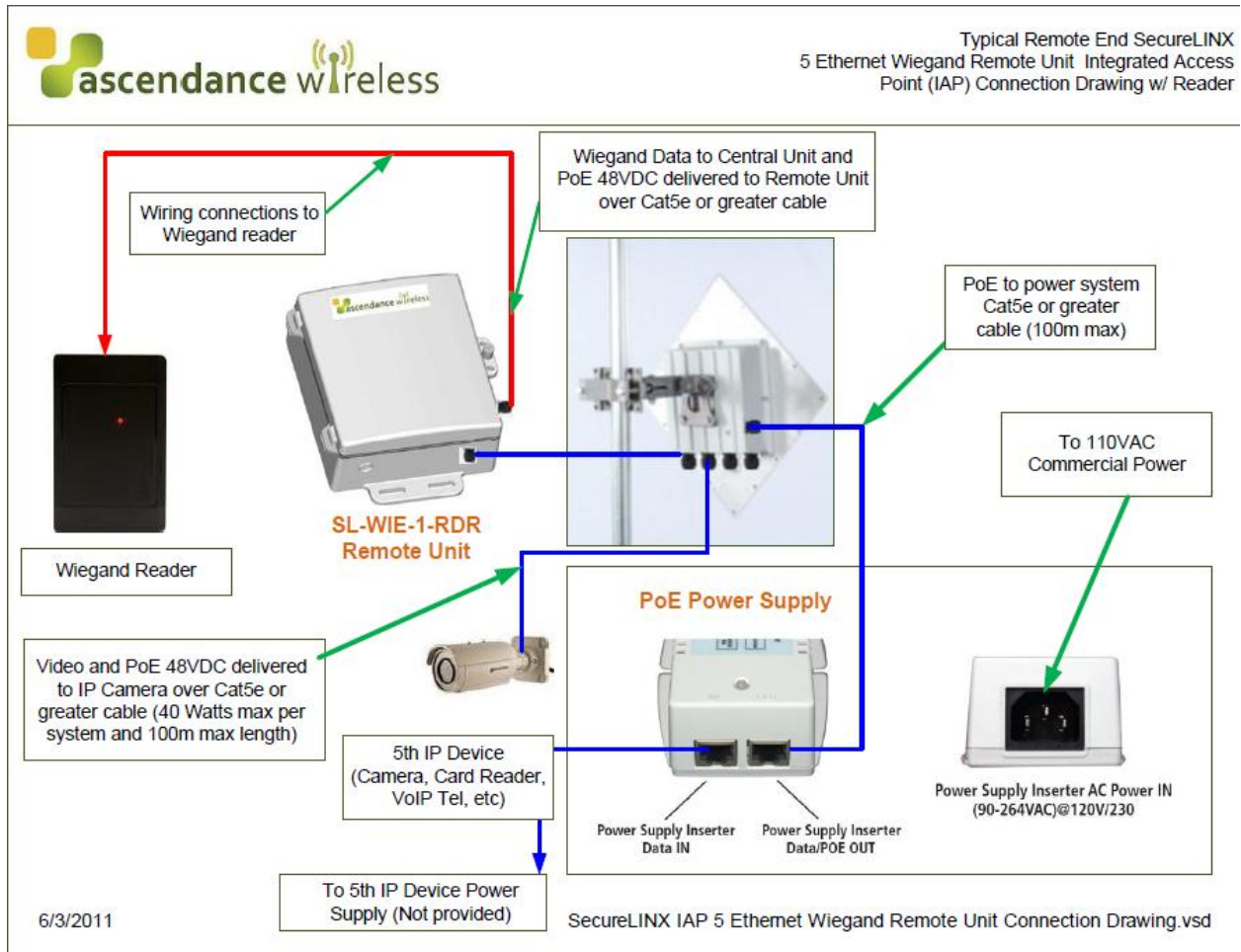


6/3/2011

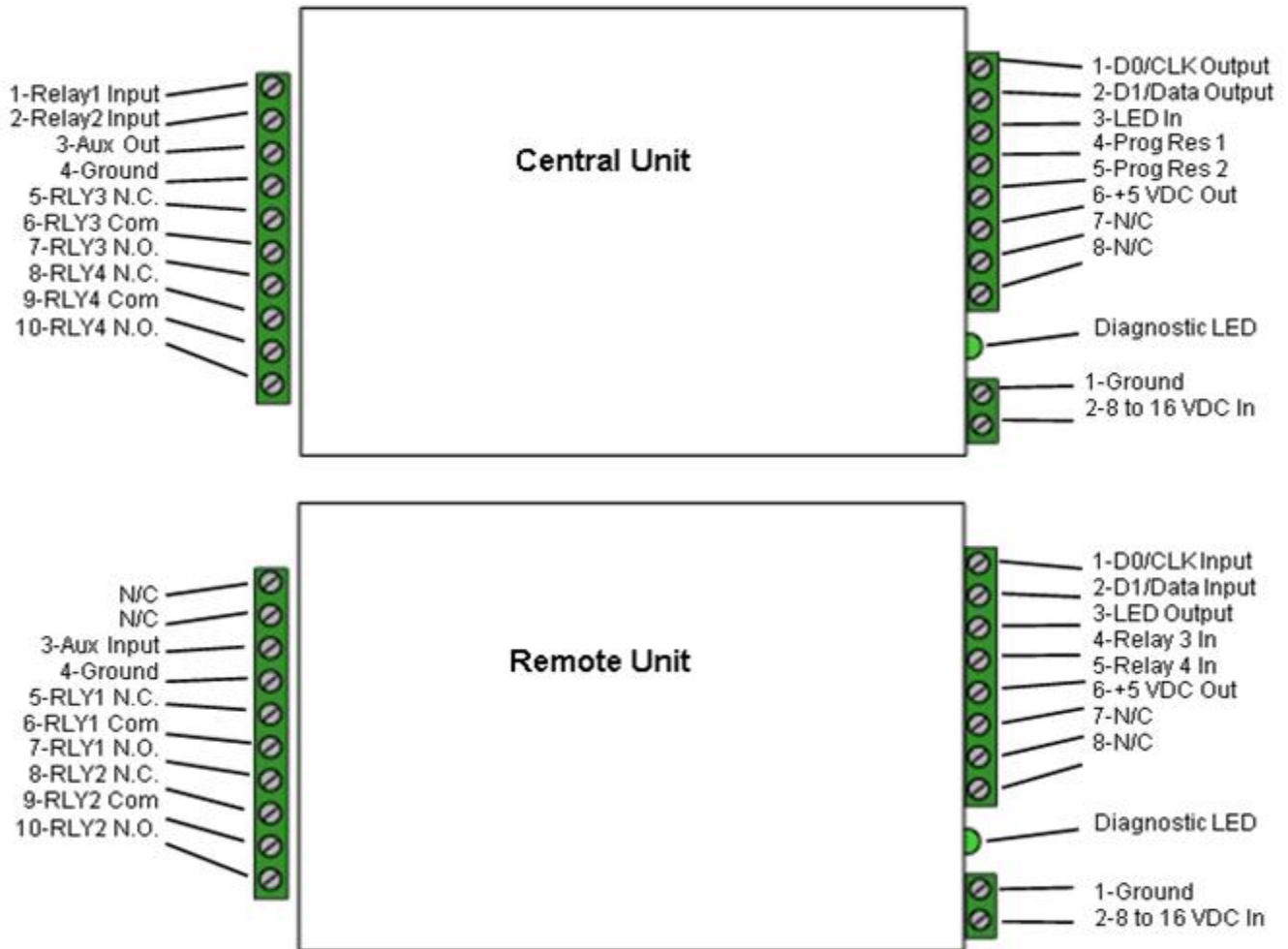
SecureLINX IAP 2 Ethernet Wiegand Central Unit Connection Drawing - Head End.vsd

Typical SecureLINX Wiegand Remote Unit Wiring Diagram (Reader End)

The following drawing shows connection to a SL-IAP-X-5E (5 Port Ethernet system). If you are connecting to a SL-IAP-X-2E, SL-WPLT-X-2E or SL-WPLT-X-5E system, your system will look different, however the concept is the same. You will want to connect to an available PoE Ethernet port.



