Introduction

S e c t i o n 1

The PC4820 is a versatile Dual Card Reader Access Control module which will enable you to meet the most demanding access control requirements of an installation. The PC4820 is monitored and programmed via the PC4010 / 4020 control panel. Up to 16 PC4820 modules can be connected to a PC4010 / 4020 via a 4-conductor Combus, using standard, unshielded station wire.

Each PC4820 is capable of providing supervision for two door inputs which may to assigned to any PC4010 / 4020 zone. Each door contact may be configured for any zone end of line option which the control panel can provide.

Each of the two PC4820 Access Card Readers can be programmed to function independently on different doors, or together controlling access for both sides of one door.

Control of the access points can be performed using a variety of equipment. The PC4820 supports four different types of card readers: the Polaris magnetic strip reader, the Shadow Prox proximity card reader, the HID proximity readers, and 26-bit standard Wiegand card readers. The PC4820 also supports the use of any request to exit device including the T-REX exit detector.

1.1 PC4820 Access Control Module Specifications

Two Zone Inputs

- Two programmable supervised zones (EOL resistors – value)
- Zones may be programmed as Standard or Auxiliary delay zone types
- PC4010 / 4020: up to 16 PC4820 can be added (up to 32 access points)

Non Volatile RAM (internal memory)

- Does not lose any system programming when the module is powered down.

Low Current Outputs

- Six low current outputs (open collector outputs switched to ground 25mA max.) :
  - Two LED terminals - To the LED input of the reader
  - Two BUZ terminals - To the Buzzer input of the reader
  - Two OUT terminals - Reserved for future use

Regulated Power Supply (1.5 Amp max.)

- Electronic shutdown protection of the battery, auxiliary output, 5 and 12 V reader power supplies, and lock device power output
- Auxiliary output supply: 12VDC, 125mA Max
- LK1 and LK2 Door Strike power: 12VDC, 250mA Max
- Reader Power 5VDC, 125mA Max
- Reader Power 12VDC, 125mA Max

***NOTE**: UL has only verified compatibility with the eff-eff Fritz Fuss model 4104 electric door strike. The 4104 will fail secure.*

Reader Technology

- Polaris, Shadow Prox, HID Proximity and 26-bit Standard Weigand format

Access Card Compatibility

- Polaris POL-C1CN - Polaris Magnetic Cards
- Shadow Prox, Module Numbers:
  SH-C1 - Shadow Prox Card
  SH-K1 - Shadow Prox Keytag
- HID Proximity:
  HID-C1325KSF - Proximity Card
  HID-C134KSP - Proximity Keytag
- Weigand - Standard 26 bit formats

***NOTE**: UL has only verified compatibility with the Motorola model ASR-500.*

Battery

- 12VDC 7.0Ah recommended rechargeable gel-cell

Transformer

- 16.5 VAC, 40VA

Operating Temperature

- 2˚C to 40˚C (35˚F to 110˚F) operational Temperature Range
- 90˚ non-condensing humidity

Output Voltage

- Output voltage = 13.8VDC (with normal AC and a fully charged battery). Devices that require power from the PC4820 should be capable of operation over the voltage range of 10 to 14VDC.
- 5V Power Supply - Devices connected to the 5V supply should be capable of operation between 4 and 6V.

Installation and Wiring

S e c t i o n 2

2.1 Plan Your Installation

When designing a security system with access control it is best to first lay out the system on paper. This will help determine the total number of zones, additional expanders, access control points and other system components that will be required to complete the installation.

When the location of all points of access are known, appropriate points may be chosen for access control. When working from the layout, be sure to locate the PC4820 module so that the wire runs from each door will be as short as possible.

When deciding the placement of the access points and module, remember to check the capacitance limit for the wire you are using for the Combus. Follow the steps outlined in your PC4010/4020 v3.0 Installation Manual (Section 2.4 "Capacitance Limits").

***NOTE**: Do not run the Combus to the PC4820 in shielded cable.*

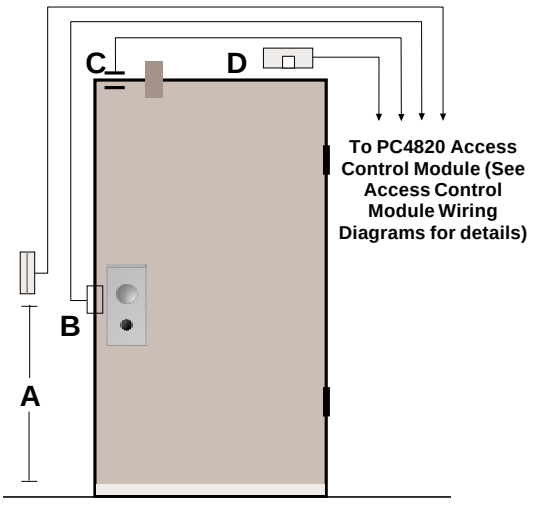
2.2 Installation Steps

Once the location of the PC4820 and each access point is determined, follow the installation steps outlined below.

1 Installation of PC4820 and accessories:

The PC4820 controller cabinet has been designed for surface mounting. The cabinet is large enough to accommodate the battery backup supply and the necessary wiring connections for most applications. The cabinet should be mounted indoors, in a dry, secure location providing normal temperature, humidity levels and access to an earth ground connection. The location should be easily accessible for servicing the equipment, and it is recommended that each PC4820 module be near the doors it controls. If the PC4820 is within the Access controlled area, keys for the controlled doors must be made available so that the PC4820 can be accessed for servicing.

Connect the various devices for each access door according to the diagram below:



A. Access card readers should be located 107cm (42") from the floor.

B. Connect door strikes using standard 18-gauge cable. Recommended door strikes are electric "Continuous Duty" devices which, when power is cut, will remain in a locked or "secured" state. When using magnetic locks, follow local regulations on the use of these devices.

***CAUTION** – Local regulations may prohibit "Lock on Power Failure" if the door is used as a Fire Escape route.*

C. Door contact must be hardwired directly to the PC4820. Wireless or addressable contacts *may not* be used.

D. Install a T-REX exit detector and door alarm (optional) inside of the protected area. (See T-REX Installation Instructions for details on wiring and proper mounting locations.)

