Keyscan LUNA™ SDAC

dormakaba

Installation Guide

WiFi Single Door Access Control Unit

Information and specifications in this document are subject to change without notice.

dormakaba Canada Inc.

901 Burns Street East

Whitby, Ontario

Canada

L1N 0E6

Phone: 1-888-539-7226 (Toll Free Canada/USA)

Phone: 905-430-7226

Fax: 905-430-7275

Web Site: www.keyscan.ca

Technical support is available to dealers and installers Monday to Friday 9:00 A.M. to 6:30 P.M. Eastern Time at the above listed telephone numbers or web address.

Table of Contents

Foreword

Keyscan systems are designed for use in various environments and applications. As such, observe stated cable, power, ground, and environment specifications for reliable and safe operation of the equipment.

About This Guide

This *Installation Guide* is designed to provide general information for installing the Keyscan SDAC single-door access control. This guide assumes the installer has knowledge of electrical, electronic, mechanical, and computer concepts, as well as having familiarity with access control systems and associated components.

Electrical Precautions

Be sure that all circuit breakers powering the system are switched off before commencing installation or modifying wiring connections. Do not apply power before the installation is complete otherwise the equipment may be damaged. Ensure all enclosures are connected to earth grounds for proper and safe system operation.

Tools

We recommend having the following tools on hand to install the access control system:

- Digital Multi Meter
- Wire Cutters
- Needle Nose Pliers
- Soldering Iron
- Tape
- Set of Screwdrivers
- Drill & Drill Bits
- Laptop Computer

Software Requirements

The SDAC single door access control is only compatible with the LUNA™ software client.

About Powering the SDAC

The SDAC single door access control can only be powered from a +12V DC power supply.

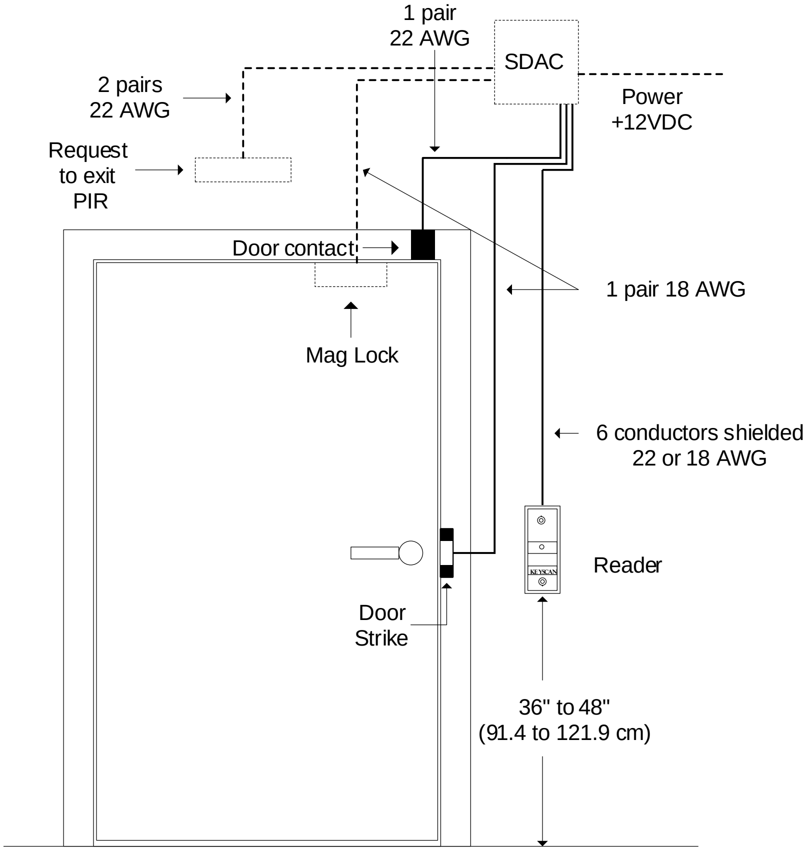
Refer to Page 32 for more about power connections and testing voltages.

Locate & Mount the SDAC

Locate the area where the SDAC and power supply are going to be mounted. Follow the mounting guidelines on the following page. We recommend a horizontal mount on a solid, smooth surface. Do not mount the access control unit close to high-voltage equipment. Comply with all local and regional codes. Record the serial number listed on the unit and the programmed IP address. The serial number and IP address are required for entry in the LUNA™ software. The SDAC includes a mounting template for drilling holes to mount the unit.

The following illustration shows a typical mounting location for the SDAC, which generally is in proximity to the door it is controlling. However circumstances may require mounting the unit farther from the door than depicted.

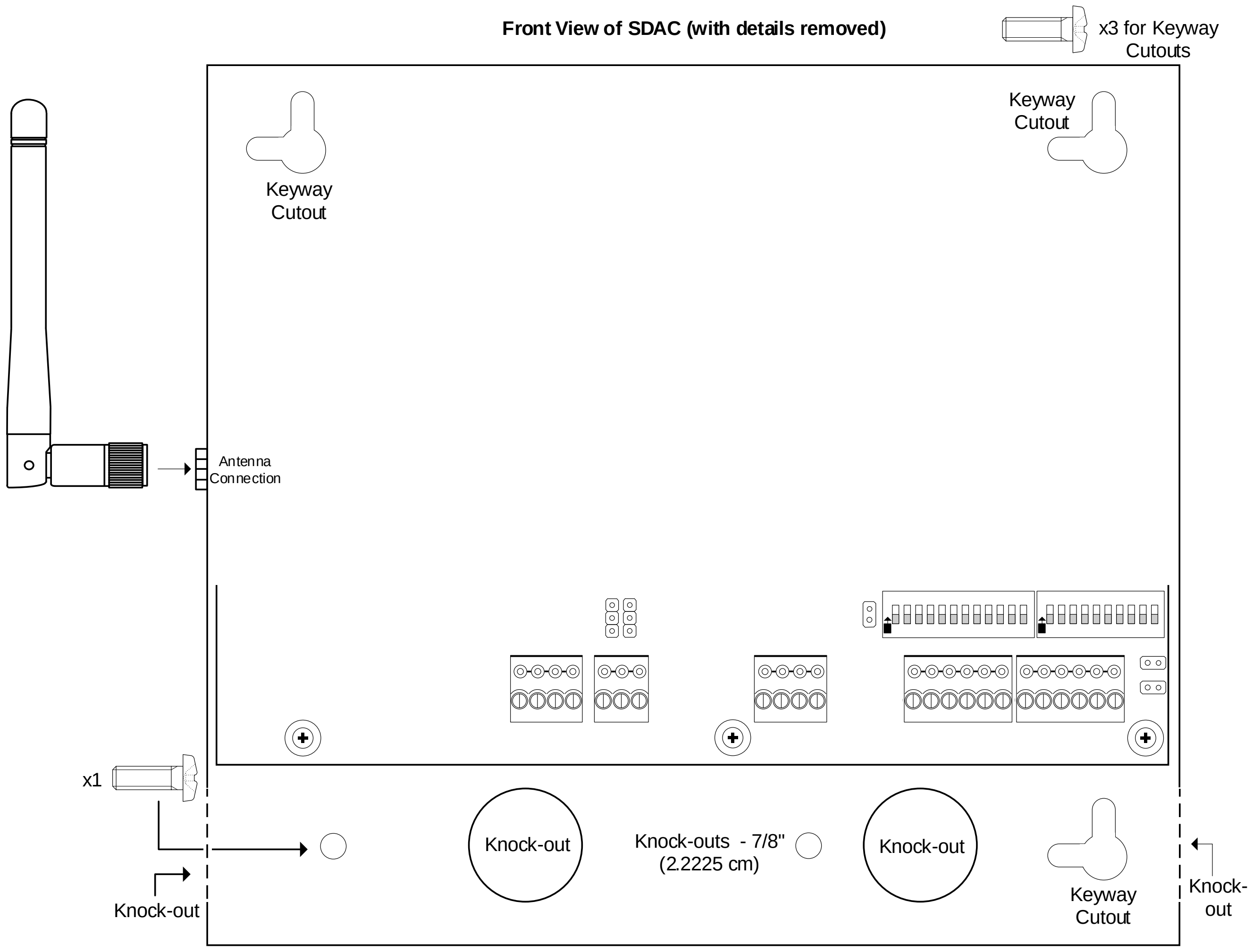
Figure 1 – Typical Door Layout



Mounting Guidelines

- Remove the front cover
- Use the enclosed mounting template and drill 4 pilot holes where indicated
- Fasten the top 2 screws and the bottom-right screw until there is a gap of approximately 1/32” between each of the screw heads and the mounting surface
- Mount the SDAC so that the 3 keyway cutouts at the back of the enclosure are over the screw heads as shown in Figure 2
- Slide the enclosure down until the 3 screws are seated at the top of the keyway cutouts
- If necessary, remove unit and adjust the screws to have the unit fit tight between the screw heads and the mounting surface, then slide the enclosure down until the 3 screws are seated at the top of the keyway cutouts
- Fasten and tighten the 4th screw in the lower-left hole

Figure 2 – Mounting the SDAC



Door Hardware & Readers

The following sub-sections review door components with related diagrams. Some jurisdictions require a qualified locksmith for installation of lock hardware. Consult with local authorities.

Door Lock Hardware

Consult with the manufacturer's documentation for mounting door lock hardware. The lock must be appropriate for the barrier and meet all applicable fire and safety codes. If necessary, consult with the proper authorities to ensure the installation conforms to municipal, state, or provincial fire regulations and building codes. Permits may be required before installing magnetic locks.

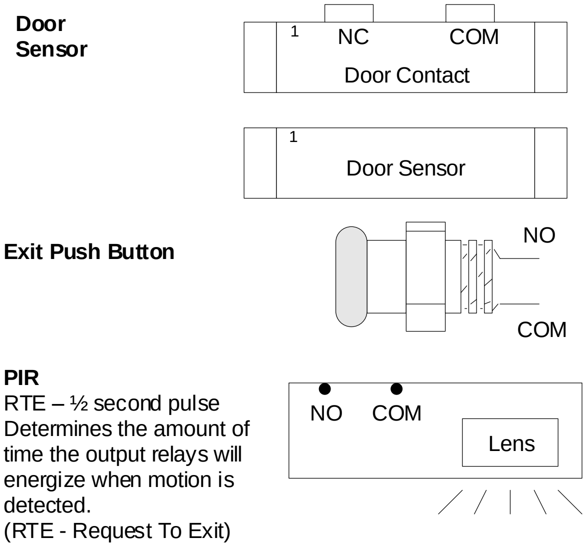
Use a battery for temporary power to ensure the door operates properly with respect to the following functions before connecting to the Keyscan SDAC.

- Alignment
- Holding
- Activation/de-activation

Door Contacts, Exit Buttons & PIRs

The following diagram illustrates the door contacts, exit buttons and PIRs. See the manufacturer's documentation for mounting instructions. Avoid running cables parallel with AC wiring or across fluorescent light fixtures; this causes AC induction and transmission interference.

Figure 3 – Door Contacts, Exit Buttons & PIRs



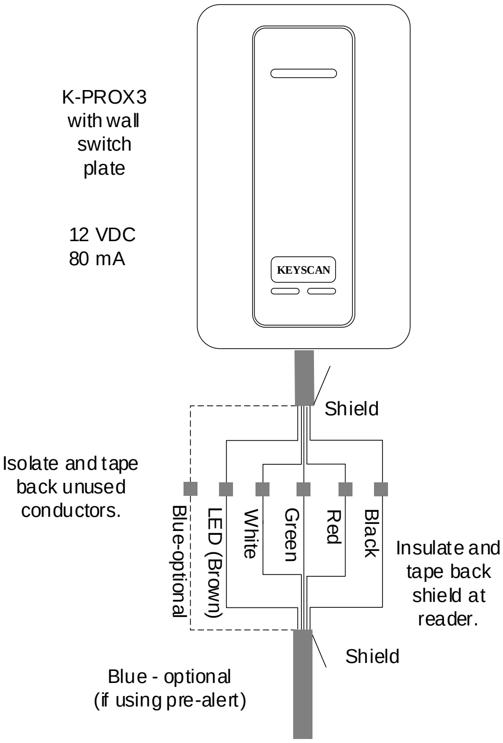
Readers

Never mount readers close to high-voltage equipment. For convenient entry, the reader should be mounted at a convenient height on the latch side of the door.

When mounting proximity readers for monitoring in and out activity at the same door, space the readers at a distance greater than the combined radio signal read ranges. As an example, if the read range is 4 inches, mount the two readers at a distance greater than 8 inches from each other.

For mounting readers to a metal surface, consult with the manufacturer's documentation.

Figure 4 – Typical Door Reader Connection



Cables & Grounding

The following table outlines system cable requirements. Please be sure to review grounding guidelines for safe system operation.

Do not connect cables at the ACU until all hardware is tested and operating correctly. Cable routes should avoid potential sources of electrical noise from fluorescent light fixtures, high-voltage equipment, high-voltage lines, and radio transmission equipment that may impede access control system communication. Avoid running access control system cables parallel with AC wires or across fluorescent light fixtures. This can cause AC induction or transmission interference.

Use specified cables with the proper gauges. Do not exceed maximum cable distances.