External connections and DIP Switch Settings



Central Unit Settings

Remote Unit Settings

DIP Switch #1 ON
-Service Mode
DIP Switch #1 OFF
-Run Mode

Dip switch #4 is ON
-Disable Pullup resistors

Dip switch #4 is OFF
-Enable Pullup resistors

	Switch			
	6	7	8	
Wiegand 0				
Wiegand / No Filter 1			x	x = ON
Strobed Rising Edge (MR-5) 2	x			
Strobed Rising Edge (Dorad0 644) 3	x	x		
Strobed Rising (Mag-Tek) 4	x			
Strobed Falling Edge 5	x		x	
Reserved 6	x	x		
F2F 7	x	x	x	

DIP Switch #1 ON
-Service Mode
DIP Switch #1 OFF
-Run Mode

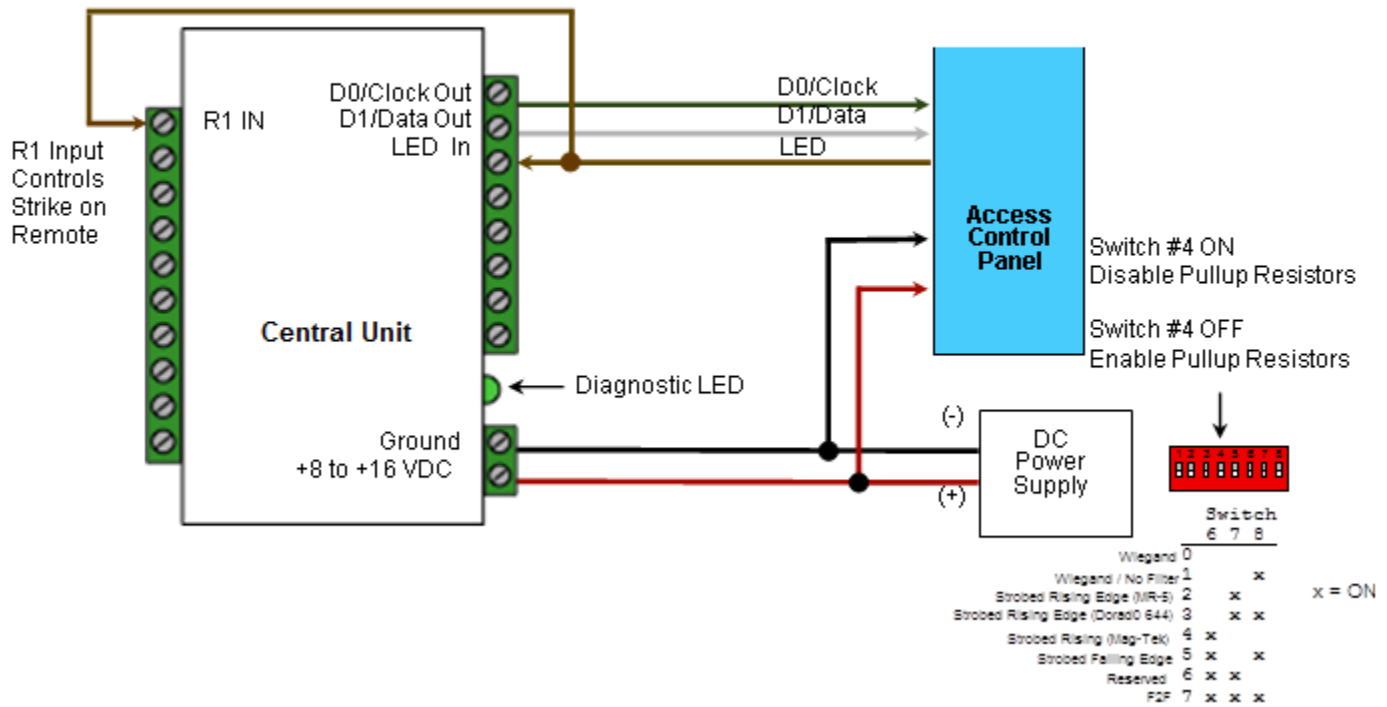
Dip switch #4 is ON
-Enable Pullup resistors

Dip switch #4 is OFF
-Disable Pullup resistors

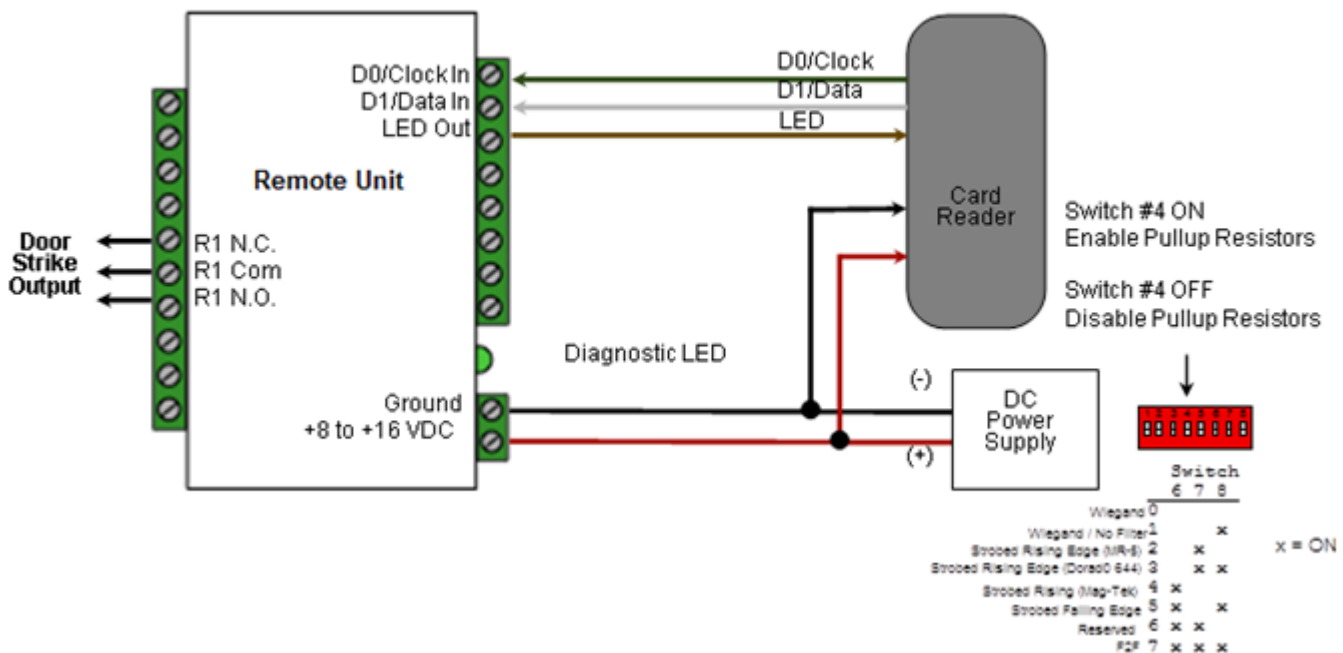
	Switch			
	6	7	8	
Wiegand 0				
Wiegand / No Filter 1			x	x = ON
Strobed Rising Edge (MR-5) 2	x			
Strobed Rising Edge (Dorad0 644) 3	x	x		
Strobed Rising (Mag-Tek) 4	x			
Strobed Falling Edge 5	x		x	
Reserved 6	x	x		
F2F 7	x	x	x	

Quick Reference for Typical Connections

Central Unit



Remote Unit



Setup and Pre-installation

This manual covers the operation and setup of the SecureLINX Wiegand series Central and Remote units.

Most products in the series will have the same operational functions and electrical connections.

Note:

In most cases, your units have been pre-installed and configured at the factory. It is recommended you familiarize yourself with this manual to understand the operation of the systems.

Features:

- Includes complete solution for Remote Unit (Reader/Gate/Door) and Central Unit (Panel) interface.
- Service mode for setup and configuration of Expansion modules.
- Field configurable reader formats
- Multifunction indicator for determining operational status of the unit
- Auxiliary I/O connections available for Door/Gate/Panel status signaling.
- Multiplexing of RF Bridge providing for additional door/gate on a single RF link.
- Economical expansion capabilities using SecureLINX technology

Electrical and Mechanical Specifications

Physical:	7" x 6" x 2" Hinged Die Cast Aluminum Enclosure with 7 Engineered knockouts. NEMA 6 Rated with pole mount bracket	
Temp:	Storage(-55°C to + 150°C) Operating(-40°C to +80°C)	
Humidity:	95% (non-condensing)	
Power:	Input	Unregulated Input 8 to 16 VDC* @ 500mA Max
	Output	+5VDC @100mA
Data I/O:	Interface	Reader -Wiegand, Strobed (Clock & Data), F/2F LED - 0 - 30V
Relays:	Max Switching	220VDC 30W (Resistive) 1A)
		250VAC 37.5VA 1A)
	Running Spec with load	30VDC 1A (Resistive), 1 x 10 ⁵ operations at 20° C
		125Vac .3A (Resistive), 1 x 10 ⁵ operations at 20° C

Indicators and Operating Modes

LED Diagnostic Indicator:

The LED Diagnostic indicator provides information on the operational status of the unit. If the units are not communicating, viewing the diagnostic indicator LED's may help to determine the nature of the problem.