2 Tamper protection

A tamper switch may be installed on the cabinet to protect it from unauthorized entry. The normally closed tamper switch is connected to the TAMP and GND (on right side of the PC4820). If the tamper switch is not used, the TAMP terminal must be terminated to any GND terminal with a wire.

*UL listed systems require tamper protection.

3 Connect all inputs, outputs, door locking devices and card readers

Follow the instructions outlined in the sections below for installing each type of device.

4 Power requirements

Install a 16-18VAC/40VA transformer outside the cabinet. Connect the red battery lead to the positive terminal and the black battery lead to the negative terminal.

NOTE**: Do not apply power until all wiring is complete. Both the AC and battery connections must be made in order for the PC4820 to function properly.* ***Connect the battery before connecting the AC.

2.3 Inputs – POST, ARM and REX

The door inputs are capable of following any type of supervision. Choose the end of line configuration (Normally Closed Loops, Single End of Line or Double End of Line) which you have selected for the rest of the security system.

The POST, ARM and REX inputs are for Auto-arm postponement, Arming buttons and Request to Exit devices, respectively. These inputs will only be capable of Normally Closed Loops or Single End of Line resistors. When using Double End of Line supervision, these inputs must only be wired for Single End of Line configuration. Please see section 3.5 "Zone Assignment for Access Doors" for information on door input zone programming.

POST Inputs

When enabled, this PC4820 input allows postponement of Autoarm of the PC4010/4020 for the partitions selected in the Arm/Disarm mask. To postpone an autoarm, the user must present their access card (during the autoarm pre-alert) and activate the device connected to the POST input. Typically the POST input will be a push button device mounted next to the access card reader (107cm (42") from the floor) which is assigned to the partition(s).

The PC4010/4020 will send an Autoarm Abort reporting code to the monitoring station if the reporting code is programmed. The autoarm will restart at the end of the Postpone Arm time (ref # [00020305]) unless the partition has been manually rearmed. The autoarm may be postponed as many times as desired.

***NOTE**: To postpone an autoarm, the user must be assigned to the partition(s) being armed, and the user's access card must have the disarm attribute enabled. See your PC4010/4020 Instruction Manual for information on programming access codes and cards.*

ARM Inputs

When enabled, this PC4820 input will allow designated users to arm the selected partitions on the PC4010/4020. To arm the partition, the user must first ensure that the partition area(s) to be armed is secure (close all protected doors and stop movement in areas covered by motion detectors). The user should present the access card and activate the device connected to the ARM input. The exit delay will begin. Typically the ARM input will be connected to a push button device and should be mounted next to the access card reader (107cm (42") from the floor) which is assigned to the partition(s).

***NOTE**: To arm partitions, the user must be assigned to the partition(s) being armed, and the user's access card must have the arm attribute enabled. See your PC4010/4020 Instruction Manual for information on programming access codes and cards.*

REX Inputs

A Request to Exit device can be used on the inside of the secured area to provide a method of unlocking the door without the need for an access card reader on the inside of the door. When the REX device is tripped, the door will unlock. This will also allow the door to be opened without the door being "Forced open." Request to exit devices can be of many different types. Be sure to read the installation sheets provided with each unit for proper installation for the REX devices.

2.4 Outputs – LED, BUZ and OUT Terminals

LED Outputs

The LED outputs for Out Door 1 and Out Door 2 are used for controlling the LED on the access card readers. This allows the PC4820 to provide visual feedback when the access card is presented to the reader. Connect the wire from the reader indicated as LED to the LED terminal of the selected output.

When using this output to switch an external device, the negative terminal of the device must be connected to the LED output terminal. The positive terminal of the external device must be connected to the AUX+ terminal.

BUZ Outputs

The BUZ outputs for Out Door 1 and Out Door 2 are used for controlling the buzzer of the access card readers. This will allow the PC4820 to provide audible feedback to indicate error conditions. Connect the wire indicated as buzzer to the BUZ terminal of the selected output.

When using this output to switch an external device, the negative terminal of the device must be connected to the BUZ output terminal. The positive terminal of the external device must be connected to the AUX+ terminal.

OUT Outputs

Reserved for future use.

2.5 Door Locking Devices – LK1 & LK2 Terminals

Connect door locks to LK1 and LK2. Each lock output can provide up to 250mA at 12VDC. Always check local regulations concerning the installation of magnetic locking devices.

The locking device outputs are controlled according to the installer programmed parameters for allowing access to, or unlocking the doors according to schedules. These door locking device outputs can operate DC-powered locking devices such as electromechanical strikes and can be configured to operate in fail-safe or fail-secure modes (normal or reverse action). The typical maximum DC for each lock output is 250mA.

***WARNING**: According to local regulations, there may be strict limitations to installing magnetic locks or other similar locking devices on doors used for exit. Be sure to check local regulations before installing any door locking device.*

***NOTE**: The need to employ separate UL listed panic hardware shall be determined by the local authority having jurisdiction.*

2.6 Access Card Readers

Each PC4820 module can control two access card readers. These can be installed on one door to control both entry and exit, or on two separate doors to control access in one direction only. Using the proper cable, the readers may be located up to 150 meters (500 feet) from the PC4820 module. The access card readers should be mounted 107cm (42") from the floor.

***WARNING:** Connecting the Red wire lead (or power lead) of a 5VDC reader to the 12VDC terminal may damage the reader. See reader installation procedure for proper power connection.*

Using Two Readers to Control One Door

When using the Two Readers option, the PC4820 can use both readers to control entry and exit from a single access control point. Each reader can be programmed to have its own access levels (allowing the ability to separately control entry and exit permissions for each door on the system), and schedules. See section 3.2 "Door Options" for programming information.