Table 1 – Cable Requirements

Device / Circuit Board	Signal Protocol	Maximum Distance	Cable Type	Notes
Readers to ACU	Wiegand	500 ft. 152.4 m	6 conductors shielded 22 AWG	Overall shielded cable accepted. CAT5 cable not acceptable with Wiegand signal protocol.
Door strikes & electro magnets to ACU	n/a	500 ft. 152.4 m	1 pair 18 AWG	Shielded wire not required.
Contacts & exit devices	n/a	500 ft. 152.4 m	1 pair 22 AWG	Shielded wire not required.
Motion sensors (PIR)	n/a	500 ft. 152.4 m	2 pairs 22 AWG	Shielded wire not required

Grounding

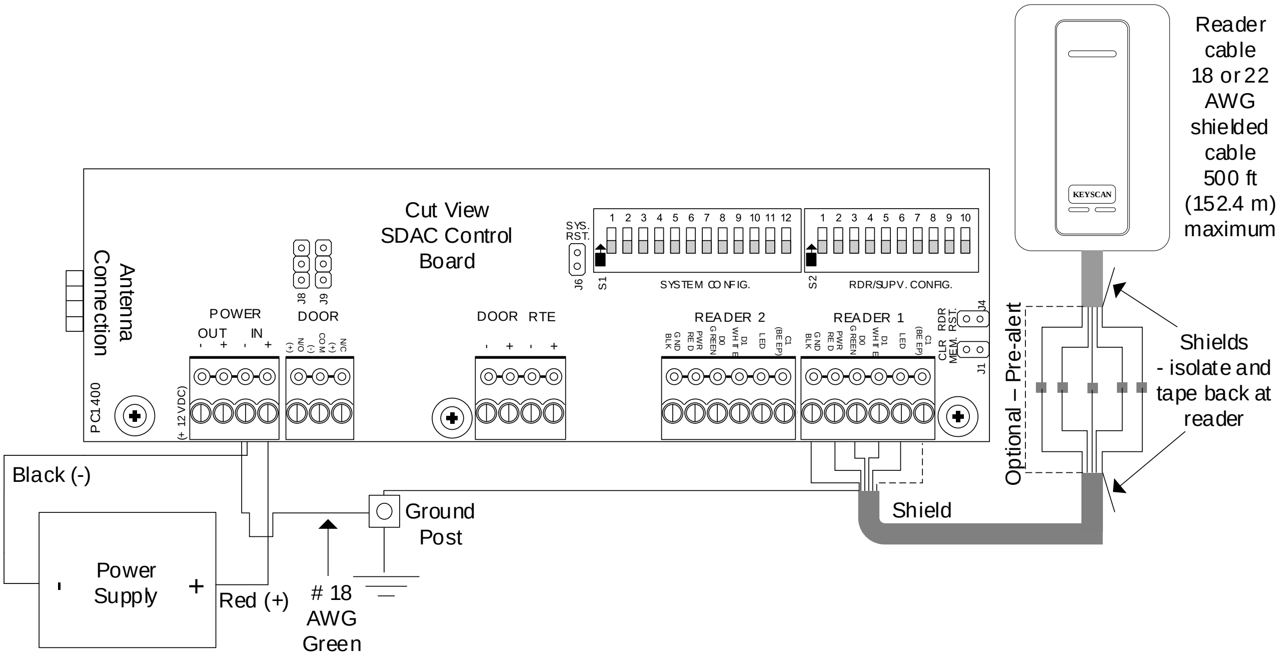
Ground the access control unit and shielded cables to a cold water pipe. Failing to ground the shields or using incorrect cables may cause noise or interference and result in improper card reads. Refer to Figure 5 – Grounding Access Control Units and Cables.

The metal enclosure includes 1 pre-mounted ground post.

Note

Keep all shield wires and cables away from the control board.

Figure 5 – Grounding Access Control Units and Cables



Terminate Wiring at the ACU

The following sub-sections review lock, input and reader wiring at the ACU.

Output Relay

The SDAC has 1 door output for terminating a door lock or magnetic lock.

Powered / Unpowered

The door output relay is fused at 500 mA. Depending on the current demand of the device connected to the output, each output must be jumpered as indicated below:

- Powered – device is powered from the SDAC relay output (500 mA or less) – Diode connected to powered device
- Unpowered – SDAC provides a dry contact, but the device requires an independent power source (over 500 mA) – Diode connected to powered device

Jumper settings are shown in the respective wiring diagrams at the end of this document.

Table 2 – Relay Specifications

Output Relay Specifications	
Relay outputs	Form C contacts, 30 VDC 4 Amps, 24 VAC 8 Amps
# of outputs	1 door output
PTC resettable fuse	500 mA per relay
Door output relay – powered/unpowered	J8 & J9

Important

Diodes are supplied with Keyscan access control unit(s).

Diodes must be connected to the device being powered from the SDAC for DC door strikes, as illustrated in the following lock diagrams on the next page. Diodes must always be used with DC locks, regardless of if the lock is powered or not.

The cathode of the diode is connected to the positive terminal of either - normally closed (NC) or normally open (NO) – depending on the lock state. The anode of the diode is connected to the common terminal. Diodes must be installed for proper operation.

NEVER use the diode with AC locks, as doing so may damage the diode.

Fail Secure/Fail Safe Lock Devices

For ‘fail-secure’ and ‘fail-safe’ door strikes, observe the following relay connections:

- ‘fail-secure’ – Connect the positive terminal on the door strike to the 'normally open' (NO) position on the door relay terminal. Connect the return wire to the common on the door relay terminal.
- ‘fail-safe’ – Connect the positive terminal on the door strike to the 'normally closed' (NC) position on the door relay terminal. Connect the return wire to the common on the door relay terminal.

Warning

Before securing any exit, please ensure all wiring to electrical door hardware conforms to federal, state, provincial, or municipal fire regulations and building codes.

Figure 6 – Terminate Magnetic Lock under 500 mA – Fail Safe

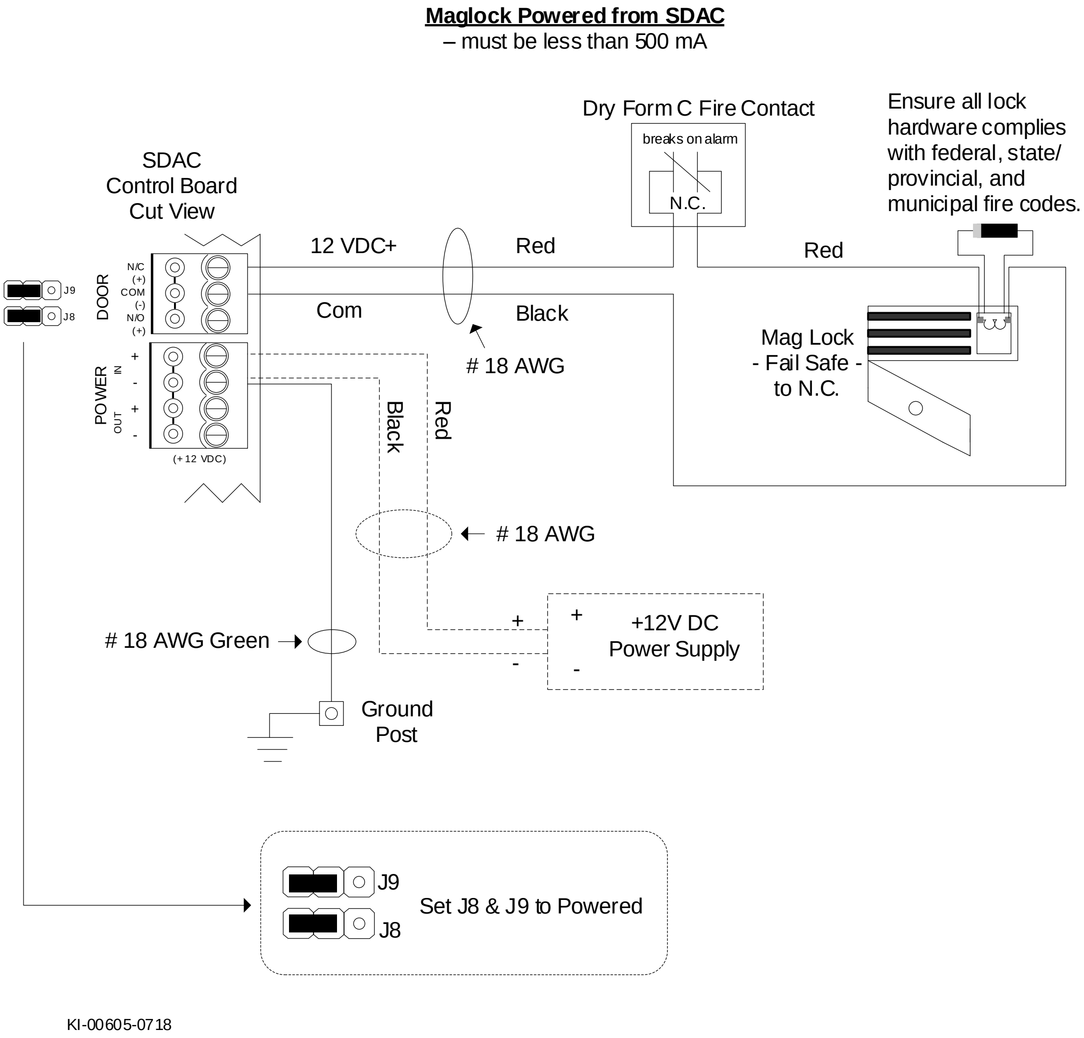
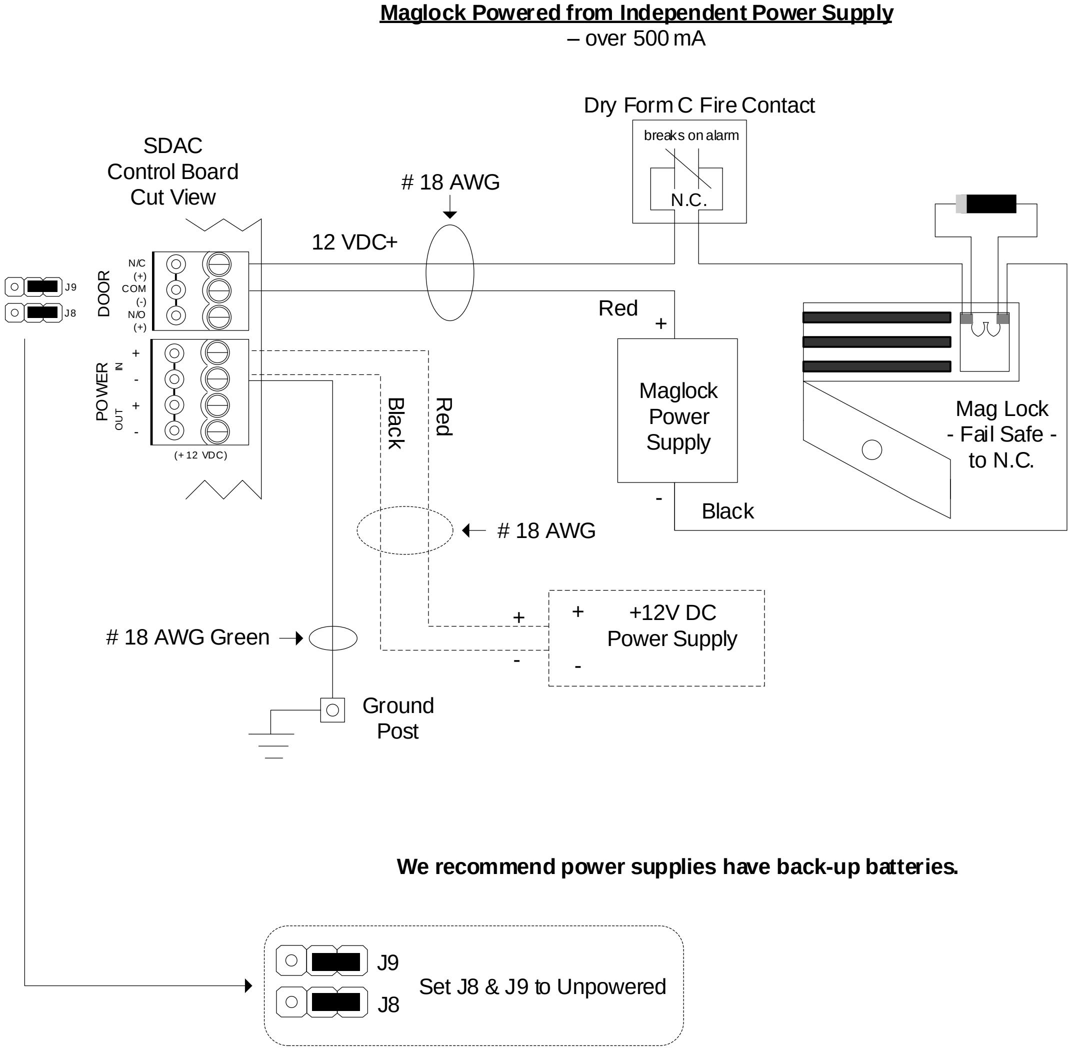


Figure 7 – Terminate Magnetic Lock over 500 mA - Fail Safe



Ensure all lock hardware complies with federal, state/provincial, and municipal fire codes.