When the SecureLINX units are operating correctly and have a valid communication channel between the Remote and Central units, the Diagnostic indicators on each unit will flash green rapidly (2-3 flashes per second) in Service / Config mode and illuminate a steady green in quiet mode.

DIAGNOSTIC LED NOT ILLUMINATED:

If the LED(s) are not illuminated on the unit(s) then the unit is not getting power or there is an electrical problem. The Diagnostic LED's will be illuminated Red/Green or flashing whenever power is applied.

CENTRAL UNIT FLASHING BETWEEN RED/GREEN:

With power applied and no communication path between the Remote and Central, the Central unit will flash the diagnostic indicator alternately between Red and Green.

REMOTE UNIT ILLUMINATED RED:

The Remote unit diagnostic LED will illuminate solid (not flashing) red if it is not receiving communication from the Central unit.

REMOTE AND CENTRAL UNITS FLASHING BETWEEN RED/GREEN:

The Central unit is not receiving communication from the Remote.

Operating Modes:

By setting DIP switch 1 to the ON position, the unit is placed in Setup / Config mode. When the switch position is changed, cycle the power to the unit to make the switch change take effect.

In "**Quiet**" mode (DIP switch #1 OFF) the units will remain quiet unless there is a status change, and will slowly poll each other about every 10 to 15 seconds to check the link integrity.

The **Setup / Config mode** places the units in a rapid polling sequence to allow troubleshooting and setup of the communication link.

The SecureLINX units use a quiet protocol when operating in Quiet mode. Communication between the Central and Remote unit only occurs when an event requires data transmission or contact needs to be made to maintain supervision. The RF channel remains quiet most of the time.

During setup or troubleshooting it may be necessary to observe the communication link between the Central and Remote units. The rapid polling used in the Setup / Config mode can help indicate whether the units can "See" each other. Additionally the Central unit Diagnostic LED will indicate Red when communication is lost.

Bench Testing:

Before installing the units in the field they should be tested at a convenient “Bench top” location. This will make it easier to verify / change settings and check operation when both units are visible at the same time.

It is also a chance to become familiar with the system if this is the first time using the SecureLINX system. It is much more difficult to setup and test the units when they are several thousand feet apart.

1. Connect the Remote and Central unit Network ports together using either a crossover cable or connect both to a common network hub.
2. Connect a suitable power supply to both units. Each unit should be provided with 8 - 16 volts DC and a minimum of 500mA.
3. Apply power. After about a 5 - 10 second delay, both units Diagnostic LED should indicate Green.
5. Touch a jumper wire from the Ground connection on Relay 1 input on the Central unit. Relay #1 on the Remote unit should activate with an audible click and the Diagnostic LEDs should flash green on both the Central and Remote units.
6. Units are shipped from the factory set for the Wiegand data format. If a different format is required set the DIP switch to the required reader and panel format.
7. If a reader and panel is accessible, connect the reader to the Remote unit and the Central unit to the panel and verify that card reads are being accepted by the access control system. If any troubleshooting is necessary, it will be easier to do with both units in close proximity to each other.
8. Once these steps are completed, the units are ready for installation at their permanent locations and final commissioning as a system.

Network Addressing:

Each SecureLINX pair is preconfigured with a factory default TCP/IP address:

SecureLINX Central unit = 192.168.49.58

SecureLINX Remote unit = 192.168.49.59

It may be necessary to change these settings to be compatible with the network that will be used in the final installation. The system requires the use of fixed IP addresses to be assigned to the units. It may be necessary to coordinate with the System Administrator before placing the devices on a network.

The Lantronix Xport Direct Device Installer program can be used to administer the units. The program can be downloaded from www.lantronix.com under support/downloads/Xport Direct/ Device Installer.

This manual will describe how to change the IP address and net mask for the units using the Xport Device Installer software. Once the Addresses have been set to be compatible with the network, final installation can be made.

Changing the IP Address

In many cases it may be necessary to change the addressing to be compatible with an existing network. The address of the Central and Remote both need to be changed using the following procedure.

It will be necessary to set the host computer to the same subnet as the SecureLINX units during this procedure.

1. Install the Lantronix "Xport Device Installer" software (Available at the Lantronix web site (www.lantronix.com)).
2. Connect the device(s) to a host computer using the crossover cable or using a Hub and straight through cables.
3. Apply power to the device(s) being configured.
4. Start the software and follow the procedures indicated in the following pages "Setting IP Address ".

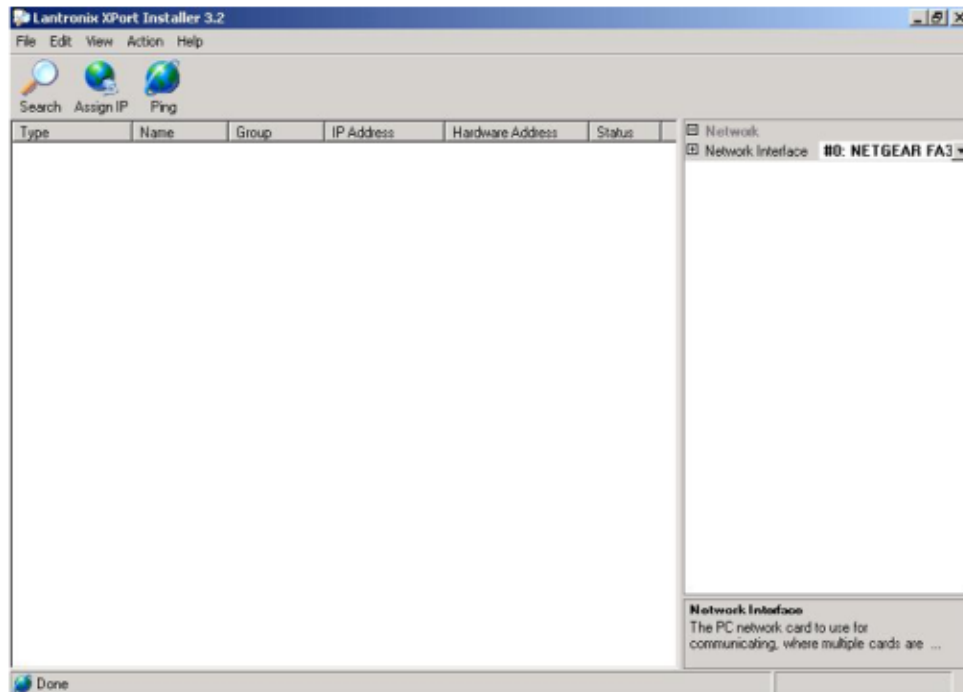
The Net mask comes set from the factory at: 255.255.255.0

The Net mask setting can be changed using the Xport Device Installer if necessary.