***NOTE:** When using the Two Reader option, the Door 2 input must be terminated to any COM terminal.*

Access Card / Keypad Readers

Access card readers with integrated keypads may be used with the PC4820. In order to use this reader type, the user must first present their access card. The LED on the reader will flash twice every second to indicate to the user that the reader is waiting for an access code to be entered. The user will have 15 seconds to enter their access code. If the code is entered successfully, the door will be unlocked. The access code entered must be the correct code for the access card used, otherwise access will not be granted, even if the code entered is a valid code on the system. When access is denied to the user due to a wrong / invalid code being entered, or time has expired waiting for the access code, the LED on the reader will flash 3 times every second and the buzzer will give an audible beep 3 times every second to indicate that access was denied.

Reader LED Flash Rates

Most access card readers will have an LED output to provide visual feedback when the access card is presented to the reader. The light will flash in different ways to indicate the following conditions:

LED State	Access Condition
Steady Red	Door is locked
Steady Green	Door is unlocked – Access granted
Slow flash (state changes every half second)	The partition that the Arm / Disarm mask is assigned to is armed
Medium Flash (state changes three times every second)	Waiting for a Privileged card to be presented
Fast flash (State change four times every second)	Access denied / Time expired waiting for a privileged card.

Buzzer Operation

Most access card readers will have a buzzer output to provide audible feedback. The Buzzer output may be connected to operate local warning devices for the following conditions:

- The access controlled door has been forced open. The buzzer will activate and remain active until the door has been closed.
- The access controlled door has been left open too long. The buzzer will activate and remain active until the door has been closed. The buzzer will pulse on and off for the last half of the programmed Door Open Time to indicate that the Door Open Too Long event is about to occur.

PC4820 Connection Chart

Reader Connection		Function	PC4820 Terminal
Polaris / Shadow Prox	**HID**		
Green	Green	Data 0	GRN
White	White	Data 1	WHT
Red	Red	+ V_{DC} or +12V_{DC}	+5V or +12V
Black	Black	Ground	GND
Blue	Yellow	Buzzer	Buzz
Brown	Brown (Red LED)	LED	LED
Orange / Yellow (Polaris only)	Terminals marked as Tamper Common & Tamper Select*	Tamper Switch	To PC4010 / 4020 zone or connected in series with the assigned door input on this module (optional)
———	Blue	Hold	Not used
———	Orange	Green LED	Not used
———	Violet	Return	GND
Purple / Grey (POL-2KP only)	--------	Independent Switch	Can be used for Arm or Post inputs. See PC4820 Wiring Diagram for wiring instructions.

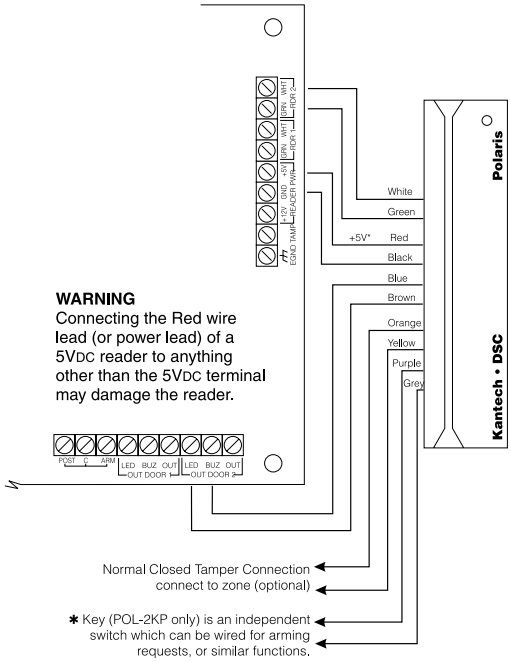
* Tamper connection not available on the MiniProx detector

PC4820 List of Supported Readers and Cards

Reader Type	Reader Part Numbers	Supply Voltage	Card Part Numbers
Magnetic Stripe	POL-1, POL-1W, POL-2, POL-2KP	+5Vdc	POL-C1CN
Bar Code	BC-201		
Proximity: Shadow Prox	SH-1, SH-2, SH-2KP	+5Vdc to 14Vdc	SH-C1, SK-K1, SH-CMG1, SH-CMG2
	SH-4, SH-5	+12Vdc	
	SH-6, SH-7	+24Vdc to 28Vdc	
HID	HID-MP5365 - MiniProx	+12Vdc	HID-1365KSF, HID-1335KSF, HID-1334KSF, HID-1365KSF, HID-1385KSF
	HID-PR5355, HID-PR5355KP - ProxPro	+10Vdc to 15Vdc	
	HID-MX5375 - MaxiProx	+14Vdc to 28.5Vdc	

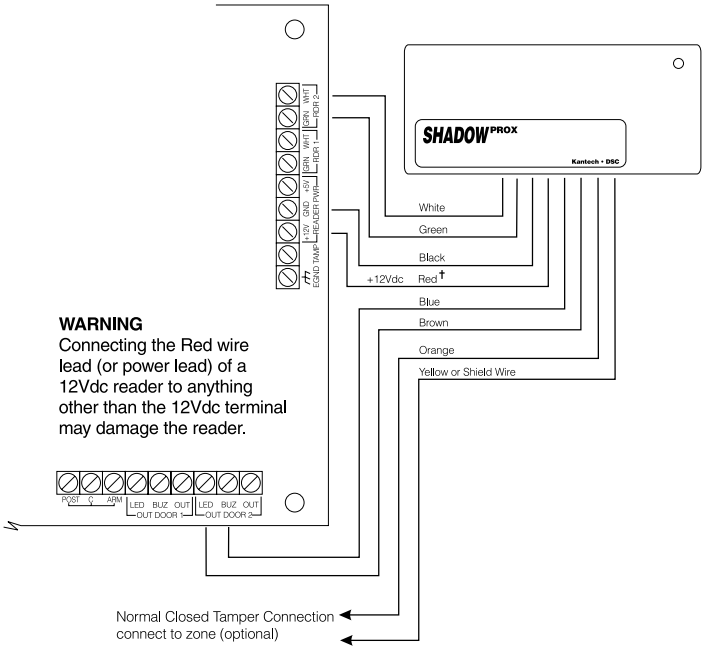
PC4820 Access Control Module Reader Connections