KI-00606-0718

Figure 8 - Terminate Door Strike - 500 mA or less - Fail Safe

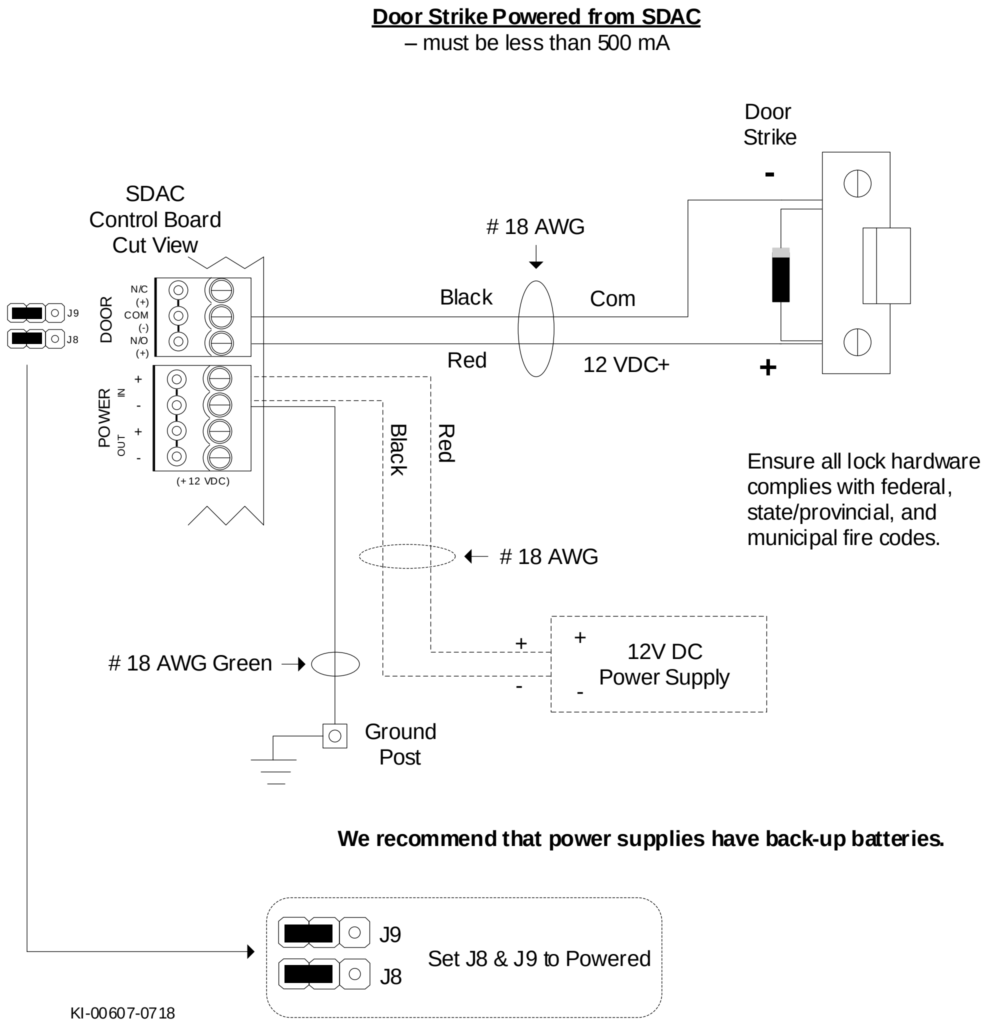
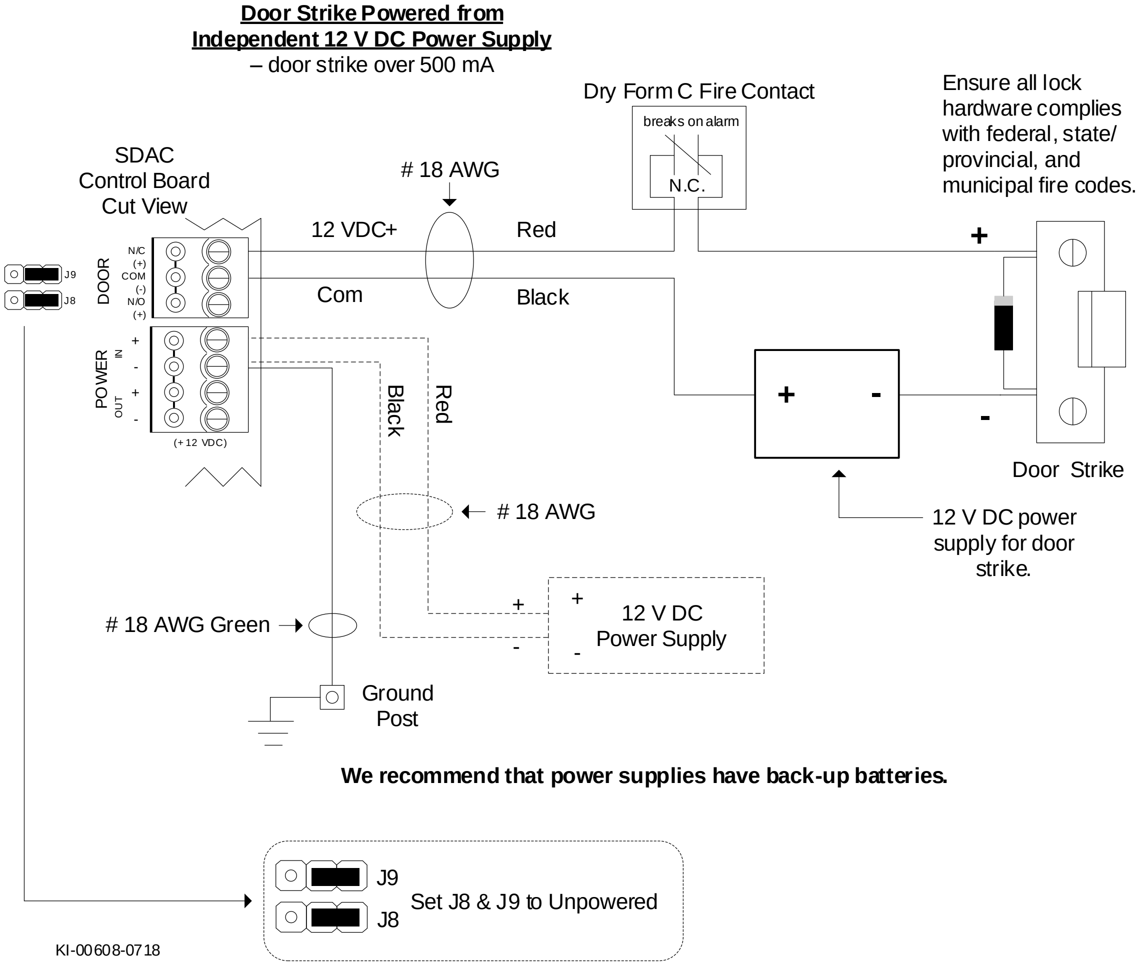


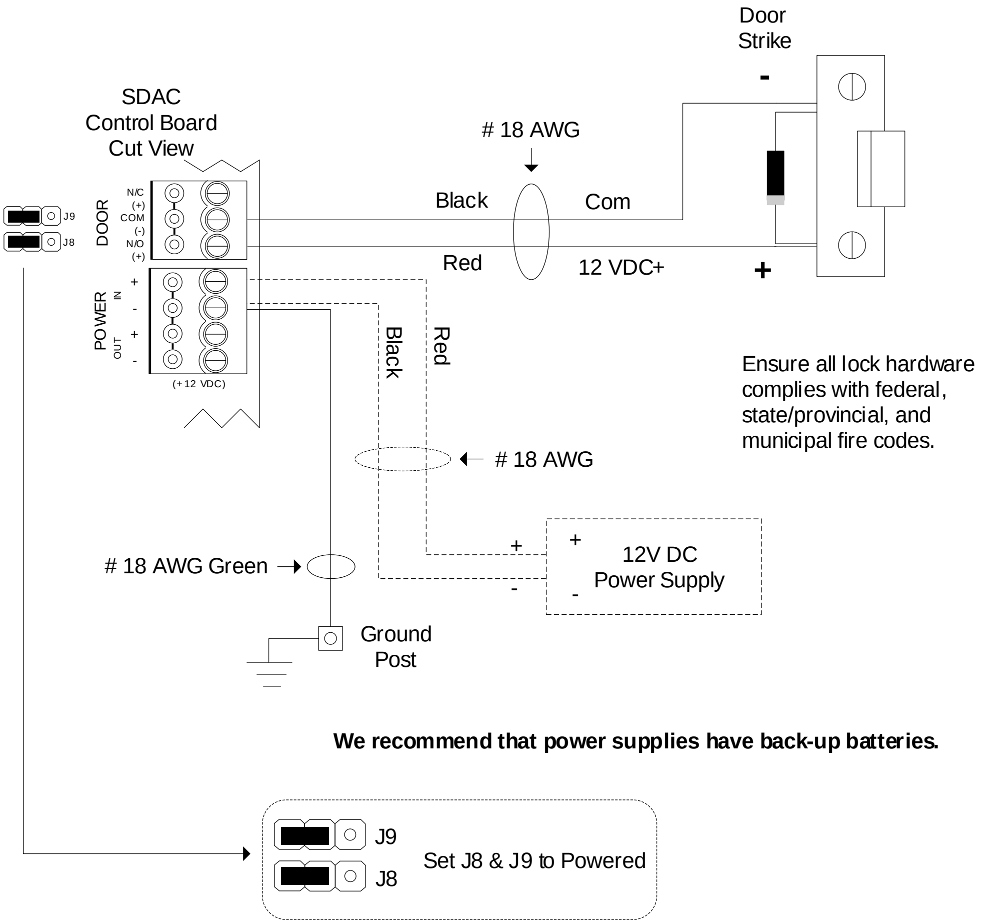
Figure 9 – Terminate Door Strike - Over 500 mA – Fail Safe



We recommend that power supplies have back-up batteries.

Figure 10 - Terminate Door Strike - Less than 500 mA - Fail Secure

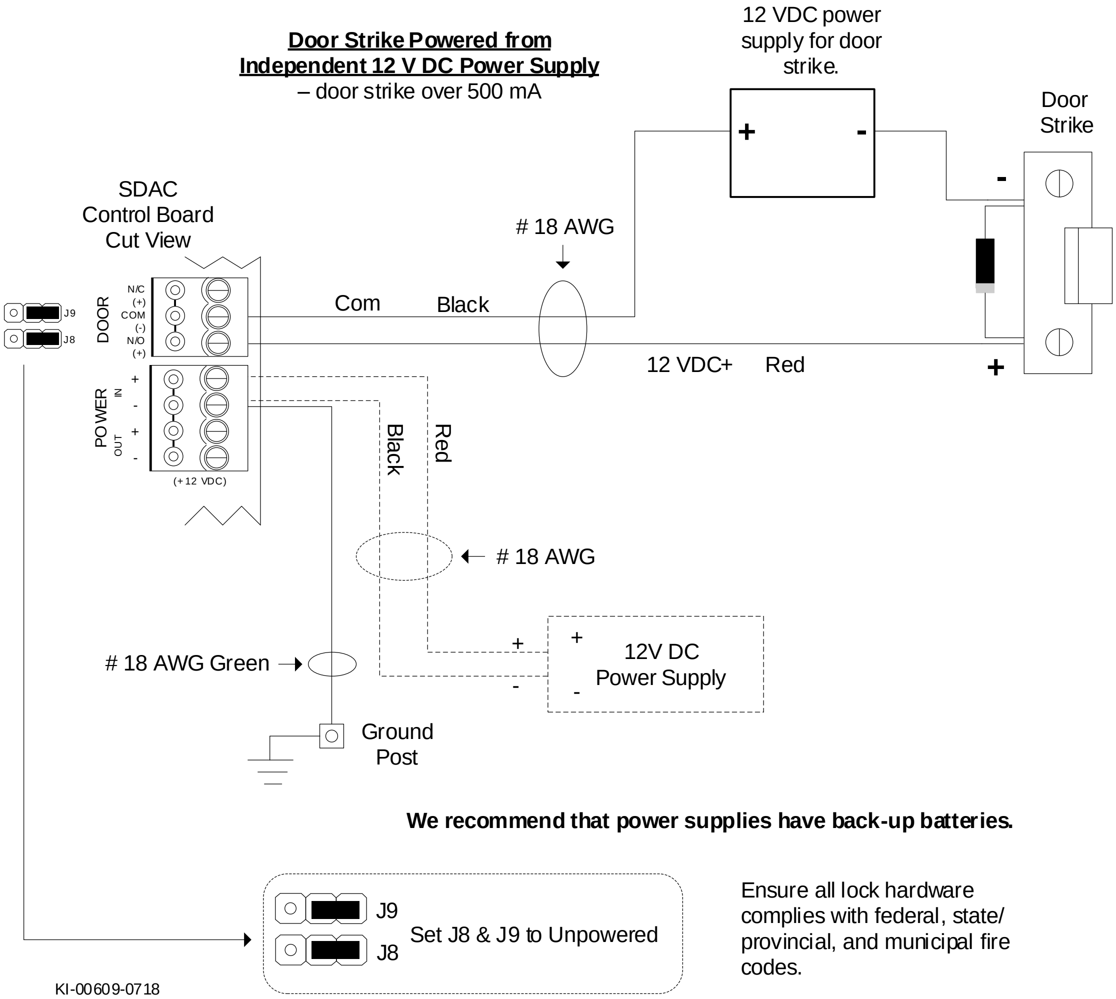
Door Strike Powered from SDAC
– must be less than 500 mA



Ensure all lock hardware complies with federal, state/provincial, and municipal fire codes.

We recommend that power supplies have back-up batteries.

Figure 11 - Terminate Door Strike - Over 500 mA - Fail Secure



We recommend that power supplies have back-up batteries.

Ensure all lock hardware complies with federal, state/ provincial, and municipal fire codes.

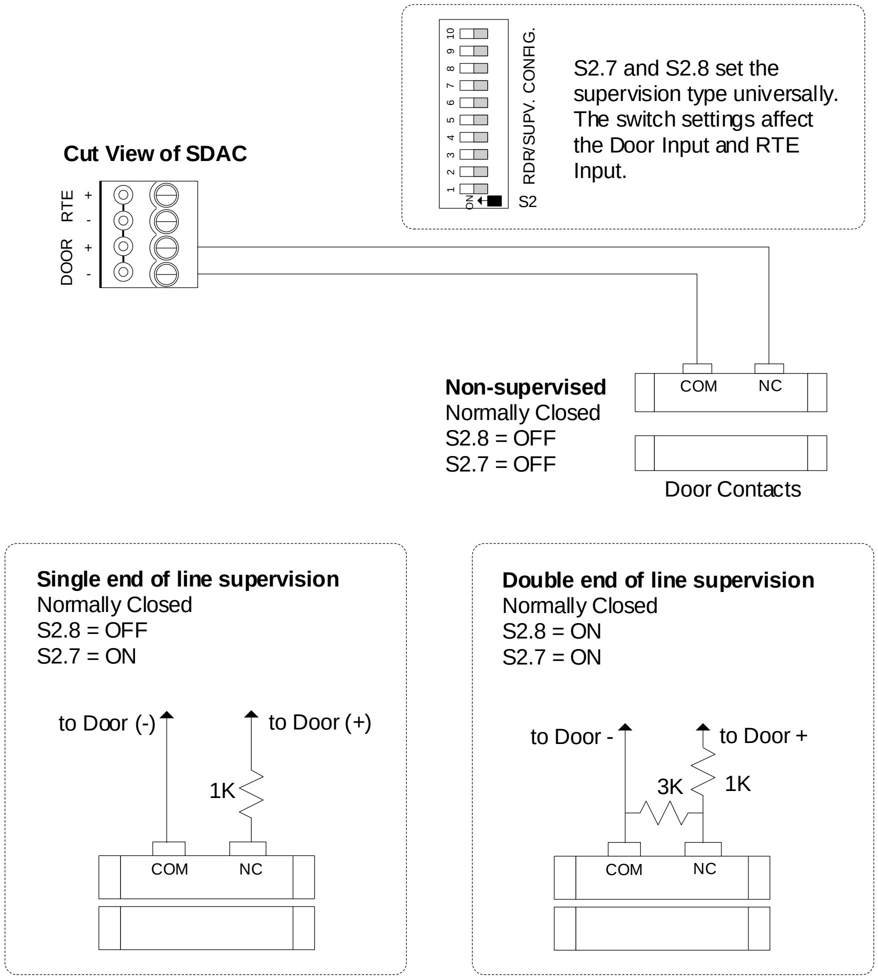
Terminate Input Wiring

The following sub-headings review termination of door and exit input wiring.

Door Monitoring Connections

A normally-closed door contact is for monitoring door security. The door input is shunted during the door relay unlock time.

Figure 12 – Terminate Input Wiring – Door Inputs (Contacts)



S2.7 and S2.8 set the supervision type universally. The switch settings affect the Door Input and RTE Input.