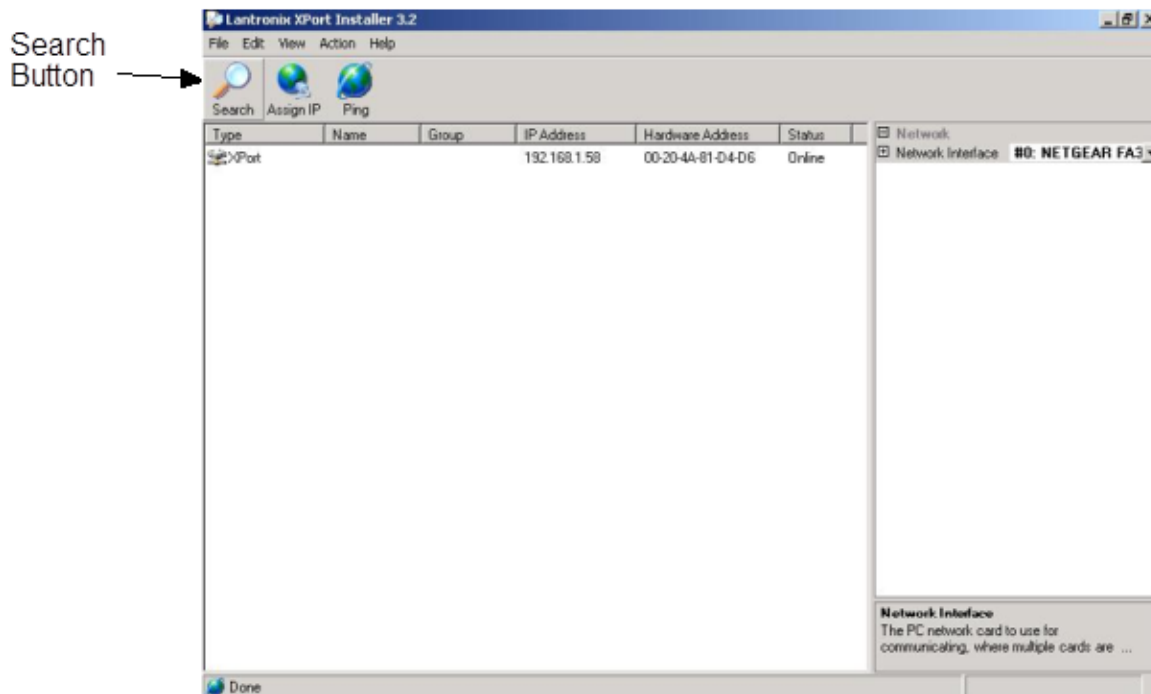
Changing the Net mask

It will be necessary for the Host Computer to be on the same subnet as the device(s) being configured for this procedure.

1. Start the software and display the Search screen.
2. Select the device from the list.
3. Click on the Telnet button.
4. A Click OK when the Telnet connection window opens.
5. A text based interface should be displayed.
6. Select 0. Server configuration. This selection will allow setting IP Address and Net mask.
Setting the IP Address



1. Start the Lantronix XPort Installer software. The startup screen is shown above.



2. Click the “Search” button, after a brief delay, the connected device(s) should appear in the device list as shown above.

Note: If the unit does not appear in the device list, check power and network connections. You will not be able to proceed if you are unable to see the unit to be configured in the device list.



3. Select the device to be configured with a mouse click. The device will highlight in blue as shown above when selected. Verify which device is to be configured by the MAC address. The MAC address is printed on the Xport module. i.e. make sure you are configuring the correct Central unit or Remote unit.

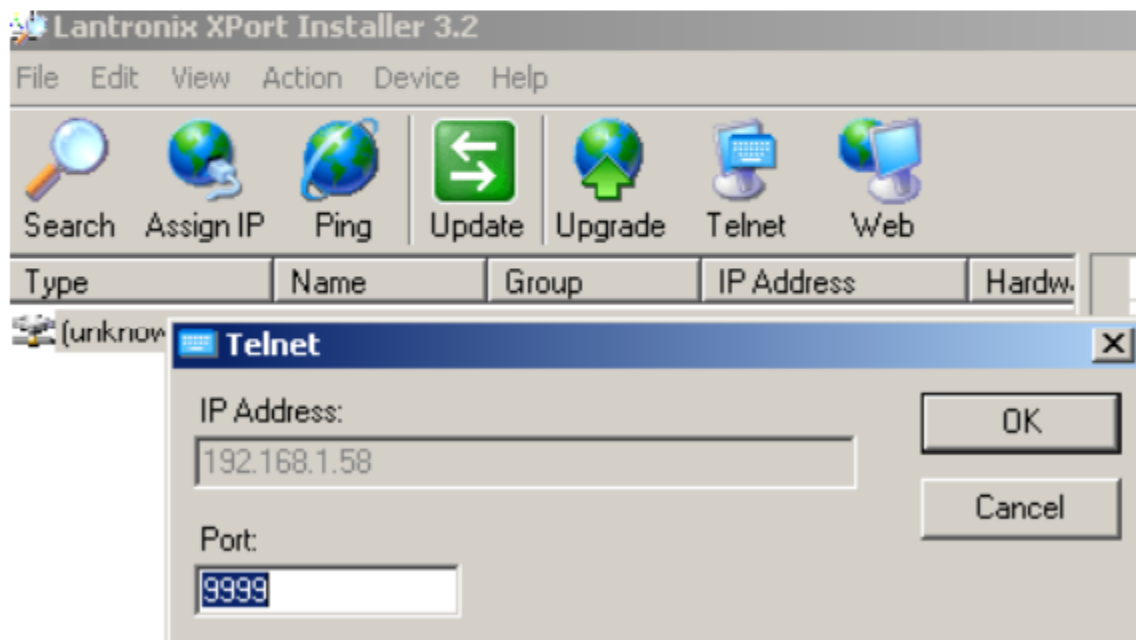


4. Click on the "Select IP" button. The dialog box shown above will open. Enter an IP address for the unit. The IP address should be unique and on the same subnet as the host computer. Click on the "OK" button after the IP address has been entered. There will be a delay while the unit reboots. After reboot the unit should reappear in the device list.

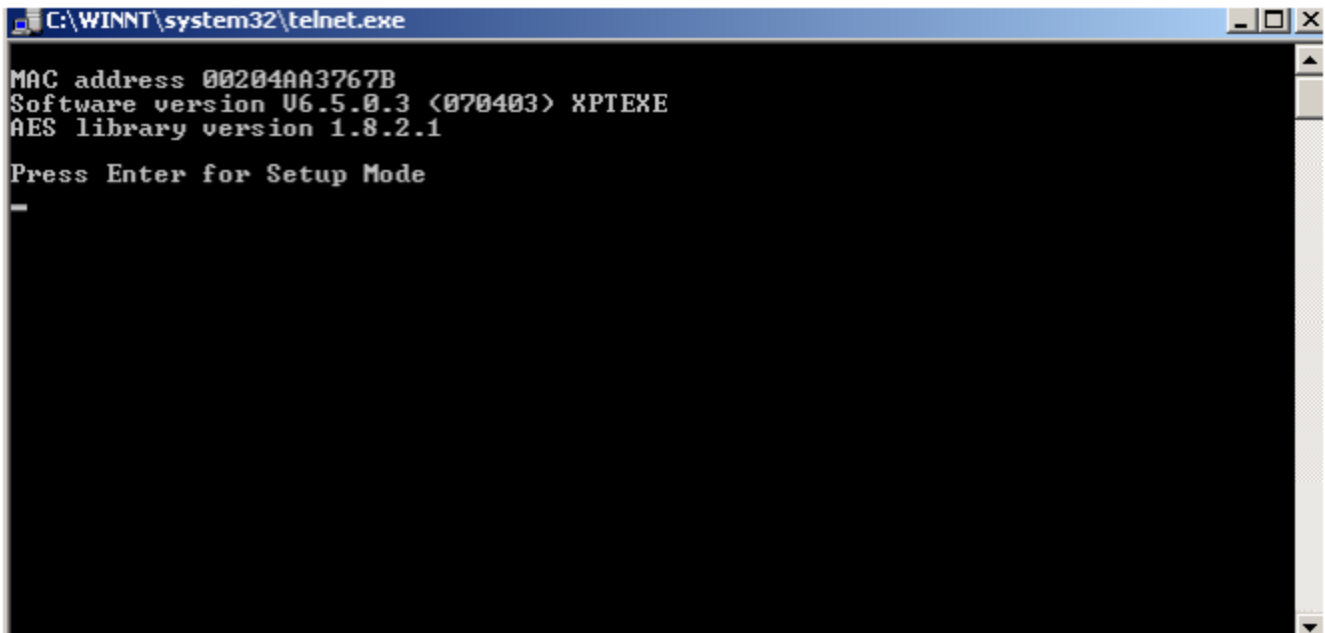
Once both units have had their IP addresses set, it will be necessary to tell the CENTRAL unit the address of the Remote unit.