Polaris Readers (POL-1, POL-2, POL-2KP)



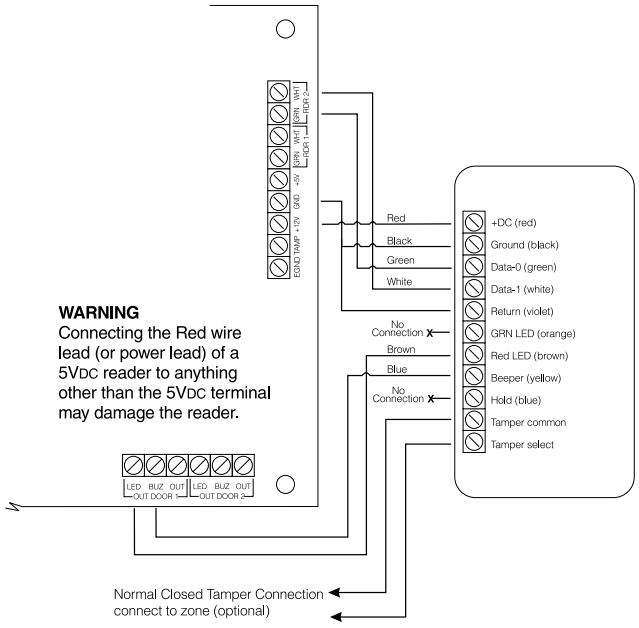
NOTE: Only use the +5V power supply when using Polaris Readers.

Shadow Prox Readers

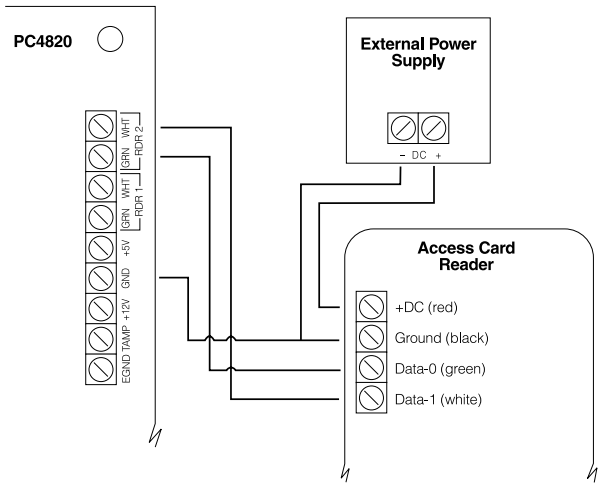


†NOTE: Only use the +12V power supply when using the Shadow Prox Reader.

HID Readers



Connecting External Power Supplies



Cabling Specifications

Component	Maximum Wire Length	Cable Description
Reader 5V	150m (500ft)	3 Pair, #18 AWG, stranded, overall shield with extra drain conductor
Reader 12V	150m (500ft)	3 Pair, #22 AWG, stranded, overall shield with extra drain conductor
Inputs (Door, REX, Post, Arm)	300m (1000ft)	2 pair, #22 AWG, twisted pairs
AC Transformer	8m (25ft)	1 pair, #18 AWG Ground 8m (25ft) 1 conductor, #18 AWG, Solid

Programming the PC4820

Section 3

Programming of the PC4820 is performed at the PC4010/4020 control panel in Installer's Programming mode. Refer to Section 4 "How to Program" of the PC4010/4020 Installation Manual for instructions.

The following programming sections must be programmed for each PC4820 enrolled on the system. To select a module, enter reference number [0011XX] where "XX" refers to the PC4820 module number.

The control panel will transfer all necessary information (access codes, scheduling, etc.) to each PC4820 module whenever one of the following occurs:

1. the main panel is powered up
2. installer's mode is exited
3. a PC4820 loses and then restores communication with the control panel
4. a PC4820 is hardware defaulted
5. a PC4820 is enrolled
6. a downloading session has disconnected.

The data transfer can take up to 2.5 minutes per PC4820 module. When the transfer is completed, all keypads will beep 16 times. Changes to PC4820 programming will not take effect until the data transfer is complete.

3.1 Programming Reader Types

Ref # [0011XX00] where XX = PC4820 module #

The PC4820 is capable of supporting different types of access card readers. The same type of reader must be used on both doors of an access card module, but different modules may use different reader types. Enter the 2-digit code for the reader type you are installing on the selected zone.

00 Polaris 1- Magnetic card reader. 7 Digits with clock and data.

01 Shadow Prox - Extended range proximity reader SH5, SH6, SH7, SH-VR 32 Bits.

02 26 Bit Standard Wiegand reader, HID Proximity readers

The default access card reader type is **00** (Polaris 1).

***NOTE**: Use reader type 01 when using Kantech Secure Format (KSF) devices.*

3.2 Reader Options

Ref # [0011XX01] where XX = module #

This section contains the programming for the selected PC4820. First, you must select which of the two doors to program. Use the arrow (< >) keys to scroll to either Door 1 or Door 2 and press the [*] key to select. A series of toggle options will be available for each door. Again, use the arrow (< >) keys to scroll through each option and press the [*] key to turn the selected option on or off.

The options available for each door are as follows:

- **Lock Reversed**: If enabled, power will be applied to lock the door. The lock will remain closed when idle and will deactivate when a valid access card is used to open the door. The programming for this option is dependent on the type of locking device being used. Check the installation sheet provided with the locking device to see what is required for power.

  If disabled, power will be applied to unlock the door. This option is for use with "Fail Secure" devices such as electronic door strikes. (Default = No)
- **Unlock on REX**: If enabled, tripping a Request To Exit device will cause the door to unlock for the programmed Door Unlock time (see Section 3.4 "Door Times"). If disabled, tripping the Request To Exit device will not cause the door to unlock. (Default = Yes)
- **Flash When Arm**: If enabled, the armed status of the assigned partition(s) will be indicated by the light on the reader assigned to the door. The LED will flash slowly for the duration of the armed period.