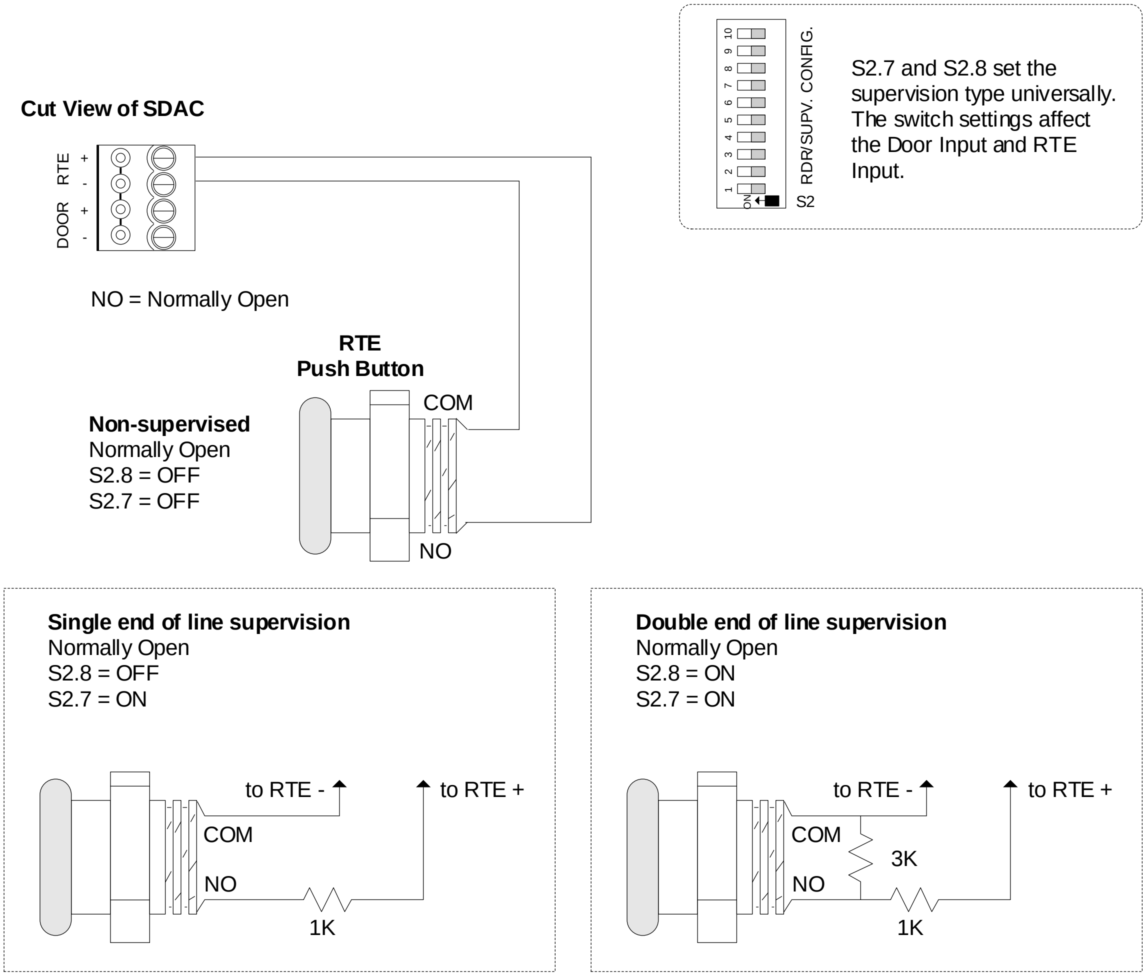
NOTE: If not using door contacts, a jumper must be installed across terminals to restore door alarm status.

Exit Device Connections

A normally-open exit device contact unlocks the door for its defined door relay unlock time and overrides the alarm input during its defined door held open time. Examples of exit devices are exit push buttons or motion sensors (PIR), etc.

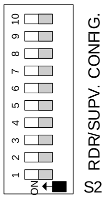
When using a motion sensor (PIR) for an exit device, we recommend a PIR with a pulse output of 1/2 second and suited to its environment.

Figure 13 – Terminate Input Wiring – RTE Push Button

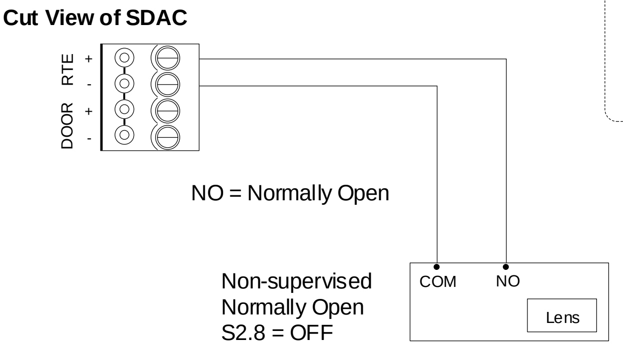


S2.7 and S2.8 set the supervision type universally. The switch settings affect the Door Input and RTE Input.

Figure 14 – Terminate Input Wiring – RTE PIR Motion Sensor



S2.7 and S2.8 set the supervision type universally. The switch settings affect the Door Input and RTE Input.



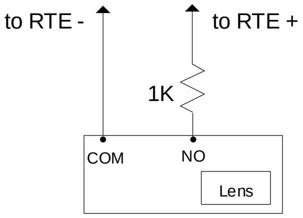
NO = Normally Open

Non-supervised
Normally Open
S2.8 = OFF
S2.7 = OFF

PIR (Request To Exit)

PIR
RTE (Request to Exit) – ½ second pulse
Determines the amount of time the output relays will energize when motion is detected.

Single end of line supervision
Normally Open
S2.8 = OFF
S2.7 = ON



Double end of line supervision
Normally Open
S2.8 = ON
S2.7 = ON

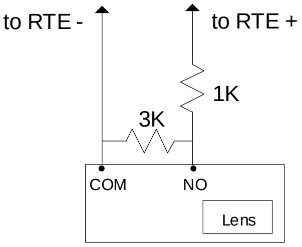
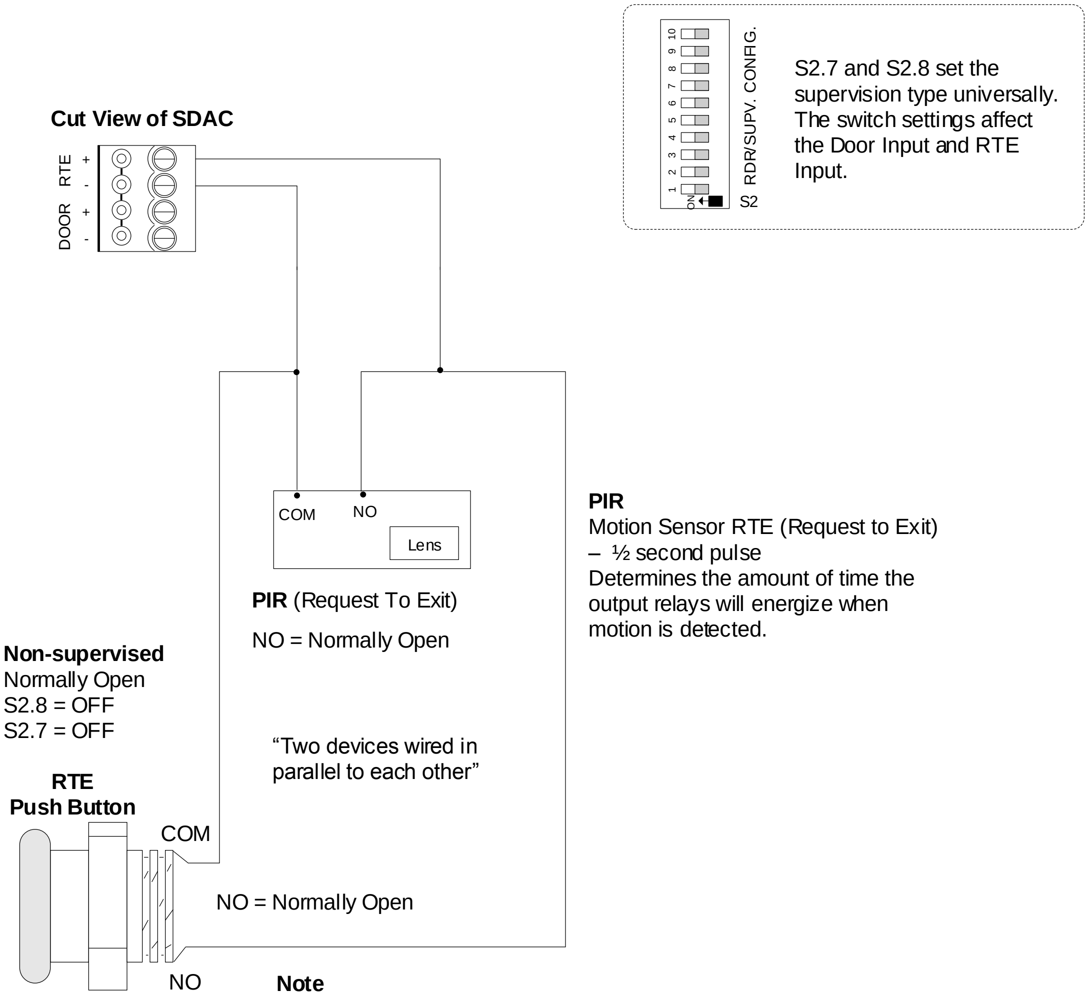


Figure 15 – Terminate Input Wiring RTE - PIR & Push Button



S2.7 and S2.8 set the supervision type universally. The switch settings affect the Door Input and RTE Input.

PIR
Motion Sensor RTE (Request to Exit)
– ½ second pulse
Determines the amount of time the output relays will energize when motion is detected.

PIR (Request To Exit)

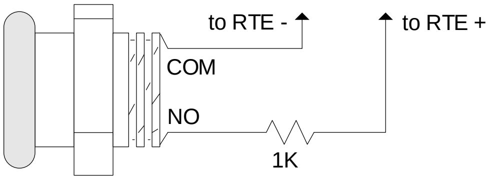
NO = Normally Open

Non-supervised
Normally Open
S2.8 = OFF
S2.7 = OFF

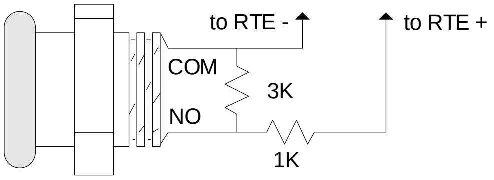
"Two devices wired in parallel to each other"

Note
If using supervision, it is only required on the device farthest from the ACU terminal. Example shows supervision on RTE Push Button.

Single end of line supervision
Normally Open
S2.8 = OFF
S2.7 = ON



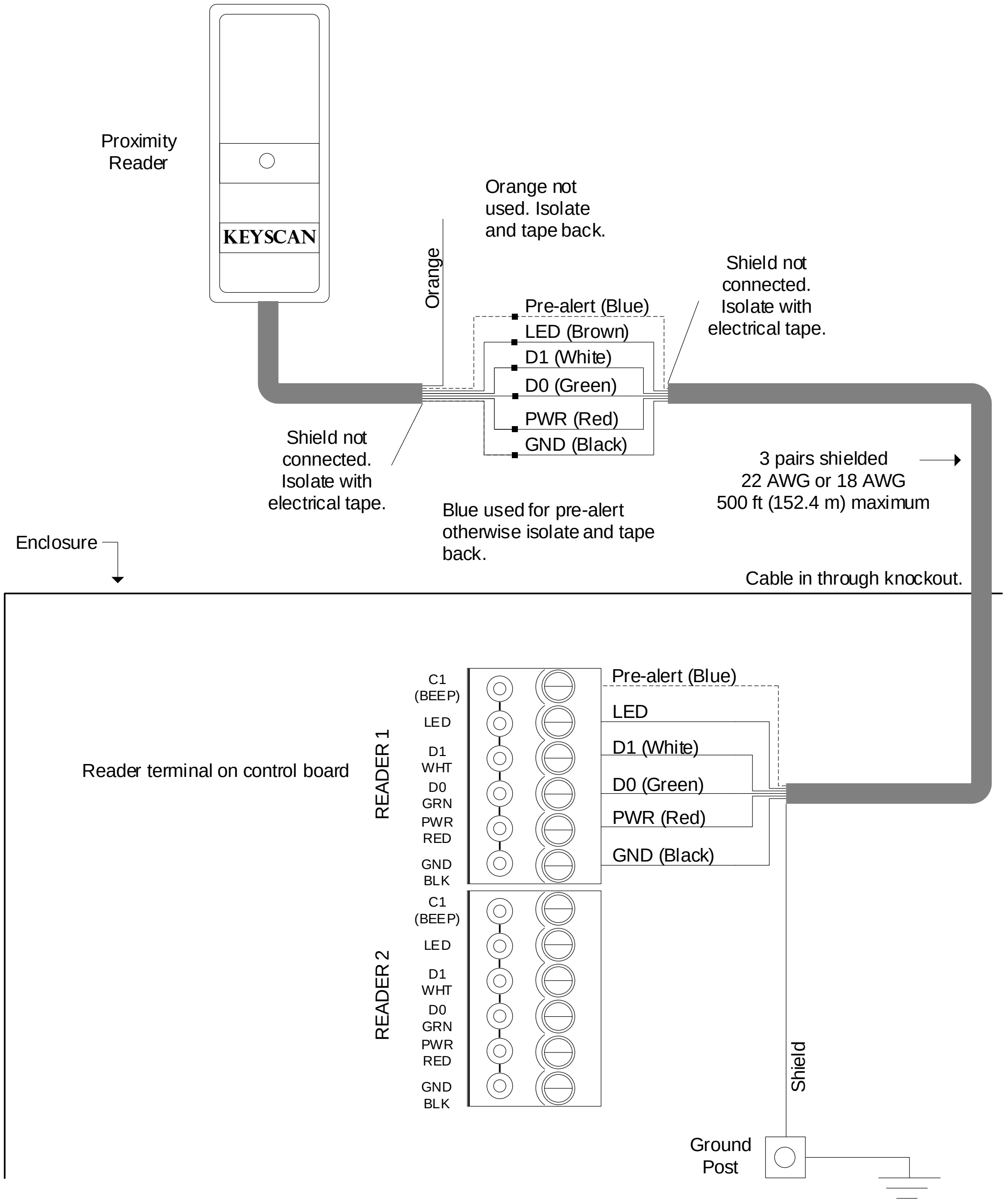
Double end of line supervision
Normally Open
S2.8 = ON
S2.7 = ON



Terminate Reader Wiring at ACU

For readers, use 6 conductors 22 AWG shielded cable or a cable with overall shielding. Use 18 AWG shielded cable for current-demanding readers. The shield wire must be connected to the earth ground post at the ACU and isolated and taped at the reader. The maximum reader distance is 500 feet (152.4 m) from the ACU when transmitting a Wiegand signal.

