dormakaba

Keyscan CA150 Installation Guide

POE under license with ChriMar Systems Inc., US Patents 8,155,012 - 8,942,107 - 9,049,019.

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.dormakaba.ca

dormakaba Canada Inc. 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

List of Figures

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 CA150 single-door, PoE, access control unit. 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
- Computer (optional)

Software Requirements

The CA150 single door control unit is compatible with the following Keyscan software versions:

- Aurora – version 1.0.1.0 or higher
- System VII – version 7.0.14 or higher
- Vantage – version 8.1.13 or higher

If you are operating with a previous version of Keyscan software you can obtain the latest version at www.dormakaba.ca. The CA150 is not compatible with any previous generation of Keyscan software.

About Powering the CA150

The CA150 single door control unit can be powered from one of the following sources:

- network switch with power over Ethernet (PoE) capabilities
- mid-span PoE injector
- +12V DC UL approved power supply

Refer to page 58 for more about power connections and testing voltages.

Important

The CA150 operates as a Class 0 PoE Powered Device (PD). As such, the CA150 requires the allocation of 15.4 Watts from the PoE switch or injector. Of the 15.4 Watts, the CA150 provides 680 mA at 12 volts – approximately 8 Watts – to power connected peripheral devices such as readers, door strikes, PIR sensors, etc.

Selection of a PoE switch must be based on the power demand of all of the loads connected to the switch. The PD Class (0-4) for each device connected to the switch must be known and the sum of all loads, for a conservative and reliable design, should not exceed 75% of the total available power. As loads are disconnected and others connected, the total power consumption must be re-assessed. We recommend the use of low port count PoE switches, maximum 8 ports, to minimize the impact of a switch failure on the access control system and, that all PoE switches be powered using a UPS.

Programming the On-board Ethernet Module

The CA150 has an on-board network module which must be programmed using the Keyscan NETCOM Program Utility when being deployed on a host network (TCP/IP).

If configuring the CA150 for reverse network communication, use the procedures outlined in the next section.

The CA150 Rev. B control board is distinguished by DIP switches, which are not present on previous CA150 control boards.

Configure the CA150 for Reverse Network Communication – License Required

If the CA150 is connected on a network using Keyscan reverse network communication, the unit's on-board Ethernet module and the control board memory have to be programmed with IP addresses.

Generally, reverse network communication is used only in centrally managed access control applications.

A license must have been purchased – K-RN, V-RN or AUR-RNx – which includes encrypted reverse network communication software.

If you have not purchased a license from dormakaba Canada Inc., do not configure the CA150 for reverse network communication.

The CA150 requires NETCOM Program Utility – version 6.0.18 or higher. Always use the latest NETCOM Program Utility on the enclosed CD when programming the on-board Ethernet module.

For an outline of requirements and procedures on configuring the CA150 for reverse network communication, see page 95.

Reset IP On Tamper

CA150 ACUs with firmware 9.45 or higher can reset the onboard NETCOM's IP to 192.168.100.254 / 255.255.255.0. This feature is used to revert to a known IP address for reprogramming. CA150 ACUs with older firmware will not possess this functionality.

NOTE: The ACU must have communications switches set to S1.10-ON/S1.11-OFF prior to using this feature.

Follow these steps to default the IP address of the onboard NETCOM module to 192.168.100.254:

1. Perform a system reset by momentarily placing a jumper on J6.
2. Press the tamper button 3 times in a row (within 15 seconds of placing a jumper on J6). The programming with begin and can take up to 20 seconds.
3. Once successful, the ACU will beep once.

Locate & Mount the CA150

Locate the area where the CA150 and, if required, the power supply, are going to be mounted. Follow the mounting procedures on the following page. We recommend a vertical 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 control board. The serial number is a required entry in the Keyscan Client software. The CA150 includes a mounting template for drilling holes to mount the unit.

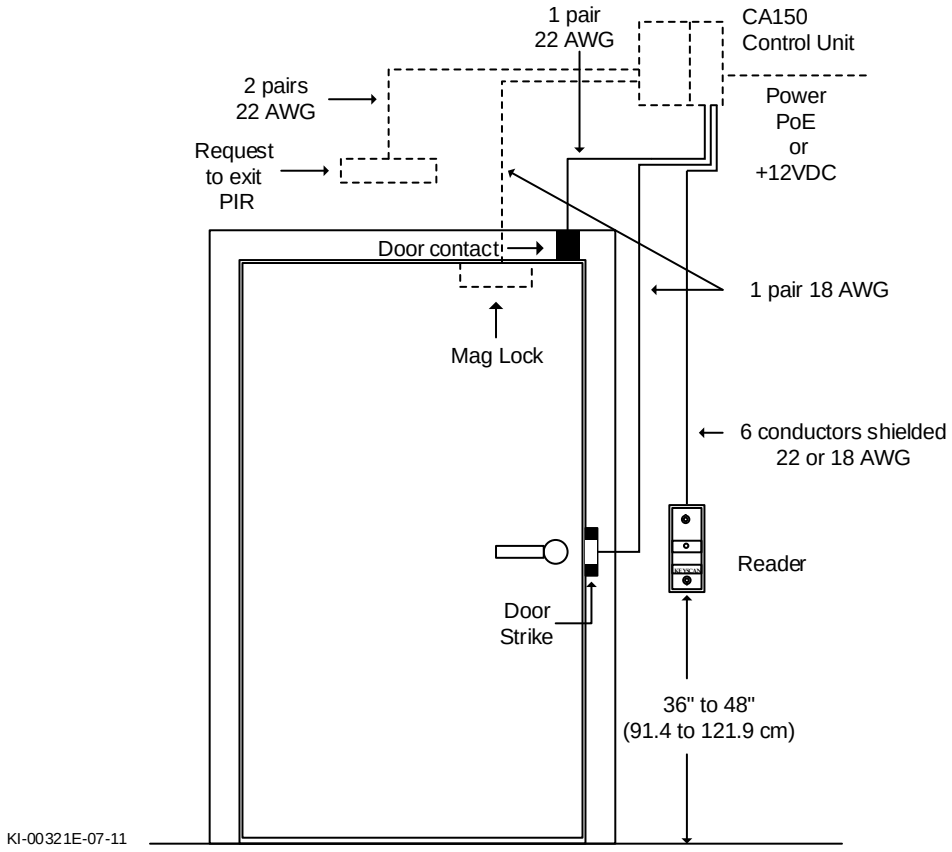
The following illustration shows a typical mounting location for the CA150 which generally is in proximity to the door it is controlling. However circumstances may require mounting the unit farther from the door than depicted.

Important

When locating a mounting position, bear in mind if the CA150 has access to the network and/or power depending on how the unit is being configured – network (TCP/IP), RS-232 (direct serial), PoE or a local +12V DC power supply.

The CA150 is a standalone single door control unit; it does not support CIM, CB-485 or CPB-10-2 connections to other control units. The CA150 does not support global functions.

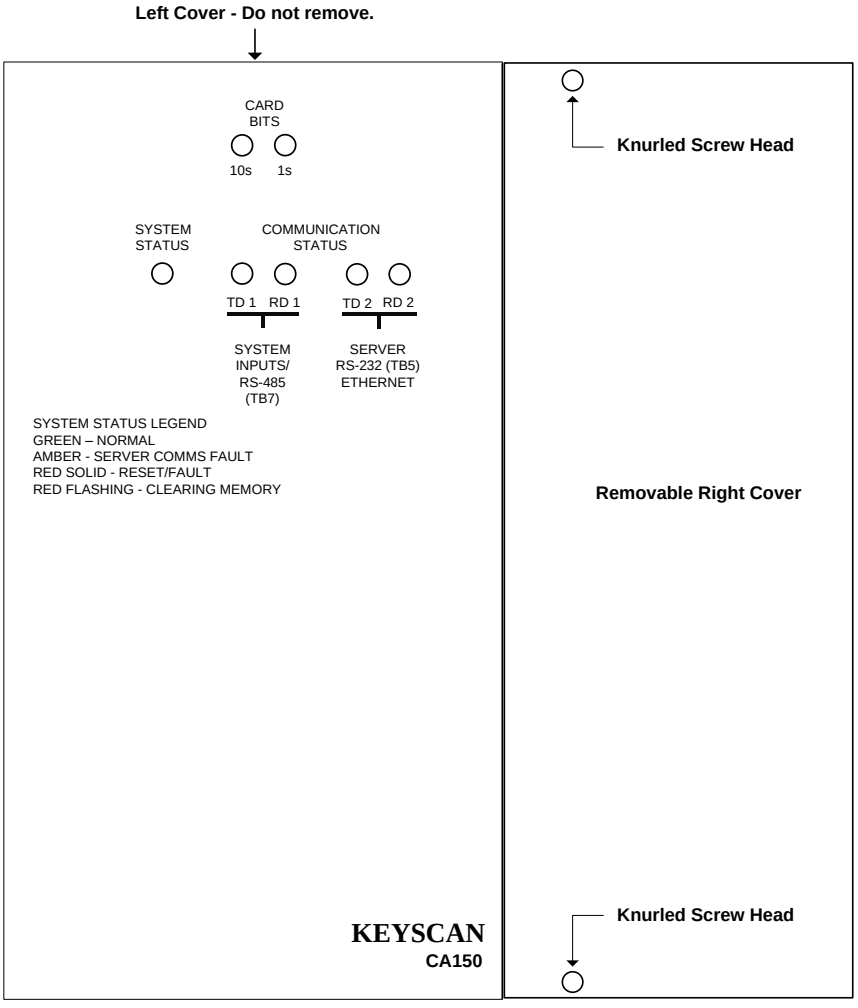
Figure 1 – Typical Door Layout



Mounting Guidelines

- Unfasten the 2 knurled screw heads on the CA150 to remove the right-side cover as shown in Figure 2
- Use the enclosed mounting template and drill 4 holes where indicated
- Fasten the top 2 screws and the lower left screw until there is a gap of approximately 1/32” between each of the screw heads and the mounting surface
- Mount the CA150 so that the 3 keyway cutouts at the back of the enclosure are over the screw heads as shown in Figure 3
- 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 right hole
- Leave the right cover off until you have connected all the door hardware, applied power, and tested the voltages

Figure 2 - Remove the Right Cover



KI-00322E-05-12

Figure 3 – Mounting the CA150

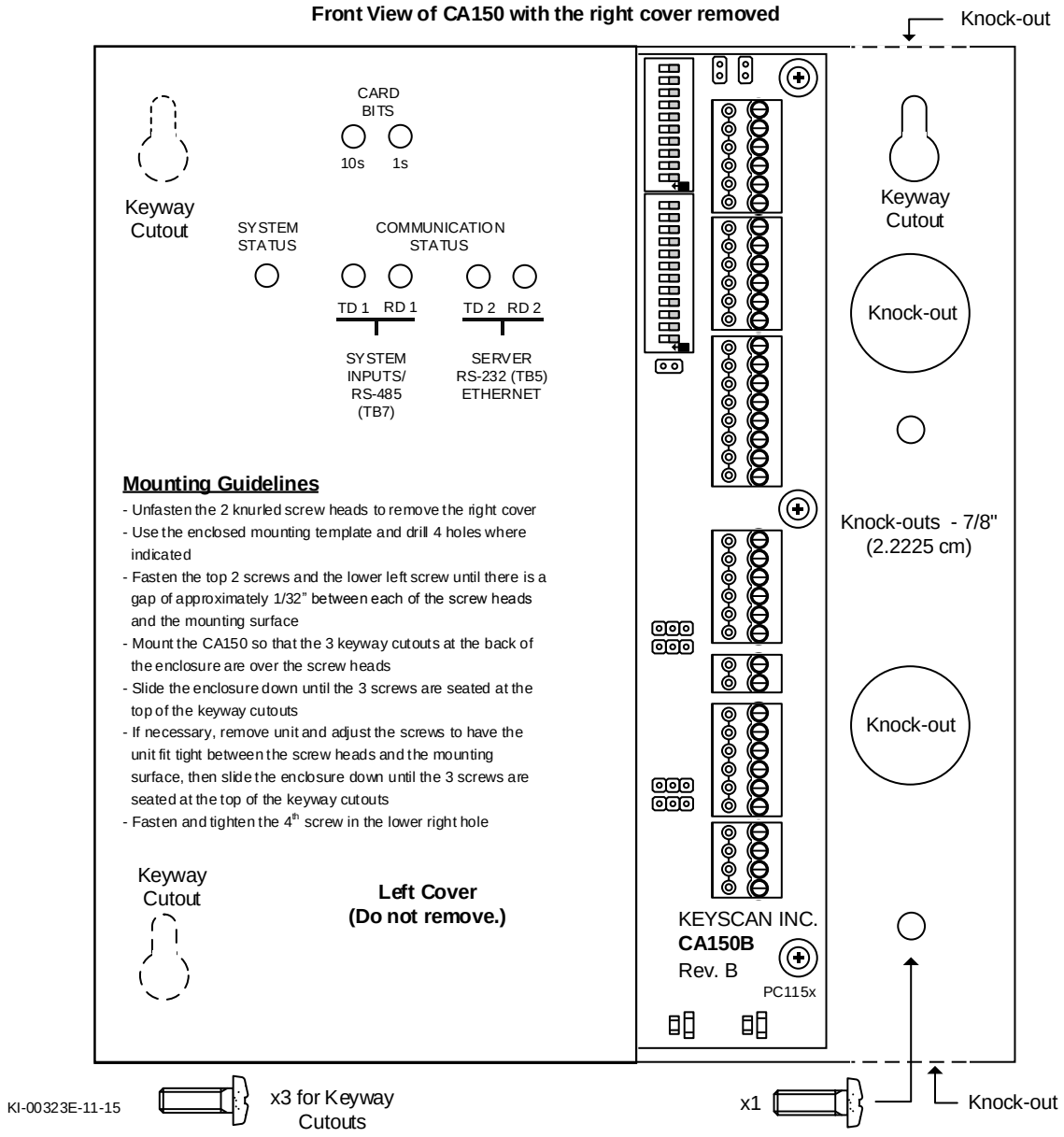
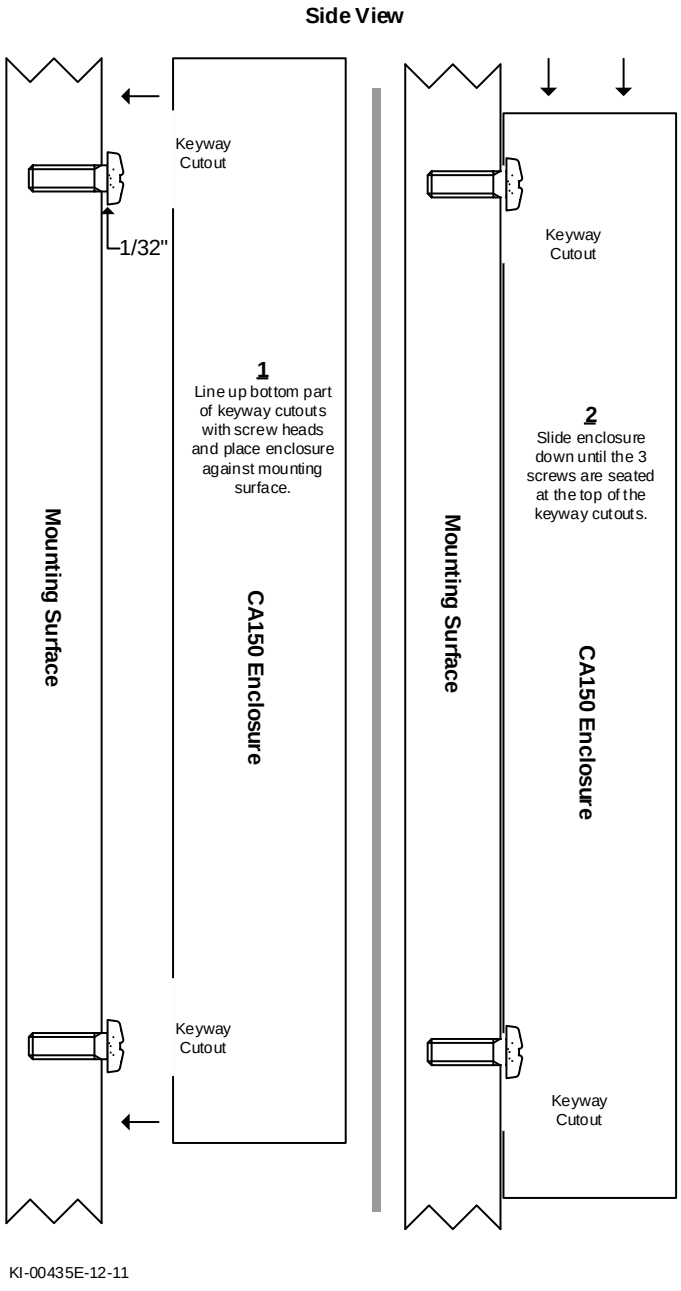


Figure 4 - CA150 Mount - Side View



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.

Important

In a PoE powered configuration, the CA150 supplies 680 mA at 12V (approximately 8 watts) to power all loads including readers, door strikes, request-to-exit PIR devices, etc.

To power devices such as magnetic locks, the CA150 or the device must be powered from a dedicated +12V DC power supply.

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.

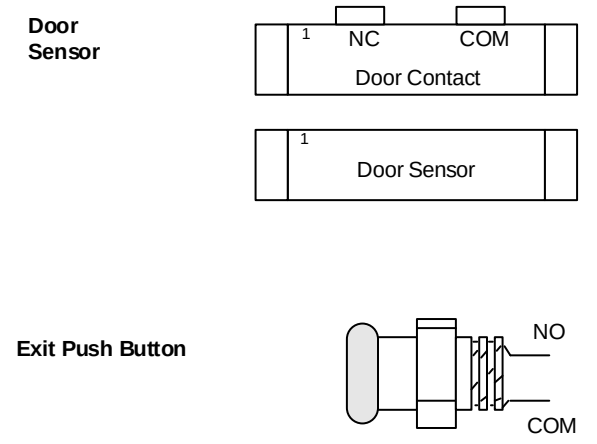
Use a battery for temporary power to ensure the door operates properly with respect to the following functions before connecting to the Keyscan access control unit.

- Alignment
- Holding
- Activation/de-activation

Door Contacts, Exit Buttons, Auxiliary Inputs

The following diagram illustrates the door contacts, exit buttons, PIRs, and auxiliary inputs. 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 5 – Door Contacts, Exit Buttons, PIRs, & Auxiliary Inputs



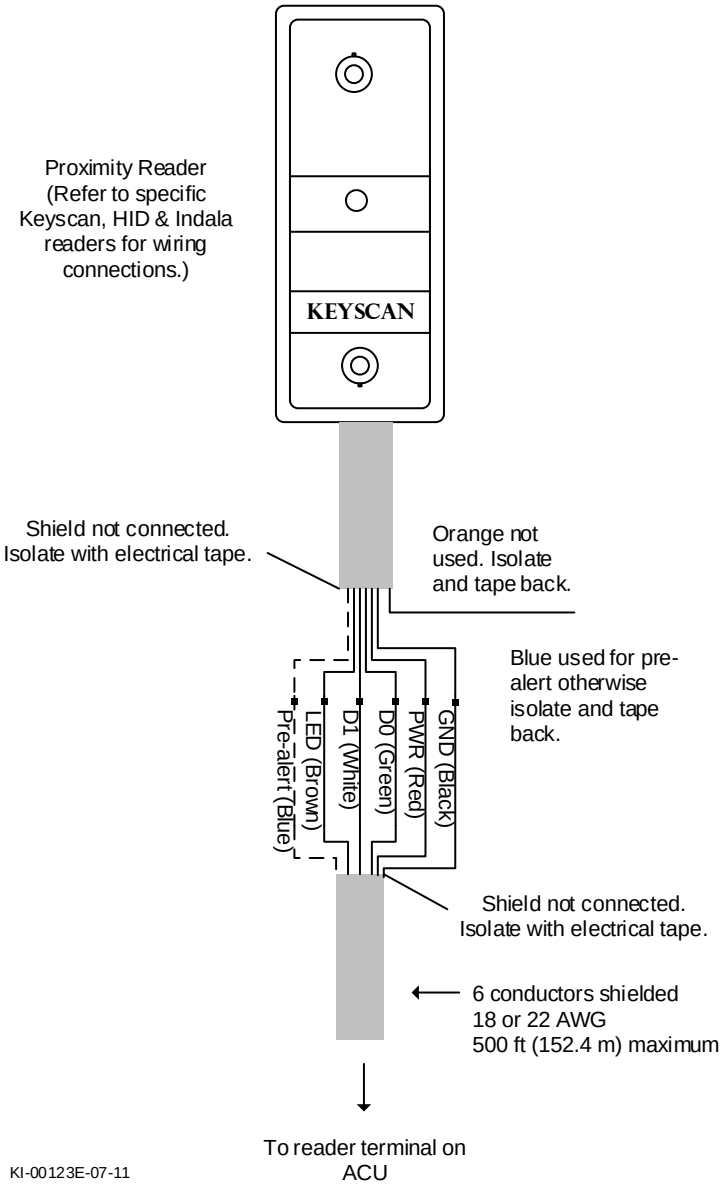
Readers

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 6 – 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 (includes HID iClass – Rev B & Rev C)	Wiegand	500 ft. 152.4 m	6 conductors shielded 22 AWG	Overall shielded cable accepted. CAT5 cable not acceptable with Wiegand signal protocol.
Exception readers to ACU – PX-620, HID-5375, MR-10, MR-20, HID-iClass (Rev A), iClass KEYRK40	Wiegand	500 ft. 152.4 m	6 conductors shielded 18 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
ACU to computer (direct serial)	RS-232 (57.6k or 115.2k BPS)	20 ft. 6 m	5 conductors 22 AWG shielded	Overall shielded cable accepted. CAT 5 cable not acceptable with RS-232 signal protocol.
Network	TCP/IP		CAT 5	

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 7 – Grounding Access Control Units and Cables.

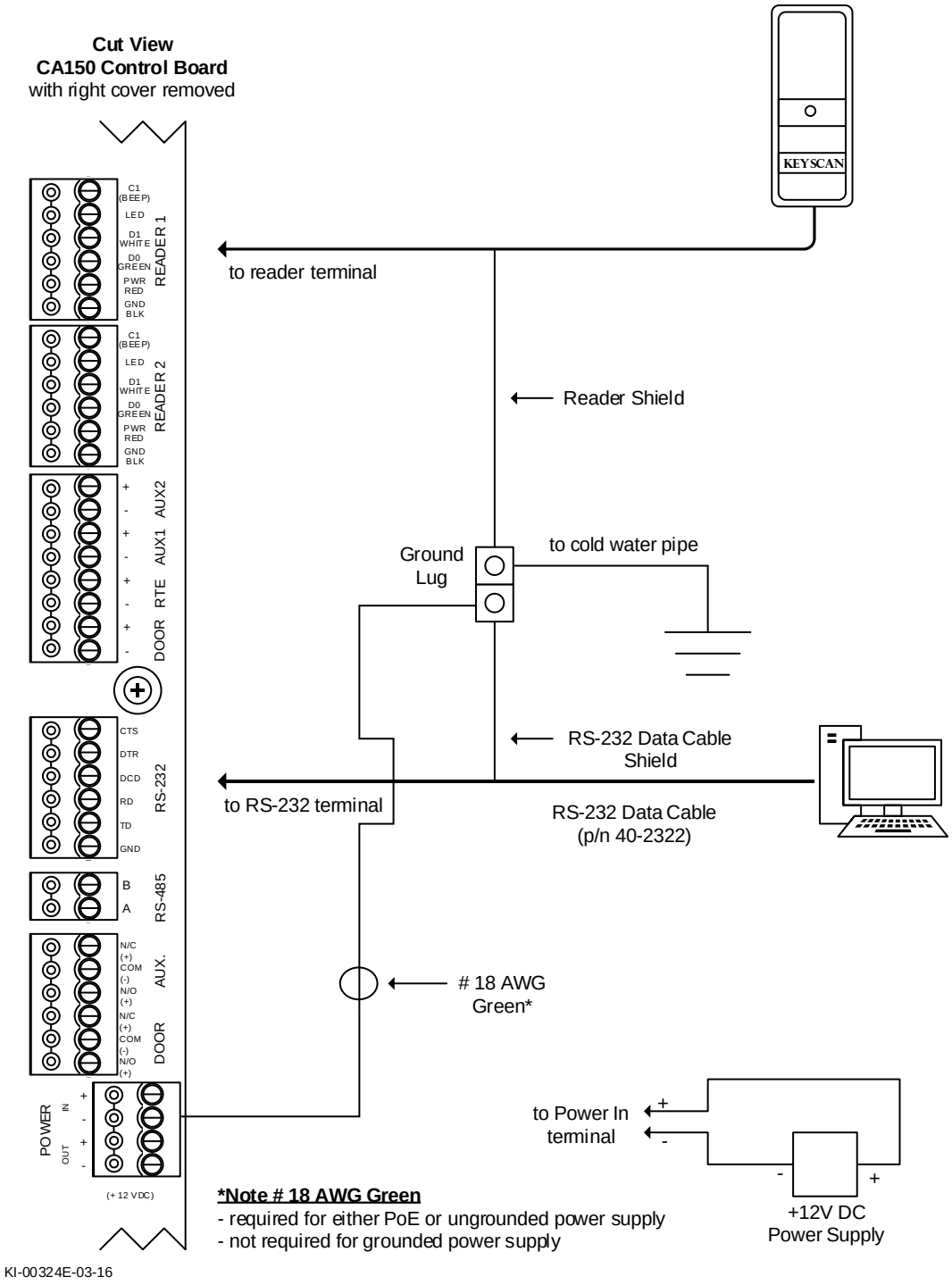
If terminating a RS-232 communication cable in the metal enclosure, ensure that the shield is insulated and connected to the ground lug. We suggest Alpha PVC 10516 - #16 clear tubing or a comparable tubing to insulate the shield. Do not connect the shield to GND on the RS-232 communication terminal block.

The metal enclosure includes 1 ground lug pre-mounted on the right side of the CA150.

Note

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

Figure 7 – Grounding Access Control Units and Cables



Terminate Wiring at the ACU

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

PoE

Before terminating connections at the control unit and if you are using power over Ethernet (PoE Class 0), please note the CA150 PoE power supply has a 680mA @ 12V maximum – approx. 8 Watts – current rating. The total number of connected hardware devices including the door strike cannot exceed this threshold; otherwise, a separate +12V DC power supply with a sufficient current rating is required. For more information on PoE, refer to page 9.

Do not use PoE to power a magnetic lock or similar device. Either, power the CA150 control board or the mag lock from a dedicated +12V DC supply.

Output Relays

The CA150 has 1 door output for terminating a door lock or magnetic lock and 1 auxiliary output for terminating an alarm/hardware device.

Powered / Unpowered

The door output relay and the AUX output relay are each 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 CA150 relay output (500 mA or less) – Counter EMF diode (CEMF) connected at terminal block
- Unpowered – CA150 provides a dry contact, but the device requires an independent power source (over 500 mA) – Counter EMF diode (CEMF) connected at strike or maglock

Jumper settings are shown in the respective wiring diagrams or refer to page 50.

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, 1 aux output
PTC resettable fuse	500 mA per relay
Door output relay – powered/unpowered	J8 & J9
AUX output relay – Powered/Unpowered	J10 & J11

Important

Counter-EMF diodes (CEMF) are supplied with Keyscan access control unit(s).

Diodes must be installed and terminated at the door relay terminal on the CA150 for DC door strikes if the CA150 supplies power to the strike via the DC power input or via PoE, as illustrated in the following lock diagrams. Diodes must always be used with DC locks, regardless of if the lock is powered or not.

If the door strike is powered via a separate DC power supply, connect the diode at the door strike.

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

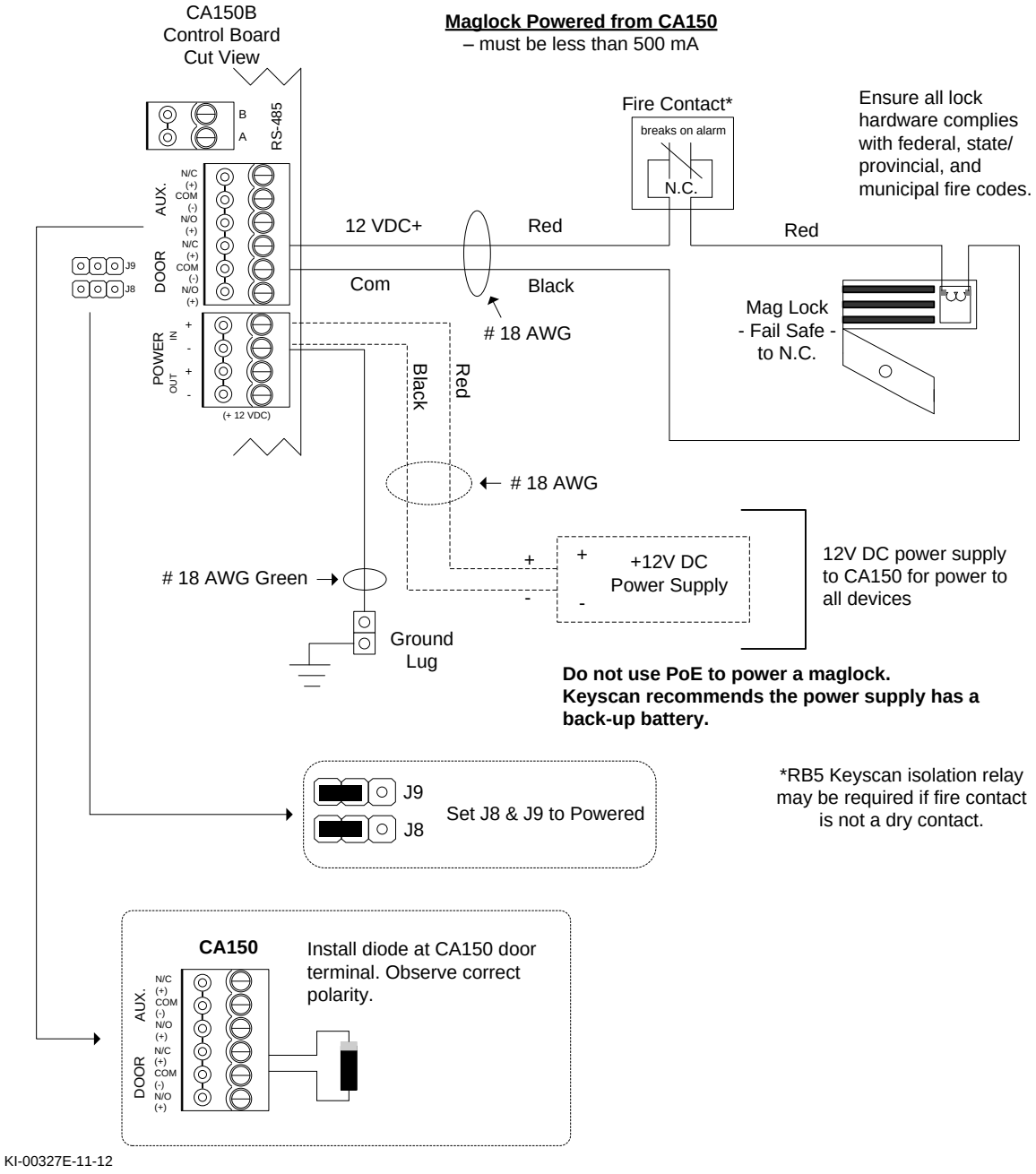
For 'fail-secure' and 'fail-safe' door strikes, observe the following relay connections:

- '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

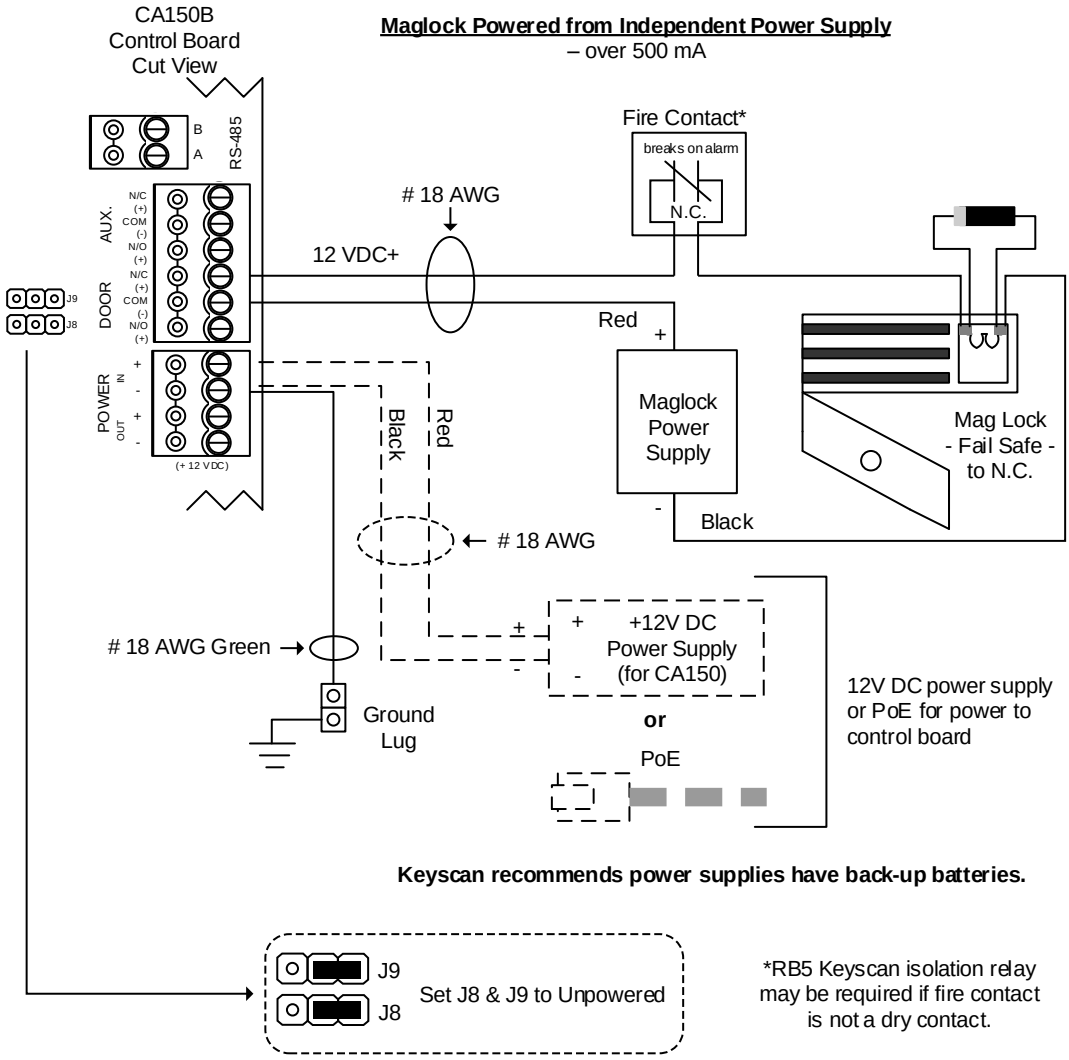
Before securing any exit, please ensure all wiring to electrical door hardware conforms to federal, state, provincial, or municipal fire regulations and building codes.