***NOTE:** The partition(s) to which the door's zone is assigned must also be selected in the Arm/Disarm Mask for proper operation of this function.*

  If disabled, the LED on the access card reader will not indicate the armed status. (Default = Yes)
- **Relock On Arm**: If enabled, a Request To Arm will relock the door when the arm input is activated. If disabled, a Request to Arm will not relock the door. (Default = No)
- **Lock On Close**: If enabled, a door unlocked by an access card or by a REX device will lock once the zone is opened and then closed. If disabled, a door unlocked by an access card or by a REX device will relock once the zone is opened. (Default = No)
- **Code Required**: If enabled, a valid access code must be entered at an adjacent keypad in addition to the card swipe in order for the door to unlock. If disabled, no code will be required. (Default = No)
- **LED Reversed**: If enabled, the normal state of the LED output on the PC4820 will be an open collector. If disabled, the output's normal state will be low. (Default = No)
- **Two Readers**: If enabled, both "doors" (card readers) will be assigned to the same zone. This will allow the PC4820 to control access both into and out of a secured area at a single access point. The zone and partition assignment of both doors on the PC4010/4020 must be the same. (See section 3.5 "Zone Assignment for Access Doors" and your PC4010/4020 Programming Manual for information on zone and partition programming.)

  Any time an access card is presented at one reader to open the door, the second reader will also allow access. This will prevent a door forced open event (both lock outputs will unlock).

Each door can still be programmed to have its own access levels (allowing the ability to control both entry and exit permissions for each door on the system), and schedules.

NOTE: *This option can only be enabled for Door 1.*

If disabled, doors 1 and 2 will have their own zone and partition assignments. (Default = No)

3.3 Arming and Disarming with Access Cards

The PC4820 can be set up so that users may arm and disarm, or postpone the autoarm of any active partition on the system. To set up partitions to be armed and disarmed from an access control module, the following must be programed:

1. The user's access card must be assigned to the appropriate partition(s); an access level must be assigned to the access card; and the access card must have the arm and or disarm attribute enabled (see section 3.8 "Programming Access Cards").
2. The access door must be assigned a PC4010/4020 zone (see section 3.5 "Zone Assignment for Access Doors"), and the zone must be assigned to the appropriate partitions (see below).
3. The Arm/Disarm mask must be programmed to include the partition(s) that are to be armed/disarmed from that access card reader (see below).
4. The Postpone Arm, Arm Request and Disarm Request schedules must be programmed with a date schedule other than [00] (see section 3.6 "Access Door Schedules").

HINT: When using the arming/disarming options of the PC4820, the use of Bell Squawk and a Partition Status output will allow for clear indication of the armed status of the partition(s). These options can be enabled/disabled on each partition (see your PC4010/4020 Installation Manual for more information on programming partitions).

Arm/Disarm Partition Mask

Ref # [0011XX01YY01] where XX = module #; YY = door #

In this section select the partition(s) which users will be able to arm and/or disarm when they present the appropriate access card at the reader for the access door.

NOTE*: The zone assigned to the door must be assigned to the same partitions selected in the Arm/Disarm Partition Mask (Partition Programming, reference # [0100XX03], where XX = partition #).*

**The PC4820 has not been evaluated by UL as a burglar alarm control unit.*

3.4 Door Times

Ref # [0011XX01YY02] where XX = module #; YY = door #

Door Unlock Time

The amount of time that the door will remain unlocked after a valid access card has been presented is programmed in this section. This is also the Request To Exit time period. The default setting is 10 seconds. Valid entries are from 001-255 seconds.

Door Open Time

This section will program the amount of time an access door can remain open before a Door Open Too Long event is generated. After half of the Door Open Time has expired, the reader buzzer will pulse on and off as a warning. At the end of the Door Open Time, the buzzer will sound steady to indicate that the door has been left open too long. The default setting is 030 seconds. Valid entries are from 001-255 seconds.

3.5 Zone Assignment for Access Doors

Ref # [0011XX01YY03] where XX = module #; YY = door #

Assign each "door" to a zone on the PC4010/4020. Any zone from Zone 17 to 128 may be used (Zone 9 to 64 on the PC4010).

You can use any zone supervision option provided by the PC4010/4020 for PC4820 zones. The end of line resistors used for the door inputs are 5600Ω for the alarm contact. If you will be using DEOL resistors, the tamper contact is also 5600Ω.

The door's zone must be programmed as a Standard Delay, or an Auxiliary Delay zone (PC4010/4020 programming reference number [0100XX03], where XX=partition number). See your PC4010/4020 v3.0 Installation Manual, section 5 "Zone Programming".

3.6 Access Door Schedules

A date schedule can be assigned to each of the following access door features. A date schedule will include the start and end times for each event, the days of the week the schedule will be active for and any holiday groups the event will observe.

Date Schedules 00 and 01

If date schedule 00 is programmed, the feature will be disabled (schedule is never active). If date schedule 01 is programmed, the feature will be always on (schedule is always active).

For more information regarding date schedule programming, please refer to your PC4010/4020 v3.0 Installation Manual, section 14.1 "Date Schedules".

There are 11 access door features which can be scheduled. They are as follows:

Postpone Arm Schedule

Ref # [0011XX01YY04] where XX = module #, YY = door #

This schedule will program at what times the auto arming sequence can be postponed by a user presenting their access card at the appropriate reader. Only the partitions to which the door's zone are assigned and that are selected in the arm/disarm mask will be affected.

The user's access card must also be assigned to the appropriate partitions and have the disarming attribute enabled for the feature to work correctly. See your PC4010/4020 Instruction Manual for information on programming access codes and cards.

The default date schedule is 01.

Arm Request Schedule

Ref # [0011XX01YY05] where XX = module #, YY = door #

This schedule will program when the selected partitions may be armed by a user presenting their access card at the appropriate reader. Only the partitions assigned to the door zone and selected in the arm/disarm mask will be affected.

The user's access card must also be assigned to the appropriate partitions and have the arming attribute enabled in order for arming to occur. See your PC4010/4020 Instruction Manual for information on programming access codes and cards.