Figure 16 – Terminate Reader Wiring


Proximity Reader
KEYSCAN
Orange
Orange not used. Isolate and tape back.
Shield not connected. Isolate with electrical tape.
Pre-alert (Blue)
LED (Brown)
D1 (White)
D0 (Green)
PWR (Red)
GND (Black)
Shield not connected. Isolate with electrical tape.
3 pairs shielded 22 AWG or 18 AWG 500 ft (152.4 m) maximum
Blue used for pre-alert otherwise isolate and tape back.
Enclosure
Cable in through knockout.
Reader terminal on control board
READER 1
C1 (BEEP)
LED
D1 WHT
D0 GRN
PWR RED
GND BLK
Pre-alert (Blue)
LED
D1 (White)
D0 (Green)
PWR (Red)
GND (Black)
READER 2
C1 (BEEP)
LED
D1 WHT
D0 GRN
PWR RED
GND BLK
Shield
Ground Post

DIP Switch/Jumper Settings

The SDAC has DIP switches and jumpers that activate or alter specific board functions to meet installation requirements.

- System configuration DIP switches S1.1 to S1.12
- Reader configuration DIP switches S2.1 – S2.6
- Input supervision DIP switches S2.7 & S.8
- Restore factory defaults jumper J1 (Clear memory)
- System reset jumper J6
- Door relays – powered/unpowered jumpers J8/J9

Depending on the installation, some jumpers may require activation in order to enable the desired settings.

After you have installed and connected the control board with a power source, be sure to reset the factory defaults by clearing memory. This procedure is reviewed later in this section.

S1.1 – S1.12 – System Configuration DIP Switches

The following outlines the functions that system configuration DIP switches S1.1 to S1.12 regulate. Refer to Table 3 – System Configuration DIP Switch S1 Settings on page 24 for function activation and DIP switch settings. If a DIP Switch isn’t listed in this section, it isn’t used in the SDAC.

S1.2 - Communication Bit Rate Selection

The communication bit rate selection regulates the number of bits the control board processes per second. The control board may be set on one of its configurable bit rates.

S1.5 - Reader LED Mode

This sets the reader condition on the door’s lock unlock status for red & green LED type readers or red LED type readers.

S1.9 - Clear Memory Enable

The S1.9 DIP switch must be on to enable the J1 Clear Memory jumper for restoring the factory defaults.

Figure 17 – System Configuration DIP Switches S1.1 – S1.12

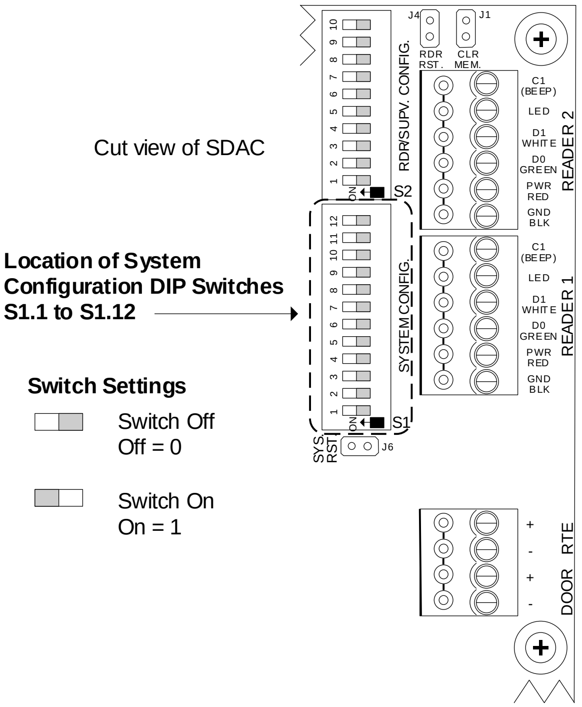


Table 3 – System Configuration DIP Switch S1 Settings (0 = OFF, 1 = ON)

S1 Switch #	Setting	Function	Notes
S1.1		**Unassigned**	
S1.2		**Communication Bit Rate**	
	0	115,200 bit/s (Default)	
	1	n/a	
S1.3		**Unassigned**	
S1.4		**Unassigned**	
S1.5		**Reader LED Mode**	
	0	Red LED type reader	
	1	Red & green LED type reader (Default)	
S1.6		**Unassigned**	
S1.7		**Unassigned**	
S1.8		**Unassigned**	

S1 Switch #	Setting	Function	Notes
S1.9		**Clear Memory Enable**	
	0	Disabled (Default)	Note – clear memory enable S1.9 activates the Clear Memory jumper J1 to reload factory defaults.
	1	Enabled	
S1.10 & S1.11		**Unassigned**	
S1.12		**Flash Program Memory Upgrade**	
	0	n/a	
	1	n/a	

S2.1 – S2.6 – Reader Format DIP Switches

DIP switches S2.1 to S2.6 set the control board for the reader format in use. Table 4 lists supported reader formats, corresponding DIP switch settings, and the security levels of the card/reader formats.

⚠

26-bit cards and tags are not secure. Duplicate card numbers exist in this format so a facility is vulnerable to unauthorized access.

Keyscan systems are factory defaulted to use Keyscan proprietary 36-bit Wiegand format cards and tags. Keyscan 36-bit proprietary Wiegand format ensures no duplicate cards or tags exist offering a high level of security.

dormakaba Canada Inc. assumes no responsibility for liability for any card format.

26-bit Waiver of Liability

Installing dealers should have an authorized end-user sign a waiver of liability before enabling 26-bit cards. dormakaba Canada Inc. has enclosed a Waiver of Liability at the back of this guide.

Advantage of Keyscan 36-bit Proprietary Wiegand Format

Keyscan 36-bit proprietary Wiegand format cards and tags, which include a manufacturer's code, offer a high level of security. Dormakaba Canada Inc. tracks all its cards and tags. This ensures that no duplicate cards or tags are sold by dormakaba Canada Inc.. When installing or upgrading a Keyscan access control system, we recommend our proprietary Keyscan 36-bit Wiegand format cards and tags, available in 125 kHz or 13.56 MHz formats, for a high level of security.

Security Levels

Table 4 on Page 28 reviews not only the supported reader formats, but also the security level of each format. Be aware that where Keyscan 36-bit proprietary cards share a combined reader format with other manufacturer's cards, the other manufacturer's card binary bits may be truncated to accommodate the joint format. This lessens the overall security, as not all bits are read.

Reader formats in Table 4 have been given one of following security ratings:

- High
- Medium
- Low

Reader formats ranked with Medium and Low are NOT recommended. The ratings are based on whether a card's binary bits are truncated and/or the cards are sold by other manufacturers, which dormakaba Canada Inc. has no control over.

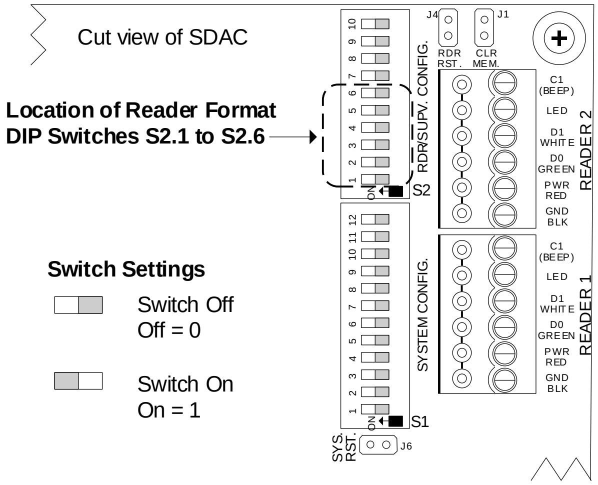
Card Number Formats

The supported card number formats fall under the following two types:

- Standard Card Number – 3 digit facility code* / 5 digit card number
  - Facility code range 1 – 255
  - Card number range 1 – 65535
- Extended Card Number – hexadecimal 0-9, A-F or decimal 0 – 9
  - Hexadecimal range 1 – FFFFFFFFFFFF
  - Decimal range 1 – 281474976710655

*The facility code may also be referred to as the site code or the batch code.

Figure 18 – Location of Reader Format DIP Switches S2.1 – S2.6



Card Number Formats

- Standard – facility code 1 – 255 / card number 1 – 65535 unless noted otherwise
- Extended – hexadecimal 1 – FFFFFFFFFFFF or decimal 1 – 281474976710655 / Checked for extended number

Reader formats apply to reader PROM version 3.4.20 or greater unless stated otherwise in the table on the next page.

Table 4 – Reader Configuration DIP Switches S2.1 – S2.6

Ref #	Reader Format	Security Level	Switch Settings S2.1 – S2.6	Card Number Format	Notes
			Off=0 / On=1		
1	Keyscan 36-bit only	High	0 0 0 0 0 0	Standard (Default)	
2	26 to 48 Pass-through Large Card Format (with first and last parity bits dropped)	Medium - Low	0 1 1 1 1 1	Extended	
3	Standard 26-bit & Keyscan 36-bit	Low	1 0 0 0 0 0	Standard	

S2.7 & S2.8 - Supervision Mode DIP Switches

The SDAC supports 3 types of input supervision as listed in Table 5. DIP switches S2.7 and S2.8 regulate the level of supervision universally for the door contact and the request to exit. All inputs must be the same type.

Figure 19 – Supervision Mode DIP Switches S2.7 & S2.8

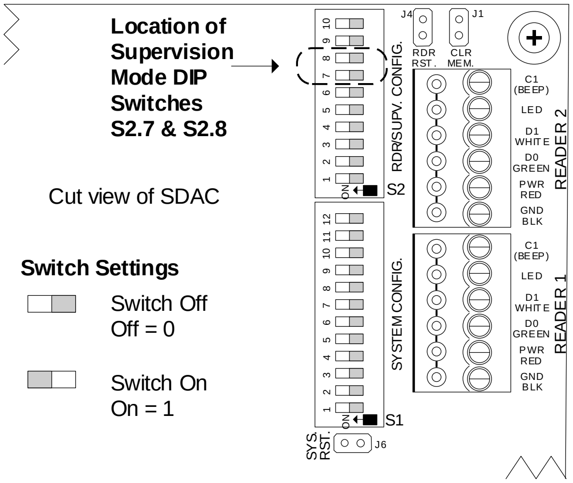


Table 5 – Supervision DIP Switch S2.7 & S2.8 Settings

S2 Switch #	Settings		Function
S2.7 & S2.8	Off=0 / On=1		**Supervised Input Mode**
	S2.7	S2.8	
	0	0	Non-supervised input or digital input (Default)
	1	0	Single end of line supervision
	1	1	Double end of line supervision

J1 - Restore Default Settings/Clear Memory

Jumper J1 is used to restore the control board's factory default settings. You must restore the factory default settings whenever one or more of the following procedures are undertaken on the SDAC control board:

- when a control board has been newly installed
- when the SDAC has had a flash memory upgrade

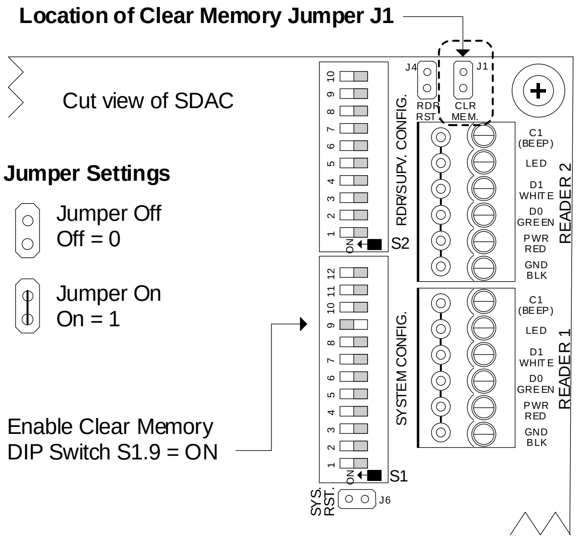
<u>Procedure</u>

To restore the factory default settings, ensure the control board has power, enable DIP switch S1.9, short J1 momentarily, and then disable DIP switch S1.9.

After placing the jumper on J1, the system status LED begins flashing red and the control board's piezo emits a cycle of 2 short beeps followed by a pause. This occurs for approximately 2 minutes while the factory default settings are loaded and the database information is erased from the on-board memory. Do not make any changes to the control board, such as altering jumpers or powering down the board, while the factory defaults are being restored or you will have to repeat the procedure. After the system status LED has stopped flashing, the factory default settings have been restored and the Keyscan database has been cleared from the on-board memory. After you have restored the factory defaults, perform an upload from a PC with a LUNA™ Client module so the Keyscan database is transferred to the control board's on-board memory.

If this is a new installation, enter the site information in the LUNA™ software and then sync the Keyscan database information to the control board(s). Until you perform a sync from LUNA™, the access control unit(s) will not function.

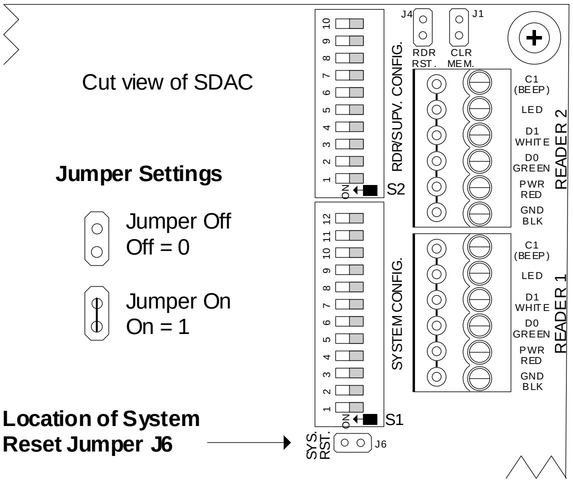
Figure 20 – Restore Default Settings (Clear Memory) J1 Location



J6 - System Reset

Excluding the changes outlined under Restore Default Settings on the preceding page, whenever you have changed the DIP switches or altered jumpers on the SDAC control board while it is powered, perform a system reset by momentarily placing a jumper on J6.

Figure 21 – Location of System Reset Jumper J6



Door Outputs – Powered/Unpowered

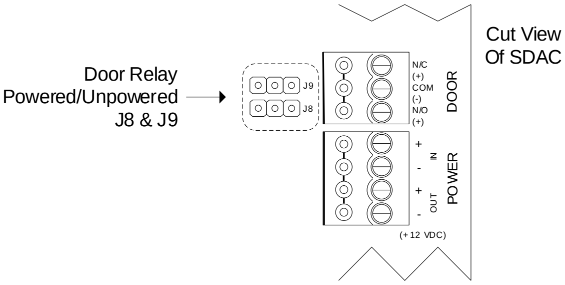
The door output relay is fused at 500 mA. This output has a set of jumpers which configures the output to source power from the SDAC or configures the output as a dry contact. When the output is configured as a dry contact, the connected device requires an independent power source.