Figure 8 – Terminate Magnetic Lock under 500 mA – Fail Safe



KI-00327E-11-12

Figure 9 – Terminate Magnetic Lock over 500 mA - Fail Safe



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

KI-00328E-11-12

Figure 10 - Terminate Door Strike - 500 mA or less - Fail Safe

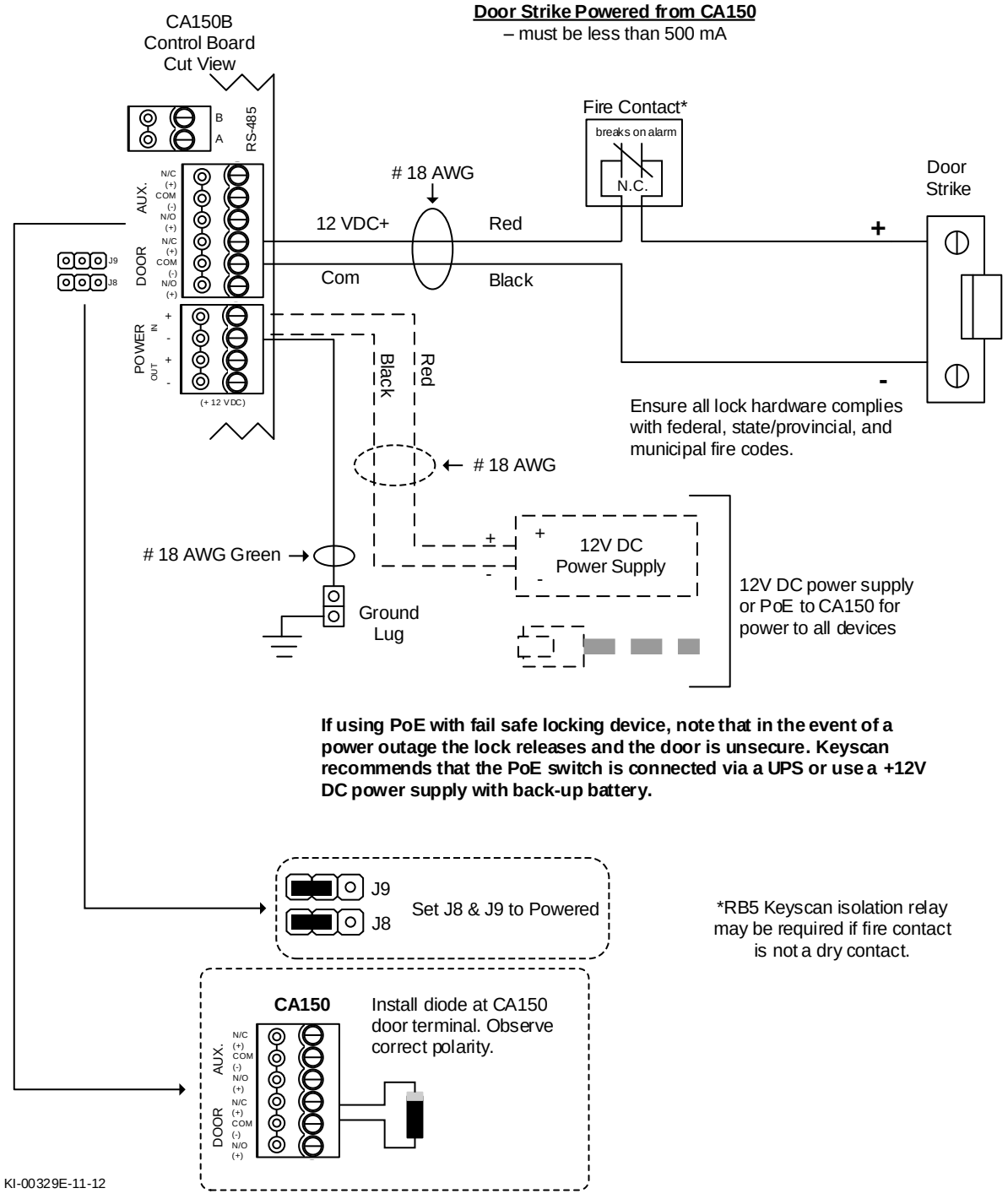


Figure 11 – Terminate Door Strike - Over 500 mA – Fail Safe

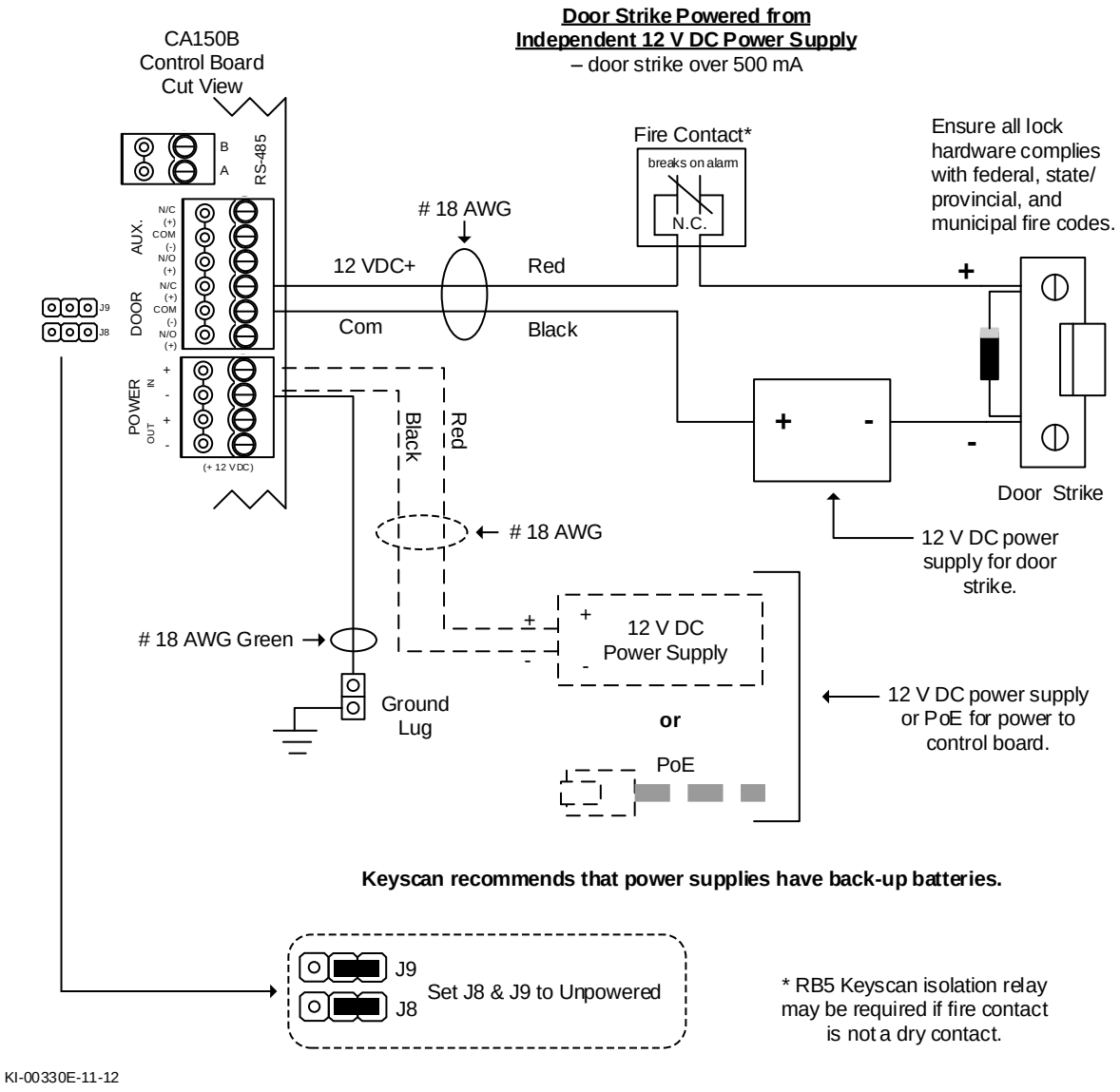


Figure 12 - Terminate Door Strike - Less than 500 mA - Fail Secure

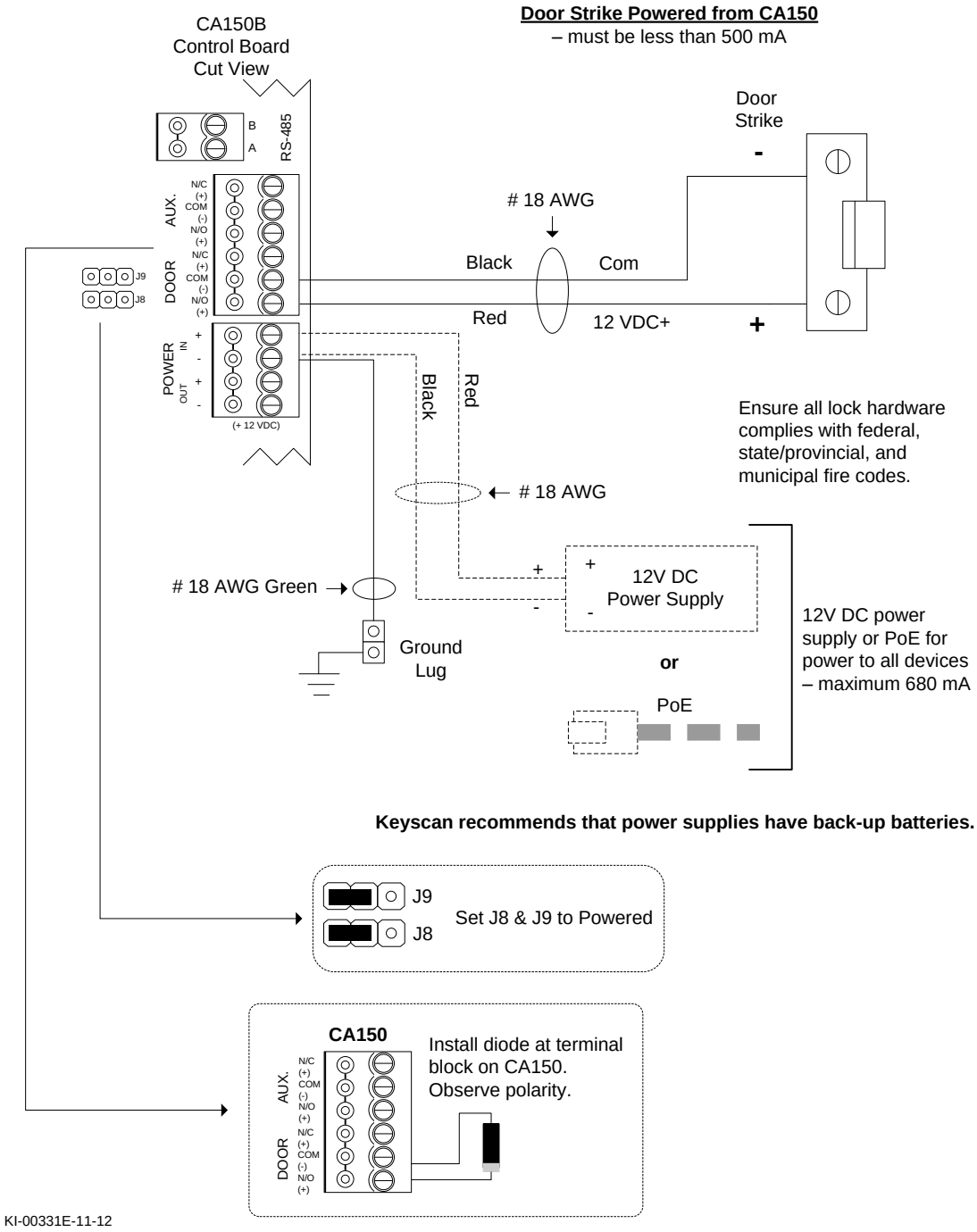
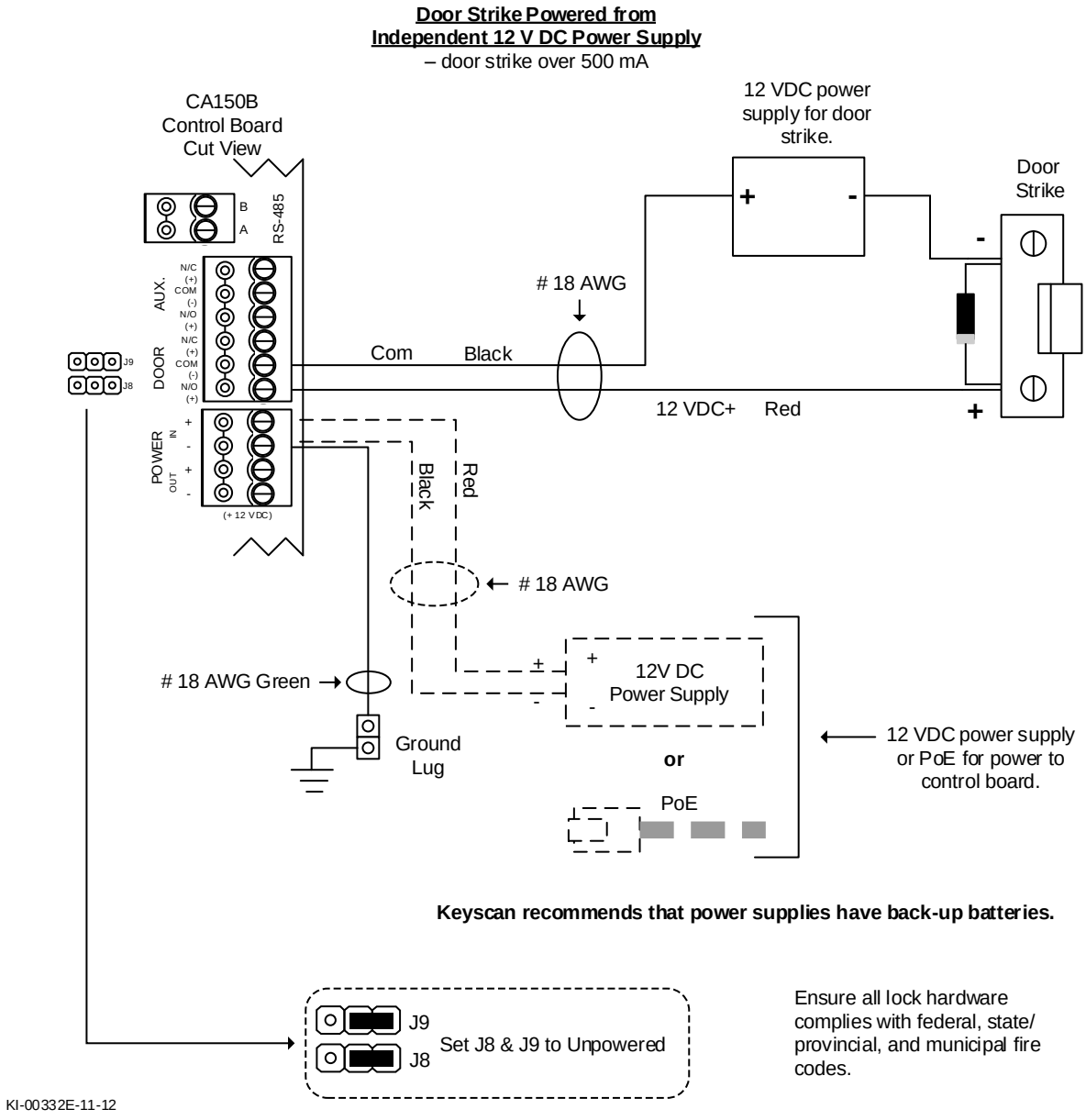


Figure 13 - Terminate Door Strike - Over 500 mA - Fail Secure



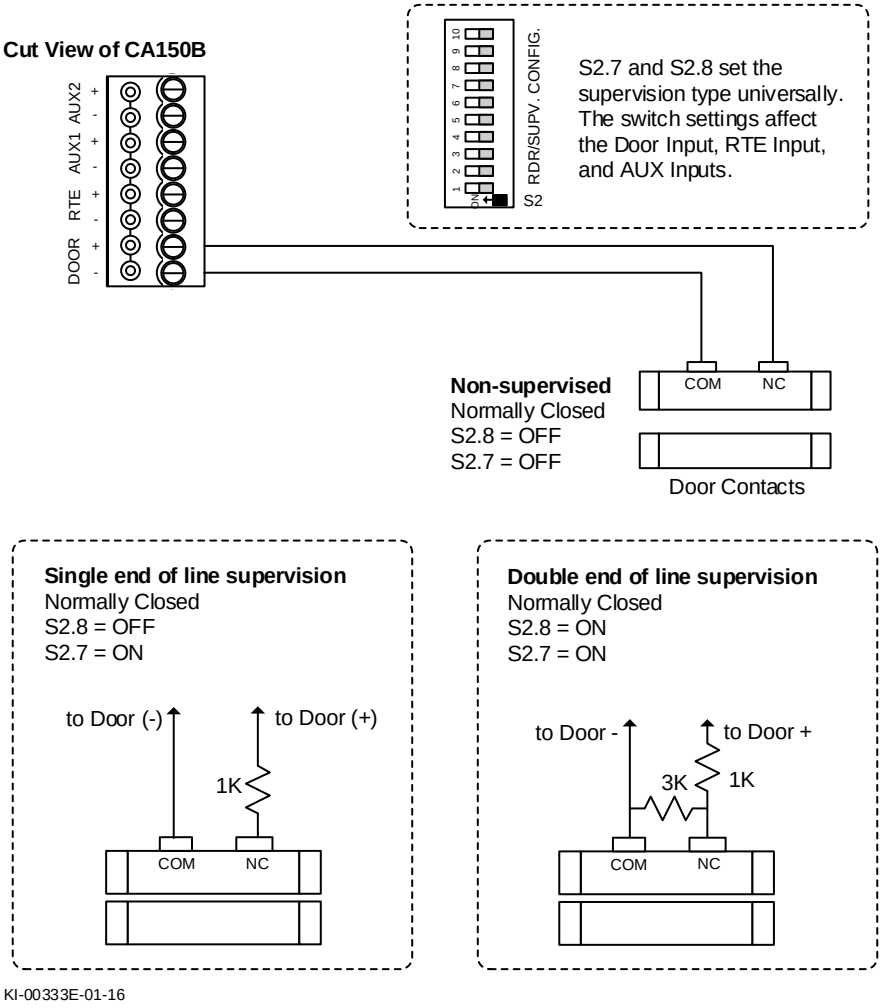
Terminate Input Wiring

The following sub-headings review termination of door, exit, and auxiliary alarm 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 14 – Terminate Input Wiring – Door Inputs (Contacts)



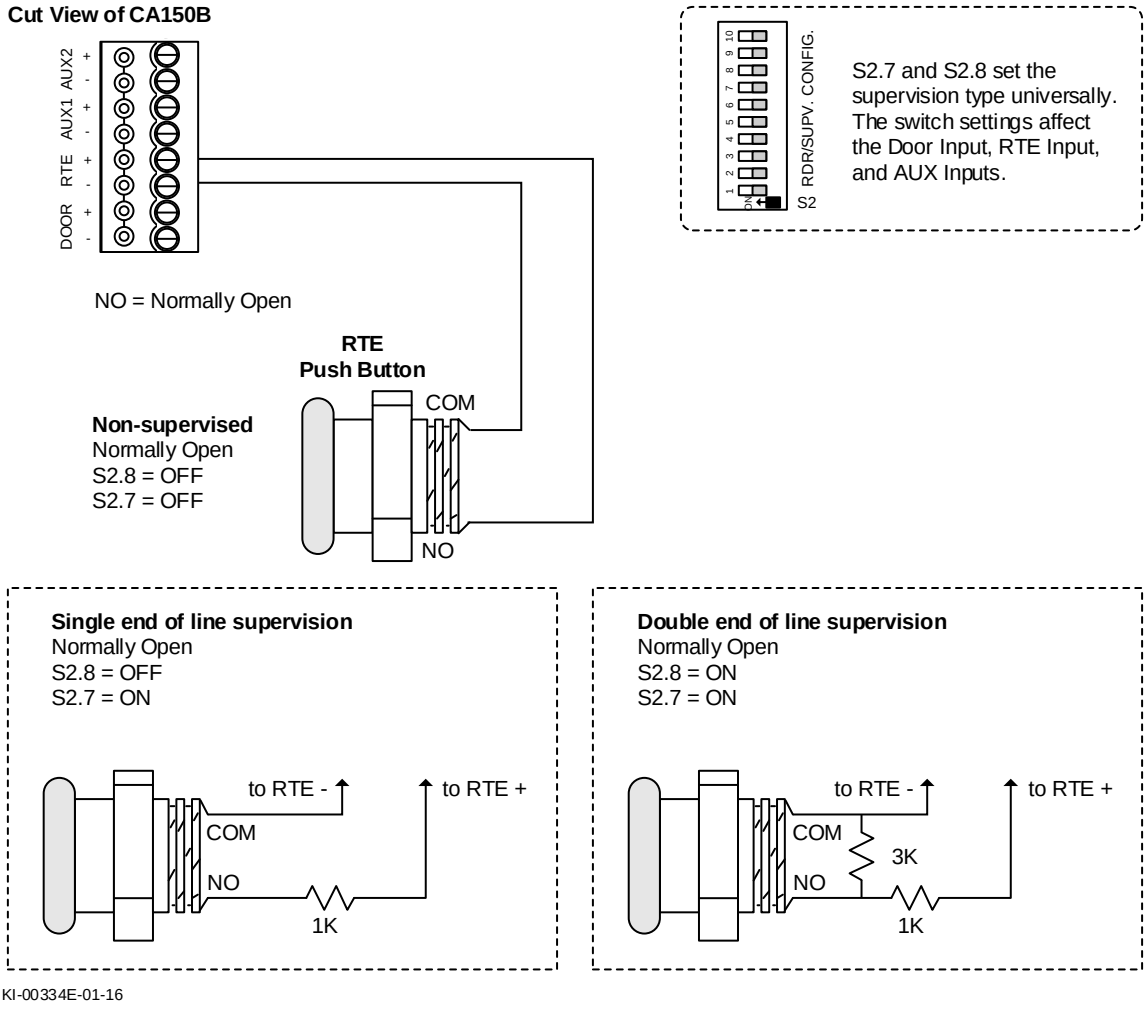
KI-00333E-01-16

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.

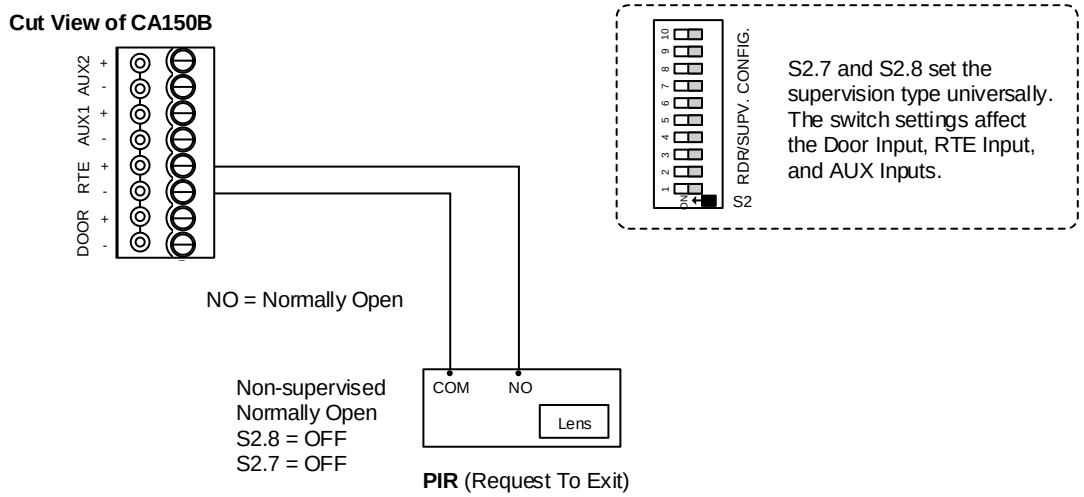
When using a motion sensor (PIR) for an exit device, we recommend a PIR with a pulse output of 1/2 second and suited to its environment.

Figure 15 – Terminate Input Wiring – RTE Push Button

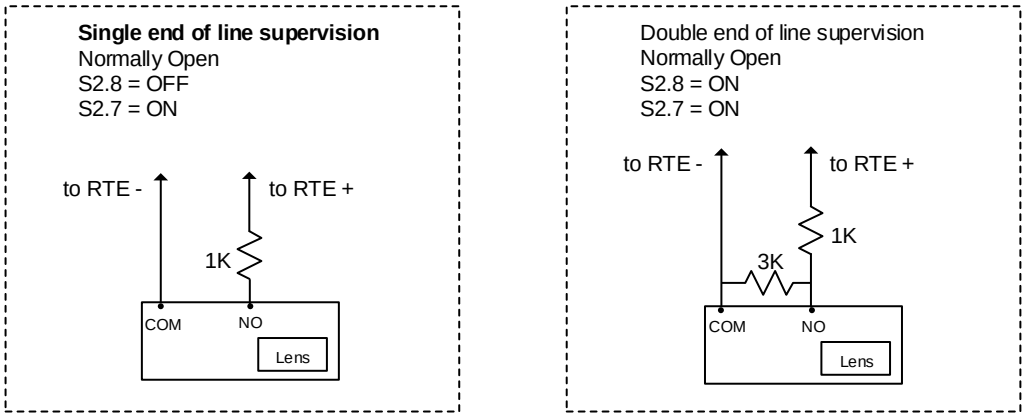


KI-00334E-01-16

Figure 16 – Terminate Input Wiring – RTE PIR Motion Sensor

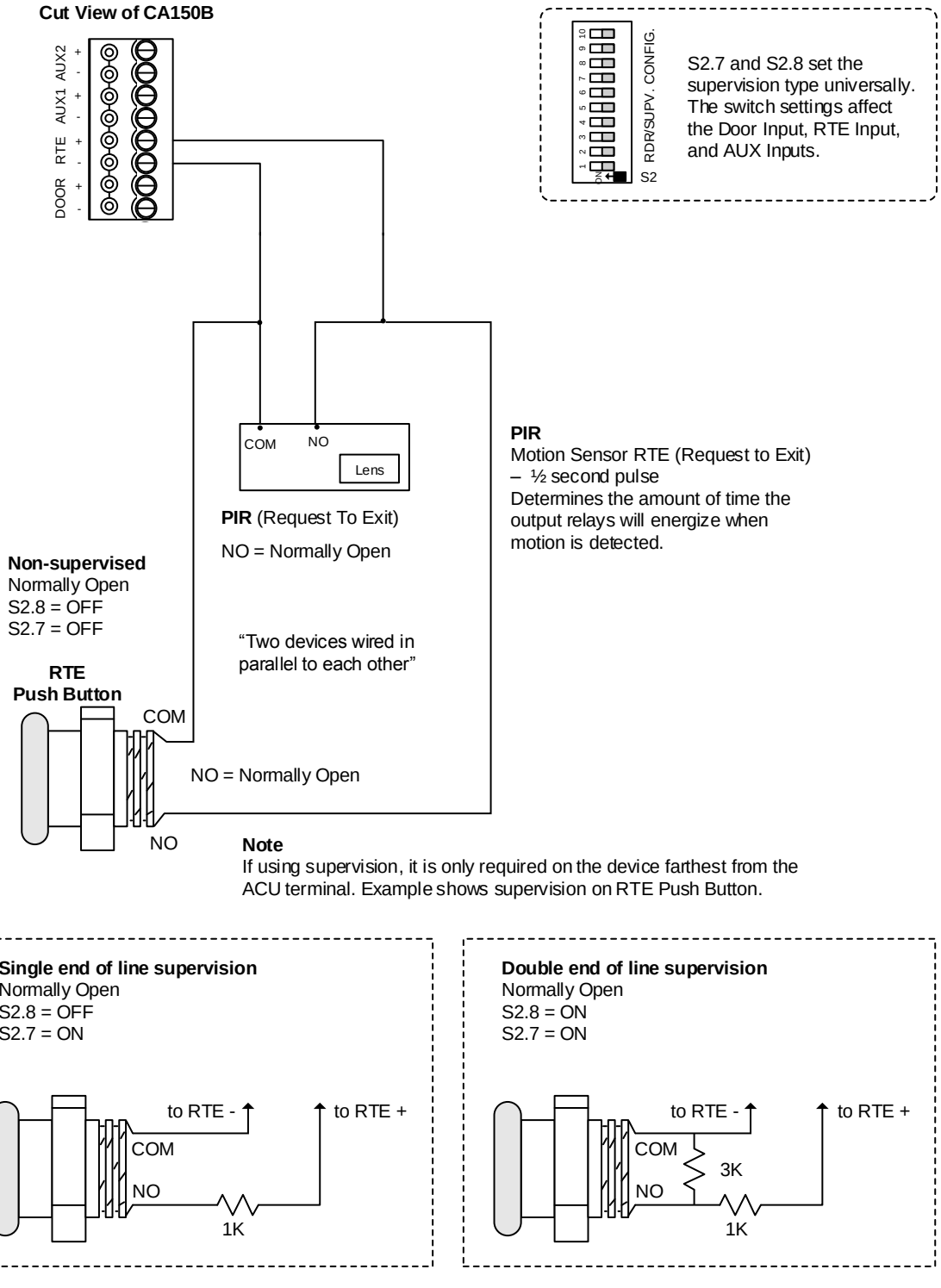


PIR
RTE (Request to Exit) – ½ second pulse
Determines the amount of time the output relays will energize when motion is detected.