5. After the IP addresses have been assigned to both units, select the CENTRAL unit in the device list.

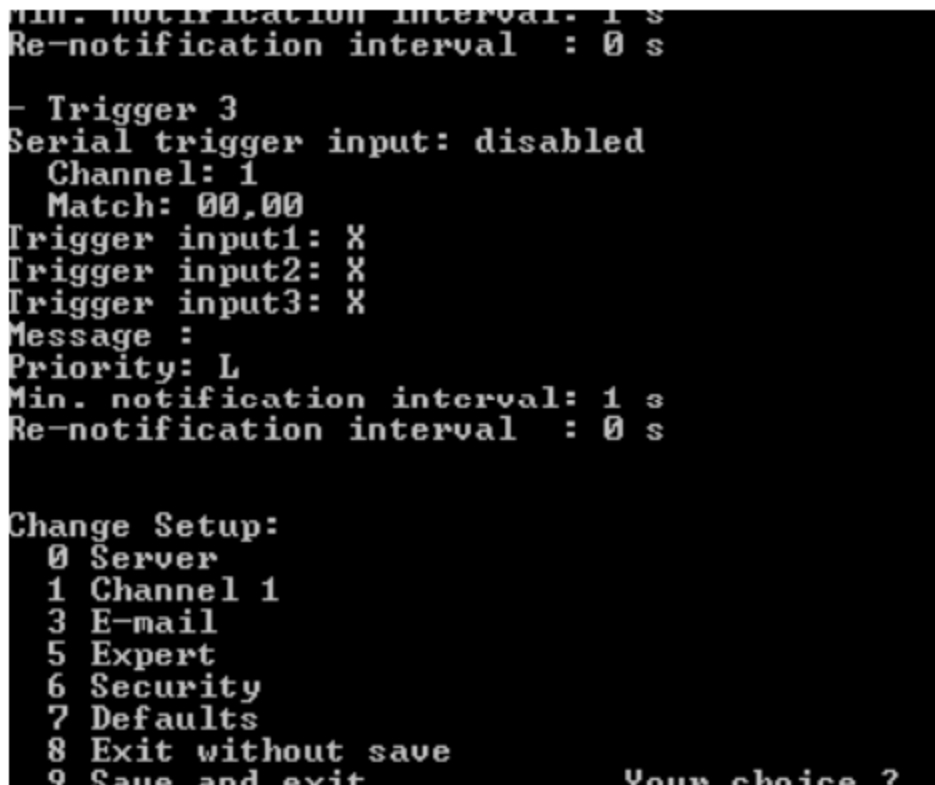


6: Select the Telnet option and click "OK"



```
C:\WINNT\system32\telnet.exe
MAC address 00204AA3767B
Software version U6.5.0.3 (070403) XPTXEXE
AES library version 1.8.2.1
Press Enter for Setup Mode
-
```

7. You should now have an open window like this. Press the ENTER key to enter setup mode.



```
Min. notification interval: 1 s
Re-notification interval : 0 s

- Trigger 3
Serial trigger input: disabled
  Channel: 1
  Match: 00,00
Trigger input1: X
Trigger input2: X
Trigger input3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval : 0 s

Change Setup:
 0 Server
 1 Channel 1
 3 E-mail
 5 Expert
 6 Security
 7 Defaults
 8 Exit without save
 9 Save and exit          Your choice ?
```

8. A list of options will be presented, select Option #1 (Channel 1).

```

Change Setup:
 0 Server
 1 Channel 1
 3 E-mail
 5 Expert
 6 Security
 7 Defaults
 8 Exit without save
 9 Save and exit          Your choice ? 1

Baudrate <9600> ?
I/F Mode <4C> ?
Flow <00> ?
Port No <10001> ?
ConnectMode <C1> ?
Send '+++ ' in Modem Mode <Y> ?
Show IP addr after 'RING' <Y> ?
Auto increment source port <N> ?
Remote IP Address : <000> 192.<000> 168.<000> 1.<000> 59

```

9. All of the parameters will have been set as factory default, it will be necessary to set the address of the REMOTE unit in the Channel 1 parameters. In the example above, the parameters for the factory default settings have been entered. Keep in mind that this is the CENTRAL unit and we are entering the address of the REMOTE unit.

```

Change Setup:
 0 Server
 1 Channel 1
 3 E-mail
 5 Expert
 6 Security
 7 Defaults
 8 Exit without save
 9 Save and exit          Your choice ?

```

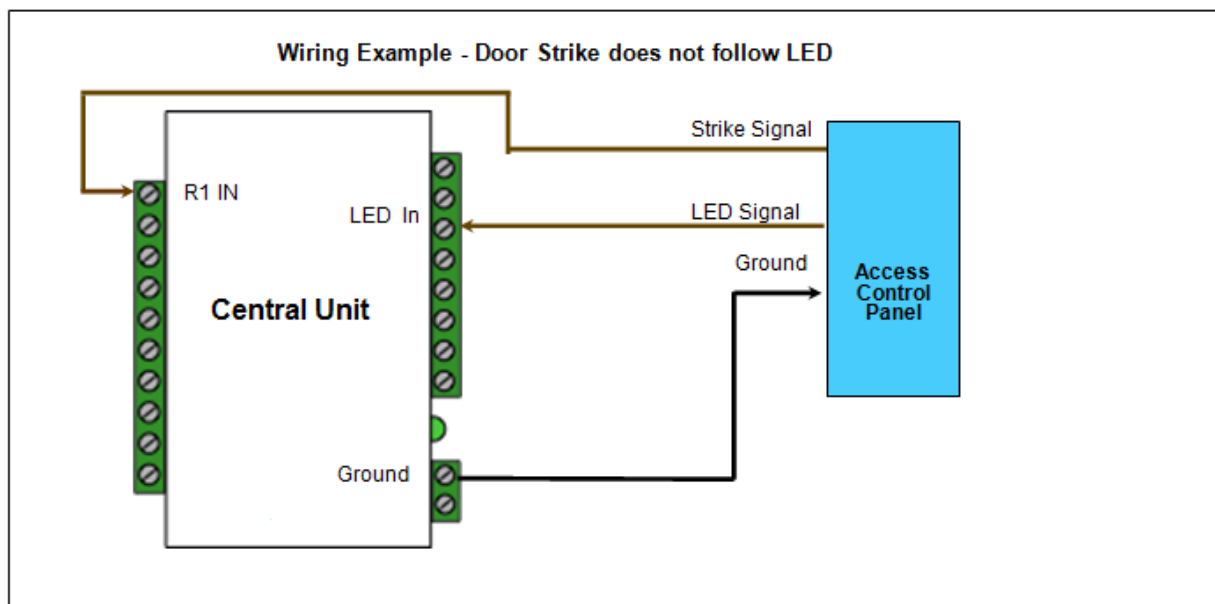
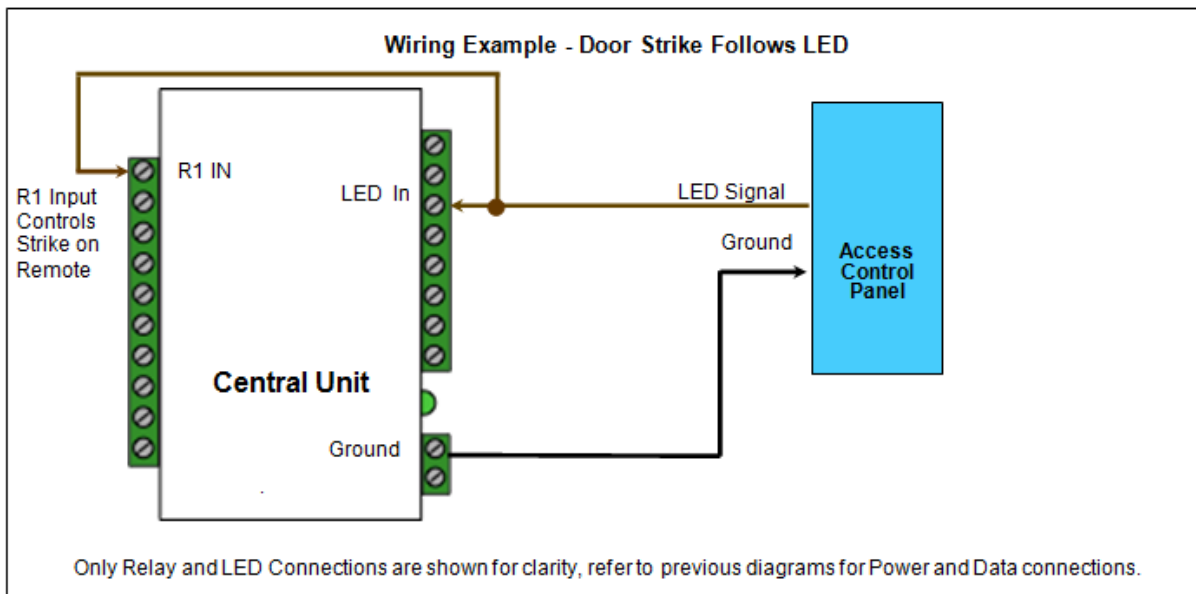
10. When the address has been entered, click through any remaining parameters without altering them and the menu should return to the setup options.