Table 6 - Powered/Unpowered Jumper Settings for Door Outputs

Output	Device Current	Power Source	Relay Contacts	Jumpers	Settings
Door	500 mA or less	SDAC via +12 VDC	Powered (Default)	J8 J9	○■■ ○■■
	Over 500 mA	Independent power supply	Unpowered	J8 J9	■■○ ■■○

Note: Unpowered relays will have the following rating: Form C Limit of 30 VDC 4 Amps or 24 VAC 8 Amps.

Figure 22 - Location of Door Relay Powered/Unpowered Jumpers



Communication

Communication must be established between the PC/server with the LUNA™ software and the SDAC access control. The SDAC control unit is wireless only.

Single Control Unit Communication Only

The SDAC is designed as a single, stand-alone control unit; it does not support CIM, CB-485 or CPB-10-2 connections to other control units. The SDAC does not support global functions.

Communication Between SDAC and LUNA™

The following contains the steps you need to take to set up your unit to communicate with your LUNA™ software.

Step 1: Connect to the Wireless Module Via WiFi Soft A/P

By connecting to the on-board wireless module, the SDAC can be configured to communicate with the LUNA™ software. Observe the following steps:

1. On the Windows task bar, locate the network information icon. Under Wireless Network Connection, locate “XpicoWiFi_” followed by the last 6 characters of the SDAC MAC Address (found on the unit). Select the network and press the Connect button.
2. The Network pop-up window will require a Security Key to continue. The Security Key is “XPICOWIFI” exactly as shown. Select the OK button to continue.

Step 2: Connect to the SDAC Wireless Network

Follow these steps to connect to the SDAC wireless network:

1. Open any internet browser on the computer and type in the IP address of the unit into the address bar. If doing this for the first time, the default IP Address is 192.168.0.1.
2. The web browser will prompt for a user name and password in order to proceed. The User Name is "SDAC" and the password is the serial number of the access control unit (exactly as shown in all caps).
3. After successfully logging in, continue to the next step.

Step 3: Set Up Your AES Credential

Follow these steps to set up the AES credentials:

1. Click on the AES Credentials tab.
2. Click on the link to edit the LunaCredential AES credential.
3. On the AES Credential Configuration screen, you will need to overwrite the existing Encrypt Key and Decrypt Key. These keys need to match the Encryption key in the LUNA™ software.
4. Open the LUNA™ application. Navigate to the Settings menu. Enter the required value in the Encryption Key field (64 characters) and then save. Copy the key value. Then head back to the SDAC menu, paste this value into both the Encrypt Key and Decrypt Key fields.

5. Once you provided the Encrypt and Decrypt Key values, a Submit button will appear. Select the Submit button to save the encryption key values for the AES credential.

   WARNING: Do NOT delete the AES Credential once created. Doing so may have adverse effects on the SDAC unit.

6. Prior to ACU configuration, the unit must first be reset for the settings to be applied before communicating with the LUNA™ software.

Step 4: Configure the IP & Network Settings

There are two ways to configure the SDAC to communicate with the LUNA™ software: Directly through point-to-point and indirectly through a wireless network.

Observe these steps for a point-to-point connection:

1. Open the LUNA™ Web Portal and click on the Network button. Select the ap0, Interface and Configuration buttons so that each is highlighted green instead of blue.

2. In the IP Address field, the default IP Address can be changed to the preferred value.

3. Select the Submit button once changes are made.

Observe these steps for a wireless network connection:

1. Open the LUNA™ Web Portal (from Step 2: Connect to the SDAC Wireless Network). Select the wlan0, Interface and Configuration buttons so that each is highlighted green instead of blue.

2. This screen provides various Configuration fields that can be changed to suit your network setup. Contact your Network Administrator for assistance.

3. Select the Submit button once changes are made.

Step 5: Configure the Access Control Software

Once you have completed the previous steps, your unit is configured to communicate with the LUNA™ software. Proceed to the LUNA™ software to continue setting up your access control in the Hardware setup menu. You can also add People/Cards so that they can start gaining access to your door.

Power-up & Test Voltages

The SDAC can only be powered via a +12V DC power supply. We recommend the SDAC power to be supplemented with an appropriate backup battery and battery charging circuit, ensuring continued operation in the event of a power failure.

Power Supply Requirements

(Typical max current draw of all connected devices = 680mA)

+

(Reserve current to handle peaks = 200mA)

=

Required ampacity of power supply (Typical 880mA)

Note: A +12V DC power supply with standby battery/charging capabilities should reach the minimum rating of the selected power supply, unless externally powering other devices, such as long RFID range readers. Lock choices will also increase power supply requirements.

Current Output Limits of SDAC outputs:

- (PTC Resettable Fuses)
- Reader port 1 – 500 mA
- Reader port 2 – 500 mA
- Door output – 500 mA

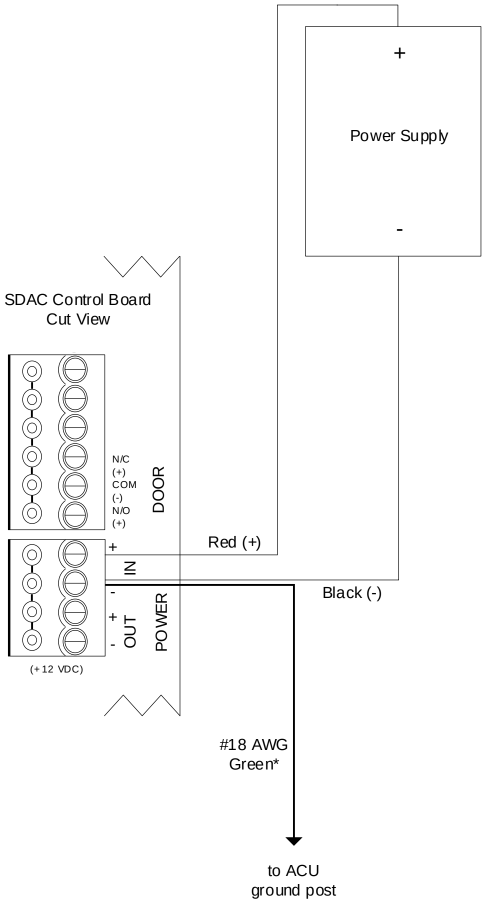
System Power-up

After the control board is powered up for the first time, be sure to reset the factory defaults by performing a clear memory procedure outlined on Page 23. After the control board is installed, powered and tested, return to a PC/server with the LUNA™ software and Home screen. From there, call up the Status screen and sync the panel manually.

DC Power Supply +12V DC

- Connect the +12V DC power supply to the POWER IN terminals (TB6) on the SDAC.
    - Upon applying power, the SDAC begins booting-up. The system status LED illuminates in amber and the on-board piezo emits a beep.
- Using a voltmeter, check the following terminals on the SDAC for +12V DC:
    - Reader 1 – PWR RED
    - Reader 2 – PWR RED
    - POWER OUT + (TB6)
    - DOOR output N/C or N/O (if set on POWERED)

Figure 23 – Power Supply Wiring



Control Board Voltage Test Points

The following table lists the correct voltages for the test points on the control boards. Be sure to comply with proper measuring techniques as noted.

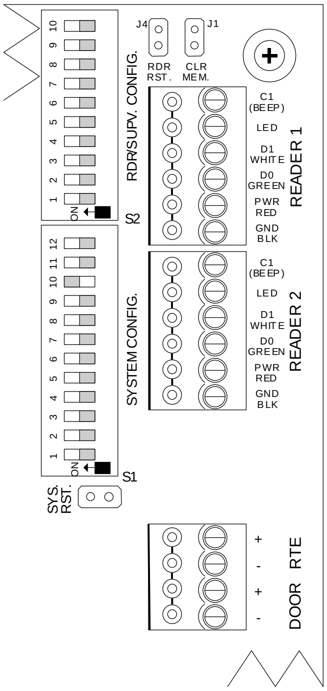
Voltmeter Connections

- Voltmeter set to VDC
- V-Ω (ohms) to test points
- Com to ground post in metal enclosure

Table 7 – Control Board Test Points - Voltages

Board Test Point	Voltage	Instructions/Notes
Reader Terminal		
D1 WHT	(+) 5 VDC	White data 1 – if reader connected
D0 GRN	(+) 5 VDC	Green data 0 – if reader connected
PWR RED	(+) 12VDC	Red DC out
Input Points		
Input points with open circuit	(+) 5 VDC	
Input points shorted to common return	0 VDC	

Figure 24 – Control Board Test Points – Voltages



Diagnostics

The SDAC has communication and system status LEDs for diagnostics.

Communication LEDs

The SDAC has on-board LEDs for communication diagnostics outlined in the table below. If calling dormakaba Canada Inc. for technical support, indicating the state of the LED assists our technicians in isolating potential difficulties.

Table 8 – Communication LEDs

CA150 Control Board		
LED	**State of LED**	**Notes**
TD 1 - Green	Flashing – normal	Main processor sending data to on-board supervised inputs processor
	Not Illuminated – abnormal condition	Troubleshoot all possibilities. As a last resort, follow restore factory defaults J1 procedure in attempt to resolve
	Illuminated – abnormal condition	Troubleshoot all possibilities. As a last resort, follow restore factory defaults J1 procedure in attempt to resolve
RD 1 - Red	Flashing – normal	Main processor receiving data from on-board supervised inputs processor
	Not Illuminated – abnormal condition	Troubleshoot all possibilities. As a last resort, follow restore factory defaults J1 procedure in attempt to resolve
	Illuminated – abnormal condition	Troubleshoot all possibilities. As a last resort, follow restore factory defaults J1 procedure in attempt to resolve Possible wiring fault
TD 2 – Green	Flashing – normal	Control board sending data via wireless communication
	Not Illuminated	If the LUNA™ software is not polling the control board
	Illuminated – abnormal condition	Troubleshoot all possibilities. As a last resort, follow restore factory defaults J1 procedure in attempt to resolve
RD 2 – Red	Flashing – normal	Control board receiving data via wireless communication
	Not Illuminated	If the LUNA™ software is not polling the control board
	Illuminated – abnormal condition	Possible wiring fault

System Status LED

System status is a tri-colour LED – red, amber and green – indicating the current system status as outlined. The control board also has a piezo that emits audible tones under certain LED states.

Table 9 - System Status LED

LED Colour/State	System Status
Red – solid	The main processor is held in reset and not operating. This can be caused by a jumper installed on J6 or by the main processor supervisory circuit if critical PCB voltages are not within normal operating parameters. The on-board piezo emits a steady tone while in this mode.
Red – flashing	The control board is in clear memory mode. The on-board piezo emits a cycle of 2 short beeps and then a pause while the control board is in this mode.
Amber – solid	The control board has not communicated to the LUNA™ software since its last system reset or clear memory.
Amber - flashing	The control board's last communication with the LUNA™ software was 3 minutes or greater.
Green – solid	The control board has communicated to the LUNA™ software since its last system reset or clear memory

Keyscan Readers

This section reviews typical connections for Keyscan readers. Wiring diagrams are on the following pages. Refer to the appropriate diagram for specific reader connections. Be sure to use a cable that complies with the reader's wiring specifications.

Power Specifications

The following table outlines Keyscan reader power requirements.

Table 10 – Keyscan Reader Power Specification

Reader	Power	Notes
K-PROX3	12V DC, 80 mA	(125 KHz HID compatible)
K-VAN	12V DC, 90 mA	(125 KHz HID compatible)
K-KPR	12V DC, 115 mA	(125 KHz HID compatible)
K-SMART (13.56 MHz)	12V DC, 210 mA	
K-SMART3	12V DC, 125 mA	

Installation Notes on Proximity Readers

Do not run reader cables in the same conduit with AC power or signal cables. Keep reader cables at least 12 inches or 30 centimetres from AC, computer data, telephone data, or electric lock device cables. Do not install readers within 3.5 feet or 1.1 metres of computer CRTs. Do not install readers where broad spectrum EMI noise may be present. Motors, pumps, generators, and AC switching relays can create EMI noise. Readers mounted on a metal surface can have reduced read ranges. See OEMs manual for operational details and recommendations.

Figure 25 – Keyscan K-PROX3

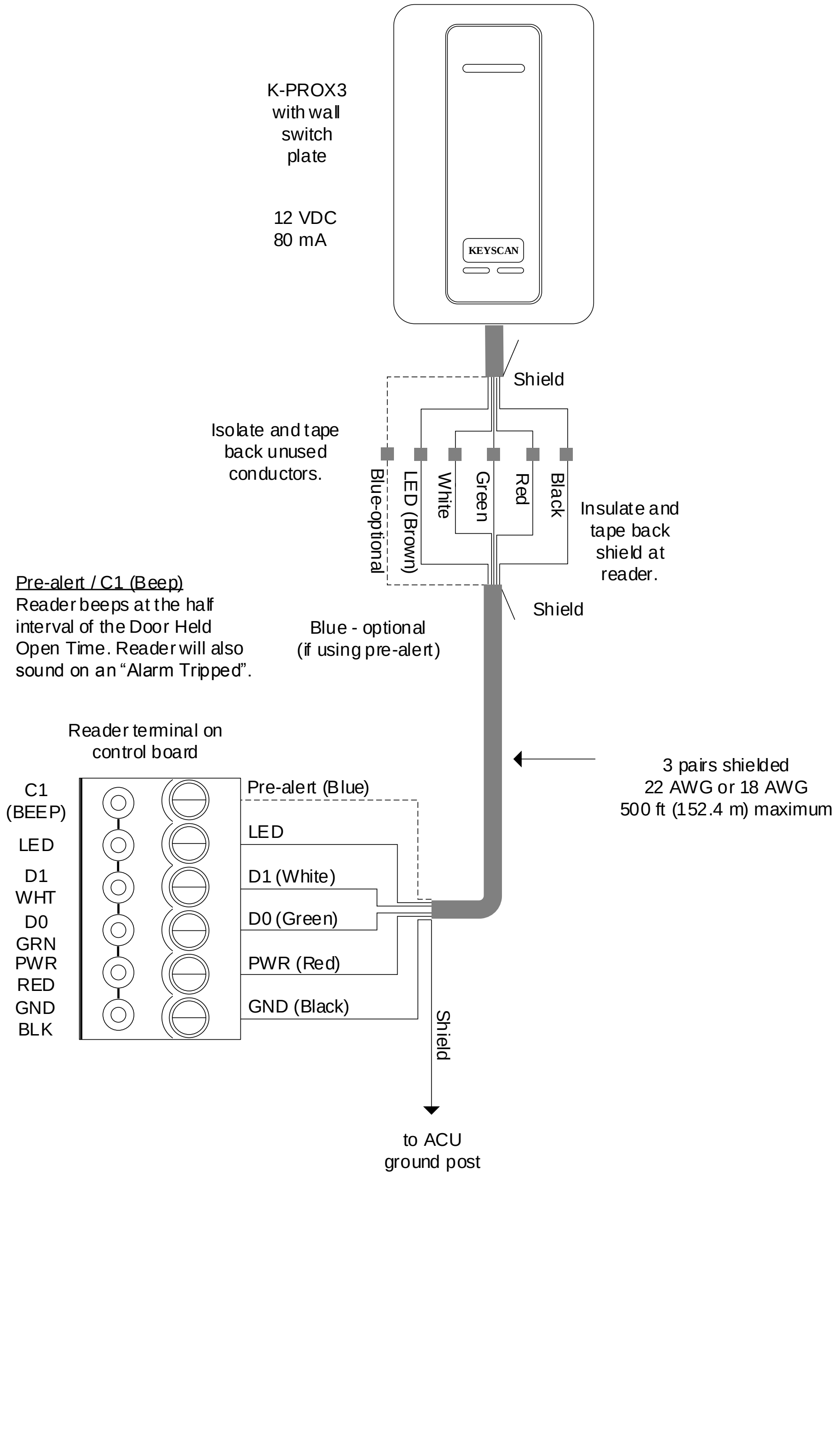


Figure 26 – Keyscan K-VAN Proximity Reader (125 kHz)