KI-00335E-01-16

Figure 17 – Terminate Input Wiring RTE - PIR & Push Button

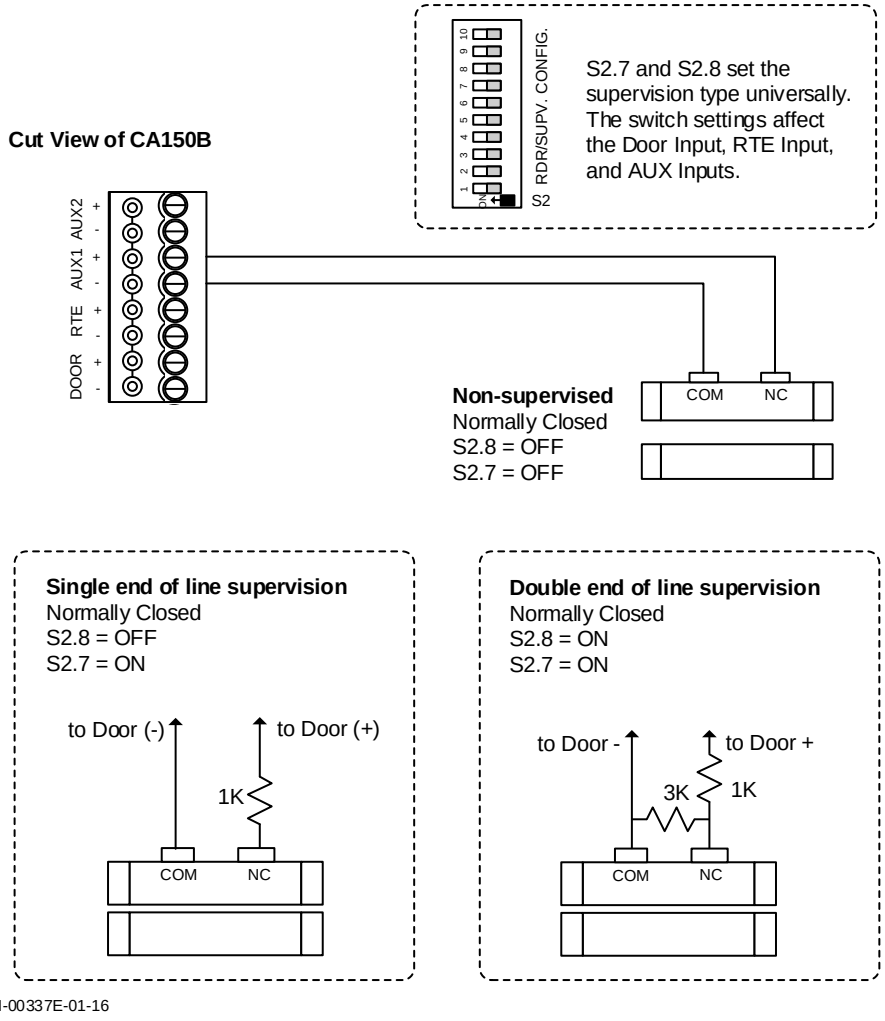


KI-00336E-01-16

Security Monitoring Connections

A normally-closed device may be connected to an auxiliary alarm input for monitoring stairwell or interior doors, or windows. The auxiliary alarm inputs may be connected to infrared sensors or to an existing alarm system with a normally-closed auxiliary output relay contact. The CA150 does not support global functions.

Figure 18 – Terminate Input Wiring – AI/SI Inputs

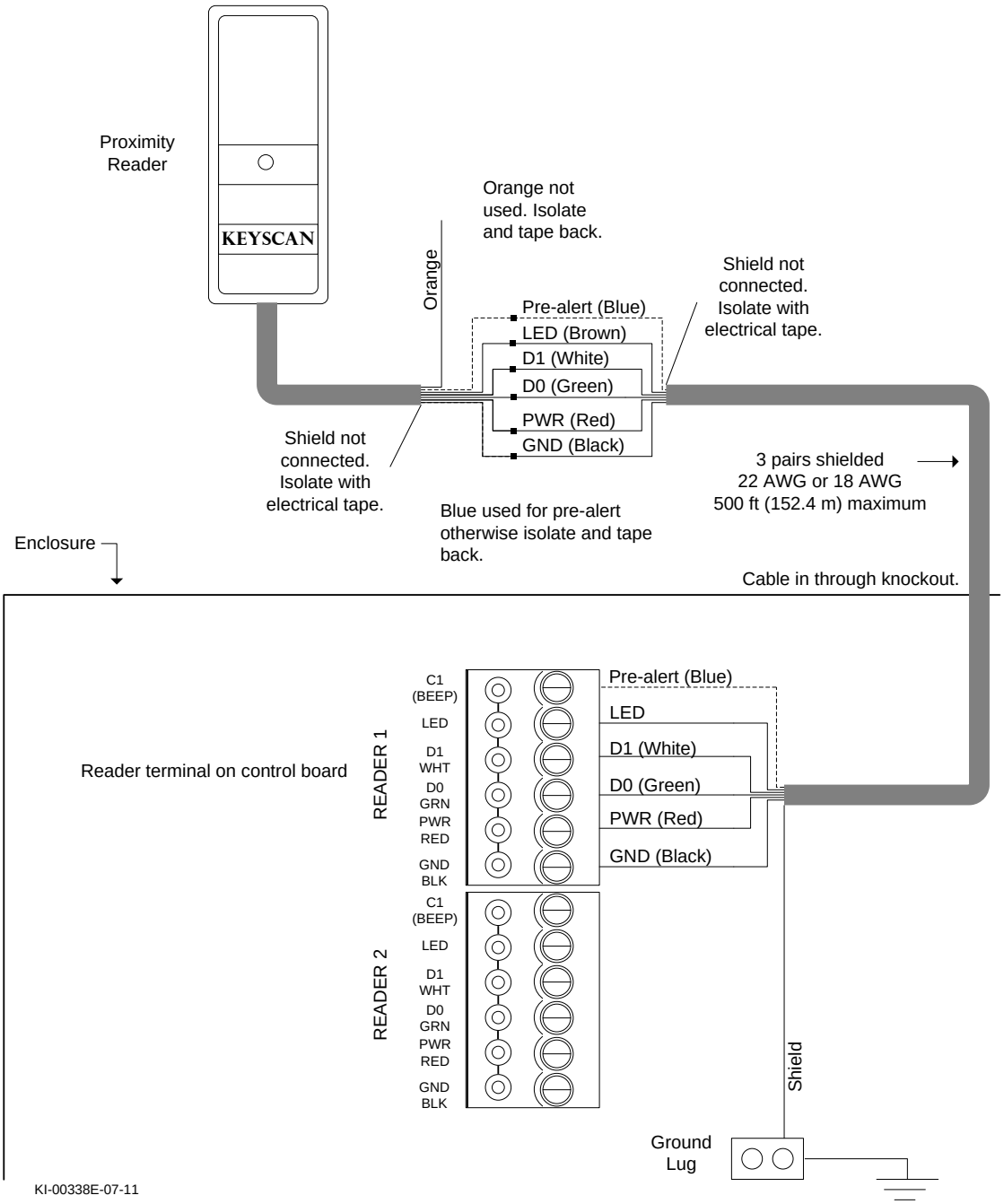


KI-00337E-01-16

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 such as the Indala PX620 or the HID5375. The shield wire must be connected to the earth ground lug 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. For more on reader connections, refer to page 67.

Figure 19 – Terminate Reader Wiring



Terminate Auxiliary Outputs with Hardware/Alarms

The door and 2 auxiliary inputs can be programmed to trip the auxiliary output relay on an alarm event. The auxiliary output relay can be connected to an alarm panel, CCTV system, etc.

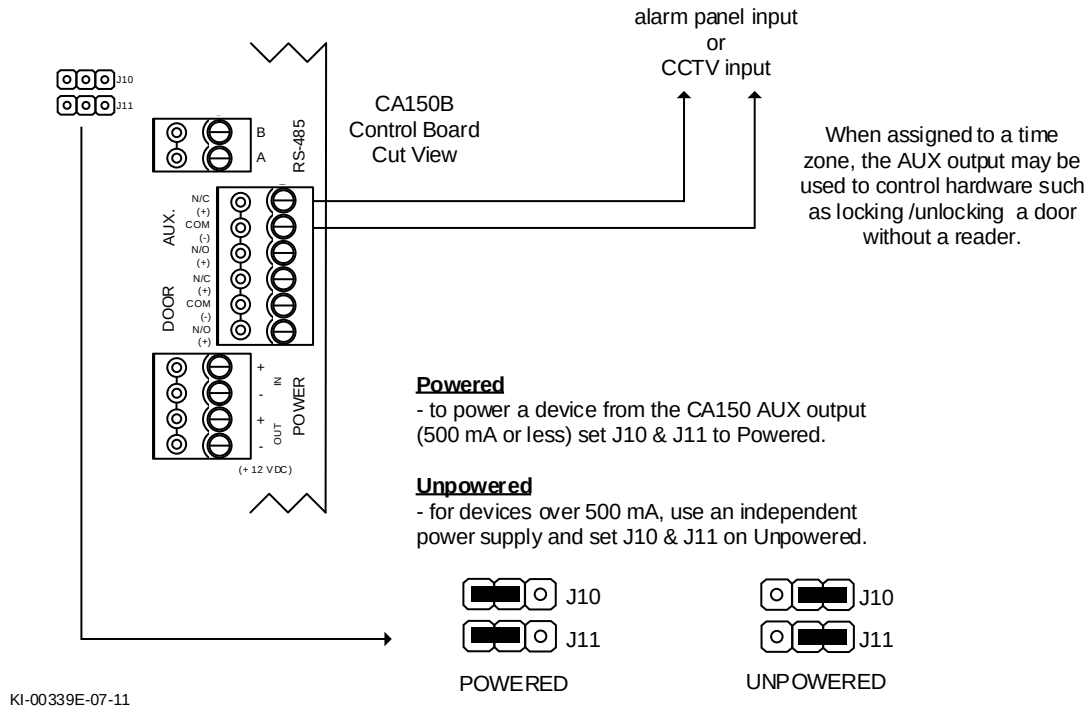
As an example, a forced entry detected by a door input could be programmed to trip the auxiliary output which initiates a CCTV system to record the intrusion at the door.

The auxiliary output relay may also be used to control hardware with an associated time zone, such as scheduling the locking/unlocking of a reader-less door to a defined time zone.

Important

Do not assign a time zone to an auxiliary output if the output has previously been assigned to an alarm event. The alarm has priority over the time zone. The CA150 does not support global functions.

Figure 20 – Terminate Auxiliary Output



DIP Switch/Jumper Settings

The CA150 has DIP switches and jumpers that activate or alter specific board functions to meet installation requirements.

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 38 for function activation and DIP switch settings.

S1.1 - Communication Mode

Keyscan CA150 control boards support serial, network and reverse network communication modes. Serial and network communication use standard polling in which communication is initiated at the communication manager server. Reverse network communication differs from standard polling in that communication is initiated at the control unit. Do not set the S1.1 switch for reverse network communication unless a license was purchased from dormakaba Canada Inc.

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. Ensure that the Keyscan Client software baud rate setting matches the control board's bit rate when using a serial connection. If using the on-board Ethernet module, ensure the module is programmed with the corresponding control board bit rate.

S1.3 - P3 Card Lockout

The Client's P3 cardholder lockout mode can be overridden when the S1.3 DIP switch is set in the on position, which allows a valid credential access on a single presentation.

S1.4 - Alternate Panel Serial Number

Each Keyscan control board is programmed with a factory-assigned serial number for identification and communication with the Keyscan software.

In the event a duplicate serial number is detected during ACU setup in the Client software, you will be prompted by the Client application to reset the control board with an alternate serial number. However, unless you are prompted in the Client software, always use the factory-assigned serial number.

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.

S1.6 - Unassigned

Reserved for future use.

S1.7 - Temporary Card Countdown

The Client software has a card usage countdown function when credentials are issued on a temporary basis. To employ this function in the Client software, the temporary card countdown DIP switch must be enabled on the CA150 control board.

S1.8 - Accessibility Output

The CA150 can convert the AUX output to an Accessibility output for connection to an electro-mechanical door operator. When configured as an accessibility output, the output follows the accessibility door timer and the accessibility door held open settings in the Client software. If using Aurora the output follows the extended entry time and extended entry door held open settings. For more about this function, see Accessibility Output Relay on page 51.

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.

S1.10 & S1.11 - Communication Terminal Activation

DIP switches S1.10 and S1.11 activate the RS-232 terminal for direct serial communication or network communication with the internal, on-board Ethernet module for run mode or program mode.

S1.12 - Flash Program Memory Upgrade

Currently, this function is unavailable.

Figure 21 – System Configuration DIP Switches S1.1 – S1.12

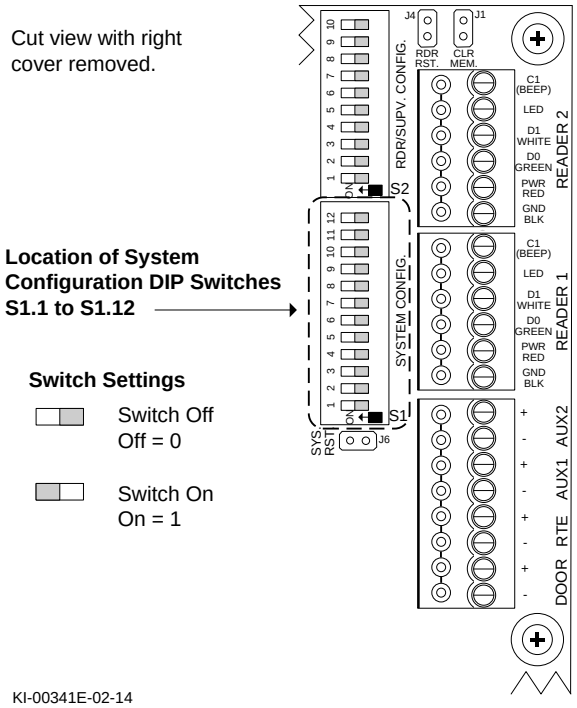


Table 3 – System Configuration DIP Switch S1 Settings

S1 Switch #	Setting	Function	Notes
S1.1	0 = Off 1 = On	**Communication Mode**	
	0	Serial Communication – standard polling	Also see S1.10 & S1.11 in the table.
	0	Network Communication – standard polling	As above.
	1	Reverse Network Communication	Requires a license from dormakaba Canada Inc.
S1.2		**Communication Bit Rate**	
	0	115,200 bit/s	
	1	57,600 bit/s	
S1.3		**P3 Card Lockout**	
	0	Enabled	
	1	Disabled	
S1.4		**Alternate Panel Serial # Selection**	
	0	Factory-assigned serial #	Only set DIP switch for alternate serial

S1 Switch #	Setting	Function	Notes
	1	Adds 1000 to factory-assigned serial #	number if prompted in the Client software when adding a panel.
S1.5		**Reader LED Mode**	
	0	Red LED type reader	
	1	Red & green LED type reader	
S1.6		**Unassigned**	
	0	n/a	
	1	n/a	
S1.7		**Temporary Card Countdown**	
	0	Disabled	If credentials are issued on a temporary basis, the temporary card countdown function must be enabled.
	1	Enabled	
S1.8		**Accessibility Output**	
	0	AUX Output	
	1	Accessibility Output	
S1.9		**Clear Memory Enable**	
	0	Disabled	Note – clear memory enable S1.9 activates the Clear Memory jumper J1 to reload factory defaults.
	1	Enabled	
S1.10 & S1.11	0=Off 1=On	**Communication Terminal Block Activation**	
	S1.10 S1.11		
	0 0	Enables RS-232 serial TB5 terminal block	For direct serial communication
	0 1	Future use	
	1 0	Enables Ethernet operation mode	For network communication
	1 1	Enables Ethernet program mode	For programming the Ethernet module
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 on page 110.

Advantage of Keyscan 36-bit Proprietary Wiegand Format

Keyscan's 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

The table on page 42 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
- Very Low

Reader formats ranked with medium, low, and very 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.

Extended Card Number – Card Enrollment

Please be advised that reader formats Ref # B, D, E, F, G, H, I, & J, listed in the following table, are referred to as extended card number reader formats. These reader formats require a different method of card enrollment in which the Client software must make hexadecimal/decimal calculations. As opposed to merely entering the facility code and card number in the cardholder record, use the following procedure to enroll a card when the control board is configured for extended card number support. You must also enable the site for extended card number support in the Client software's Site Information screen.

If a high volume of cards is involved, you may wish to connect a reader close to a computer with the Keyscan Client and use it as a designated card enrollment reader. You can access the Client help by pressing F1.

- From the Client software, select the Display On-line Transactions quick button on the main screen.
- Ensure that the On-line Transactions screen is open. Present the card at a reader.
- At the computer with the Keyscan Client, the card is listed in the transaction table. The card will show 'access denied' under Transaction Type in the On-line Transaction screen. This is normal as the card has not yet been enrolled. Hold down the Ctrl key on the keyboard and double click on the card number under the card heading.
- The Cardholder Information screen opens and you will see the card number (hex) field is populated from the reader scan. The card number is displayed below.
- Complete the remaining cardholder fields and then save the record.

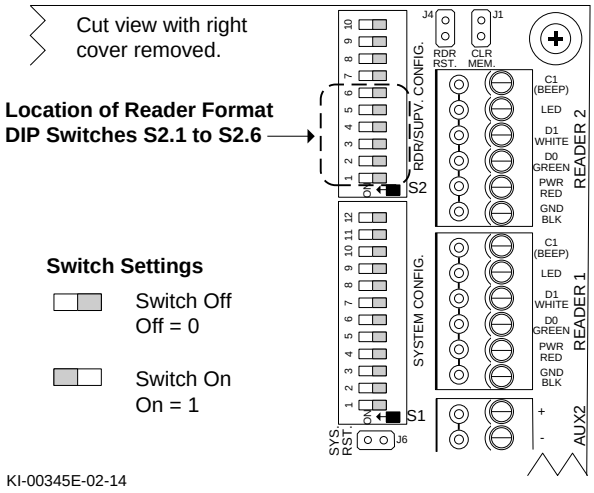
Supported Keypad Wiegand Outputs

dormakaba Canada Inc. supports the following keypad PIN data Wiegand outputs:

- HID Wiegand with 4-bit word burst
- Indala unbuffered mode Wiegand with 8-bit word burst
- WSSKP-1 facility code 0 (zero) with 36-bit Keyscan Wiegand output

If using 3rd party biometric devices connected to Keyscan CA or EC control board reader ports, do not use reserved facility code 0 (zero).

Figure 22 – 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 3.4.03 or greater unless stated otherwise in the table below.

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		
A	Keyscan 36-bit only	High	0 0 0 0 0 0	Standard	
B	FIPS/TWIC – 75-bit output (48-bit FASC-N, 25-bit expiration date, 2 parity bits)	High	0 0 0 0 0 1	Extended	Legacy support only
C	HID Corporate 1000 - 35-bit output	Medium	1 0 0 0 0 1	Extended	
D	MIFARE – CSN 32-bit output	Low	0 1 0 0 0 1	Extended	Only reads the card serial number sector
E	MIFARE – Reverse CSN 32-bit output	Low	1 1 0 0 0 1	Extended	Only reads the card serial number sector
F	MIFARE – 40-bit CSN (32-bit CSN, 8-bit Checksum)	Low	0 0 1 0 0 1	Extended	Only reads the card serial number sector
G	26 to 48 Pass-through Large Card Format	Medium - Low	1 1 1 1 1 1	Extended	

Ref #	Reader Format	Security Level	Switch Settings S2.1 – S2.6	Card Number Format	Notes
H	26 to 48 Pass-through Large Card Format (with first and last parity bits dropped)	Medium - Low	0 1 1 1 1 1	Extended	
I	University 1000 - 56-bit	Medium	0 1 1 0 0 1	Extended	Custom order only. Facility code required when ordering.
J	MIFARE Reverse 40-bit (32-bits reverse CSN + 8-bits checksum = 40 bits	Low	1 0 1 0 0 1	Extended	Only reads the card serial number sector
K	MLF Indala Format = 16039 (Available on custom order only. Letter required from dealer.)	Medium	1 1 1 0 0 1	Extended	Custom order only. Letter required from dealer.
L	FIPS/TWIC – 75-bit output (48-bit FASC-N, 25-bit expiration date, 2 parity bits) & Keyscan 36-bit	High	1 0 0 1 0 1	Extended	Legacy support only
M	FIPS/TWIC – 75-bit output (48-bit FASC-N, 25-bit expiration date, 2 parity bits) & Keyscan 36-bit & Mifare – 40-bit CSN (32-bit CSN, 8-bit Checksum)	High	0 1 0 1 0 1	Extended	Legacy support only
N	37-bit H10304 & Keyscan 36-bit	Medium	1 1 0 1 0 1	Extended	Reader PROM version 3.4.04 or higher
O	37-bit H10302 & 35-bit Corporate 1000	Medium	0 0 0 1 0 1	Extended	Reader PROM version 3.4.04 or higher
P	HID Corporate 1000 48-bit & Keyscan 36-bit	Medium	0 0 1 1 0 1	Extended	Reader PROM version 3.4.06 or higher
Q	HID Corporate 1000 48-bit, HID Corporate 35-bit, HID H10302 37-bit & Keyscan 36-bit**	Medium - Low	1 0 1 1 0 1	Extended	Reader PROM version 3.4.07 or higher
R	HID Corporate 1000 48-bit, HID Corporate 35-bit, HID H10302 37-bit, Standard 26-bit & Keyscan 36-bit**	Low	0 1 1 1 0 1	Extended	Reader PROM version 3.4.07 or higher
S	Kaba Integrated 17-byte	High	1 0 1 1 1 1	Extended	Reader/IO PROM version 3.6.00 or greater
	Keyscan 36-bit is only supported in this context when **Enable Keyscan Credentials for Extended Card format is enabled within the Aurora software client. Read the Aurora software help file for more information.				
	The following Reader Formats Ref # 1 – 31 are NOT recommended.				
1	Standard 26-bit & Keyscan 36-bit	Low	1 0 0 0 0 0	Standard	
2	Legacy Northern 34-bit, Standard 26-bit & Keyscan 36-bit	Low	0 1 0 0 0 0	Standard	

Ref #	Reader Format	Security Level	Switch Settings S2.1 – S2.6	Card Number Format	Notes
3	Corby 30-bit & Keyscan 36-bit	Medium	1 1 0 0 0 0	Standard	
4	Kantech 32-bit & Keyscan 36-bit	Medium	0 0 1 0 0 0	Standard	
5	DSX 33-bit & Keyscan 36-bit	Medium	1 0 1 0 0 0	Standard	
6	Intercon 32-bit & Keyscan 36-bit	Low	0 1 1 0 0 0	Standard	
7	Legacy Chubb 36-bit (5 & 6 digit cards) & Keyscan 36-bit	Low	1 1 1 0 0 0	Standard	
8	Keyscan 36-bit with zero batch number	Low	0 0 0 1 0 0	Standard - except Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
9	Standard 26-bit & Keyscan 36-bit	Low	1 0 0 1 0 0	Standard – except for 26-bit cards Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
10	Northern 34-bit & Keyscan 36-bit	Low	0 1 0 1 0 0	Standard – except for 34-bit cards Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
11	Corby 30-bit & Keyscan 36-bit	Low	1 1 0 1 0 0	Standard - except for 30-bit cards Facility Code = 0	Enter 0 (zero) for the facility code in the Client software to ignore the FC output from the reading device.
12	Legacy GE 40-bit or Casi-Rusco Ex. Prox-Lite 941-W RDR	Low	0 0 1 1 0 0	Standard	
13	Legacy 37-bit (37 Bit Corp H10302) & Keyscan 36-bit	Low	1 0 1 1 0 0	Standard	
14	Legacy Keyscan England 36-bit with no manufacturer's code check	Low	0 1 1 1 0 0	Standard	Format does not support Keyscan WSSKP-1 Keypad with PIN use.
15	Legacy HID 35-bit & Keyscan 36-bit	Low	1 1 1 1 0 0	Standard – except for HID 35-bit cards - Company ID Code ignored.	See Reader Format – Ref # C – preferred option.
16	HID Computrol 34-bit & Keyscan 36-bit	Medium	0 0 0 0 1 0	Standard	
17	Legacy 37-bit (alternate 37 Bit Corp H10304) & Standard 26-bit & Keyscan 36-bit	Low	1 0 0 0 1 0	Standard	

Ref #	Reader Format	Security Level	Switch Settings S2.1 – S2.6	Card Number Format	Notes
18	Legacy Chubb 36-bit & Keyscan 36-bit	Low	0 1 0 0 1 0	Standard	No parity check on Chubb card.
19	Honeywell 40-bit & Keyscan 36-bit	Medium	1 1 0 0 1 0	Standard	
20	Unassigned		0 0 1 0 1 0	Standard	
21	Unassigned check		1 0 1 0 1 0	Standard	Format does not support Keyscan WSSKP-1 Keypad with PIN use.
22	ITI 29-bit & 26-bit & Keyscan 36-bit	Low	0 1 1 0 1 0	Standard	
23	Legacy 37-bit (37 Bit Corp H10302) & Standard 26-bit & Keyscan 36-bit	Low	1 1 1 0 1 0	Standard	
24	Kantech XSF 36-bit IO Prox & Keyscan 36-bit	Low	0 0 0 1 1 0	Standard	
25	CardKey 34-bit & Keyscan 36-bit	Medium	1 0 0 1 1 0	Standard	
26	Keyscan 36-bit & 26-bit with no parity checking format	Low	0 1 0 1 1 0	Standard – except 26-bit no parity check	26-bit format designed for Keri part # SM-2000X
27	Modern 30-bit & 26-bit & Keyscan 36- bit	Low	1 1 0 1 1 0	Standard	
28	Intercon 32-bit & Keyscan 36-bit & Standard 26-bit	Medium	0 0 1 1 1 0	Standard	
29	Indala 27-bit (format 10251) & Keyscan 36-bit	Medium	1 0 1 1 1 0	Standard	
30	Cards between 26-bit & 40-bit read as 26 bit card location with parity check	Very Low	0 1 1 1 1 0	Standard	
31	Legacy Diagnostic Mode- evaluates cards between 26-bit & 40-bit for Keyscan engineers.	Display Only	1 1 1 1 1 0	Standard	Format ignores card's stored values at ACU producing access denied for all cards. Format does not support Keyscan WSSKP-1 Keypad with PIN use.

Card Number Formats

Standard card number – facility code 1 – 255 / card number 1 – 65535

Extended card number – hexadecimal = 1 – FFFFFFFFFFFF or decimal = 1 – 281474976710655 / Checked for extended number

For other custom Wiegand protocol firmware or development, contact dormakaba Canada Inc. technical support.

LED Wiegand Bit Counters

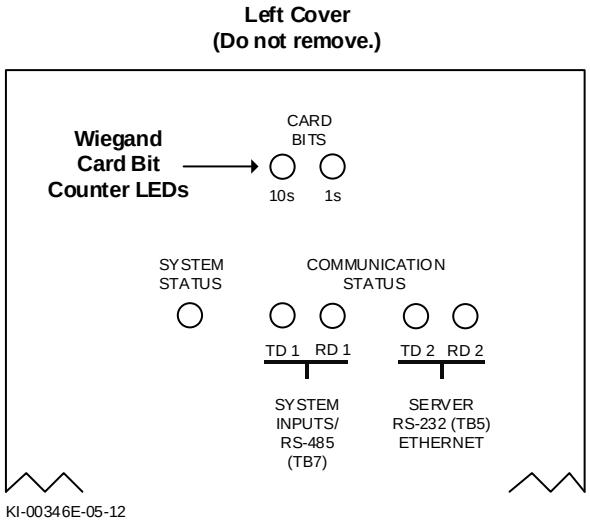
The CA150 control board has LED Wiegand bit counters – 10s and 1s – to indicate the card's binary bits. You must be able to observe the control board to do this procedure. To verify the binary bits, present the card or tag at the reader and count the number of times each LED blinks:

- 10s counts the 1st binary digit
- 1s counts the 2nd binary digit

Example

If the 10s LED blinks 3 times and the 1s LED blinks 6 times, the card has 36 binary bits (36-bit Wiegand card).

Figure 23 - Location of Wiegand Card Bit Counter LEDs



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

The CA150 supports 3 types of input supervision as listed in the table below. DIP switches S2.7 and S2.8 regulate the level of supervision universally for the door contact, the request to exit, and the auxiliary/supervised alarm inputs on the control board. All inputs must be the same type.

Figure 24 – Supervision Mode DIP Switches S2.7 & S2.8

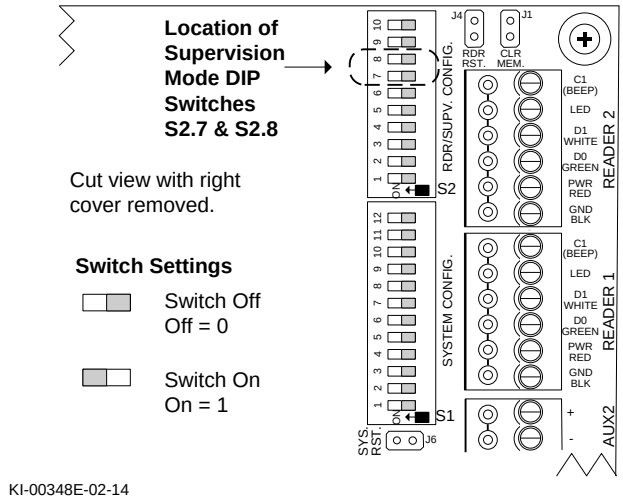


Table 5 – Supervision DIP Switch S2.7 & S2.8 Settings

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

S2.9 & S2.10 System Software Mode DIP Switches

DIP switches S2.9 and S2.10 select the Keyscan software application that is currently installed on the computer/server operating the CA150 control unit. Refer to Table 6 – System Software Mode DIP Switch on page 48 to configure the control board for the appropriate Keyscan software application.

Important

After the control board has been in operation, if the system software mode DIP switches are altered, you must perform a clear memory on the control board. Procedures are outlined on page 49.

The system software mode DIP switches do not require modifications for a software version upgrade.

Figure 25 - System Software Mode DIP Switches S2.9 & S2.10

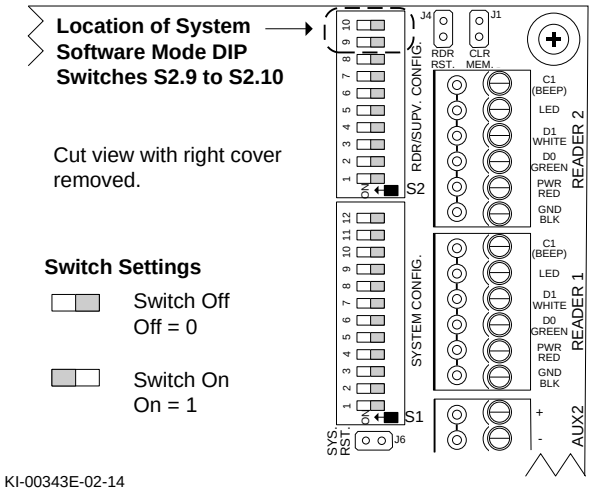


Table 6 – System Software Mode DIP Switch Settings

S2 Switch #	Settings		Keyscan Software	Version
S2.9 & S2.10	Off=0 / On=1		**System Software Mode**	
	S2.9	S2.10		
	0	0	System VII	7.0.14 or higher
	0	1	Vantage	8.1.13 or higher
	1	0	Future use	
	1	1	Aurora (requires firmware 9.20 or higher)	1.0.1.0 or higher

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 CA150 control board:

- when a control board has been newly installed
- when the CA150 has had a flash memory upgrade
- when system software mode DIP switches S2.9 / S2.10 have been changed
- when temporary card countdown DIP switch S1.7 has been changed

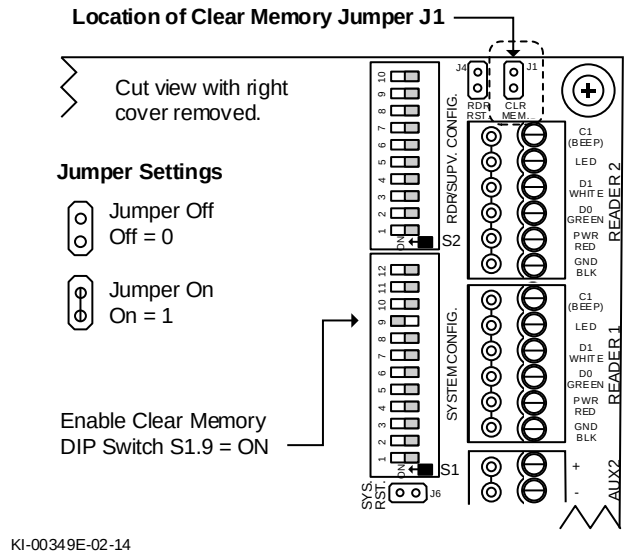
Procedure

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 computer with a Keyscan Client software 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 Keyscan Client software and then upload the Keyscan database information to the control board(s). Until you perform an upload from a Keyscan Client, the access control unit(s) will not function.