The default date schedule is 01.

Door Unlock Schedule

Ref # [0011XX01YY06] where XX = module #, YY = door #

This schedule will determine when an access door will be unlocked. When the door is unlocked, a user will not require an access card to open the door. The door will remain unlocked for the duration of the schedule. Opening the door will not cause a door forced open event.

When the partition(s) to which the door zone is assigned are armed, the door will automatically lock at the beginning of the exit delay. If the Door Unlock schedule becomes active while the partition(s) are armed, the door will not unlock. However, if the partition is disarmed while the door unlock schedule is active, the door will unlock, and will remain unlocked until the scheduled end time.

NOTE: *If the door is assigned to more than one partition, the door will only lock once the last partition to be armed has begun its exit delay.*

The default date schedule is 00 (disabled).

Request To Exit (REX) Schedule

Ref # [0011XX01YY07] where XX = module #, YY = door #

This schedule controls the Unlock on REX option. When the schedule is active, tripping a Request To Exit device will cause the door to unlock for the programmed Door Unlock time (see section 3.5 "Door Times"). If the schedule is not active, a Request To Exit will not cause the door to unlock.

The default date schedule is 01.

Second Card Schedule

Ref # [0011XX01YY08] where XX = module #, YY = door #

This schedule will determine when users with the Wait For Privilege option enabled will require a Privileged user to grant them access to the area. If the Second Card Schedule is active, the following will occur:

The user with the Wait For Privilege card presents their card first. The LED on the card reader will flash slowly for 10 seconds. If during this time a Privileged card is used, the door will be unlocked. Only privileged cards are capable of allowing access to the system. If a non-privileged card is used, the door will not be unlocked and a log will be made to the buffer. This feature is used for monitoring the access of users on the system.

The default date schedule is 00 (disabled).

Disarm Request Schedule

Ref # [0011XX01YY09] where XX = module #, YY = door #

This schedule will program the times when the selected partitions may be disarmed by a user presenting their access card at the appropriate reader. Only partitions which have the door's zone assigned to them, and that are selected in the arm/disarm mask will be affected.

To disarm the partition(s), the user must present their access card and open the door. The partition(s) will be disarmed if the Disarm Request schedule is active. If the user presents their card is outside of the Disarm Request schedule time window, the door will be unlocked but the partition(s) will not be disarmed when the door is opened. The user must then enter their access code at a keypad to disarm the partition(s).

NOTE*: To disarm a partition or enter a partition which is armed, the user must be assigned to the partition, and the user's disarm attribute must be enabled in access code and card programming. See your PC4010/4020 Instruction Manual for information on programming access codes and cards.*

The default date schedule is 00 (disabled).

Code Schedule

Ref # [0011XX01YY11] where XX = module #, YY = door #

When this schedule is active, the door will not unlock until the card is presented AND a valid access code is entered on the keypad. When the schedule is inactive, the door will unlock when an access card is presented.

If Schedule [00] is programmed into this section, the door will be unlocked by an access card only when the partition(s) the door is assigned to are disarmed. When the partitions are armed, an access code will also be required.

NOTE*: The Code Required option must be enabled in order for this feature to work.*

The default date schedule is 01.

Forced Open Schedule

Ref # [0011XX01YY12] where XX = module #, YY = door #

When this schedule is active and a door is opened without tripping a REX device, a Door Forced Open event will be logged to the event buffer and transmitted to central station. When the schedule is inactive and a door is forced open, the event will be logged, but not transmitted.

NOTE*: In order for this option to work, the door must be assigned a zone and that zone must be assigned to one or more partitions.*

The default date schedule is 00 (disabled).

Forced Open Bell Schedule

Ref # [0011XX01YY13] where XX = module #, YY = door #

When this schedule is active and a door is opened without tripping a REX device, the partition(s) the door is assigned to will go into alarm. The alarm will be on until the bell cut-off time expires, or until an access code is entered to silence the alarm.

NOTE*: In order for this option to work, the door must be assigned a zone and that zone must be assigned to one or more partitions.*

The default date schedule is 00 (disabled).

Open Too Long Schedule

Ref # [0011XX01YY14] where XX = module #, YY = door #

When the schedule is active and the assigned door is left open past the Door Open time, an Open Too Long event will be logged to the event buffer and transmitted. When

the schedule is inactive and the door is left open past the Door Open time, the event will be logged but not transmitted. The Door Open time is default set at 30 seconds but can be changed (see Section 3.4 “Door Times”).

***NOTE**: In order for this option to work, the door must be assigned a zone and that zone must be assigned to one or more partitions.*

The default date schedule is 00 (disabled).

Open Too Long Bell Schedule

Ref # [0011XX01YY15] where XX = module #, YY = door #

When the schedule is active and the assigned door is left open past the Door Open time, the partition(s) the door is assigned to will go into alarm. The alarm will remain on until the bell cut-off time expires, or until an access code is entered to silence the alarm. The Door Open time is set at 30 seconds by default, but can be changed (see Section 3.4 “Door Times”).

***NOTE**: In order for this option to work, the door must be assigned a zone and that zone must be assigned to one or more partitions.*

The default date schedule is 00 (disabled).

3.7 Access Level

Ref # [0011XX01YY10] where XX = module #, YY = door #

Access levels allow specific users to have access to areas of the system at various times of the day. Each door can have multiple access levels assigned to it. Each access level will follow one date schedule.

There are 63 access levels for each door. To program access levels, select an access level number (02-63) and then enter the schedule number that the access level will follow. Access cards programmed with access level 01 always have access to all doors. Access levels 02 - 63 will be recognized by the card reader during the windows provided by the assigned date schedule.

Date Schedules 00 and 01

Access levels programmed with date schedule 01 will always be recognized by the door. Access levels programmed with date schedule 00 will never be recognized by the door. In order to disable an access level for a door, assign the access level to Date Schedule 00.

By default all access levels are assigned to Date Schedule 00 (disabled).