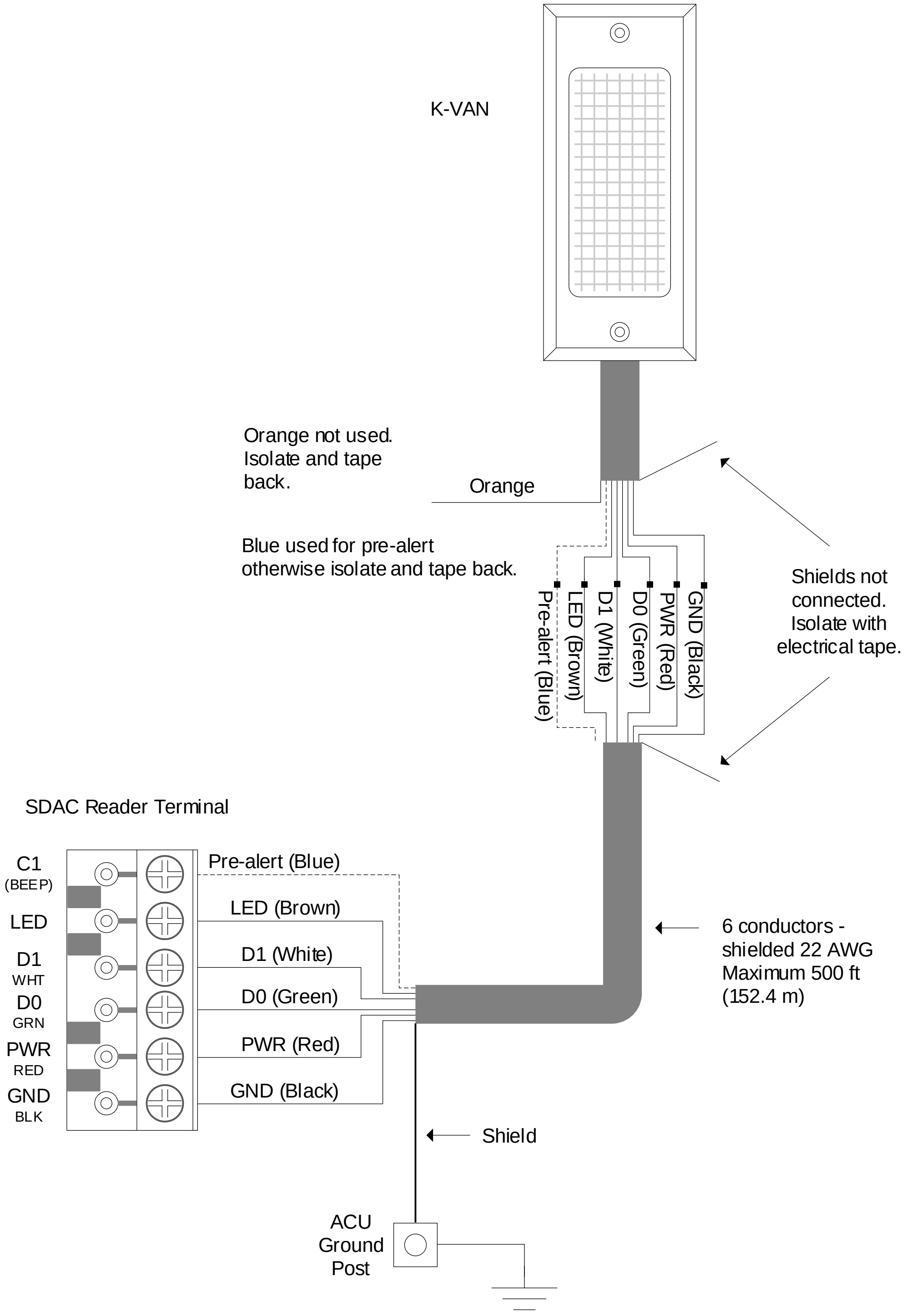


Figure 27 – Keyscan K-KPR Keypad / Proximity Reader (125 KHz)

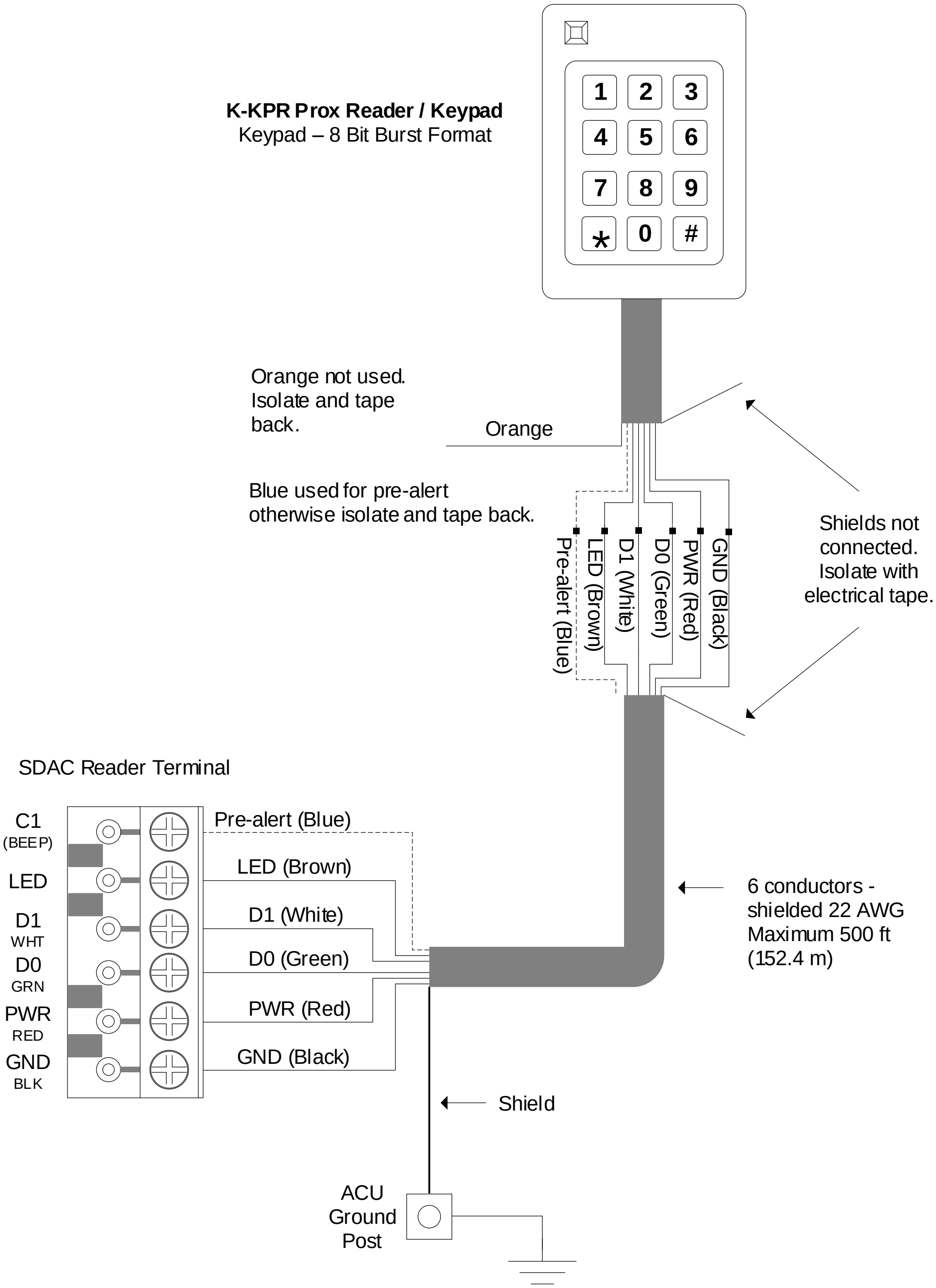
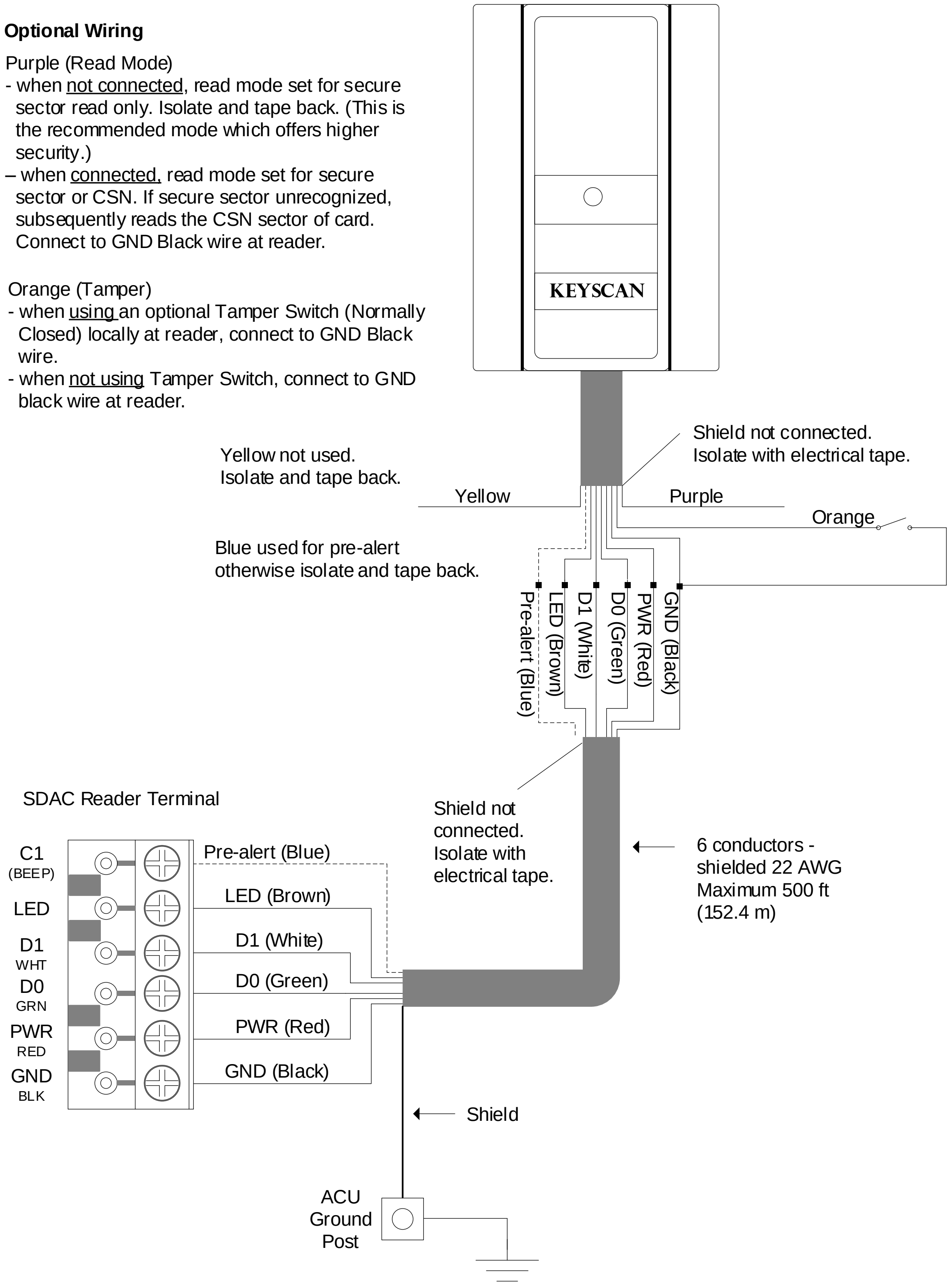

K-KPR Prox Reader / Keypad
Keypad – 8 Bit Burst Format
1
2
3
4
5
6
7
8
9
*
0
#
Orange not used. Isolate and tape back.
Orange
Blue used for pre-alert otherwise isolate and tape back.
Pre-alert (Blue)
LED (Brown)
D1 (White)
D0 (Green)
PWR (Red)
GND (Black)
Shields not connected. Isolate with electrical tape.
SDAC Reader Terminal
C1
(BEEP)
LED
D1
WHT
D0
GRN
PWR
RED
GND
BLK
Pre-alert (Blue)
LED (Brown)
D1 (White)
D0 (Green)
PWR (Red)
GND (Black)
6 conductors - shielded 22 AWG Maximum 500 ft (152.4 m)
Shield
ACU Ground Post

Figure 28 – Keyscan K-SMART Reader



Optional Wiring

Purple (Read Mode)

- when not connected, read mode set for secure sector read only. Isolate and tape back. (This is the recommended mode which offers higher security.)

– when connected, read mode set for secure sector or CSN. If secure sector unrecognized, subsequently reads the CSN sector of card. Connect to GND Black wire at reader.

Orange (Tamper)

- when using an optional Tamper Switch (Normally Closed) locally at reader, connect to GND Black wire.
- when not using Tamper Switch, connect to GND black wire at reader.

Yellow not used. Isolate and tape back.