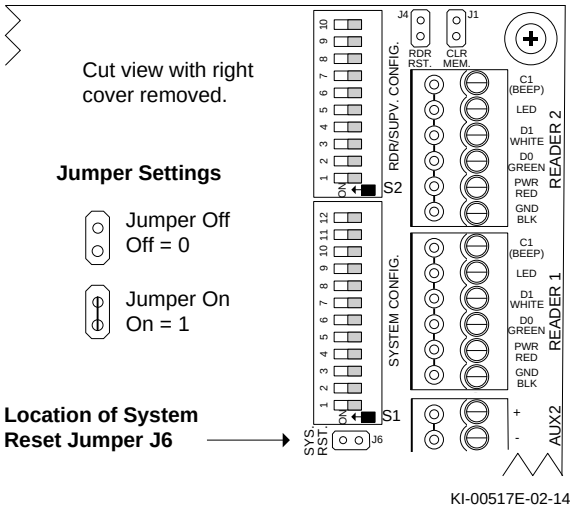
Figure 26 – Restore Default Settings (Clear Memory) J1 Location



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 CA150 control board while it is powered, perform a system reset by momentarily placing a jumper on J6.

Figure 27 – Location of System Reset Jumper J6



Door & AUX Outputs – Powered/Unpowered

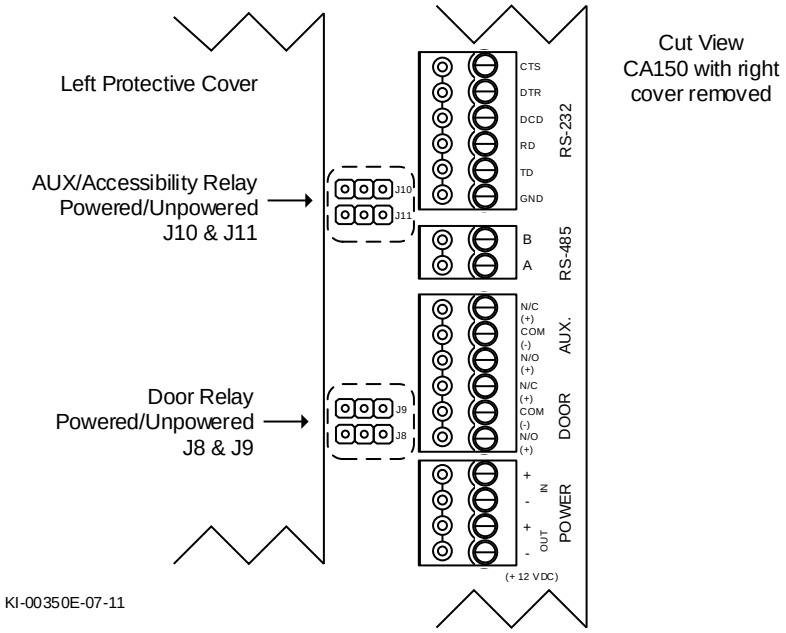
The door output relay and the AUX output relay are each fused at 500 mA. Each output has a set of jumpers which configures the output to source power from the CA150 or configures the output as a dry contact. When the output is configured as a dry contact, the connected device requires an independent power source.

The AUX output may also be configured as an accessibility output. See page 51.

Table 7 - Powered/Unpowered Jumper Settings for Door & AUX Outputs

Output	Device Current	Power Source	Relay Contacts	Jumpers	Settings
Door	500 mA or less	CA150 via PoE or +12 VDC	Powered	J8 J9	
	Over 500 mA	Independent power supply	Unpowered	J8 J9	
AUX	500 mA or less	CA150 via PoE or +12 VDC	Powered	J10 J11	
	Over 500 mA	Independent power supply	Unpowered	J10 J11	

Figure 28 - Location of Door & AUX Relay Powered/Unpowered Jumpers



Accessibility Output Relay

The AUX output relay on the CA150 can be set as an accessibility relay to connect with an electro-mechanical operator that opens and closes a door. System configuration DIP switch S1.8 regulates the relay as either an AUX output or accessibility output.

When DIP S1.8 is enabled, the AUX output is converted to an accessibility output relay. The accessibility output relay pulses an electro-mechanical operator to open the door. The control unit imposes the door unlock time based on the accessibility door timer setting and monitors the door contact based on the accessibility door held open time setting in the Client software. Credential holders assigned with an Accessibility designation in the Keyscan Client software on a card presentation at the reader will automatically trigger the output with its accessibility properties.

Note – Aurora Software

If using Aurora, the output follows the extended entry time and extended entry door held open settings in the Client. Credential holders must have the extended entry setting enabled in their records in the Client to trigger the output with its extended entry properties.

Figure 29 – AUX/Accessibility Switch S1.8

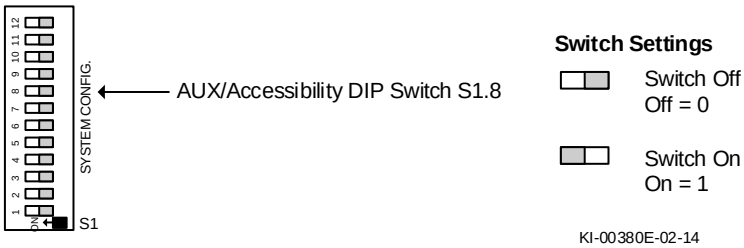
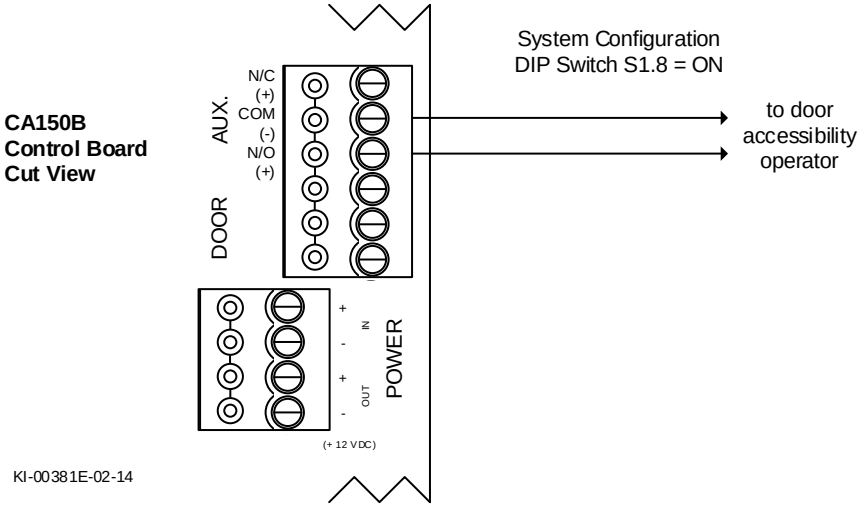


Table 8 – AUX / Accessibility Relay DIP Switch Settings

Mode	DIP Switch #	Setting
		Off=0 / On=1
AUX output	S1.8	0
Accessibility output	S1.8	1

Figure 30 – Accessibility Output Relay Connections



Communication

Communication must be established between the computer/server with the Keyscan software and the CA150 access control unit. The CA150 control unit supports the following modes of communication:

- Serial RS-232
- USB (USB 1.1 & USB 2.0 supported) / RS-232
- Network (TCP/IP)

Network (TCP/IP) Communication

If the CA150 is connected on a network, ensure that you review either Program On-board Ethernet Module on page 93 or Configure CA150 for Reverse Network Communication on page 97. Before the CA150 can become operational on a network, it must be programmed using the procedures outlined in one of the aforementioned topics.

The CA150 requires NETCOM Program Utility – version 6.0.18 or higher. Always use the latest NETCOM Program Utility on the enclosed CD when programming the on-board Ethernet module.

Single Control Unit Communication Only

The CA150 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 CA150 does not support global functions.

Keyscan RS-232 Data Cable

If using the Keyscan RS-232 data cable, it has multiple applications for various Keyscan products and as such has a generic configuration for the loose wires. When it is used in applications where the shield must be connected to the metal enclosure ground lug, we suggest one of following wiring options:

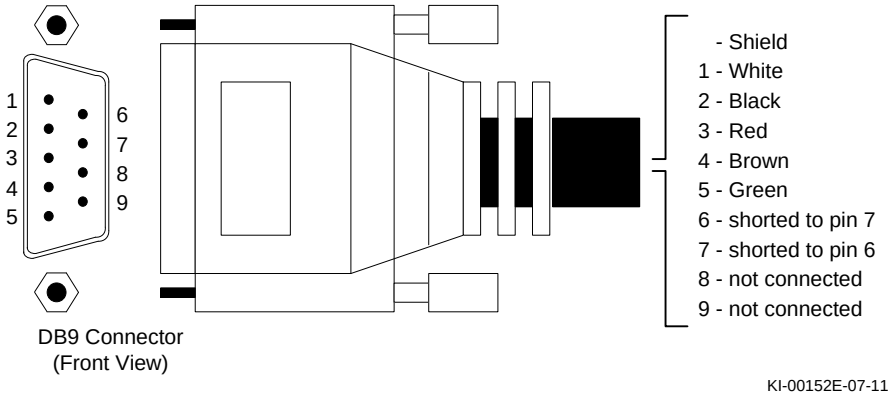
- Option A – trim back the shield wire to approximately 0.5” (1.5 cm) then solder an appropriate length of green # 20 AWG wire to the shield and terminate the shield at the ground lug
- Option B – remove sufficient cable jacketing allowing the shield wire to return to the ground lug from the communication connector. Trim the 5 communication wires to a length of 2.5” (6.5 cm) and strip the ends

Insulate the shield wire with a length of tubing to prevent it from shorting. Terminate the shield.

Configure a 9-pin RS-232 Data Cable

In the event that you are establishing a serial connection from the computer to the control board and you have to make a 9 pin, RS-232, data cable, ensure that you follow the pin to wire colour assignments on the following diagram. It is strongly recommended that you use a Keyscan 9 pin, RS-232 data cable (dormakaba Canada Inc. part # 40-2322) which is manufactured specifically for Keyscan serial data connections.

Figure 31 – RS-232 Data Cable Connections



Installation Notes

Typically, the black wire of the RS-232 cable from the computer, which is the receive data input of the computer, is connected to the serial port TD pin of most Keyscan products.

Typically, the red wire of the RS-232 cable, which is the transmit data output of the computer, is connected to the RD pin of most Keyscan products.

Figure 32 – Communication – RS-232 Direct Serial

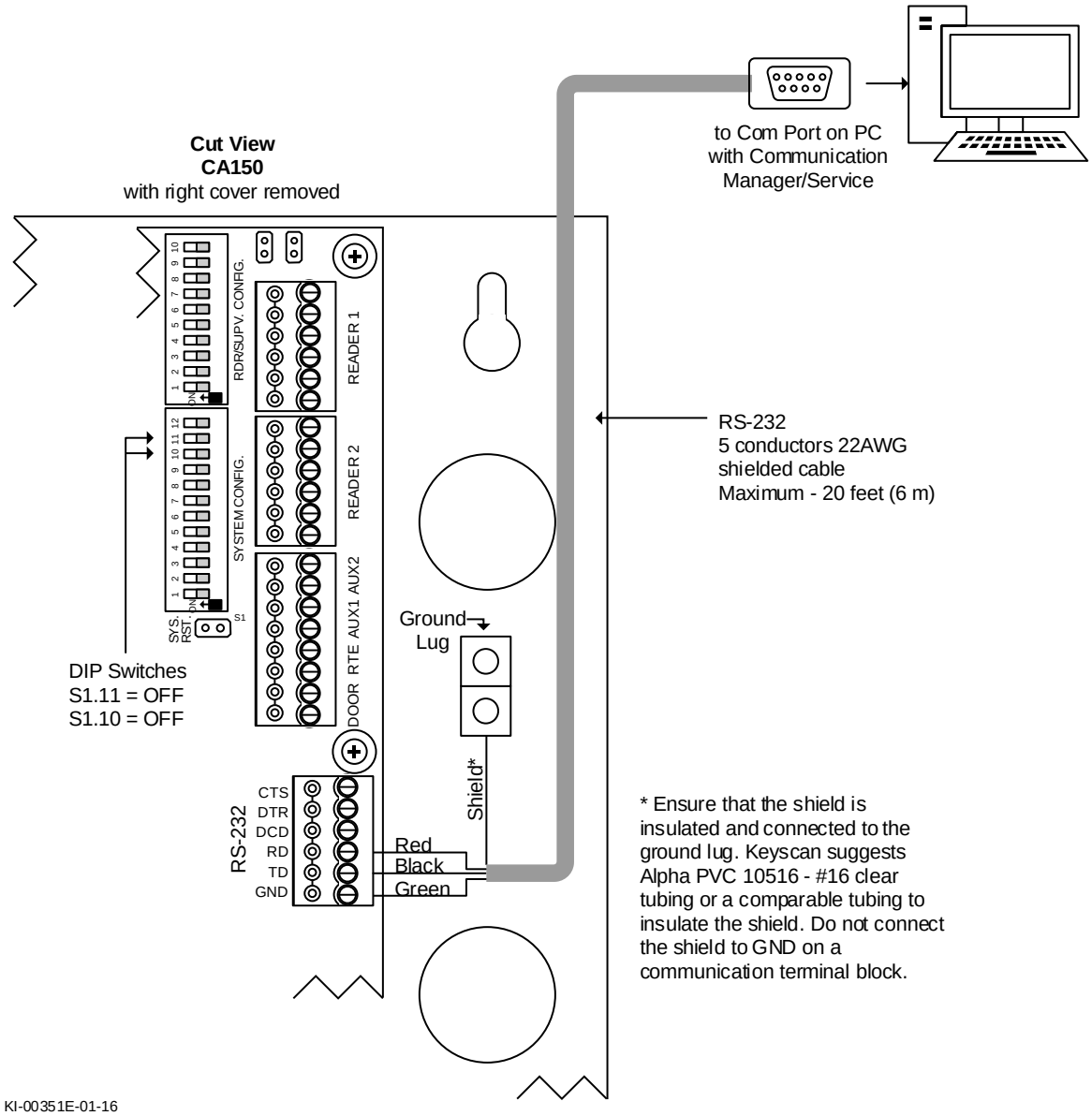


Figure 33 – Communication - USB Adaptor/Computer

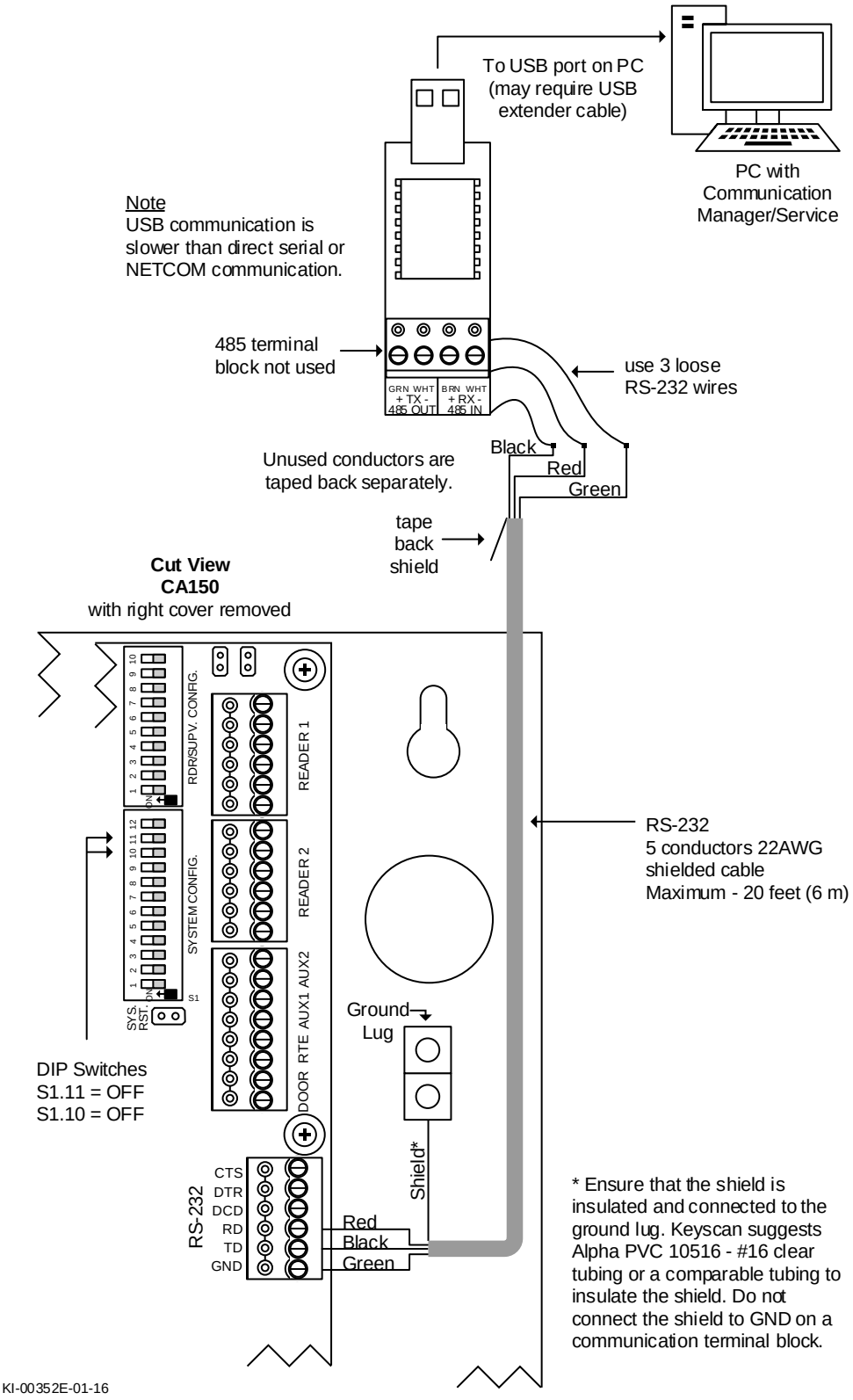
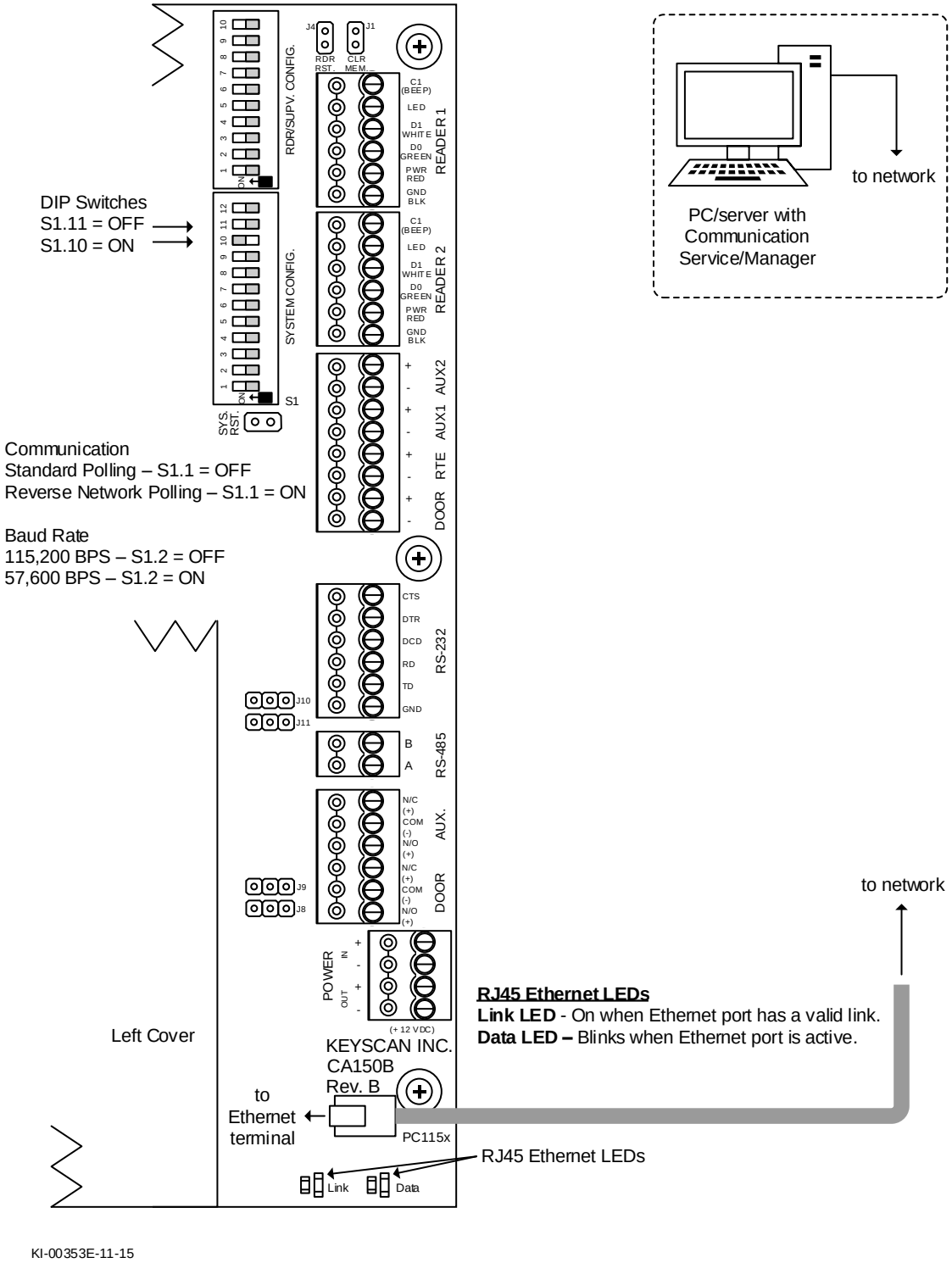


Figure 34 - Communication – Ethernet

Also see Figure 7 – Grounding Access Control Units and Cables – to properly ground the unit when using PoE.



Power-up & Test Voltages

The CA150 can be powered via the following sources:

- Ethernet connector using PoE (Class 0)
- TB6 with a +12V DC, UL approved, power supply

We recommend the CA150 power is supplemented with an appropriate backup battery ensuring continued operation in the event of a power failure.

PoE

The CA150 has a built-in PoE power supply which provides power to the control board and the connected hardware. The PoE power supply has the following maximum current rating:

- 680mA @ 12V (approximately 8 Watts)

The CA150 operates as a Class 0 PoE Powered Device (PD). As such, the CA150 requires the allocation of 15.4 Watts from the PoE switch or injector. Of the 15.4 Watts, the CA150 provides 680mA at 12 volts - approximately 8 Watts - to power connected peripheral devices such as readers, door strikes, PIR sensors, etc.

When using the CA150's on-board PoE power supply, the total number of connected hardware devices including the door strike cannot exceed the 680 mA threshold; otherwise, a separate +12V DC power supply with a sufficient current rating is required. See PTC resetting fuses for maximum port currents.

PTC Resetting Fuses

The power sourcing ports on the CA150 are current limited with PTC resetting fuses with the following ratings:

- Reader 1 port – 500 mA
- Reader 2 port – 500 mA
- Door output – 500 mA
- Aux/Accessibility output – 500 mA
- RTE port – 300 mA

System Power-up

Depending how the CA150 is connected for power – PoE (Class 0) or a +12V DC separate supply – refer to the relevant power up instructions.

Important

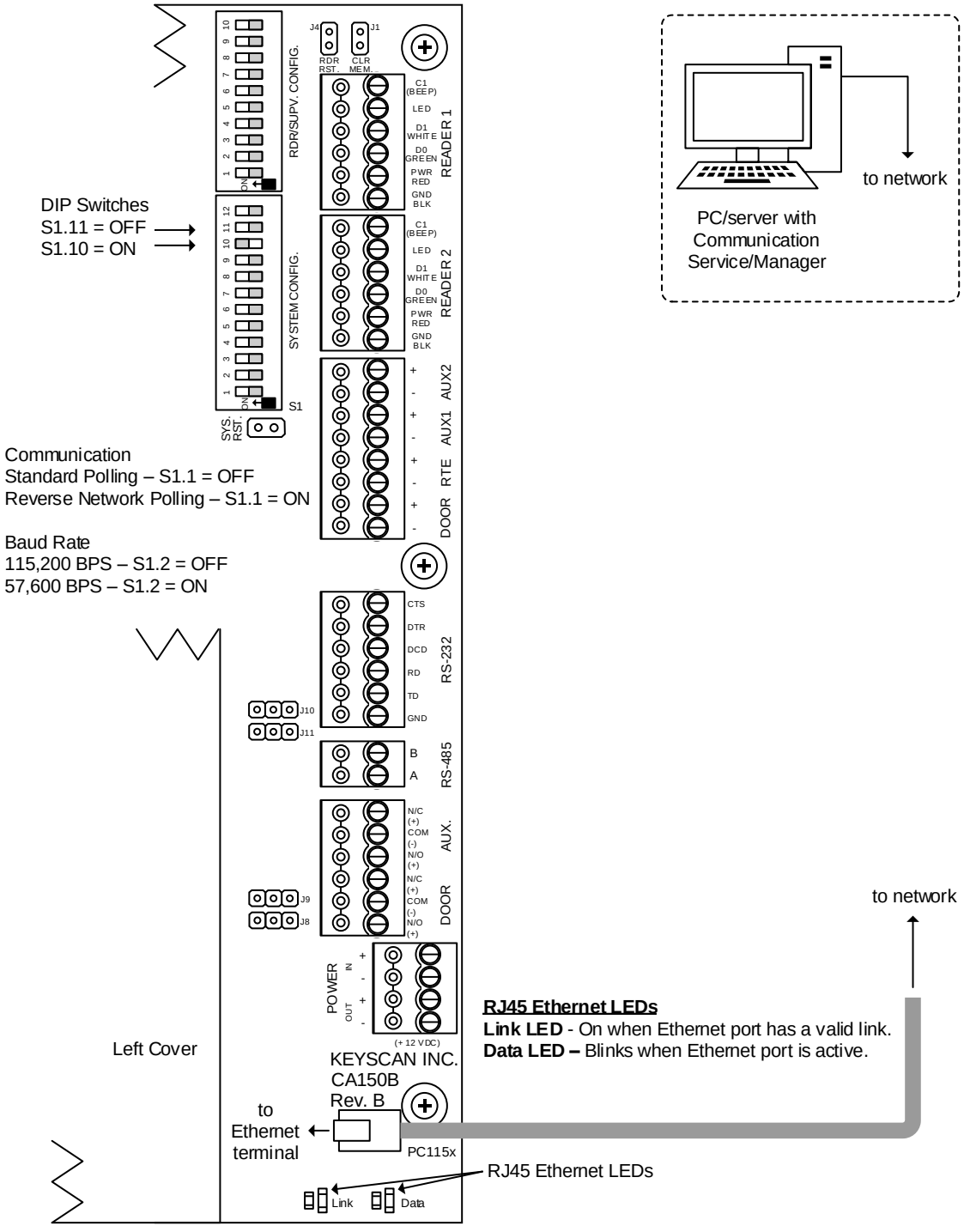
After the control board has been powered up for the first time, be sure to reset the factory defaults by performing a clear memory procedure outlined on page 49. After the control board has been installed, powered and tested, return to a computer/server with the Keyscan Client software and perform a full panel upload to populate the control board with the Keyscan database.

PoE

- Ensure the right cover on the CA150 control board has been removed.

- Connect the Ethernet cable from the PoE power source – the network switch or the injector – into the Ethernet terminal on the CA150 control board.
    - Within 5 seconds of establishing the connection, the CA150 should receive power from the PoE source and begin 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 CA150 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)
    - AUX output N/C or N/O (if set on POWERED)

Figure 35 - PoE Connections

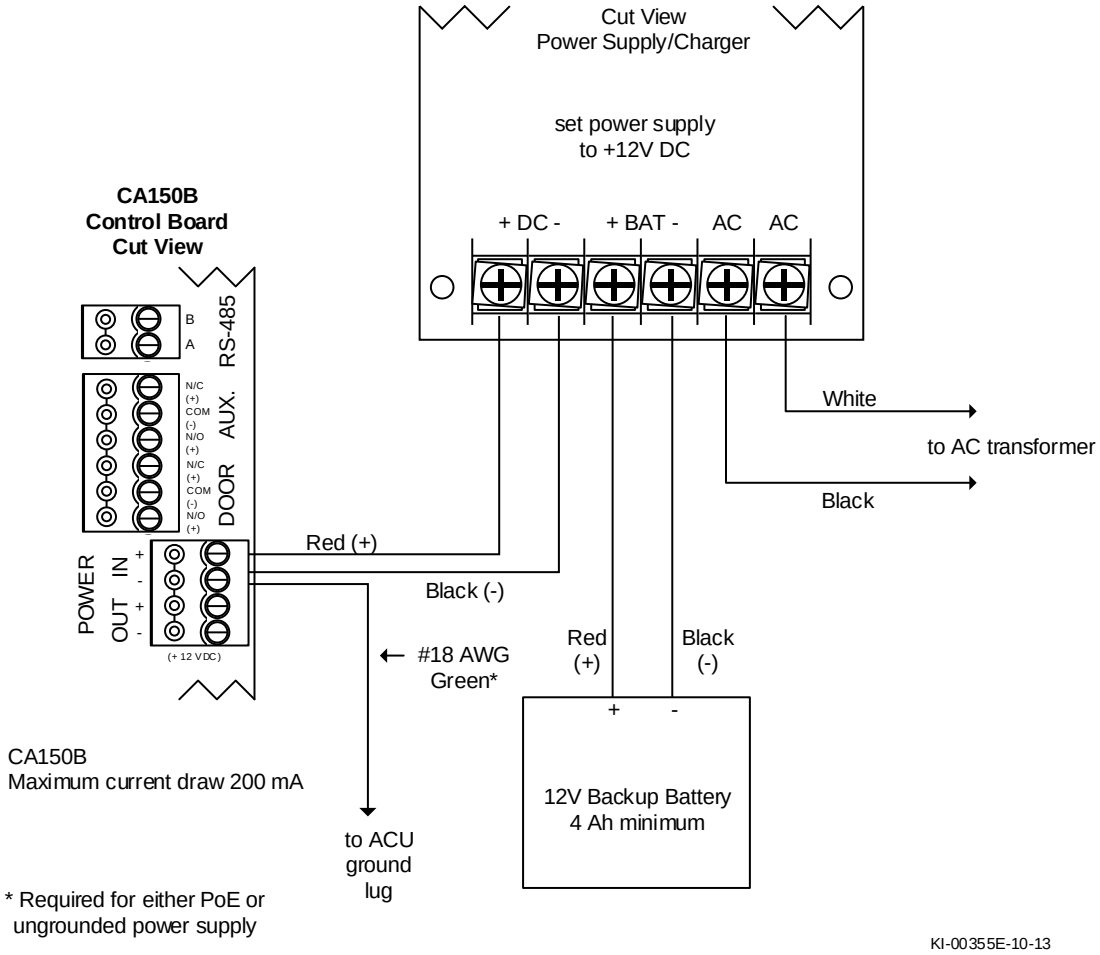


KI-00353E-11-15

DC Power Supply +12V DC

- Ensure the right cover on the CA150 control board has been removed.
- Connect the +12V DC power supply to the POWER IN terminals (TB6) on the CA150.
  - Upon applying power, the CA150 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 CA150 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)
  - AUX output N/C or N/O (if set on POWERED)

Figure 36 – 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.