3.8 Programming Access Cards

In order for an access card to function on the PC4820 the card must first be programmed into the PC4010/4020. This is done through user programming (enter [*][5][system master code] or [supervisory code]). See your PC4010/4020 Instruction Manual for more information on programming access codes and cards.

Diagnostics

Section 4

4.1 Hardware Reset

On occasion, it may be necessary to perform a reset of the PC4820 to factory default programming. To perform a hardware reset of the PC4820, the following steps must be performed:

1. Power down the PC4010/4020 by removing both AC and battery power from the control panel.
2. Power down the PC4820 modules by removing both AC and battery power from the units.
3. Remove all connections from the following PC4820 terminals; OUT (for OUT DOOR 1), Door (for INPUTS DOOR 1) and AUX+.
4. On the selected PC4820, connect a short from the terminals marked as OUT (for OUT DOOR 1) and Door (for INPUTS DOOR 1). Next connect a 5600 ohm resistor from the Door input to the AUX+ terminal.
5. Restore AC power to the PC4820 module(s).
6. Wait for 10 seconds then remove AC power to the PC4820 module(s).
7. Remove the connections made in Step 4.
8. Any terminal connections removed in Step 3 can now be reconnected.
9. Restore AC and battery power to the PC4820 module(s)
10. Restore AC and battery power to the PC4010/4020 control panel.

The PC4820 will now indicate to the PC4010/4020 that a hardware default has been performed and the PC4010/4020 will retransmit all programming information back to the PC4820 modules. All keypads on the system will beep quickly 16 times to indicate that the programmed information has been sent to the PC4820.

Be sure to remove all connections involved in the hardware default procedure when the hardware default has been completed.

***NOTE**: When performing a hardware or software default of the PC4010/4020 be sure to also perform a hardware default on the PC4820. This will insure that all unwanted programming has been removed from the module.*

4.2 Diagnostics via VTAL LED (L1)

The VTAL LED (located on the right hand side of the circuit board) of the PC4820 is capable of providing diagnostics information for various conditions that may appear on the module.

- Steady flash (once per second) indicates normal operation.
- Fast flash indicates that communication to the PC4010/4020 has been lost (Combus fault).
- On steady (1/2 second) indicates data is being received from an access card reader.

PC4820 Programming Worksheet

Record your PC4820 module programming information here. Make one copy of this sheet for each PC4820 you will install.

NOTE: XX = module #; YY = door #

		Door 01	Door 02
[0011]	**PC4820 Options**		
[0011XX]	**PC4820 Module Number:**	⌊__⌋	
[0011XX00]	Reader Type Default: 00	⌊__⌋	
[0011XX01YY]	**Select Door Number:**		
[0011XX01YY00]	Toggle Options:	Default	Default
	Lock Reversed?	N ⌊_⌋	N ⌊_⌋
	Unlock on REX?	Y ⌊_⌋	Y ⌊_⌋
	Flash When Arm?	Y ⌊_⌋	Y ⌊_⌋
	Relock on Arm?	N ⌊_⌋	N ⌊_⌋
	Lock on Close?	N ⌊_⌋	N ⌊_⌋
	Code Required?	N ⌊_⌋	N ⌊_⌋
	LED Reversed?	N ⌊_⌋	N ⌊_⌋
	Two Readers?	N ⌊_⌋	N
[0011XX01YY01]	Arm / Disarm Mask:		
	Partition: 1 2 3 4 5 6 7 8	⌊N N N N N N N N⌋	1 2 3 4 5 6 7 8 ⌊N N N N N N N N⌋
[0011XX01YY02]	Door Times:		
	Door Unlock Time	010 ⌊__⌋	010 ⌊__⌋
	Door Open Time	030 ⌊__⌋	030 ⌊__⌋
[0011XX01YY03]	Zone Assignment	000 ⌊__⌋	000 ⌊__⌋
[0011XX01YY04]	Postpone Arm Schedule	01 ⌊__⌋	01 ⌊__⌋
[0011XX01YY05]	Arm Request Schedule	01 ⌊__⌋	01 ⌊__⌋
[0011XX01YY06]	Door Unlock Schedule	00 ⌊__⌋	00 ⌊__⌋
[0011XX01YY07]	REX Schedule	01 ⌊__⌋	01 ⌊__⌋
[0011XX01YY08]	Second Card Schedule	00 ⌊__⌋	00 ⌊__⌋
[0011XX01YY09]	Disarm Request Schedule	00 ⌊__⌋	00 ⌊__⌋
[0011XX01YY10]	Access Level (enter 02 - 63)	Default (all levels): [00]	

Access Level	Schedule Number	Access Level	Schedule Number	Access Level	Schedule Number
02	⌊__⌋	23	⌊__⌋	44	⌊__⌋
03	⌊__⌋	24	⌊__⌋	45	⌊__⌋
04	⌊__⌋	25	⌊__⌋	46	⌊__⌋
05	⌊__⌋	26	⌊__⌋	47	⌊__⌋
06	⌊__⌋	27	⌊__⌋	48	⌊__⌋
07	⌊__⌋	28	⌊__⌋	49	⌊__⌋
08	⌊__⌋	29	⌊__⌋	50	⌊__⌋
09	⌊__⌋	30	⌊__⌋	51	⌊__⌋
10	⌊__⌋	31	⌊__⌋	52	⌊__⌋
11	⌊__⌋	32	⌊__⌋	53	⌊__⌋
12	⌊__⌋	33	⌊__⌋	54	⌊__⌋
13	⌊__⌋	34	⌊__⌋	55	⌊__⌋
14	⌊__⌋	35	⌊__⌋	56	⌊__⌋
15	⌊__⌋	36	⌊__⌋	57	⌊__⌋
16	⌊__⌋	37	⌊__⌋	58	⌊__⌋
17	⌊__⌋	38	⌊__⌋	59	⌊__⌋
18	⌊__⌋	39	⌊__⌋	60	⌊__⌋
19	⌊__⌋	40	⌊__⌋	61	⌊__⌋
20	⌊__⌋	41	⌊__⌋	62	⌊__⌋
21	⌊__⌋	42	⌊__⌋	63	⌊__⌋
22	⌊__⌋	43	⌊__⌋		