11. Select option 9 (Save and exit) and press enter. The settings will be written to memory and the Duprex units are now configured to operate in the new network environment.

Door Strike and LED I/O Wiring Example

To activate the relay on the Remote unit, connect as shown below. These connections can be used to allow the Remote relay to operate a DOOR STRIKE, GATE, or other locking hardware. Refer to following pages in this document for details of each I/O operation and connection.

There are two relays available for accessory outputs at the Remote end. Either relay can be used to provide the Door Strike or Gate activation function. This example uses Relay 1.

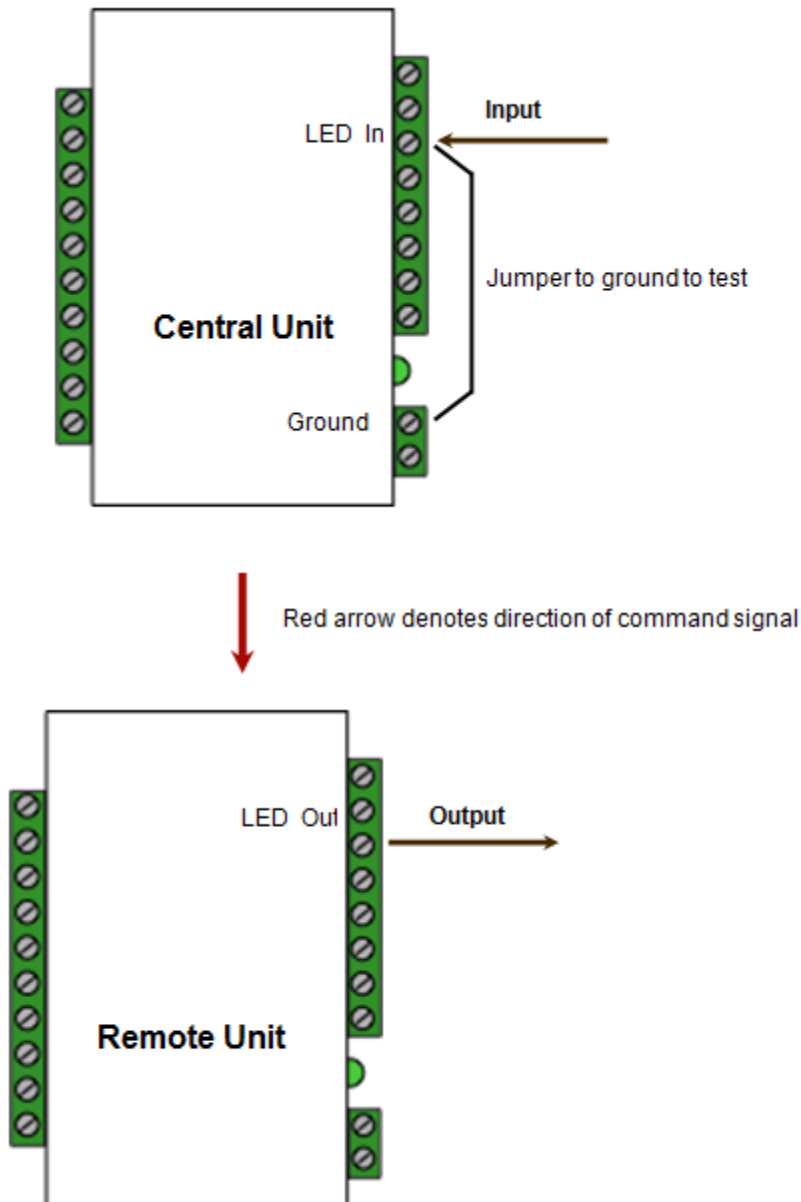


Door Strike and LED I/O

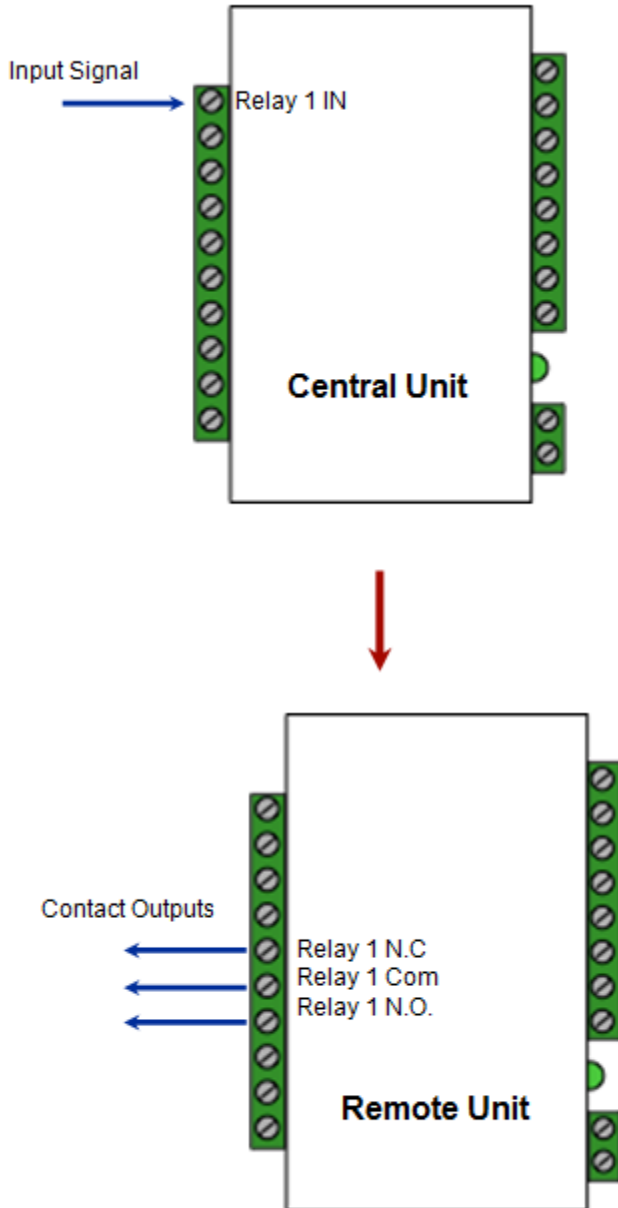
The SecureLINX Wiegand Series provides additional data channels to support access control hardware such as door strikes, tamper alarms, request to exit status, etc. These signals are sent to and from the Remote and Central units without the need to run additional wiring.

The accessory control I/O uses active low inputs. When the inputs are floating (nothing connected) the associated output will be set to a high level. When the input is set to 0 Volts (Ground) the input will activate its associated output. All Accessory outputs are Open Collector type and will switch to Ground when activated.

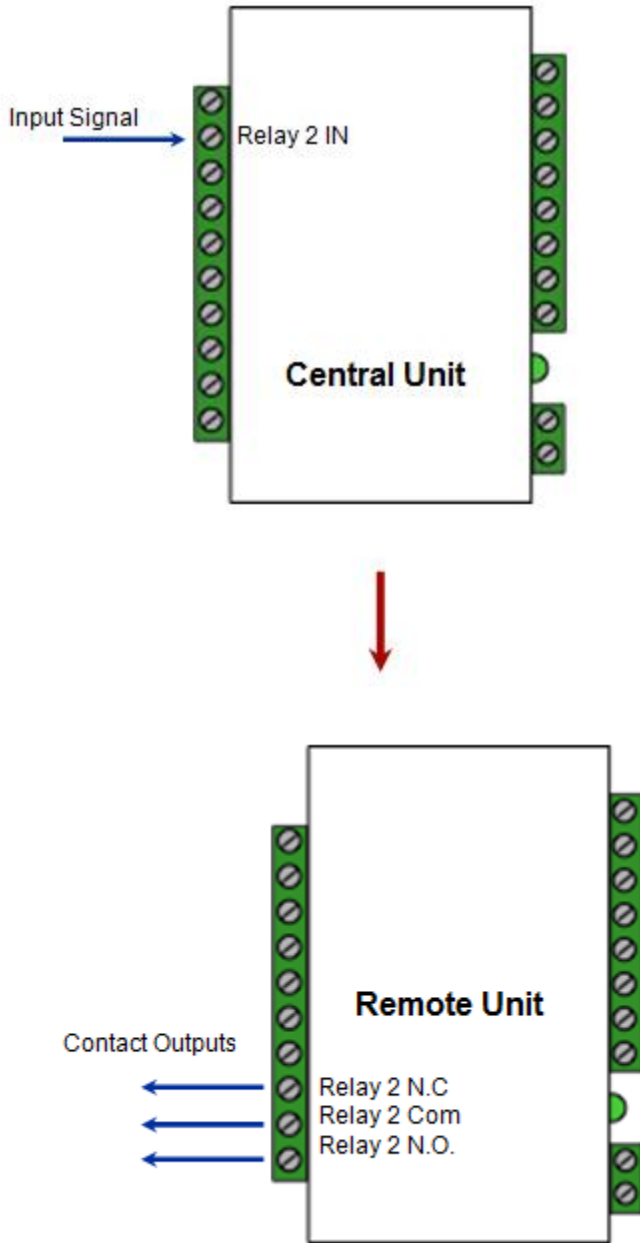
Each input will have an associated output. See the following pages for a diagram of each I/O pair. Inputs can be tested by making a jumper connection to ground and monitoring the associated output.