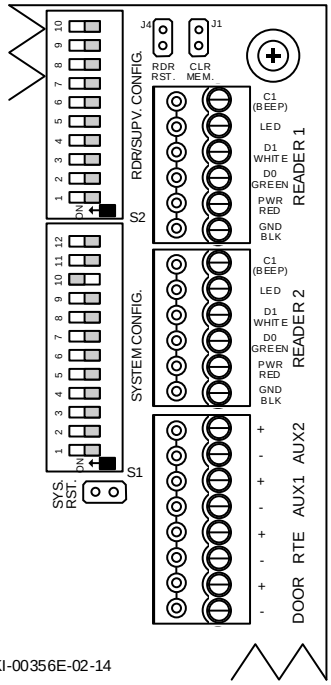
Voltmeter Connections

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

Table 9 – 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 37 – Control Board Test Points – Voltages



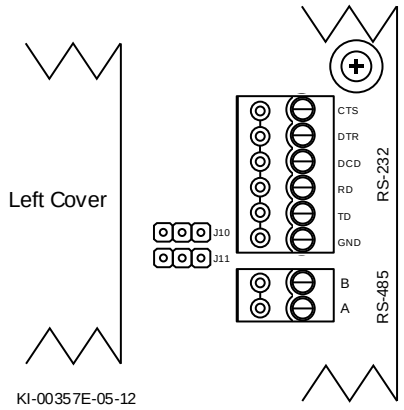
Test Points – Communication Terminals

The following table outlines the correct voltages for the test points on the RS-232 communication terminal.

Table 10 – Communication Voltage Test Points

Communication Test Point	Voltage	Instructions/Notes
Control Board Communication Terminal RS-232 connected to ACU		Connect Voltmeter COM to GND on ACU communication terminal block or green on data cable.
GND		
TD	(-) 9 VDC	TD is an ACU generated voltage
RD	(-) 10 VDC	RD is a computer generated voltage
DCD		Used for modems only
DTR	n/a	
CTS	n/a	

Figure 38 – Control Board Communication Test Points



Diagnostics

The CA150 has communication and system status LEDs on the left side of the control unit for diagnostics.

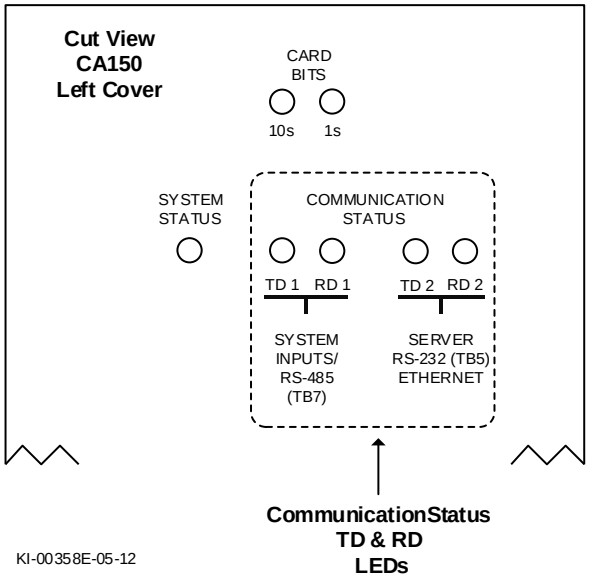
Communication LEDs

The CA150 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 11 – 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 or RS-485 port
	Not Illuminated – abnormal condition	Follow restore factory defaults J1 procedure in attempt to resolve.
	Illuminated – abnormal condition	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 or RS-485 port
	Not Illuminated – abnormal condition	Follow restore factory defaults J1 procedure in attempt to resolve
	Illuminated – abnormal condition	Follow restore factory defaults J1 procedure in attempt to resolve Possible wiring fault
TD 2 – Green	Flashing – normal	Control board sending data via communication path determined by S1.10 & S1.11 to Client/Communication Mgr
	Not Illuminated	If Client/Comms not polling the control board If S1.10 & S1.11 are configured for on-board NETCOMP programming
	Illuminated – abnormal condition	Follow restore factory defaults J1 procedure in attempt to resolve
RD 2 – Red	Flashing – normal	Control board receiving data via communication path determined by S1.10 & S1.11 from Client/Communication Mgr
	Not Illuminated	If Client/Comms not polling the control board If S1.10 & S1.11 are configured for on-board NETCOMP programming
	Illuminated – abnormal condition	Possible wiring fault

Figure 39 – Communication Status LEDs



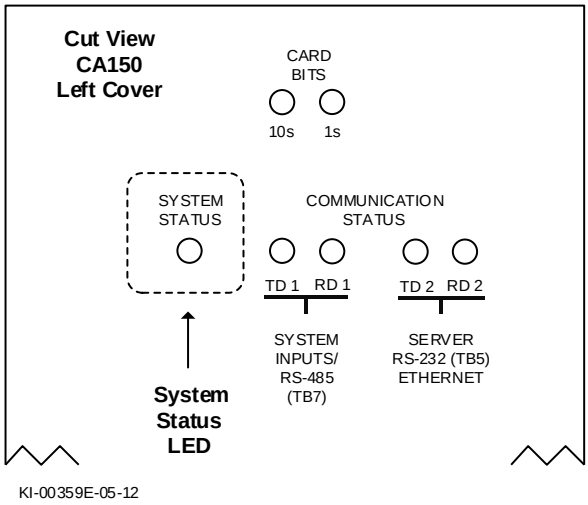
System Status LED

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 12 - 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 Client software since its last system reset or clear memory.
Amber - flashing	The control board's last communication with the Client software was 3 minutes or greater.
Green – solid	The control board has communicated to the Client software since its last system reset or clear memory

Figure 40 - Location of System Status LED



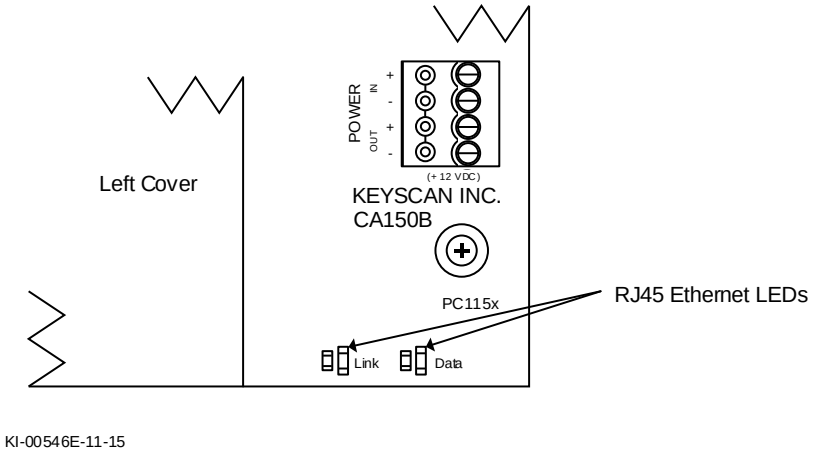
RJ45 Ethernet LEDs

The RJ45 Ethernet terminal has a Link LED and a Data LED positioned on the face of the control board in the lower right corner which indicate network communication as outlined:

Table 13 – RJ45 Ethernet LEDs

Link LED Colour/State	Data LED Colour/State
Green - On when Ethernet port has a valid link	Green – Blinks when Ethernet port is active

Figure 41 – Location of RJ45 Ethernet LEDs



Keyscan / HID Readers

This section reviews typical connections for Keyscan readers and HID 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 and HID reader power requirements.

Table 14 – Keyscan & HID Reader Power Specifications

Reader	Power	Notes
K-PROX2 & K-PROX SG (125 kHz)	12 VDC, 80 mA	
K-VAN	12 VDC, 90 mA	
K-KPR	12 VDC, 115 mA	
K-SMART (13.56 MHz)	12 VDC, 210 mA	
K-SMART GOV (Legacy)	12 VDC, 210 mA	
HID-5365	12 VDC, 110 mA	
HID-5395	12 VDC, 115 mA	
HID-6005	12 VDC, 75 mA	
HID-5455	12 VDC, 125 mA	
HID-5355KP	12 VDC, 120 mA	
HID 5375	24 VDC, 1.5 A	Requires 18 AWG cable. Connect to separate 24 VDC 2 Amp linear power supply. (Not supplied with ACU)
KR90L – HID iClass Long Range Reader	12 VDC 1300 mA in-rush 110 mA standby 300 mA peak	12 VDC - 2 amps independent power supply per KR90L with 18 AWG cable recommended
HID iClass Legacy		**HID Base Part #**
KR10L	12 VDC, 60 mA	900N
KR40L	12 VDC, 65 mA	920N
KRK40L	12 VDC, 85 mA	921N

Reader	Power	Notes
HID multiClass Legacy		
KRP10L	12 VDC, 75 mA	900P
KRP15L	12 VDC, 75 mA	910P
KRP40L	12 VDC, 85 mA	920P
KRPK40L	12 VDC, 95 mA	921P
HID pivClass Legacy		
R10HGOV	12 VDC, 60 mA	900NHR
RP10HGOV	12 VDC, 75 mA	900PHR
R15HGOV	12 VDC, 60 mA	910NHR
RP15HGOV	12 VDC, 75 mA	910PHR
R40HGOV	12 VDC, 65 mA	920NHR
RP40HGOV	12 VDC, 85 mA	920PHR
RK40HGOV	12 VDC, 85 mA	921NHR
RPK40HGOV	12 VDC, 95 mA	921PHR
HID iClass SE		
KR10SE	12 VDC, 60 mA	900N
KR40SE	12 VDC, 65 mA	920N
KRK40SE	12 VDC, 85 mA	921N
HID multiClass		
KRP10SE	12 VDC, 75 mA	900P
KRP15SE	12 VDC, 75 mA	910P
KRP40SE	12 VDC, 85 mA	920P
KRPK40SE	12 VDC, 95 mA	921P

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. The following diagrams illustrate HID readers with dual LEDs. On models 5365, 5395, and 6005 do not use the brown wire with "00" LED. If readers are single LED type "06", substitute the brown wire in place of the orange wire.

- S16 – 5 ON dual LED = 00
- S16 – 5 OFF single LED = 06

C1 Beep

When the pre-alert wire is connected to C1 (Beep) on the reader terminal, the reader will also sound on an "alarm tripped".

Figure 42 – Keyscan K-PROX2 (125 kHz)

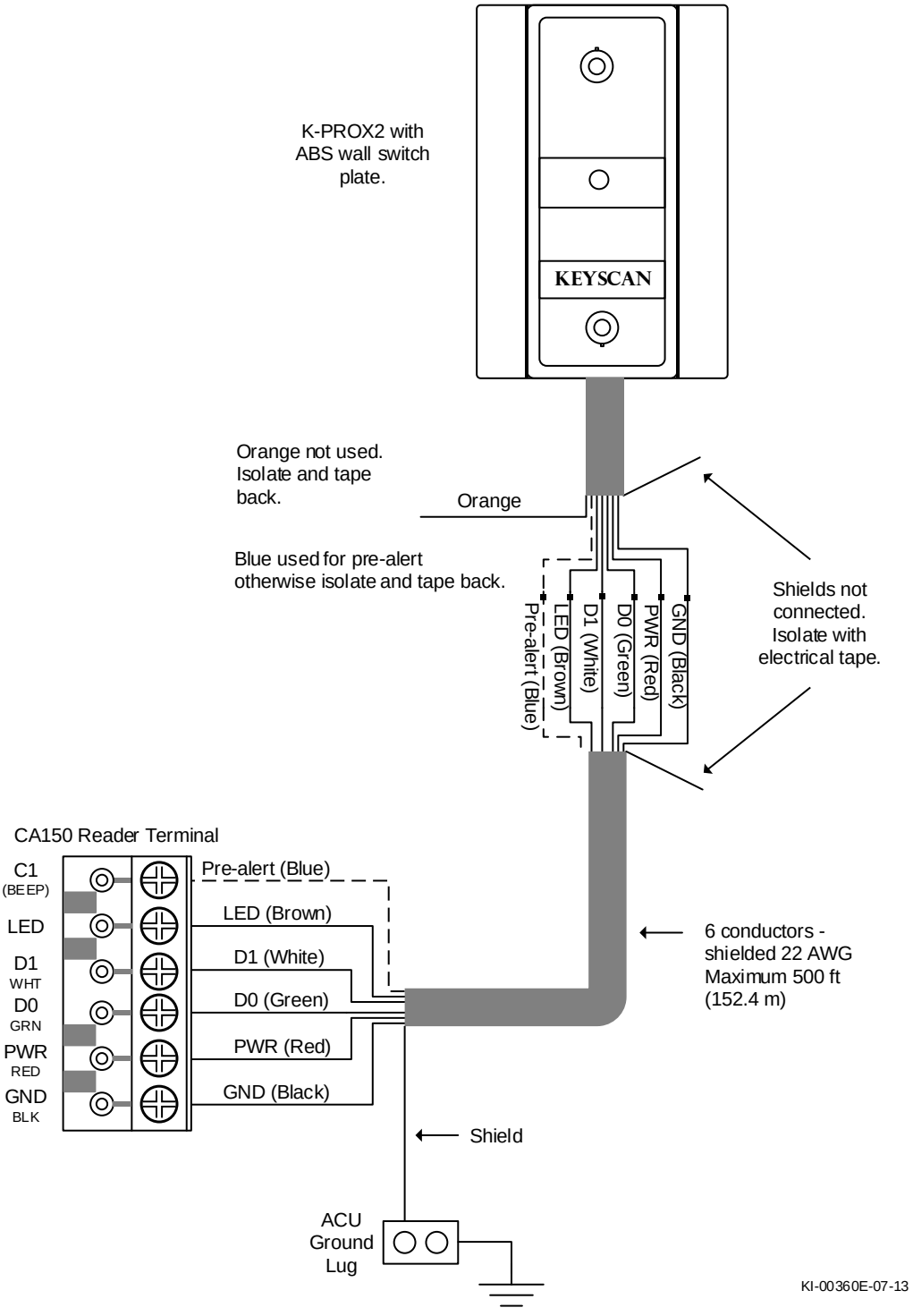


Figure 43 – Keyscan K-VAN Proximity Reader (125 kHz)

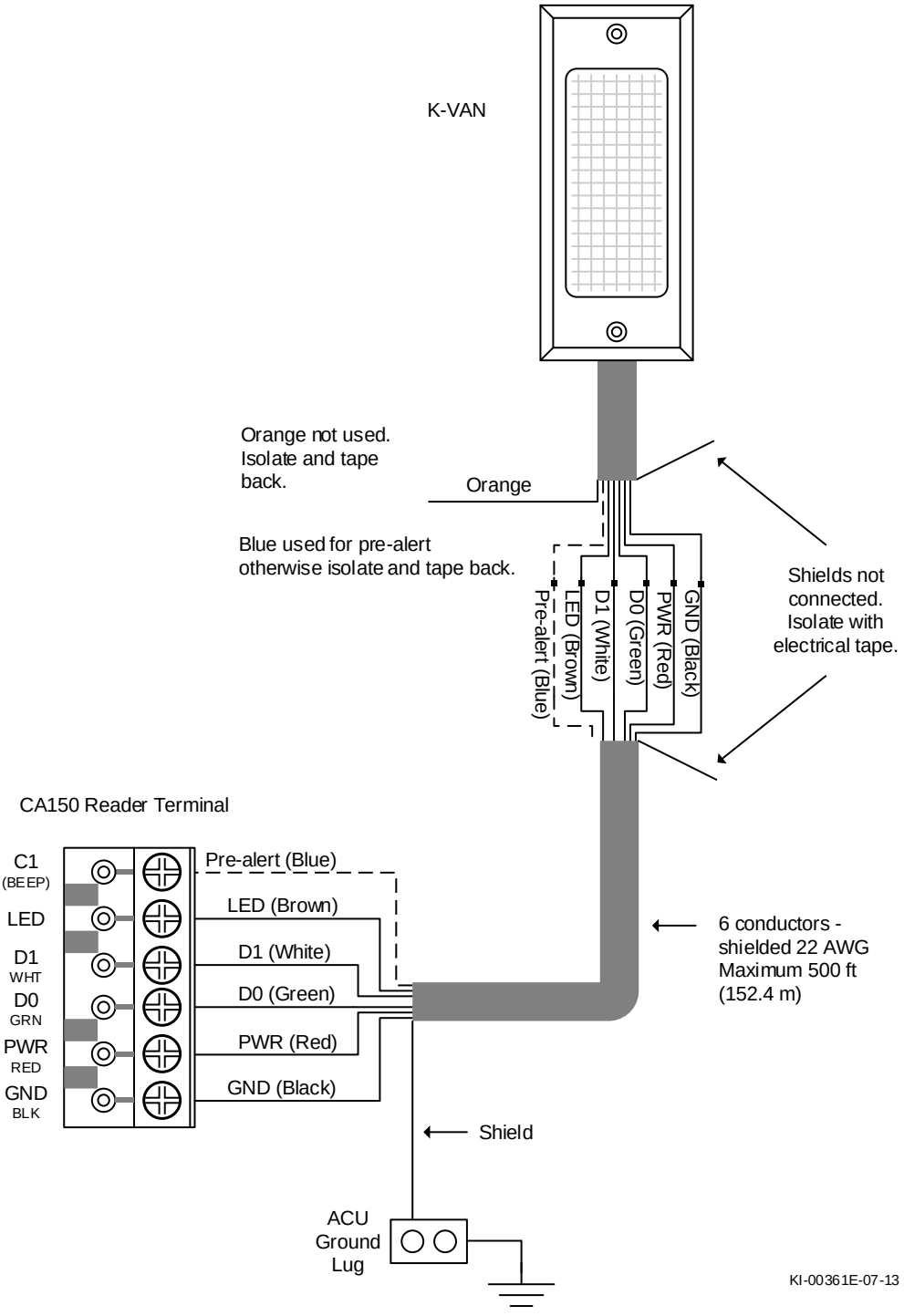


Figure 44 – Keyscan K-KPR Keypad / Proximity Reader (125 KHz)