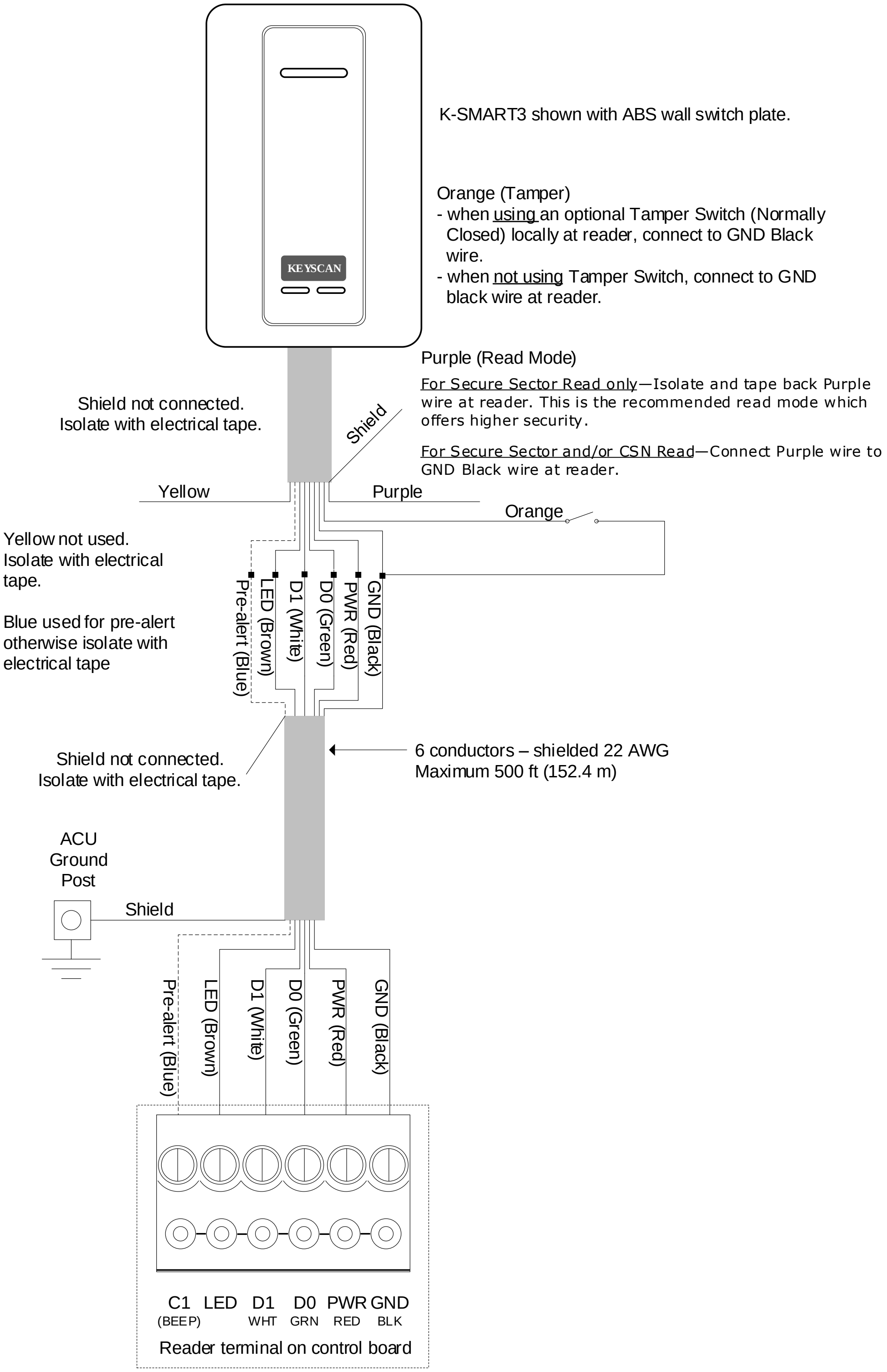
Shield not connected. Isolate with electrical tape.

Blue used for pre-alert otherwise isolate and tape back.

Shield not connected. Isolate with electrical tape.

6 conductors - shielded 22 AWG Maximum 500 ft (152.4 m)

Figure 29 – Keyscan K-SMART3 Reader



K-SMART3 shown with ABS wall switch plate.

Orange (Tamper)
- when using an optional Tamper Switch (Normally Closed) locally at reader, connect to GND Black wire.
- when not using Tamper Switch, connect to GND black wire at reader.

Purple (Read Mode)

For Secure Sector Read only—Isolate and tape back Purple wire at reader. This is the recommended read mode which offers higher security.

For Secure Sector and/or CSN Read—Connect Purple wire to GND Black wire at reader.

Shield not connected.
Isolate with electrical tape.

Yellow not used.
Isolate with electrical tape.

Blue used for pre-alert otherwise isolate with electrical tape

6 conductors – shielded 22 AWG
Maximum 500 ft (152.4 m)

Shield not connected.
Isolate with electrical tape.

SDAC Quick Reference

Figure 30 – SDAC Control Board

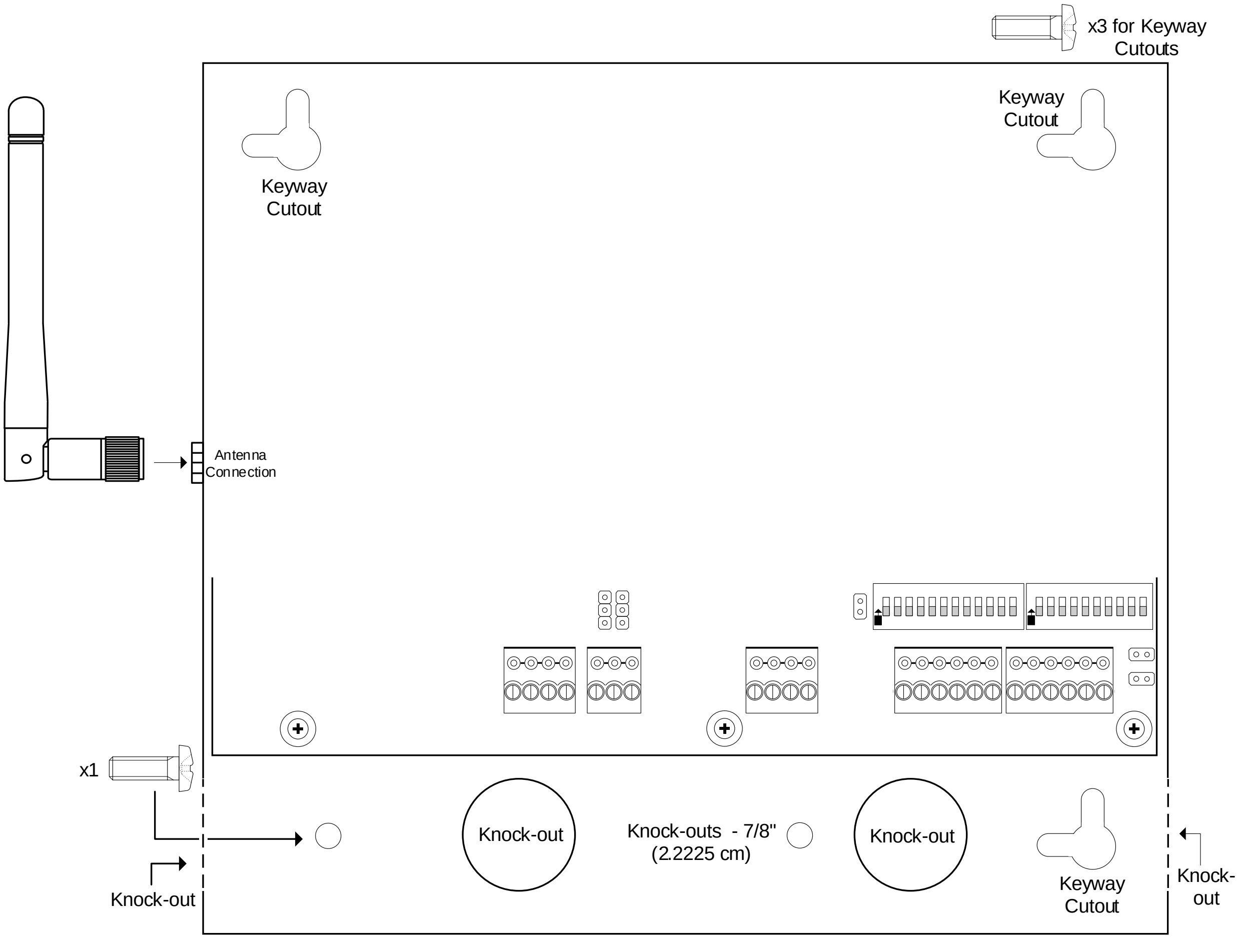


Table 11 – SDAC Quick Reference

Function	Location	Instructions/Notes
Power	12 VDC – Power In (+) & (-) terminals	
Reader 1 and 2	Data 0, Data 1	Wiegand signal
DIP Switches & Jumpers	J1 – Clear Memory	Resets board to factory defaults
	S1.1 to S1.12 – System Configuration	For communication and system settings
	S2.1 to S2.6 – Reader Configuration	Sets system to specific reader format/type
	S2.7 to S2.8 – Supervision Mode	Sets the input supervision type
	S2.9 to S2.10 – System Software Mode	Sets the board for the LUNA™ system software application
	J6 – System Reset	Resets the control board to effect communication or jumper changes
	J8 to J9 – Door Output Relay Powered/Unpowered	Sets Door relay with power from control board or as a dry contact
Wiegand LED Card Bits	10s, 1s	10s counts first binary digit 1s counts the second binary digit

SDAC/LUNA™ Specifications

The SDAC is designed as a single, stand-alone control unit; it does not support CIM, CB-485 or CPB-10-2 connections to other control units. The SDAC does not support global functions. The tables below outline SDAC specifications and LUNA™ computer specifications.

Table 12 - SDAC Specifications

Specification	Measurements/Standards
Dimensions	W - 6.875 " (17.46 cm) x H – 7.625 " (19.37 cm) x D – 1.75 " (4.45 cm)
Housing	22 GA steel, black powder coat
Environmental	Operating Temperature: 32^0 F to 120^0 F (0^0 C to 49^0 C) Humidity: 0 % to 90 % R.H, non-condensing
Power Inputs	+12V DC independent power supply
SDAC Current	170 mA to maximum 200 mA
Communication	802.11 Wireless b/g/n Adapter
PTC Resettable Fuses	Reader port 1 – 500 mA Reader port 2 – 500 mA Door output – 500 mA RTE port – 300 mA
Software Requirements	LUNA™
Applications	Indoor installations only

Table 13 - LUNA™ Computer Specifications

Type	Specification
Processor	Intel Core i3 equivalent or better
RAM	8 GB RAM, 2400 MHz, DDR4
Hard Drive	7200 RPM Hard Drive with 100 GB of free space
Operating Systems	Windows 10 Home/Professional/Enterprise Windows 8 Professional/Enterprise Windows 7 Home/Professional/Ultimate
Communication	802.11 Wireless b/g/n Adaptor
Peripherals	Keyboard & Mouse USB Port Video Card with minimum screen resolution of 1024 x 768

Liability Warning – 26 Bit Wiegand Card Format

Keyscan systems are factory defaulted for Keyscan proprietary 36-bit Wiegand format cards.

Keyscan systems can be modified to recognize a wide range of additional access card formats. Some of these formats are proprietary to other system manufacturers. Some other formats, notably 26-bit Wiegand, are "open". This means that card manufacturers will supply any card number sequence requested. The "open" 26-bit format means duplicate cards exist.

Installing dealers and end-users should be aware of the risk. Because the 26-bit format is unregulated, duplicated card numbers can be easily obtained and could be used to gain unauthorized access to a facility.

Dormakaba Canada Inc. strongly recommends that installing dealers apprise the end user customer of the risks posed by 26-bit cards and have the end user customer acknowledge they understand the risk by signing the "Waiver of Liability".

Waiver of Liability

Keyscan system end user (End User Name -)
acknowledges that he/she has been advised that the Keyscan system installed by

(Dealer Name -) in the end-user premises
has been modified from the factory original settings to accept Wiegand 26 bit format cards.

End user acknowledges that he/she is aware that duplicate cards may exist in this format and that a duplicate card could be used to gain illegal access to his/her facility.

(Dealer Name -) SHALL NOT BE RESPONSIBLE FOR ANY CONSEQUENTIAL, CONTINGENT, SPECIAL OR INCIDENTAL DAMAGES whatsoever, except as specifically set forth in the LIMITED WARRANTY, caused by illegal use of duplicate 26 bit access cards.

DEALER NAME:	**END USER NAME:**
PER:	**PER:**
SIGNED:	**SIGNED:**
DATED:	**DATED:**

Warranty

Limited Warranty

Dormakaba Canada Inc. warrants that all Keyscan manufactured products shall be free of defects in materials and workmanship under normal use for a period of two years from the date of purchase. In fulfillment of any breach of such warranty, dormakaba Canada Inc. shall, at its option, repair or replace defective equipment upon return to its facilities. This warranty applies only to defective parts or workmanship. This warranty does not apply to damage that occurred during shipping or handling, or damage due to causes beyond the control of dormakaba Canada Inc. such as lightning, excessive voltage, mechanical shock, water damage, or damage arising out of abuse, alteration or improper application of the equipment.

This warranty does not extend to products distributed by dormakaba Canada Inc. that are manufactured by 3rd parties. The original equipment manufacturer's warranty shall apply.

The foregoing warranty shall apply only to the original buyer and is and shall be in lieu of any and all other warranties, whether expressed or implied and of all other obligations or liabilities on the part of dormakaba Canada Inc. This warranty contains the entire warranty. Dormakaba Canada Inc. 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.

In no event shall dormakaba Canada Inc. be liable for any direct, indirect, or consequential damages, loss of anticipated profits, loss of time or any other losses incurred by the buyer in connection with the purchase, installation, or operation or failure of this product.

WARNING – dormakaba Canada Inc. 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.

Seller’s Right of Possession

In addition to all remedies dormakaba Canada Inc. may possess, dormakaba Canada Inc. shall have the right at any time for credit reasons or because of buyer’s defaults, to withhold shipments in whole or in part, to recall goods in transit, retake same and repossess all goods which may be stored, without the necessity of taking any other action.

Buyer consents that all merchandise so recalled, retaken, or repossessed shall become the absolute property of dormakaba Canada Inc. provided that buyer is promptly notified of such action and is given full credit therefore.

Product Installation and Operation

Buyer assumes all responsibility for the proper selection, installation, operation, maintenance and adherence to any and all federal, state/provincial and municipal building and fire codes of the merchandise purchased from dormakaba Canada Inc. Dormakaba Canada Inc. SHALL NOT BE RESPONSIBLE FOR ANY CONSEQUENTIAL, CONTINGENT, SPECIAL OR INCIDENTAL DAMAGES whatsoever, except as specifically set forth in the LIMITED WARRANTY.