		Door 01	Door 02
		Default	Default
[0011XX01YY11]	Code Schedule	01 ⌊__⌋	01 ⌊__⌋
[0011XX01YY12]	Forced Open Sched.	00 ⌊__⌋	00 ⌊__⌋
[0011XX01YY13]	Forced Open Bell	00 ⌊__⌋	00 ⌊__⌋
[0011XX01YY14]	Open Too Long Schedule	00 ⌊__⌋	00 ⌊__⌋
[0011XX01YY15]	Open Too Long Bell	00 ⌊__⌋	00 ⌊__⌋

1645 Flint Road, Downsview, Ontario, Canada M3J 2J6
(416) 665-8460 • Fax (416) 665-7498 • 1-800-387-3630
Printed in Canada 29003128 R0

MAXSYS™

PC4820 v1.2 • Installation Manual

WARNING: *This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer. The entire manual should be carefully read.*

LIMITED WARRANTY

Digital Security Controls Ltd. warrants the original purchaser that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, Digital Security Controls Ltd. shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labour and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original owner must promptly notify Digital Security Controls Ltd. in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period.

International Warranty

The warranty for international customers is the same as for any customer within Canada and the United States, with the exception that Digital Security Controls Ltd. shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure

To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to Digital Security Controls Ltd. must first obtain an authorization number. Digital Security Controls Ltd. will not accept any shipment whatsoever for which prior authorization has not been obtained.

Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage incurred in shipping or handling;
- damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- damage due to causes beyond the control of Digital Security Controls Ltd. such as excessive voltage, mechanical shock or water damage;
- damage caused by unauthorized attachment, alterations, modifications or foreign objects;
- damage caused by peripherals (unless such peripherals were supplied by Digital Security Controls Ltd.);
- defects caused by failure to provide a suitable installation environment for the products;
- damage caused by use of the products for purposes other than those for which it was designed;
- damage from improper maintenance;
- damage arising out of any other abuse, mishandling or improper application of the products.

Digital Security Controls Ltd.'s liability for failure to repair the product under this warranty after a reasonable number of attempts will be limited to a replacement of the product, as the exclusive remedy for breach of warranty. Under no circumstances shall Digital Security Controls Ltd. be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property.

Disclaimer of Warranties

This warranty contains the entire warranty and shall be in lieu of any and all other warranties, whether expressed or implied (including all implied warranties of merchantability or fitness for a particular purpose) And of all other obligations or liabilities on the part of Digital Security Controls Ltd. Digital Security Controls Ltd. neither assumes nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

This disclaimer of warranties and limited warranty are governed by the laws of the province of Ontario, Canada.

WARNING: Digital Security Controls Ltd. recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Installer's Lockout

Any products returned to DSC which have the Installer's Lockout option enabled and exhibit no other problems will be subject to a service charge.

Out of Warranty Repairs

Digital Security Controls Ltd. will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to Digital Security Controls Ltd. must first obtain an authorization number. Digital Security Controls Ltd. will not accept any shipment whatsoever for which prior authorization has not been obtained.

Products which Digital Security Controls Ltd. determines to be repairable will be repaired and returned. A set fee which Digital Security Controls Ltd. has predetermined and which may be revised from time to time, will be charged for each unit repaired.

Products which Digital Security Controls Ltd. determines not to be repairable will be replaced by the nearest equivalent product available at that time. The current market price of the replacement product will be charged for each replacement unit.

WARNING Please Read Carefully

Note to Installers

This warning contains vital information. As the only individual in contact with system users, it is your responsibility to bring each item in this warning to the attention of the users of this system.

System Failures

This system has been carefully designed to be as effective as possible. There are circumstances, however, involving fire, burglary, or other types of emergencies where it may not provide protection. Any alarm system of any type may be compromised deliberately or may fail to operate as expected for a variety of reasons. Some but not all of these reasons may be:

■ Inadequate Installation

A security system must be installed properly in order to provide adequate protection. Every installation should be evaluated by a security professional to ensure that all access points and areas are covered. Locks and latches on windows and doors must be secure and operate as intended. Windows, doors, walls, ceilings and other building materials must be of sufficient strength and construction to provide the level of protection expected. A reevaluation must be done during and after any construction activity. An evaluation by the fire and/or police department is highly recommended if this service is available.

■ Criminal Knowledge

This system contains security features which were known to be effective at the time of manufacture. It is possible for persons with criminal intent to develop techniques which reduce the effectiveness of these features. It is important that a security system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.

■ Access by Intruders

Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a warning device, or interfere with or prevent the proper operation of the system.

■ Power Failure

Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be charged, in good condition and installed correctly. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment such as a security system. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

■ Failure of Replaceable Batteries

This system's wireless transmitters have been designed to provide several years of battery life under normal conditions. The expected battery life is a function of the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.

■ Compromise of Radio Frequency (Wireless) Devices

Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent radio signal interference.

■ System Users

A user may not be able to operate a panic or emergency switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm.

■ Smoke Detectors

Smoke detectors that are a part of this system may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls or roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.

Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fires equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches or arson.

Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.

■ Motion Detectors

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbeques, fireplaces, sunlight, steam vents, lighting and so on.

■ Warning Devices

Warning devices such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. If warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened. Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

■ Telephone Lines

If telephone lines are used to transmit alarms, they may be out of service or busy for certain periods of time. Also an intruder may cut the telephone line or defeat its operation by more sophisticated means which may be difficult to detect.

■ Insufficient Time

There may be circumstances when the system will operate as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time to protect the occupants or their belongings.

■ Component Failure

Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.

■ Inadequate Testing

Most problems that would prevent an alarm system from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an earthquake, an accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

■ Security and Insurance

Regardless of its capabilities, an alarm system is not a substitute for property or life insurance. An alarm system also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation.

Table of Contents

PC4820 Access Control Module

Wiring Diagram

- Battery and AC Connections
- Combus Connections
- Lock device and Reader Connections
- Typical Zone Circuits