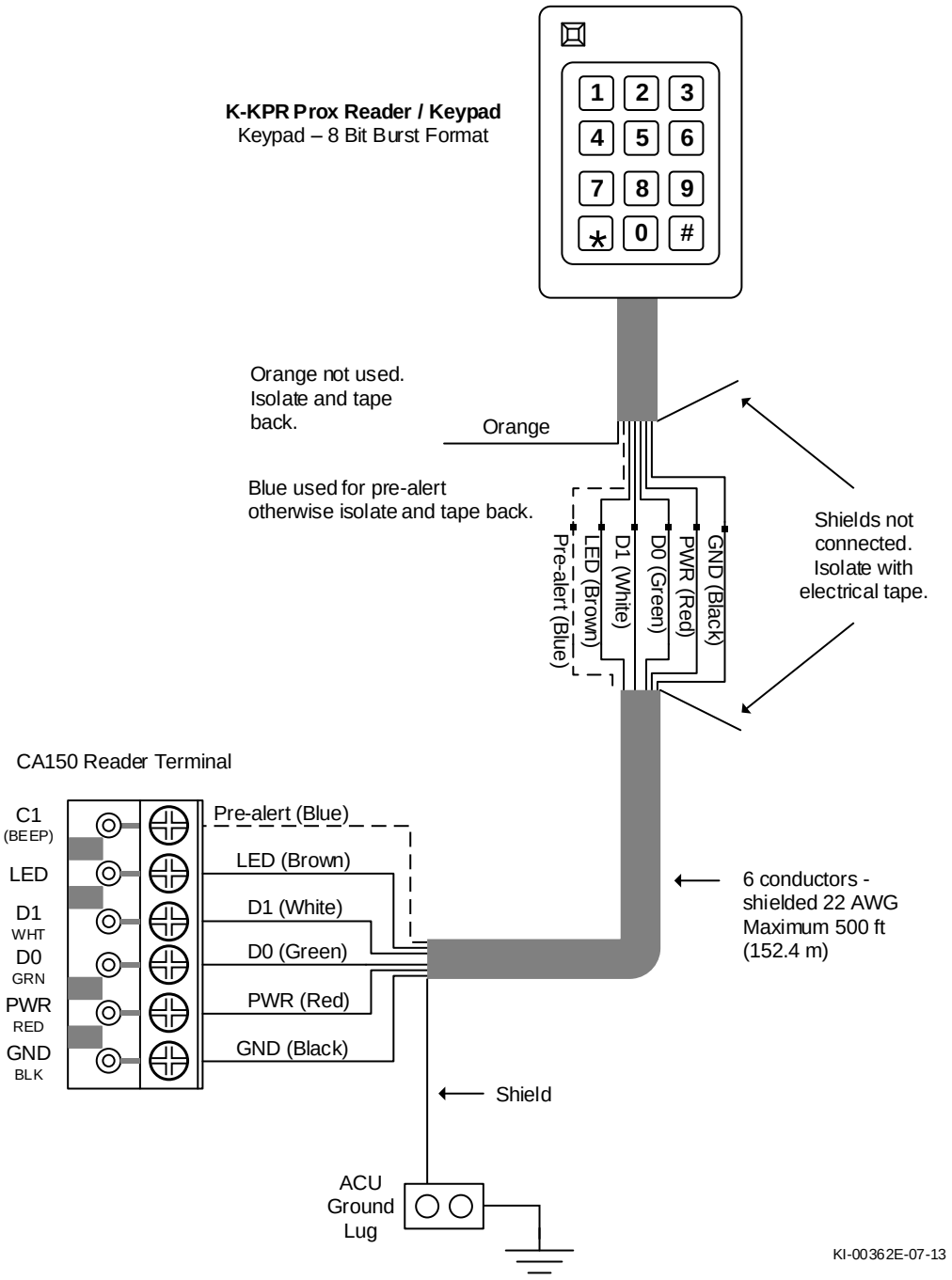


Figure 45 – Keyscan K-SMART Reader

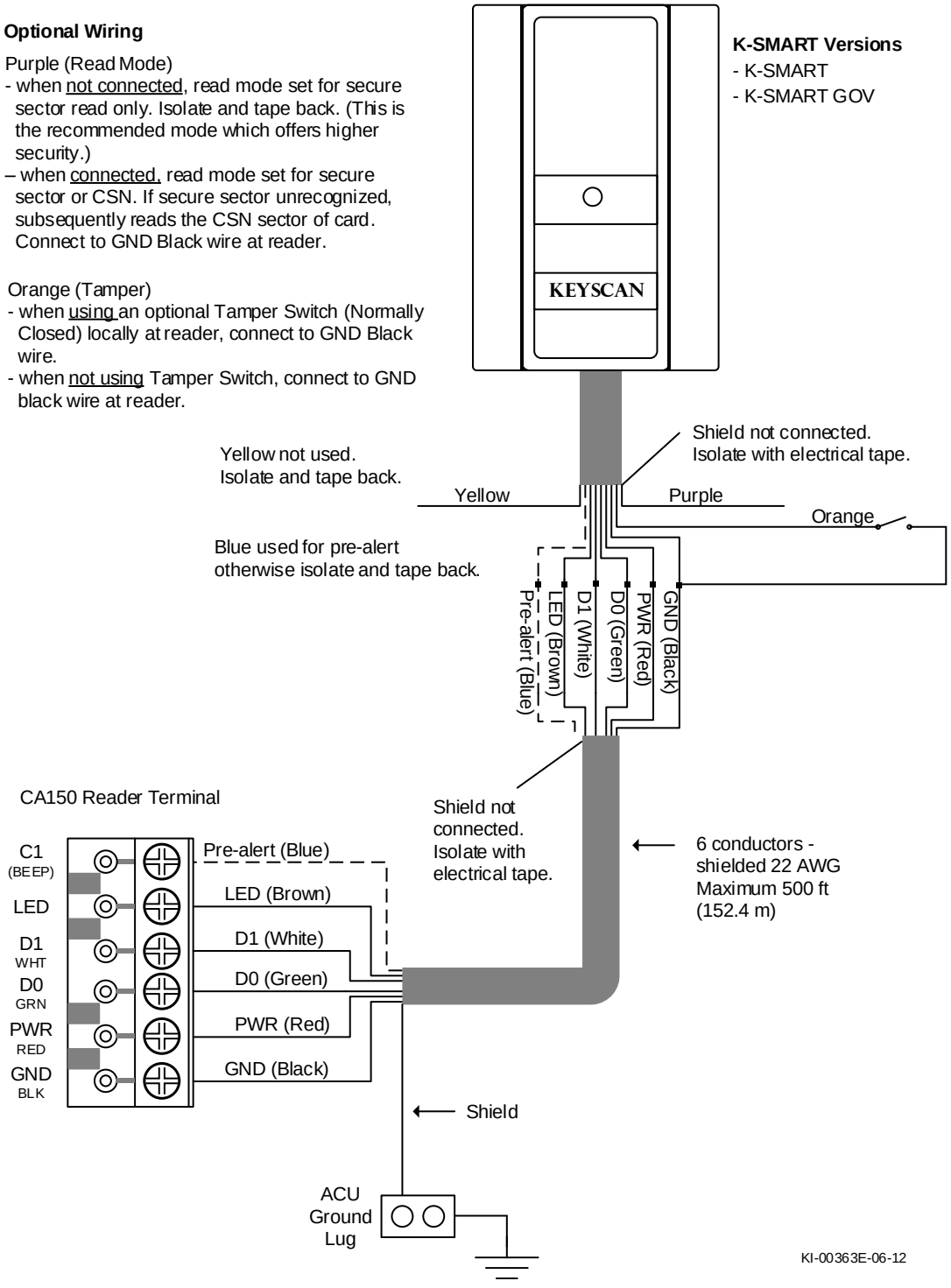


Figure 46 – HID-5395 Wiring

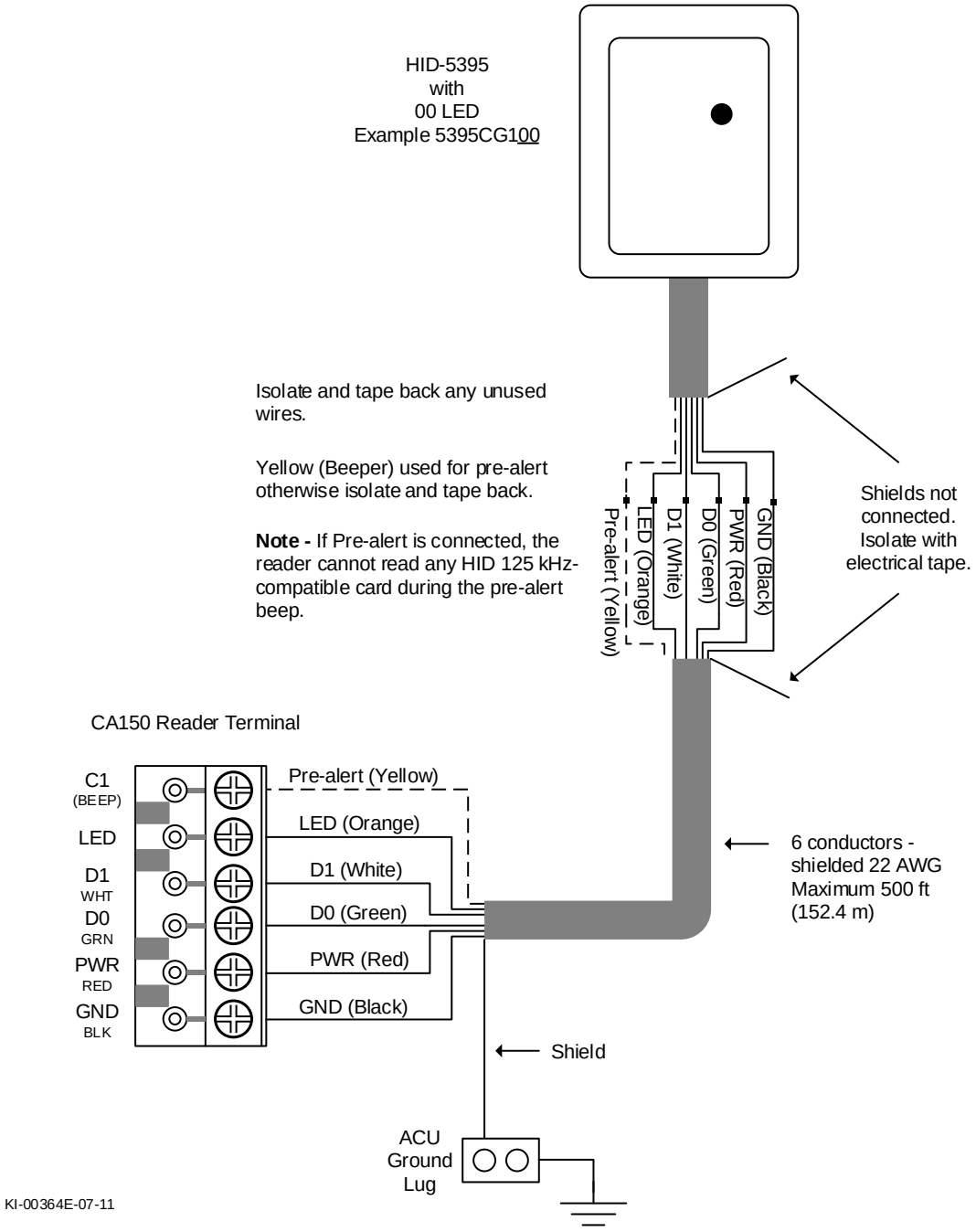


Figure 47 – HID 5365 / 6005 Wiring

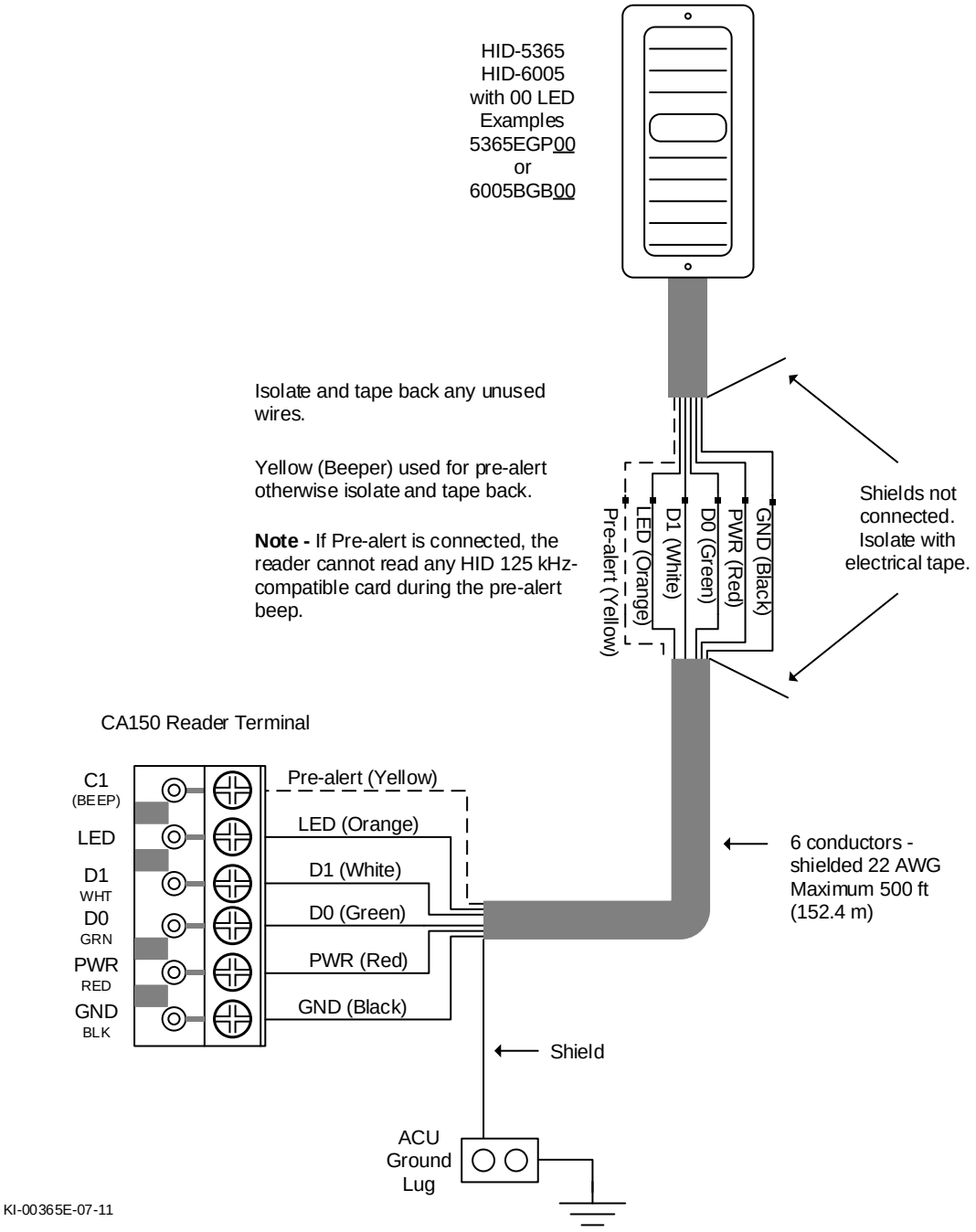
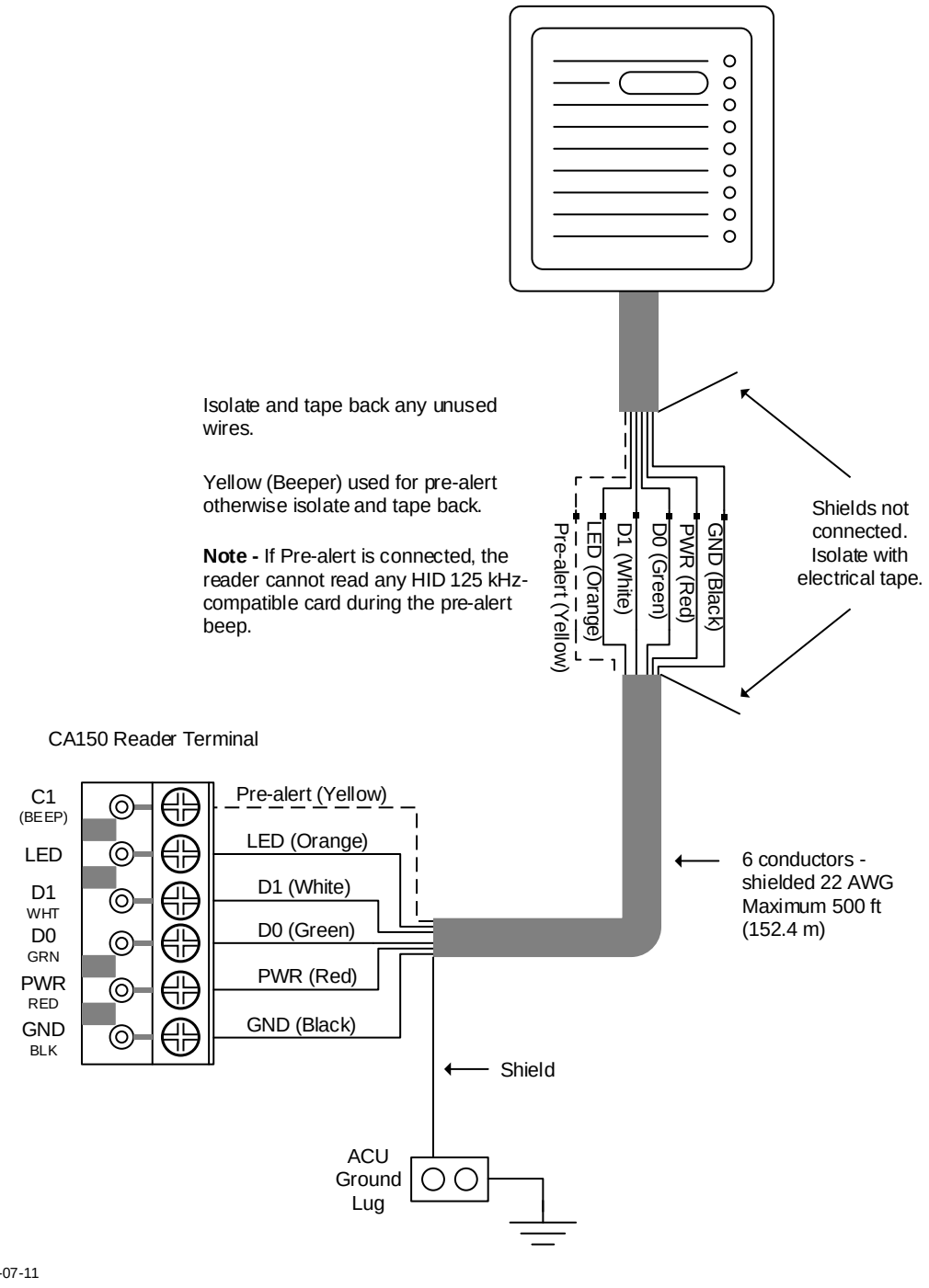


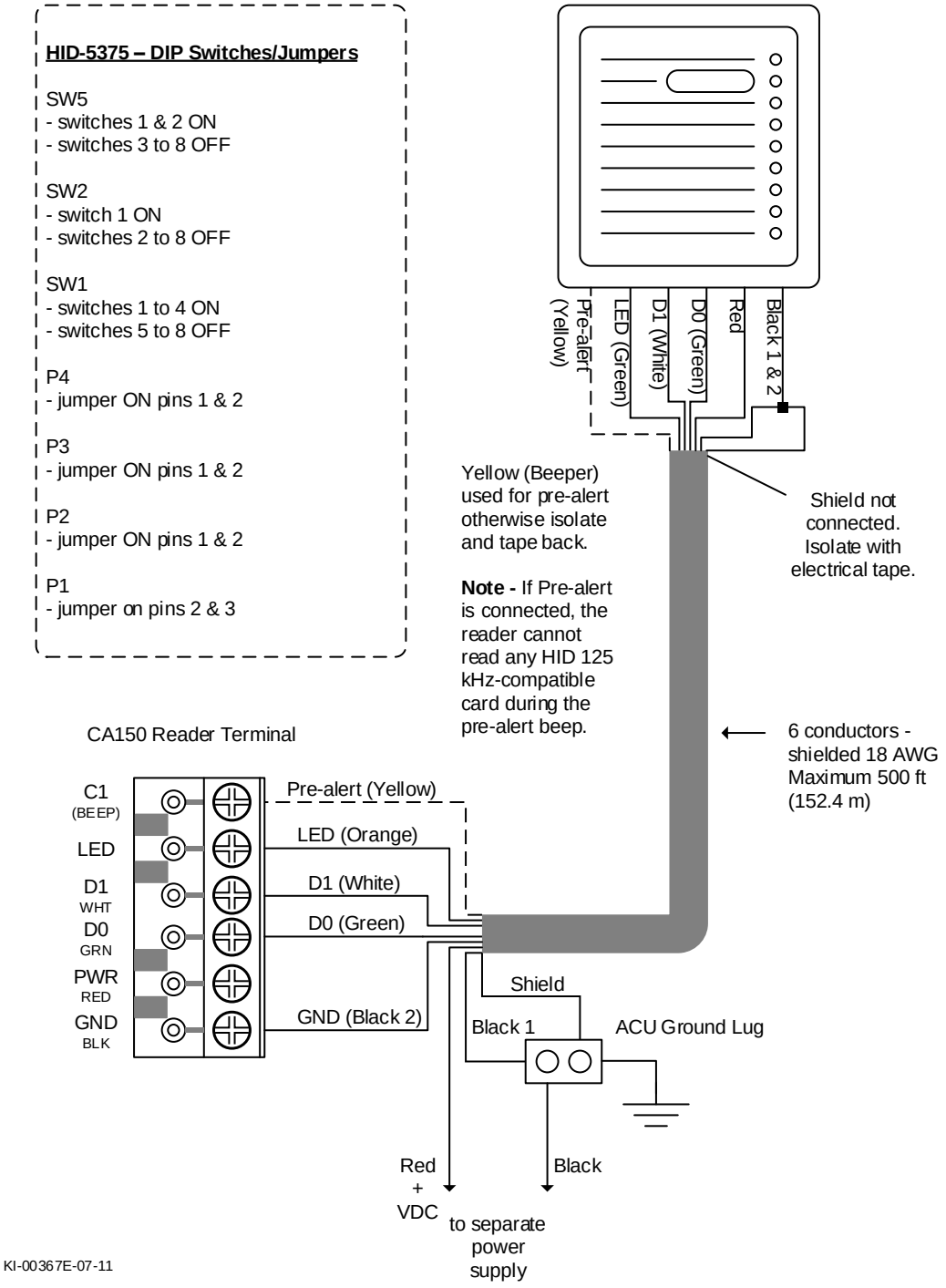
Figure 48 – HID 5455 Wiring



<u>Notes on HID 5455</u>

The HID 5355 is suitable for indoor and outdoor use. Maximum read range at 12VDC – ProxCard II card is 9" (22 cm) – ISOProxII card is 8" (20 cm).

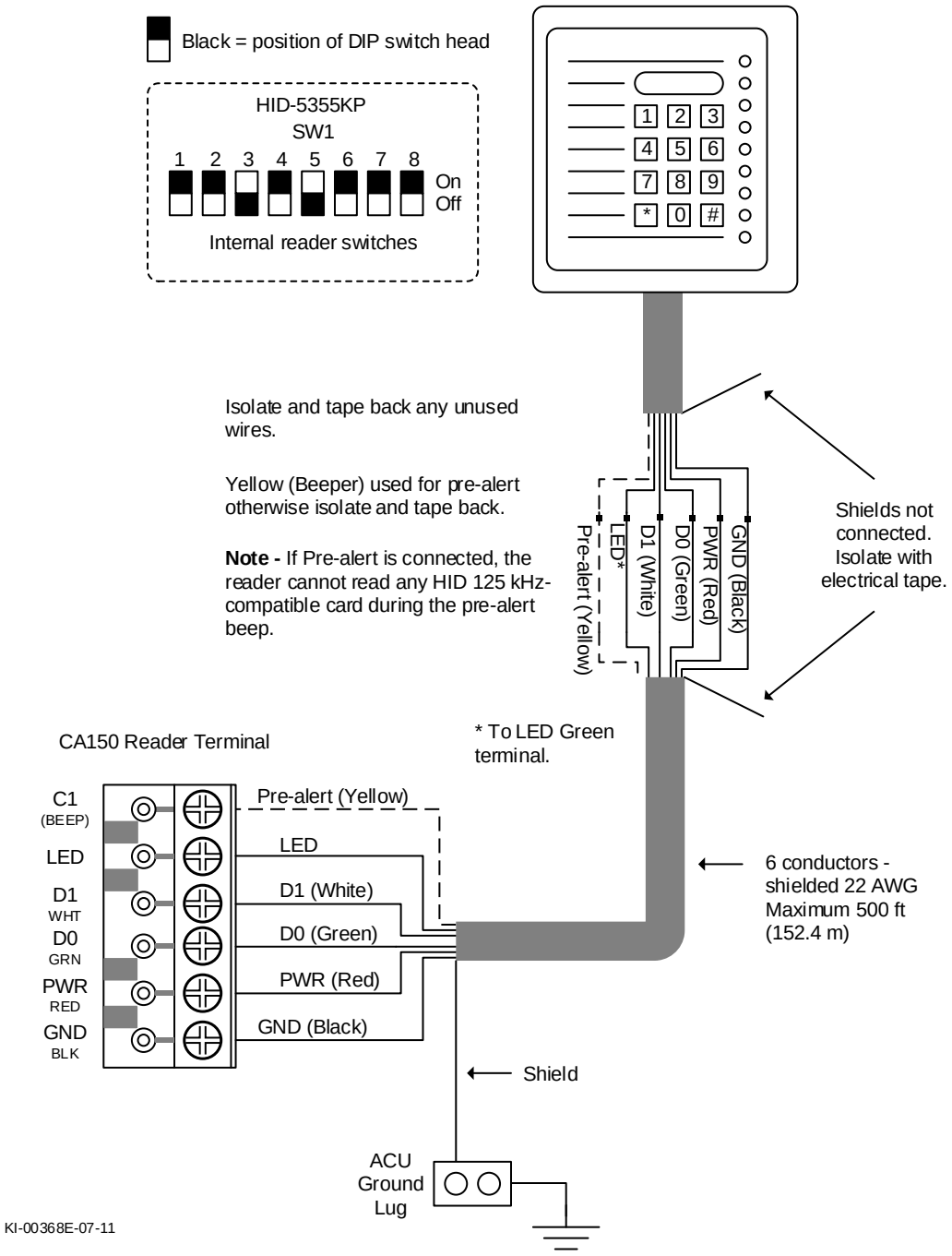
Figure 49 – HID 5375 Wiring



Notes on HID 5375

HID 5375 operates at 12 VDC or 24 VDC. Refer to HID literature for correct jumper settings. If configured for 12 VDC, do not connect to 24 VDC power supply, otherwise damage to the reader circuit board will result.

Figure 50 – HID 5355KP Wiring



<u>Note on HID 5355 KP</u>

Reader/Keypad/LED ordered as 00 (4 bit burst) example 5355AGK00 (Red/Green colour)

Figure 51 – HID iClass KEYR10

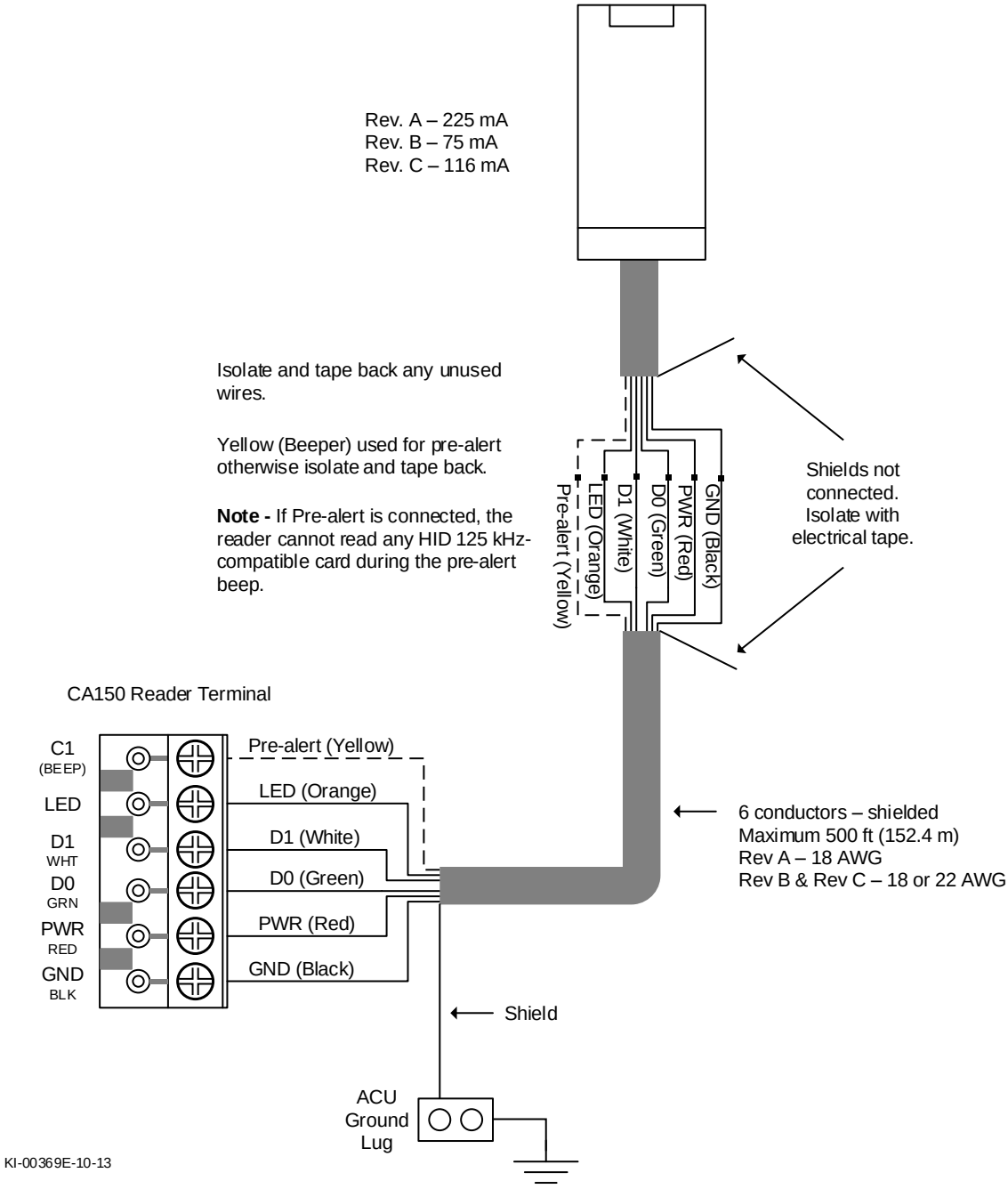


Figure 52 – HID iClass KEYR40

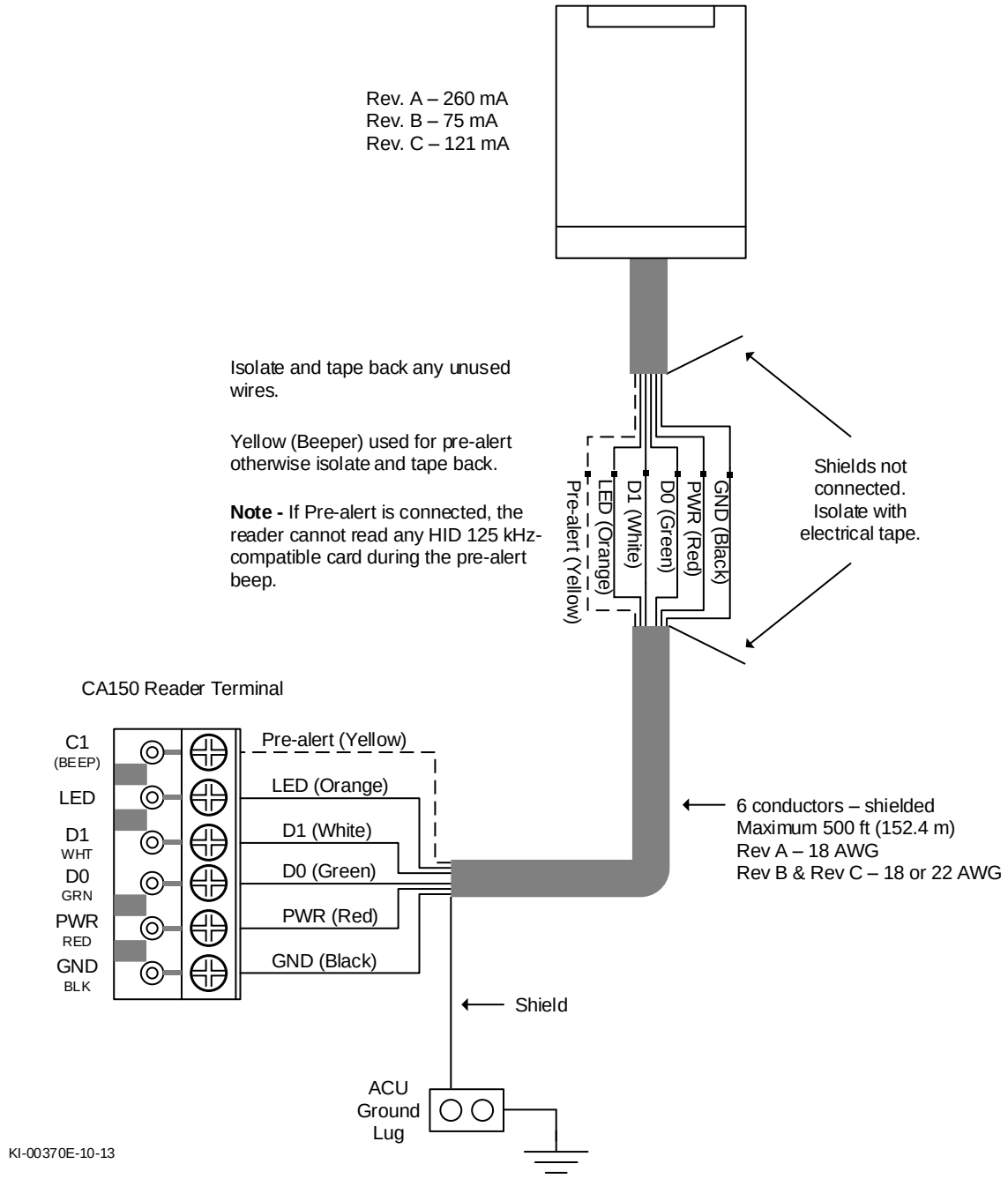


Figure 53 – HID iClass KEYRW400

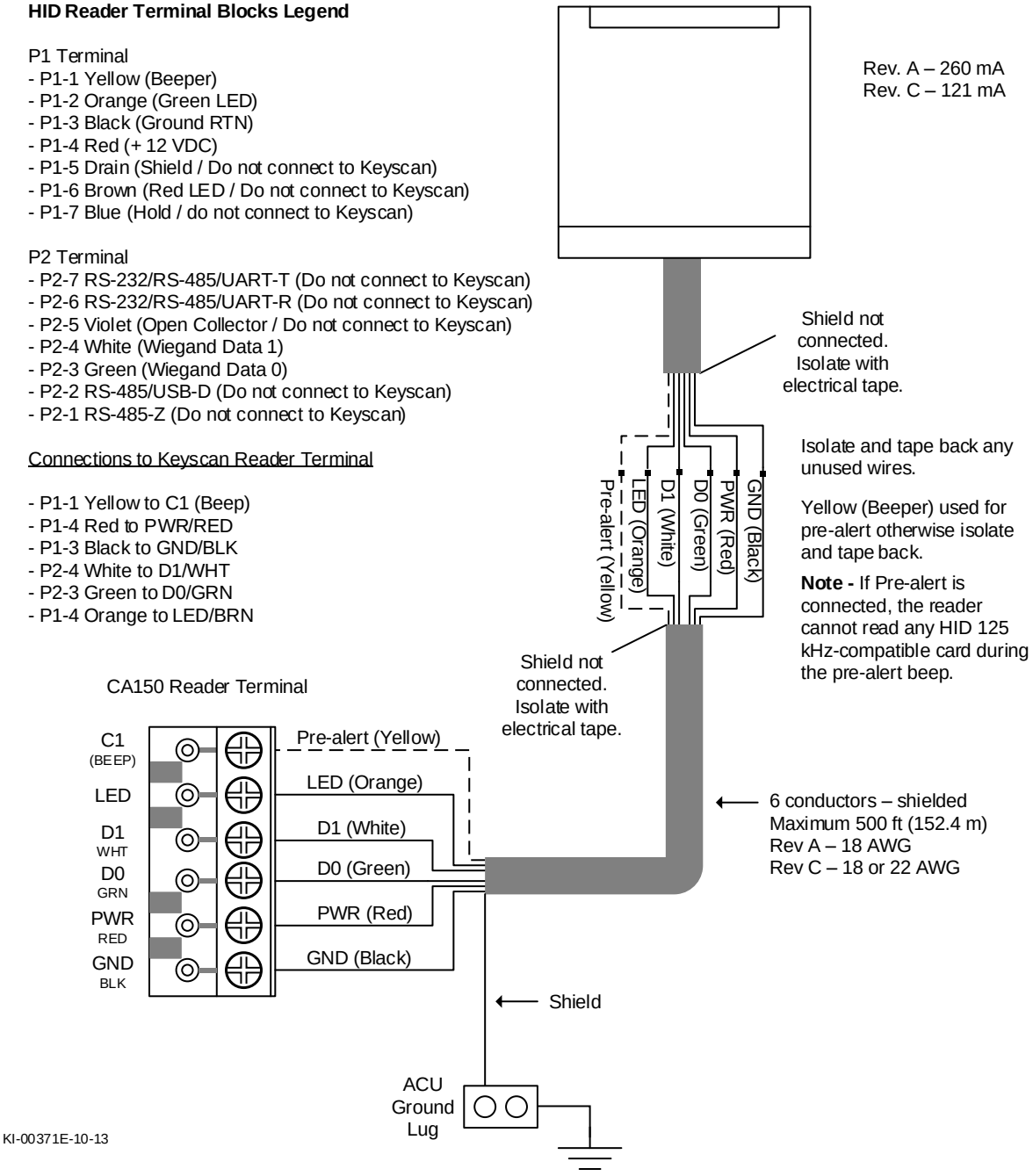
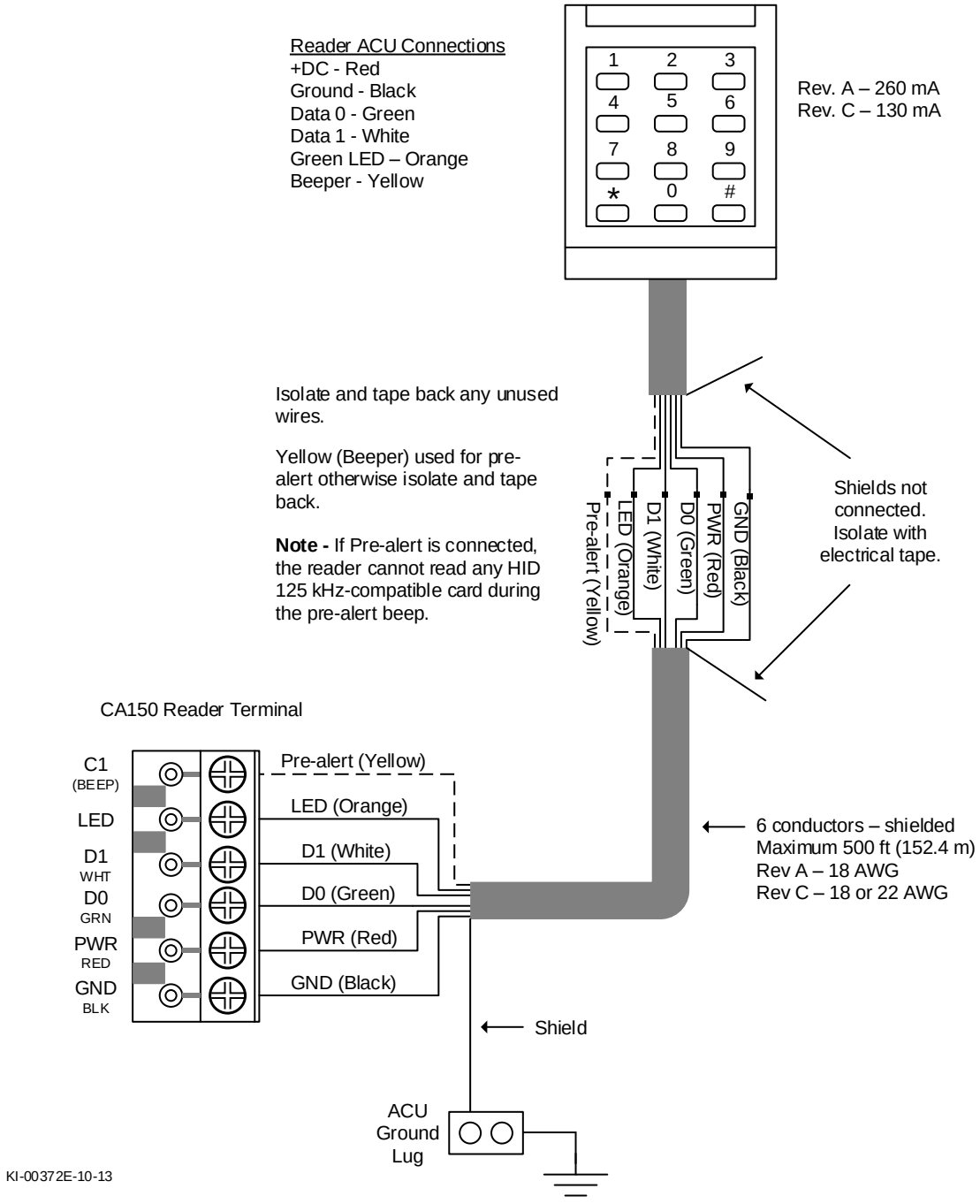


Figure 54 – HID iClass KEYRK40



Note on HID iClass KEYRK40

Reader/Keypad/LED ordered as 00 (4 bit burst) – example 6131AKN00100 (Red/Green colour)