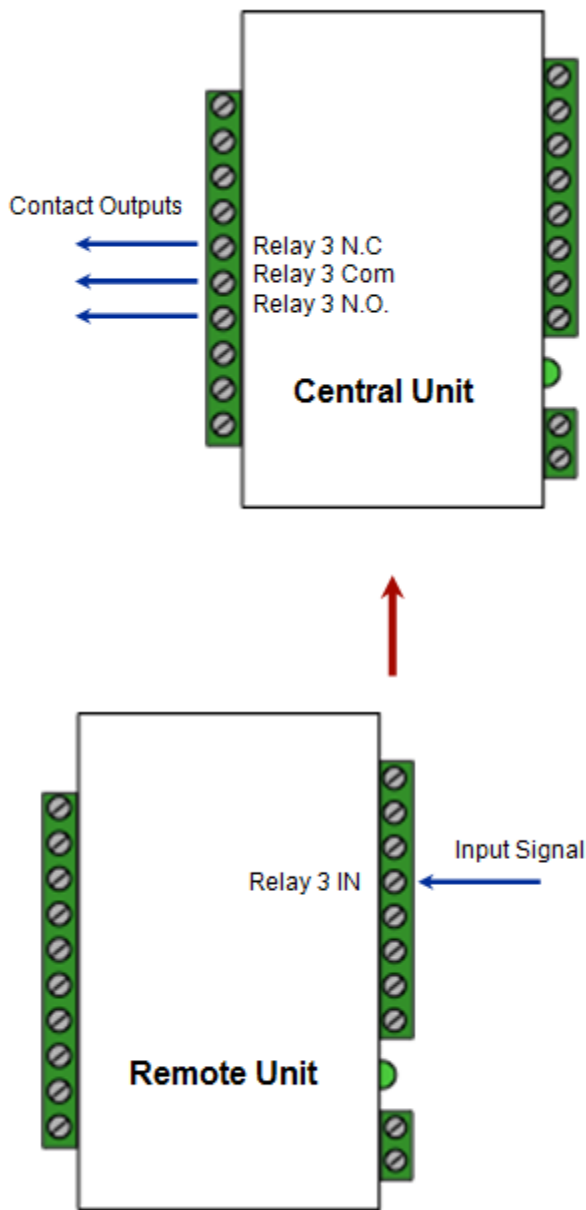
Relay 1 Controls



Relay 2 Controls



Relay 3 Controls

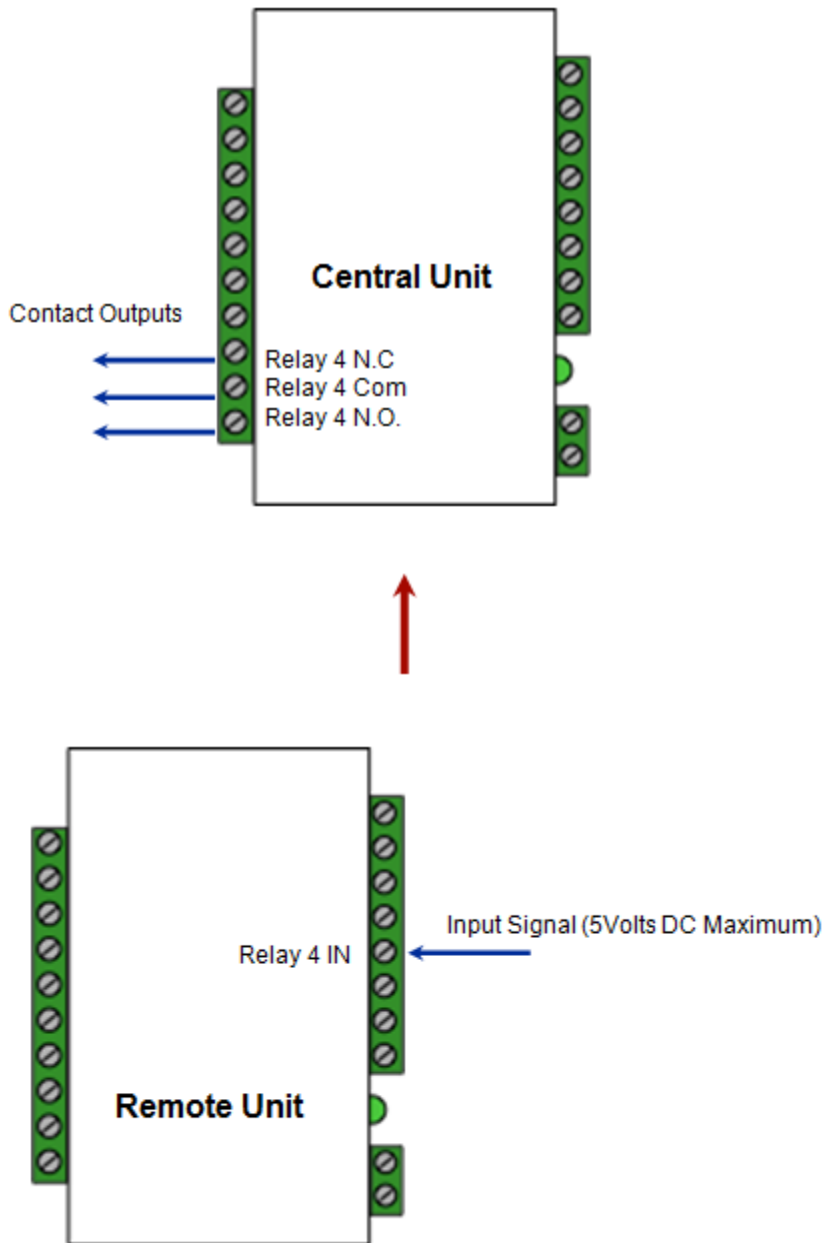


Relay 3 functions as an Alarm relay and monitors the condition of the communication link between the Central and Remote units.

Relay 3 is activated when power is applied and the communication link between the Central and Remote is functioning.

Relay 3 will become deactivated (Alarm condition) when either the Relay 3 input on the remote is active OR the Remote unit is unable to communicate with the Central unit.