Figure 55 - HID iClass KR90L Long Range Reader

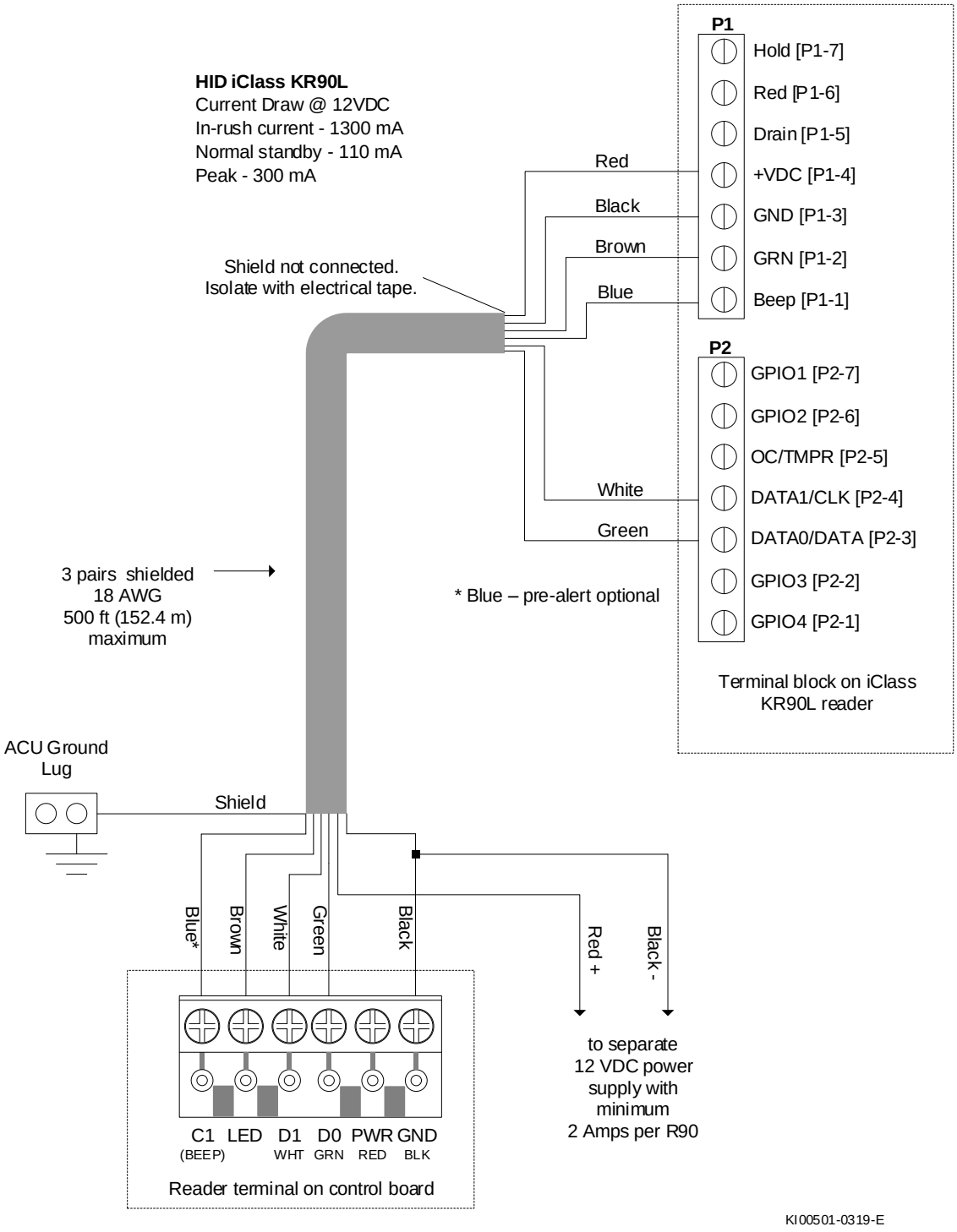


Figure 56 – HID iClass R10 Series

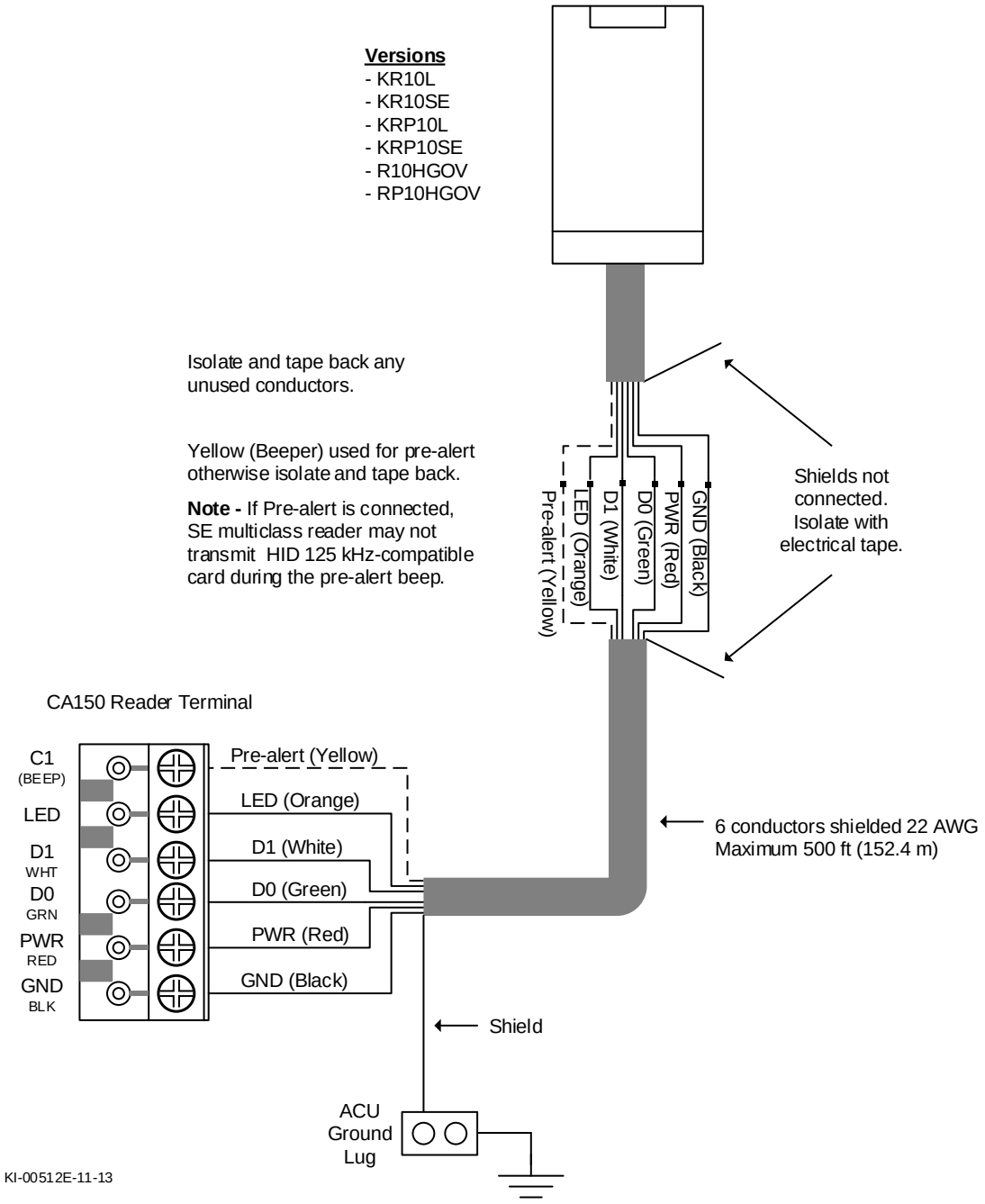


Figure 57 – HID iClass R15 Series

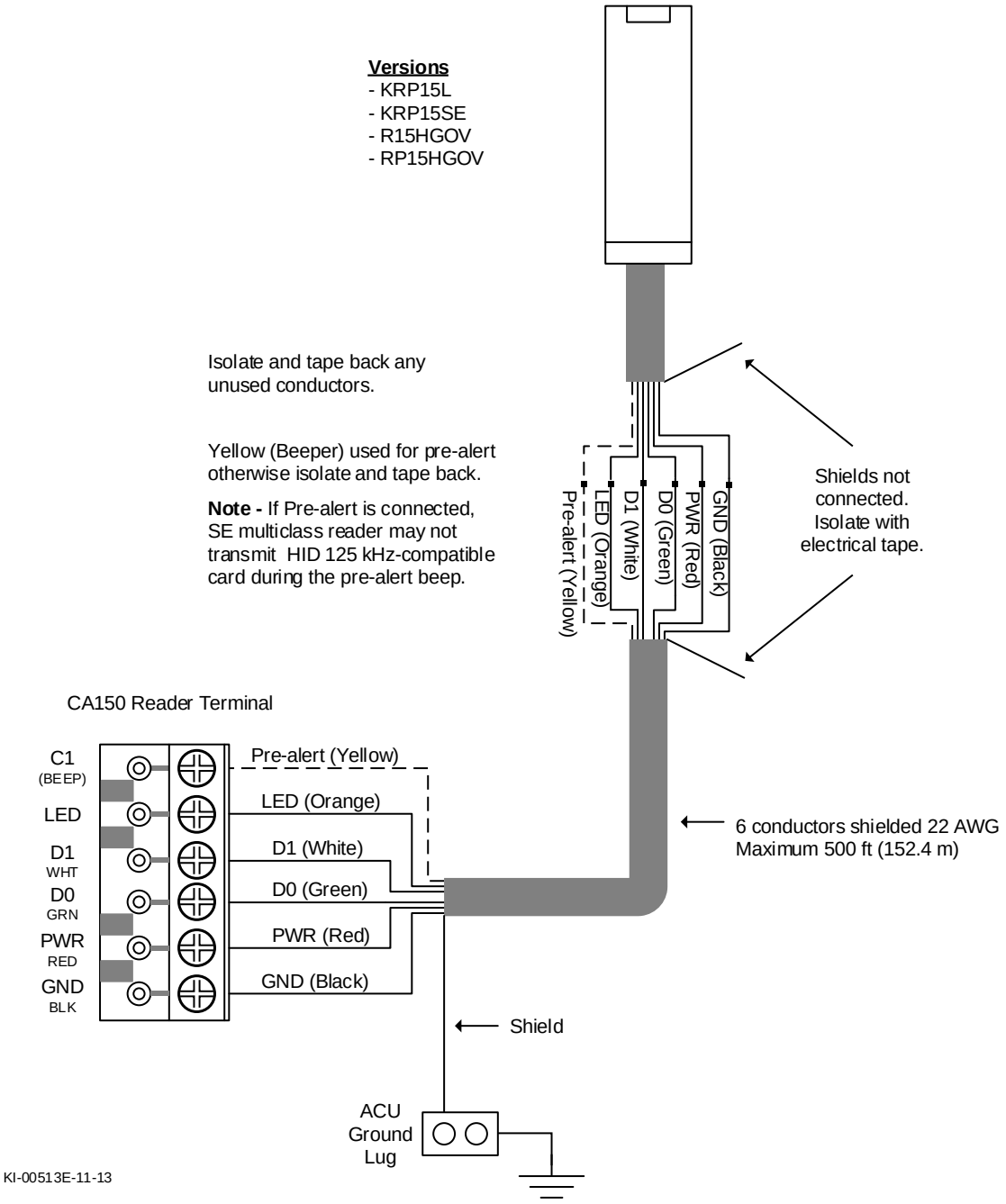


Figure 58 – HID iClass R40 Series

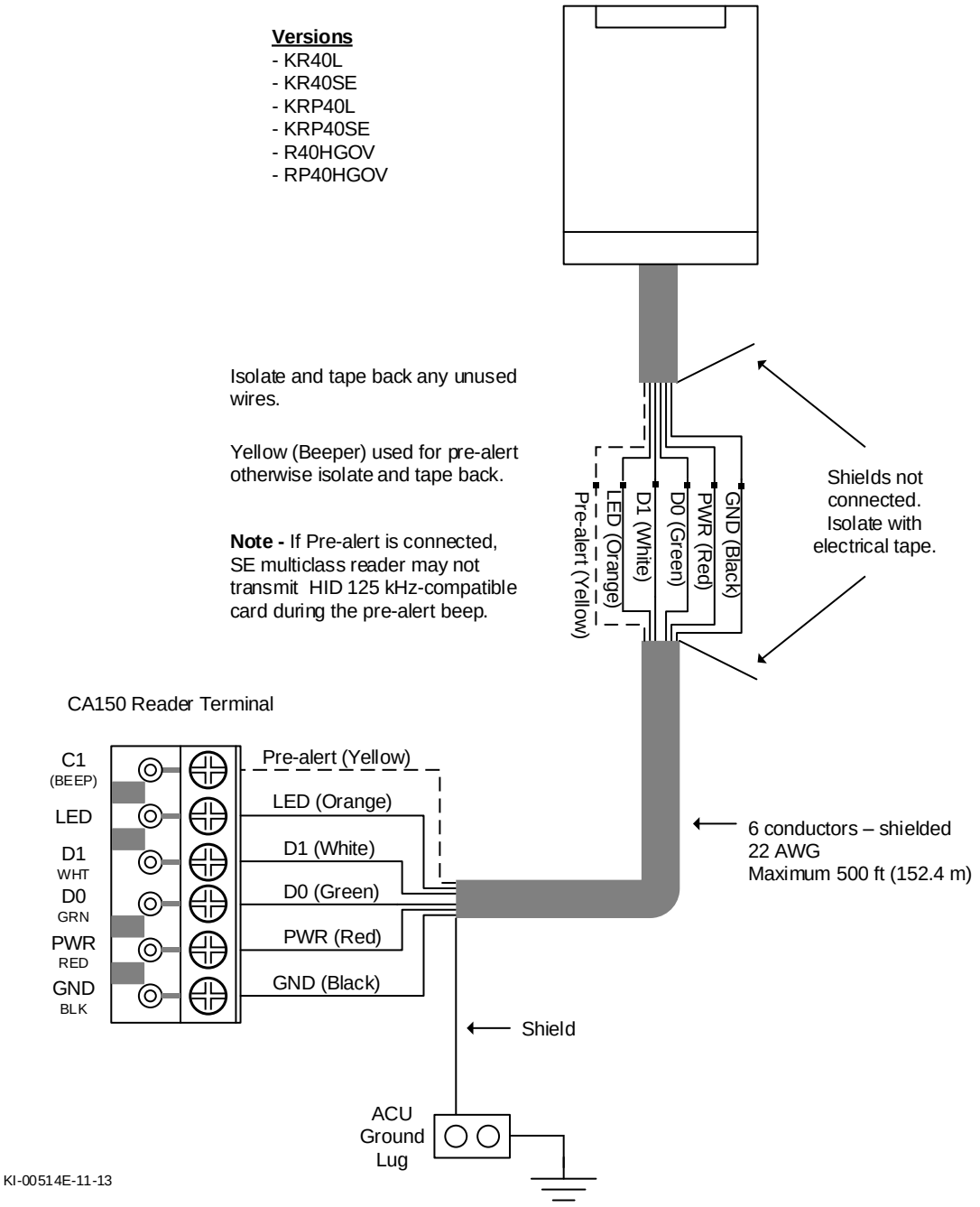
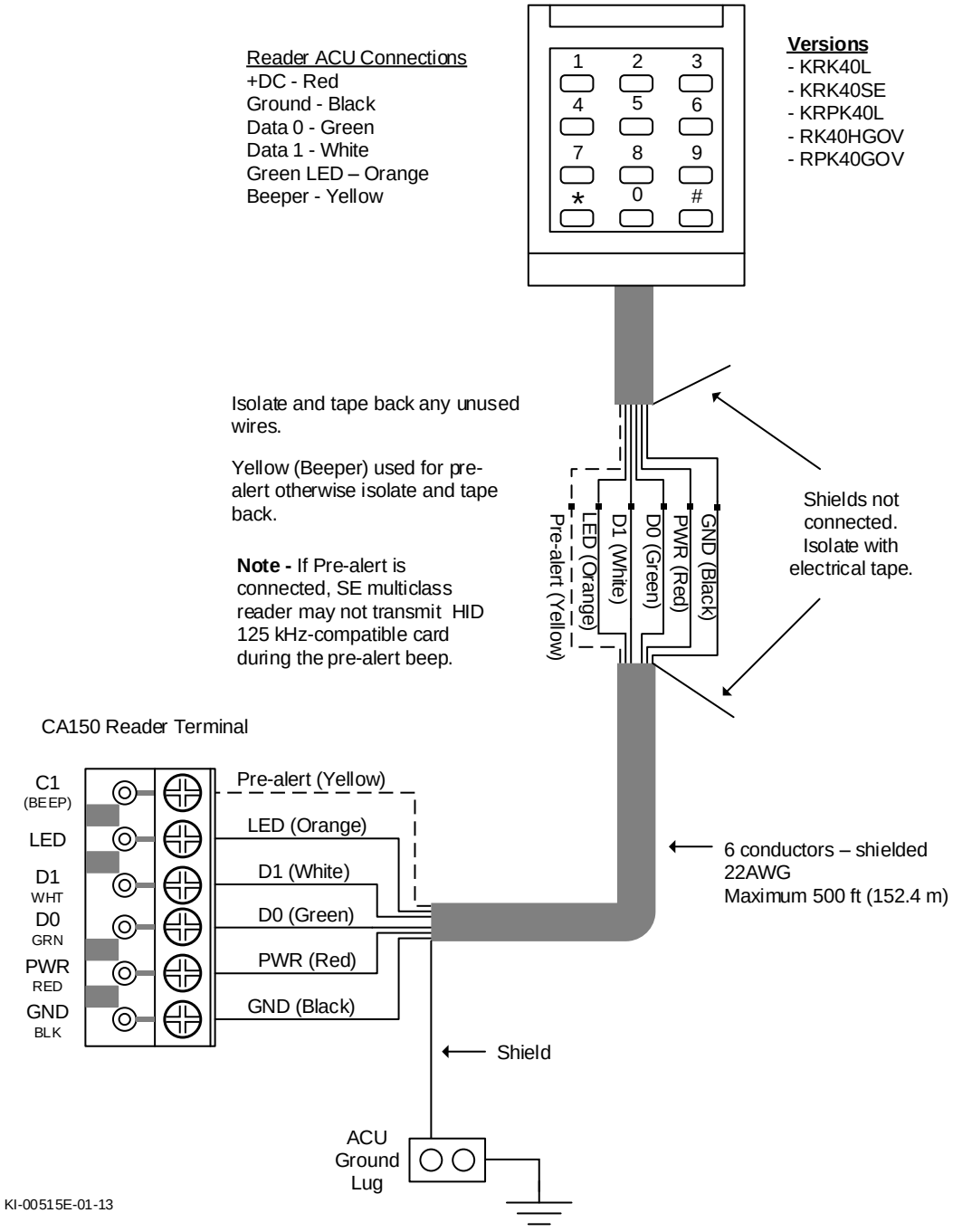


Figure 59 – HID iClass RK40 Series



Indala Readers

This section reviews typical Indala proximity reader connections. 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 Indala reader power specifications:

Table 15 – Indala Reader Power Specifications

Reader	Power	Notes
PX 603	12 VDC, 100 mA	
PX 605	12 VDC, 100 mA	
PX 610	12 VDC, 150 mA	
PX 620	24 VDC, 1.2 A	Requires 18 AWG cable. Connect to separate 24VDC 2 Amp linear power supply. (Not supplied with ACU kit.)
PXK 501	12 VDC, 80 mA + 20 mA interface = 100 mA	Current consumption includes interface circuit board

Installation Notes on Proximity Readers

Do not run reader cables in the same conduit with AC power or signal cables.

Keep reader cables at a minimum distance of 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 in areas where broad spectrum EMI noise may be present. Devices such as motors, pumps, generators, and AC switching relays can create EMI noise.

Readers mounted on a metal surface can reduce the read range. See the Indala manual for recommendations.

Figure 60 – Indala PX 603 and PX 605 Wiring

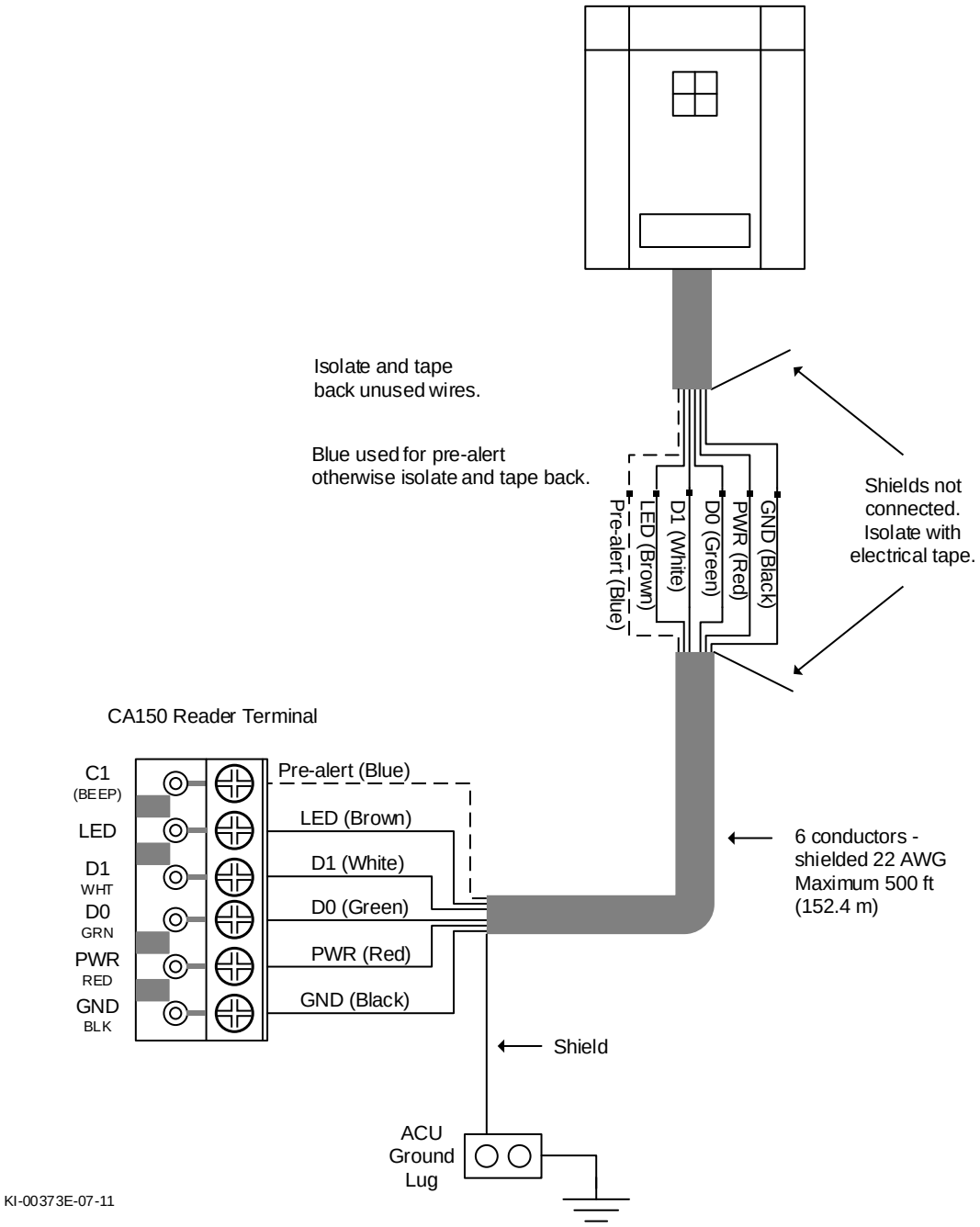


Figure 61 – Indala PX610 Wiring

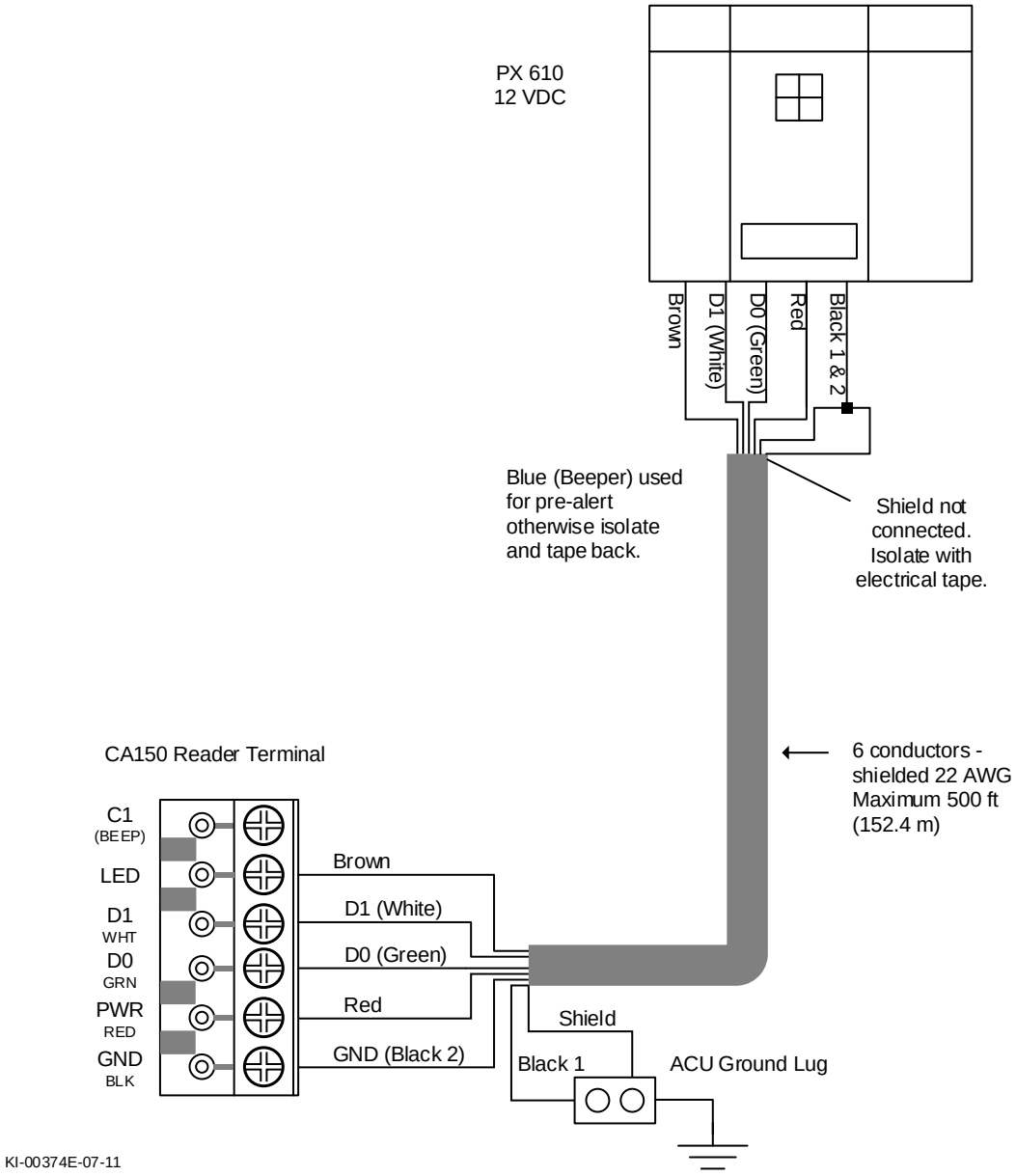
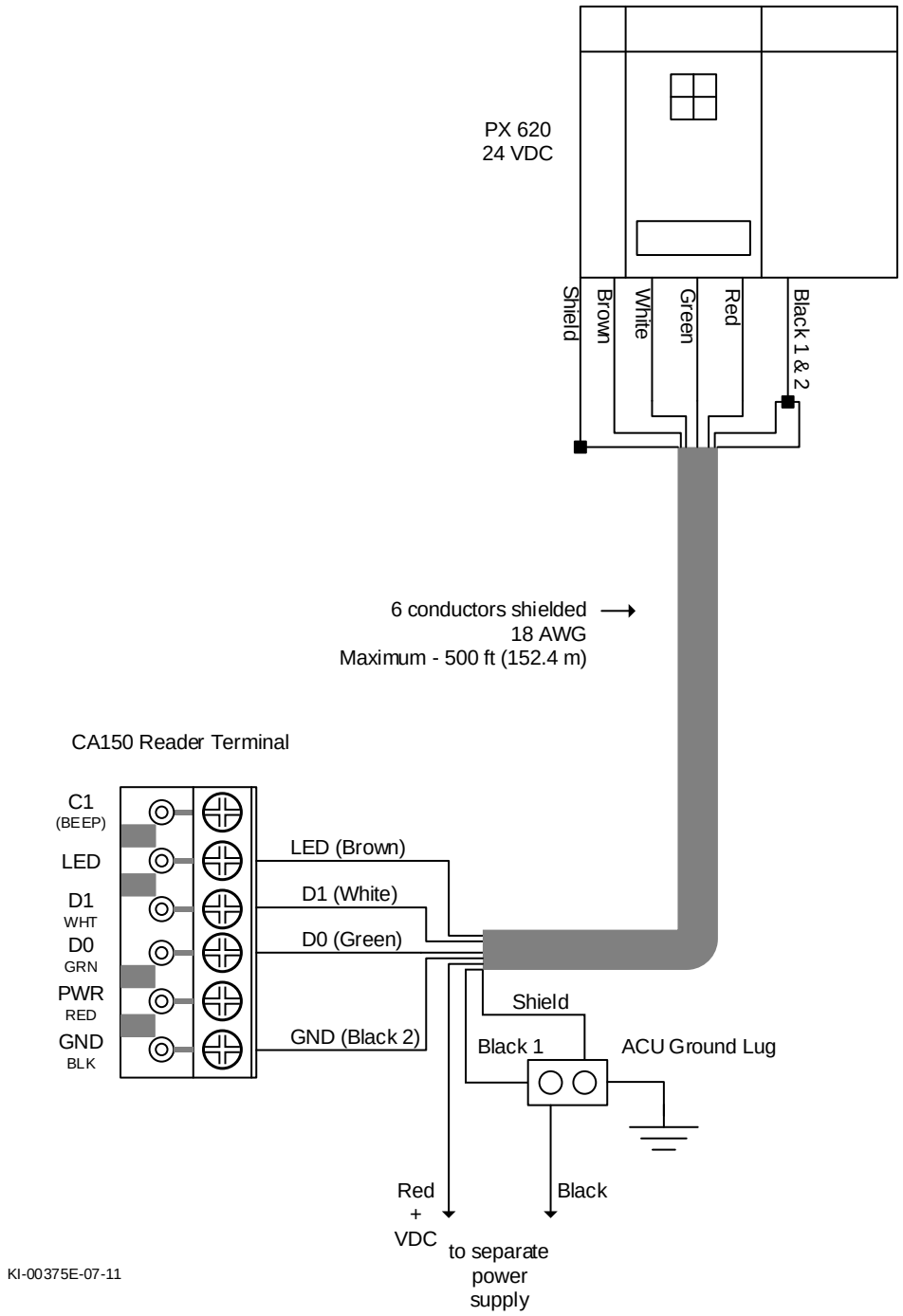


Figure 62 – Indala PX 620 Wiring

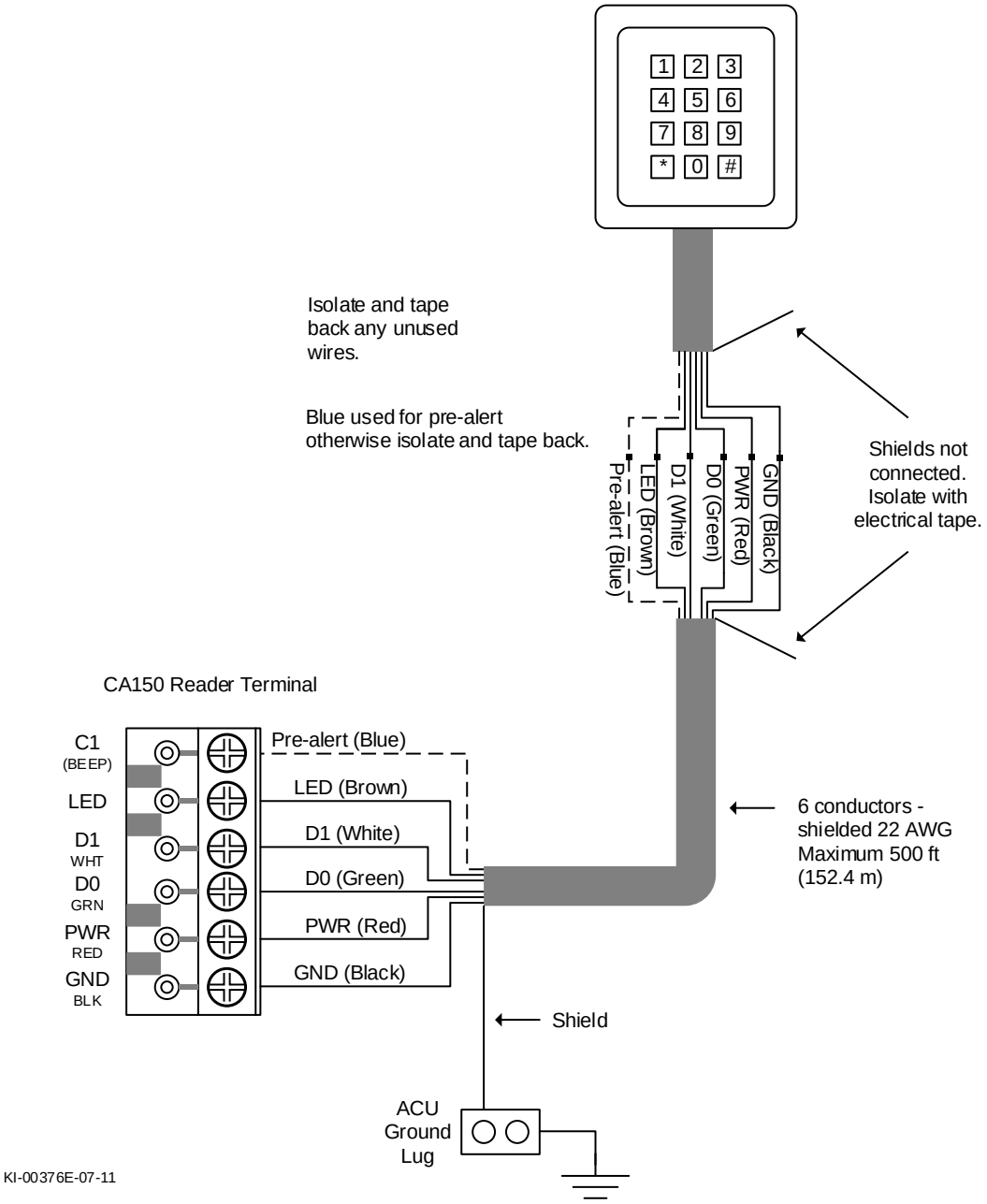


<u>Important</u>

Do not mount an Indala PX 620 reader in an elevator car. The environment is unsuitable and causes the reader to malfunction.

The PX 620 is factory tuned. If a PX 620 requires tuning, tune only once. Excessive tuning may cause the reader to permanently malfunction. Refer to the Indala documentation for instructions on tuning.

Figure 63 – Indala PXK 501 Wiring



<u>Note on Indala PXK 501 Wiring</u>

Reader/Keypad/LED ordered as 8 bit burst – example FP5061B-8 Bit Burst (Red only)

Program On-board Ethernet Module

The CA150 has an on-board Ethernet module – serial to Ethernet converter – which must be programmed using the Keyscan NETCOM Program Utility when the CA150 is used on a network (TCP/IP).

If you are configuring the CA150 for reverse network communication use the procedures outlined in the next section – Configure CA150 for Reverse Network Communication.