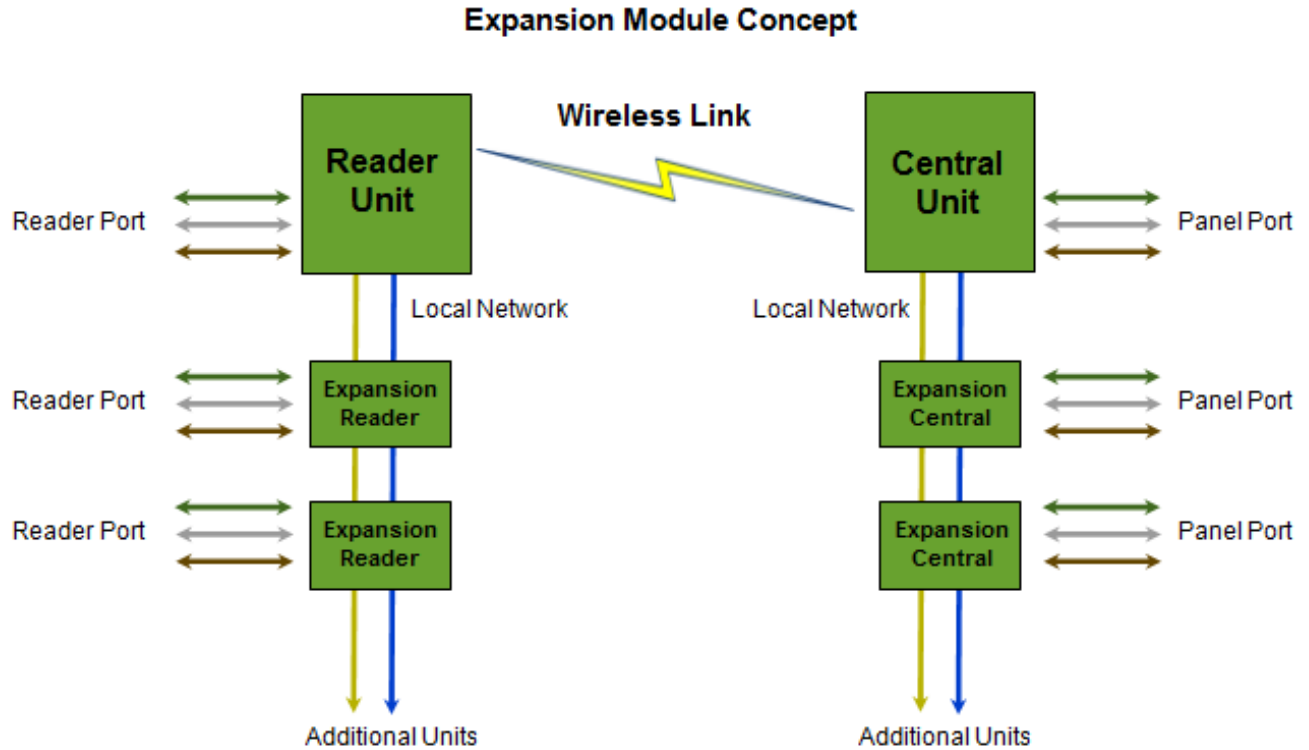
Relay 4 Controls



Expansion Modules

The SecureLINX Wiegand Expansion Modules allows additional reader/panel connections to be added to a single communication link.

Systems with a firmware revision of 2.00 or greater will function as a gateway device where additional Remote and Central units can be added through a multidrop RS-485 local network. Up to 7 additional Central/Remote pairs can be added to a system.



Using the Expansion Modules

Before using Expansion modules with the SecureLINX Wiegand system, it will be necessary to perform a short configuration process. This process determines if the system will utilize expansion modules, and if so, how many will be used with the system. Each link can support up to 7 expansion modules.

SecureLINX Wiegand system units are shipped in the factory default condition. Factory default units will be setup to function as SecureLINX Wiegand system units without expansion modules. Only communications between the 2 gateway units will be active.

Setup Process:

1. With power off, set the DIP switch on the Central unit according to the table below.
2. Apply power. The Diagnostic LED should display a steady Green indication.
3. Remove power. Set DIP switch #1 OFF. Any other DIP switches can now be set as required (Reader family/ Pull-up resistors). The Central unit is now configured. No expansion module configuration is required for the Remote unit.
4. The expansion modules will need to be setup and correctly addressed. See Expansion Module manual for details of Expansion module setup and configuration. The Expansion units are addressed, and added to the system as pairs.
5. Connect the Expansion modules into the system as indicated in this wiring diagram.

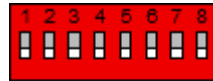
Operation with Expansion Modules:

The SecureLINX Wiegand system Remote and Central gateway units will operate as a standard pair unit, all of the I/O and data terminals are available for use with readers and access control systems. There are some minor differences in operation when using the expansion modules.

1. The Diagnostic LED on the Gateway units will indicate the status of the main (gateway) communication link only.
2. The Alarm relay on the Central Gateway unit will deactivate (indicate alarm condition) when the communication fails between the Gateway units or ANY of the Remote or Central Expansion units.

Central Unit Configuration Mode Settings

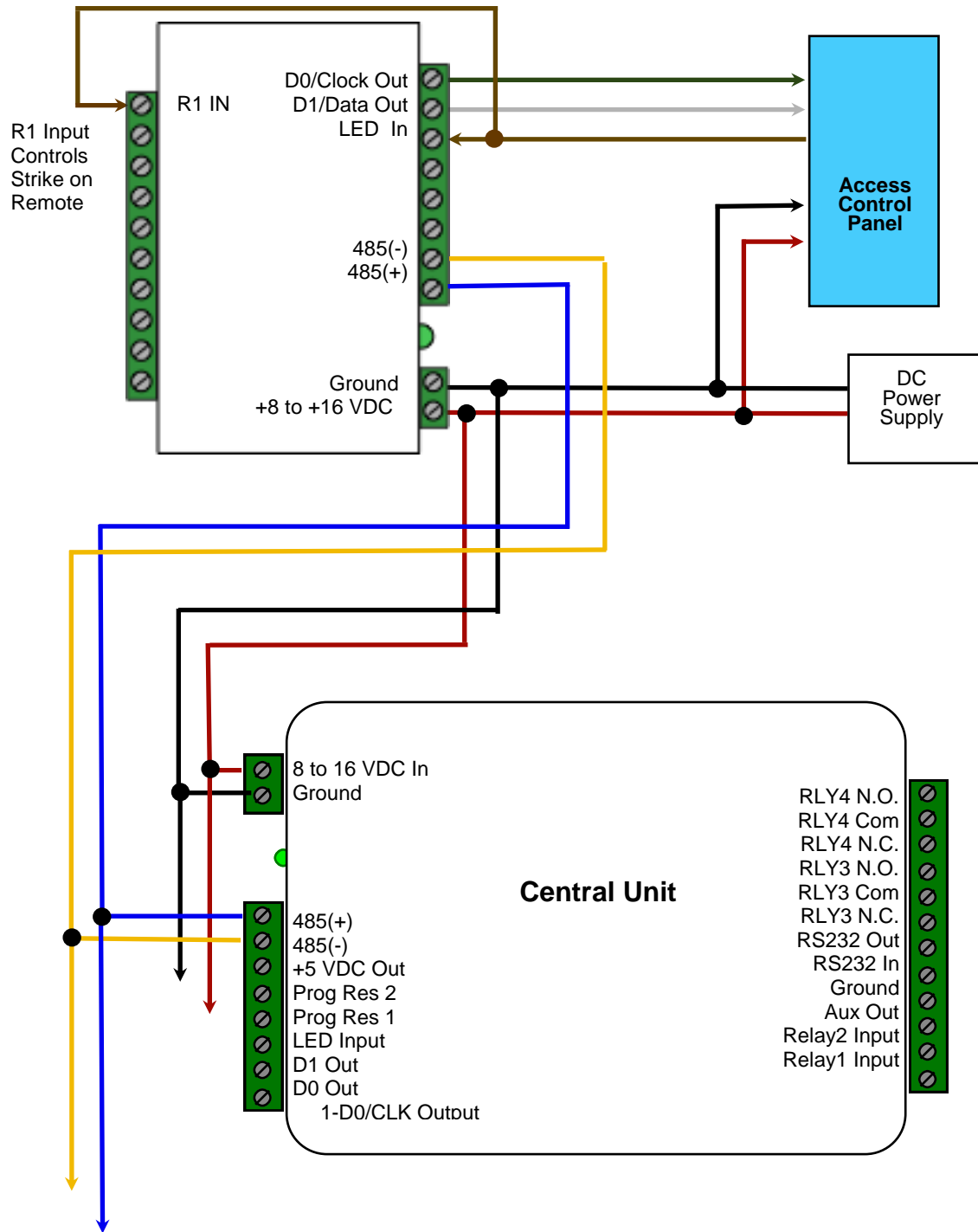
	Switch							
	1	2	3	4	5	6	7	8
Gateway only - No EXP	1	0	0	1	0	0	0	0
1 EXP Pair used	1	0	0	1	0	0	0	1
2 EXP Pair used	1	0	0	1	0	0	1	0
3 EXP Pair used	1	0	0	1	0	0	1	1
4 EXP Pair used	1	0	0	1	0	1	0	0
5 EXP Pair used	1	0	0	1	0	1	0	1
6 EXP Pair used	1	0	0	1	0	1	1	0
7 EXP Pair used	1	0	0	1	0	1	1	1
8 EXP Pair used	1	0	0	1	1	0	0	0



1 = ON

0 = OFF

Expansion Module - Panel "Central" Interface



Expansion Module Reader/Door "Remote" interface