NETCOM Program Utility

The CA150 Rev. B control board requires NETCOM Program Utility – version 6.0.18 or higher. Always use the latest NETCOM Program Utility on the enclosed CD when programming the on-board Ethernet module. The CA150 Rev. B control board is distinguished by DIP switches which are not on previous CA150 control boards.

Before You Start Programming

Before you start programming the CA150's on-board network module, ensure have the necessary items for your method, outlined below.

Serial Programming

- Latest NETCOM Program Utility (version 6.0.20 or newer) installed from the driver CD included or downloaded from the www.dormakaba.ca website
- Serial data cable with loose conductors (Part #40-2322)
- USB to serial convertor for computers without a true serial port (Part #USB-SER)
- IP Address, Subnet and Default Gateway (if required)
- Determine the baud rate used (115200 is the default)
- Know the serial port number of the computer

Network Programming

- CA150 ACU with firmware 9.45 or higher
- Latest NETCOM Program Utility (version 6.0.20 or newer) installed from the driver CD included or downloaded from the www.dormakaba.ca website
- Network patch or cross-over cable (preferred)
- IP Address, Subnet and Default Gateway (if required)
- Determine the baud rate used (115200 is the default)
- Ensure that the computer is set to a static IP address within the same IP and subnet range as the CA150 (the default is 192.168.100.254 / 255.255.255.0)

Installing the NETCOM Program Utility

The NETCOM Program Utility is a Keyscan application that programs the CA150's on-board Ethernet module with an IP address and other settings. The utility must be installed on a computer that can be serially

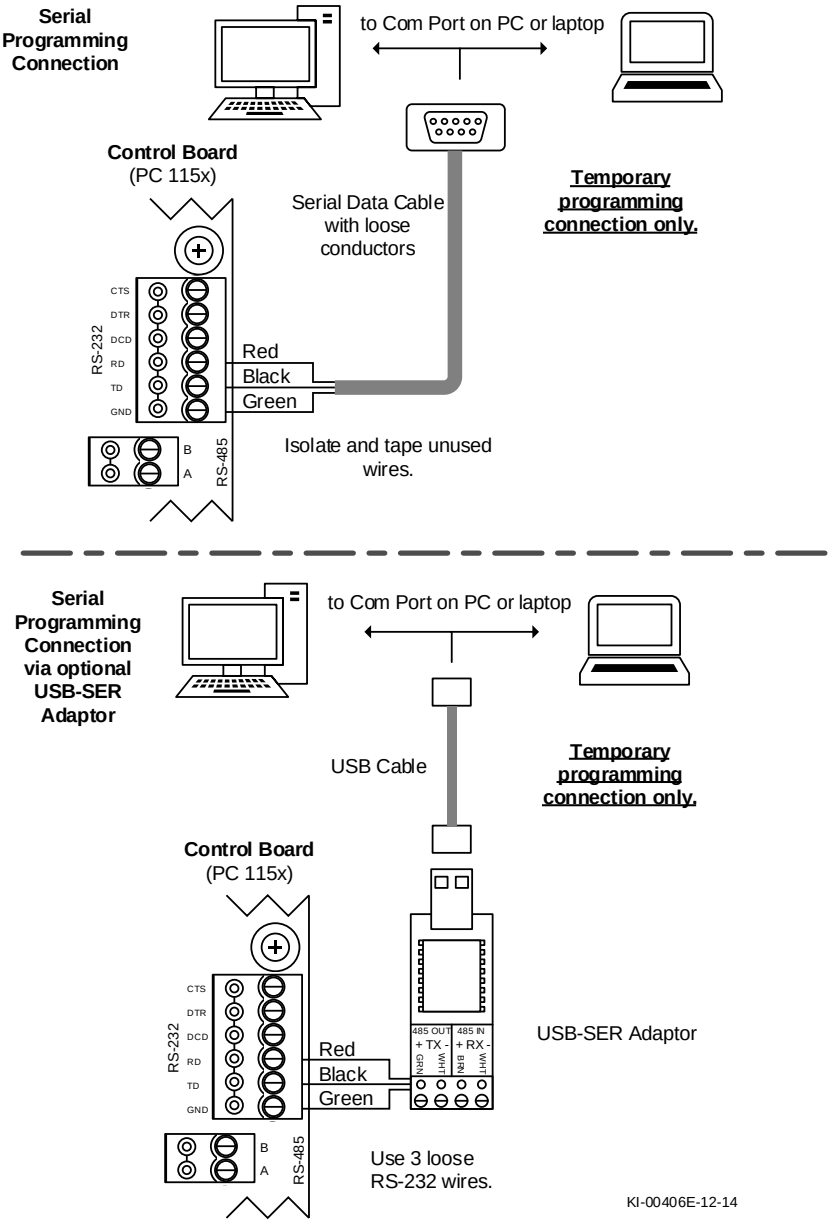
connected to the CA150's RS-232 communication terminal. If the computer only has USB ports, use the optional Keyscan USB-SER adaptor.

To install the NETCOM Program Utility, insert the Utilities & Drivers CD in the computer CD or DVD drive. The utility is programmed to auto-start when the disk is inserted in the disk drive. Follow the on-screen prompts. Please remember the NETCOM Program Utility must be installed before you can program the CA150 on-board Ethernet module.

Programming the CA150 Serially

1. Power the CA150 via POE or DC power supply (requires 15.4W @ 12VDC).
2. Connect the serial cable from the computer to the CA150 using one of the following diagram:

Figure 64 - Temporary Connection for Programming the Ethernet Module

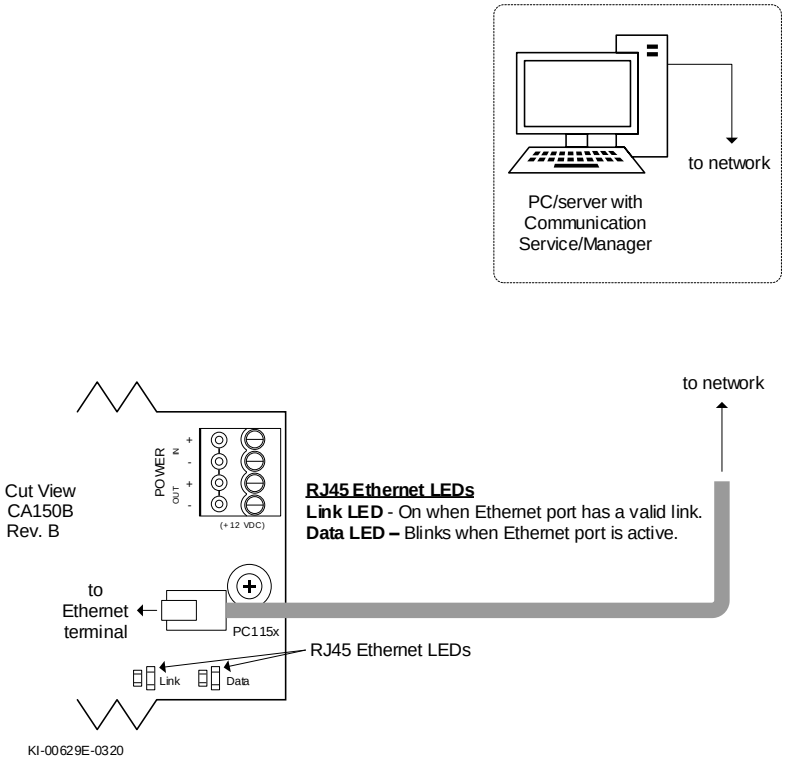


3. Set the CA150 system configuration DIP switches S1.10 and S1.11 to ON.
4. Launch the NETCOM Program Utility.
5. Select the Program CA150 Rev.B Device button.
6. Complete the data entry for desired network settings.
    - If using reverse networking, the option for DHCP is set by entering 0.0.0.0 for the IP Address
    - A default gateway is required for reverse network setup
7. Select the correct Communications Port in Program via Connection.
8. Leave the Communications Baud Rate at 115200.
9. Ethernet Connection Type and Discovery Port setup items are not used, unless necessary.
10. Reverse Network Setup and Encryption Key:
    - If Reverse network settings are required, skip to the supplemental steps in Programming the CA150 Ethernet Module for Reverse Communication found on Page 106
    - Continue setup after completing the additional steps
11. Select the CA150 Rev.B button, then select OK in the prompt.
12. Reset the CA150 by momentarily placing a jumper on J6 (or power cycle the device).
13. After programming is complete, disconnect the serial cable.
14. Set the CA150 system configuration DIP switch S1.11 to OFF.
15. Reset the CA150 by momentarily placing a jumper on J6.
16. Connect the CA150 to the host network.
17. Close the NETCOM Program Utility.
18. If the computer does not have a network connection, complete any remaining connections for permanent operation, relocate to a computer with a network connection and ping the CA150's IP address using the command prompt.
    - IP Success indicates the Ethernet module has network communication
    - IP Times Out indicates the Ethernet module does not have network communication. Verify settings and connection

Programming the CA150 VIA Cross-Over or Patch Cable

1. Power the CA150 via POE or DC power supply (requires 15.4W @ 12VDC).
2. Connect the cross-over or patch cable from the computer to the CA150 using the following diagram:

Figure 65 – CA150B Rev.B Board Direct Connection



3. Set the CA150 system configuration DIP switches S1.10 ON and S1.11 OFF.
4. Reset the CA150 by momentarily placing a jumper on J6.
5. Launch the NETCOM Program Utility.
6. Select the Program CA150 Rev.B Device Button.
7. Complete the data entry for desired network settings.
8. Select Network Connection via 192.168.100.254 in Program via Connection.
9. Leave the Communications Baud Rate at 115200.
10. Ethernet Connection Type and Discovery Port setup items are not used, unless necessary.
11. Reverse network settings cannot be setup with cross-over/patch cable programming.
12. Click the Program CA150 Rev.B button.
13. After programming is complete, disconnect the patch cable and connect the CA150 to the host network.
14. Close the NETCOM Program Utility.
15. If the computer does not have a network connection, complete any remaining connections for permanent operation, re-locate to a computer with a network connection and ping the CA150's IP address using the command prompt.
    - IP Success indicates the Ethernet module has network communication
    - IP Times Out indicates the Ethernet module does not have network communication. Verify settings and connection

Configure CA150 for Reverse Network Communication

If you are configuring the CA150 Rev. B for reverse network communication, you must first complete the procedures outlined in this section. The procedures include setting DIP switches, programming the access control board with an IP address, and programming the on-board network module with an IP address for reserve network communication.

About Reverse Network Communication

Reverse network communication requires a license from dormakaba Canada Inc. (Part #K-RN), which operates with an encrypted reverse network communication application. Generally, reverse network communication is used for centrally managed access control, where the software, including the encrypted communication application, is installed at a host location with the control board installed at a remote location with communication over a public or private network.

Note: If you have not purchased a Reverse Network License, do not configure the CA150 Rev.B for reverse network communication.

NETCOM Program Utility

The CA150 Rev. B control board requires NETCOM Program Utility – version 6.0.18 or higher. Always use the latest NETCOM Program Utility on the enclosed CD when programming the on-board Ethernet module. The CA150 Rev. B control board is distinguished by DIP switches which are not on previous CA150 control boards.

Installation Coordination – Host & Remote Locations

The RN license involves installing and configuring reverse network encrypted communication software at a host location and installing hardware components at a remote location. You must coordinate certain settings between the two locations in order that the CA150 control unit at the remote location can establish network communication back to the computer with the encrypted communication software at the host location.

- the technician installing the hardware components must have a host-location IP address that the CA150 control unit connects to on the network
- both the host and remote locations must have the same encryption key

The hardware technician must program the access control board with a host-location IP address along with other settings. The IP address the technician programs into the control board depends on the network configuration. We have provided two general network configuration outlines: an Internet/Intranet/WAN configured network that is exposed publicly and a LAN that is closed. Refer to the network configuration that best approximates your network application.

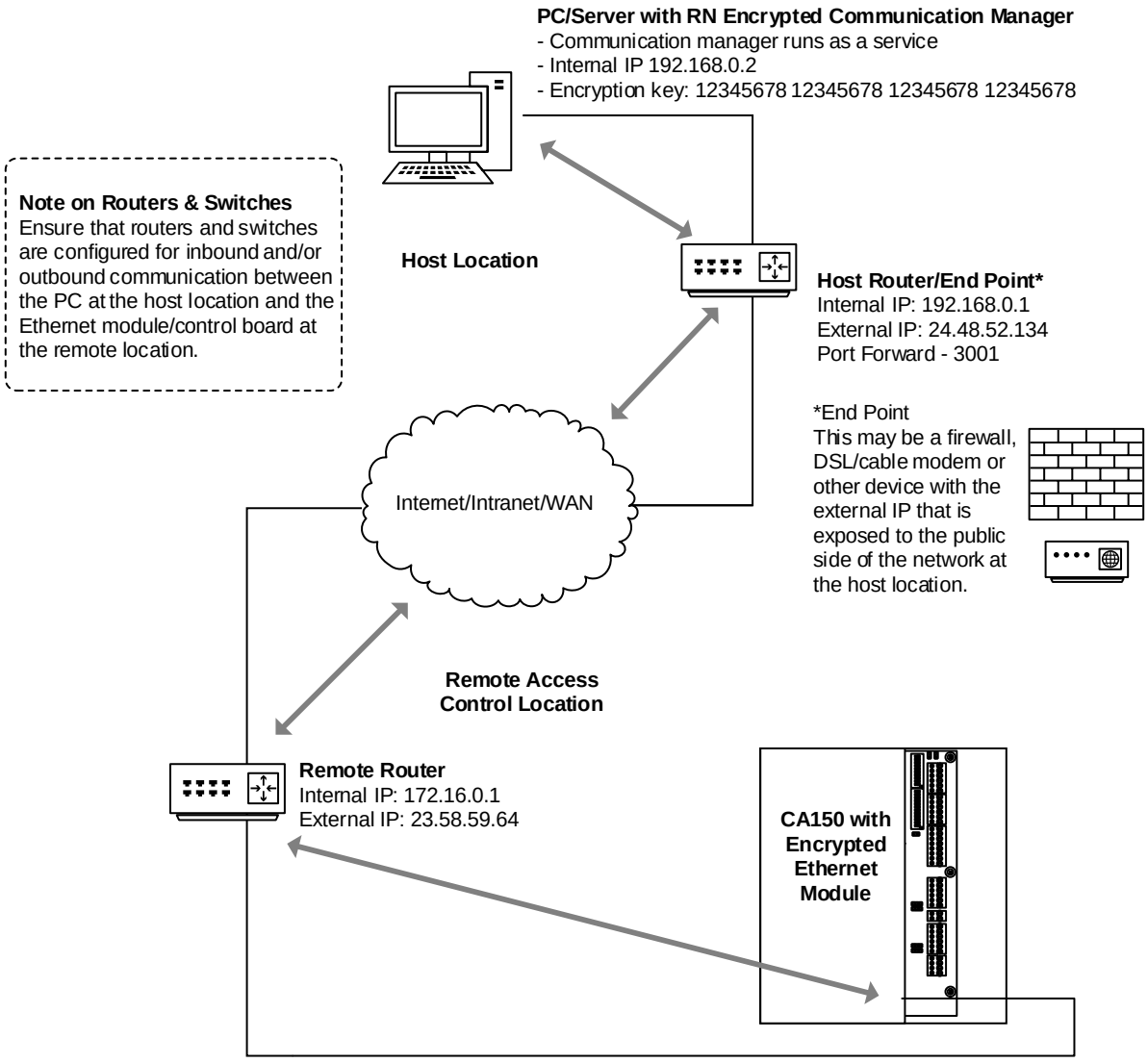
Important

You may require the assistance of a qualified network administrator. Without correct host/remote network settings and connectivity, you will be unable to establish communication.

Table 16 - Reverse Network IP Address Settings

Network Configuration – Internet/Intranet/WAN – Host Router or End Point with External IP Address				
Example	**Settings**	**Host Location**	**Remote Location**	
See Figure	IP Address Port # Gateway Encryption key	Router with port forward or router table to computer/server with Keyscan reverse network encrypted communication Same encryption key/bit setting as remote location	**ACU**	Programmed with host router or end point external IP address Port # of host router/end point
			ACU Ethernet Module	Programmed with static IP address or if using DHCP server dynamic IP Gateway (if static IP above) Port # of host router/end point Same encryption key/bit setting as host location
Network Configuration – LAN – Closed Network with No Public Exposure				
See Figure 67	IP Address Port # Encryption key	Computer/server with Keyscan reverse network encrypted communication Same encryption key/bit setting as remote location	**ACU**	Programmed with IP address of host computer/server with Keyscan reverse network encrypted communication Port # of Host computer/server
			ACU Ethernet Module	Programmed with static IP address or if using DHCP server dynamic IP Port # of Host computer/server Same encryption key/bit setting as host location

Figure 66 - Example of Internet/Intranet/WAN with Router or End Point External IP



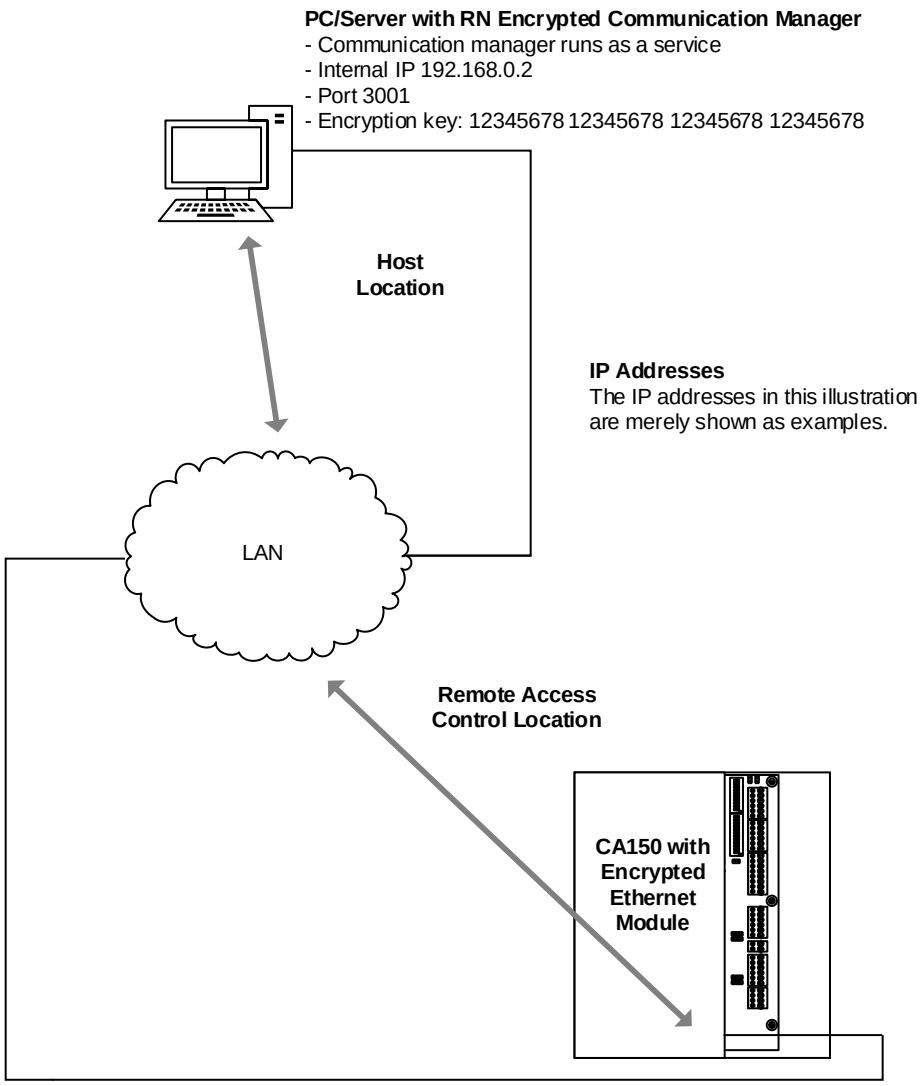
IP Addresses
The IP addresses in this illustration are merely shown as examples.

KI-00459E-02-16

CA150 Encrypted Ethernet Module
Internal Static IP: 172.16.0.2
Gateway: 172.16.0.1
Port: 3001
Encryption Key: 12345678 12345678 12345678 12345678

CA150 Control Board
Reverse Network Programming:
- Host Router/EndPoint External IP: 24.48.52.134
- Port: 3001
(May also include an alternate host router external IP address if available)

Figure 67 - LAN with no public exposure



KI-00460E-02-16

Before Programming

Before programming the CA150's on-board network module, ensure that you have all necessary items for your method:

- Latest NETCOM Program Unity (version 6.0.20.0 or newer) installed from the driver CD included or downloaded from the www.dormakaba.ca website
- Serial data cable with loose conductors (Part #40-2322)
- USB to serial convertor for computer without a true serial port (Part #USB-SER)
- If required: IP Address, Subnet and Default Gateway (operating DHCP is preferred)
- Determine the baud rate used (115200 is the default)
- Know the serial port number on the computer
- Host location IP address and port being assigned
- Encryption key being used

About the Encryption Key

The encryption key for the CA150's on-board network module must consist of 32 characters (128 bit) or 64 characters (256 bits). Characters can be as follows in any combination:

- Alpha A – F
- Numeric 0 – 9
- Example of 128 bits key – A91376F1 C3621FBC DD68917E 1006B167

The encryption key can be created at either the host/central monitoring location or the remote access control location. The key must be entered accurately in the following Keyscan software utilities:

- Aurora – Application Utilities screen (host location)
- System VII Settings – reverse network utility (host location)
- Vantage Settings – reverse network utility (host location)
- NETCOM Program Utility (remote location)

Set System Configuration DIP Switches

Set DIP switch S1.1 for reverse network communication and DIP switch S1.2 for the bit rate as outlined in the table below.

Figure 68 – Location of S1.1 / S1.2 DIP Switches

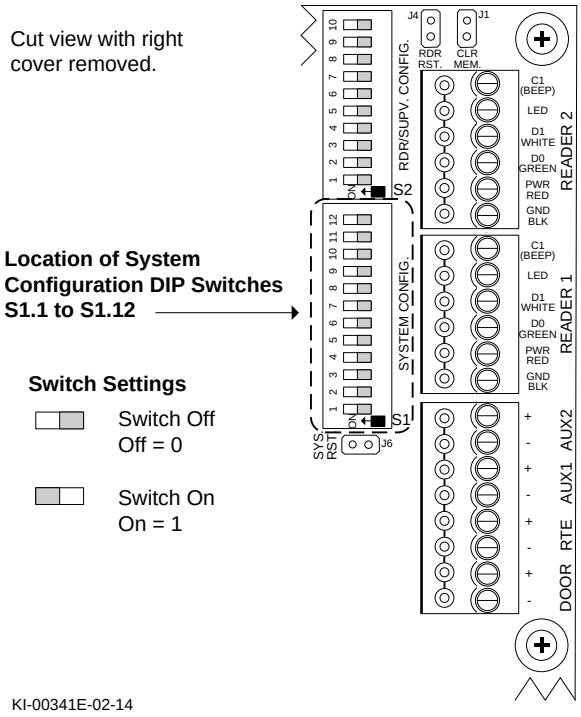


Table 17 - System Configuration DIP Switches S1.1 & S1.2 – Reverse Network Settings

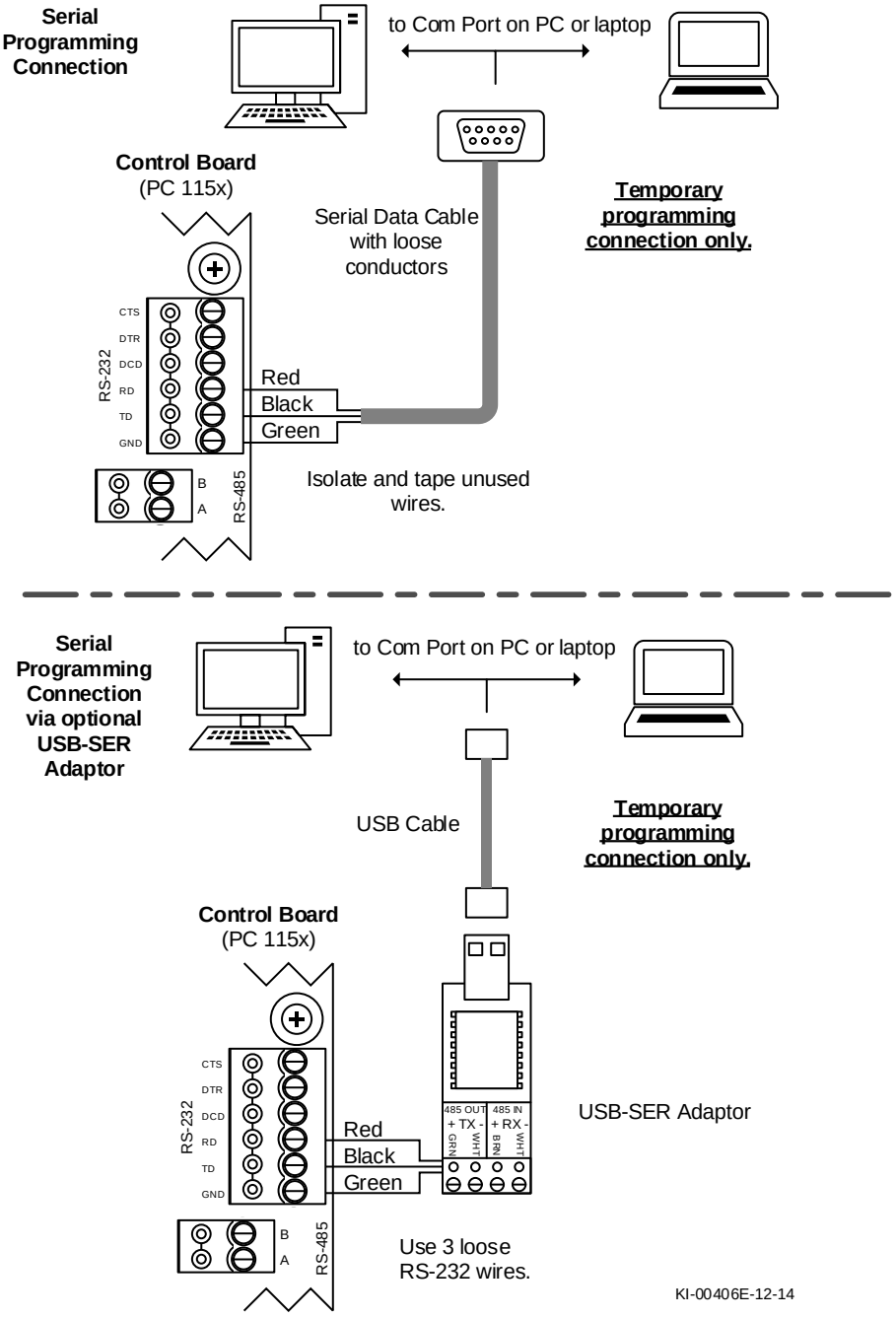
Function	Mode	Switch #	Settings
			Off=0 / On=1
Communication	Reverse network	S1.1	1
Bit rate	57,600	S1.2	1
	115,200	S1.2	0

Host Connect Setup VIA Serial Connection

This procedure requires the Keyscan Hyper Terminal application on a computer that can connect to the access control unit serially. The Keyscan Hyper Terminal application is accessible from the NETCOM Program Utility on the Drivers & Utilities CD.

1. Power the CA150 via POE or DC power supply (requires 15.4W @ 12VCD).
2. Connect the serial cable from the computer to the CA150 using one of the following diagrams:

Figure 69 – Temporary Programming Connection for Reverse Network



3. Set the CA150 system configuration DIP switches S1.10 and S1.11 to OFF.
4. Reset the CA150 by momentarily placing a jumper on J6.
5. Launch the NETCOM Program Utility and select the Keyscan Hyper Terminal button.
6. In the Open Comm Port Selection screen, select the COM port assigned to the serial port being used to program the CA150.
7. Select the baud rate that matched the S1.2 setting on the CA150 (115200 is the default).
8. Select the Open Port button.

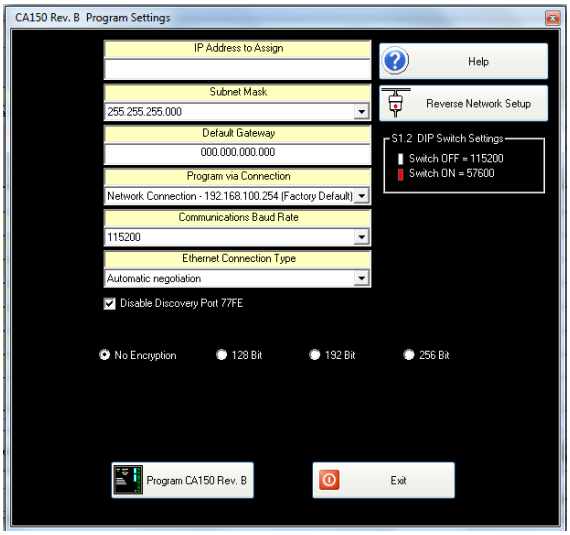
9. With the Hyper Terminal screen open, momentarily switch S1.1 OFF and then switch it back ON. Immediately press and hold the 'C' key on the keyboard until the Hyper Terminal menu opens. Release the 'C' key and wait until the menu stabilizes before moving on to the next step.
10. From the Hyper Terminal menu, select 1) Set Primary IP Address.
11. Enter the Primary IP address of the host's router, end point, or computer with the Keyscan reverse network communication application, depending on the network setup.
    - If you make an error, do not use the Backspace key. Press the Enter key and repeat Steps 11 and 12
    - Ensure the correct IP address format is used with periods separating appropriate digits as shown in the example: 192.168.100.12
12. Press the Enter key.
13. From the Hyper Terminal menu, select 2) Set Secondary IP Address.
14. Enter the Secondary IP address of the host's router, end point, or computer with the Keyscan reverse network communication application, depending on the network setup.
    - If no Secondary IP address is used, enter the Primary IP Address again
    - If you make an error, do not use the Backspace key. Press the Enter key and repeat Steps 14 and 15
    - Ensure the correct IP address format is used with periods separating appropriate digits as shown in the example: 192.168.100.12
15. Press the Enter key.
16. From the Hyper Terminal menu, select 5) Set Port Number.
17. Enter the port number of the host router, end point or the computer with the Keyscan reverse network communication application, depending on the network setup.
    - If port number 00 is entered, the CA150 resets the port number to 3001 by default
    - If you make an error, do not use the Backspace key. Press the Enter key and repeat Step 17
18. Press the Enter key.
19. Verify the correct settings are programmed by selecting 3) Display IP Setting.
    - Repeat the required steps to correct any errors
20. Select 9) Exit.
21. Close the Keyscan Hyper Terminal application.
22. Set the CA150 system configuration DIP switches S1.10 ON and S1.11 OFF.
23. Reset the CA150 by momentarily placing a jumper on J6.

Programming the CA150 Ethernet Module for Reverse Communication

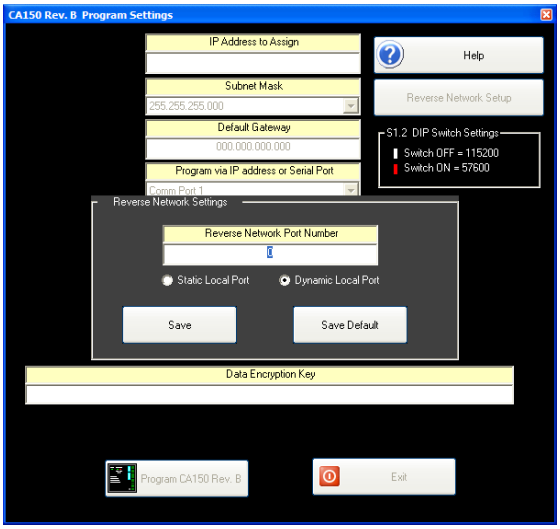
Before proceeding, this assumes that you continued from Programming the CA150 Serially section and that the control board is powered and connected via the serial data cable to the computer with the NETCOM Program Utility.

The following steps are supplemental to the Reverse Network Setup and Encryption Key sections on Page 95:

1. Select a radio button that corresponds to the encryption key setting at the host location – 128 Bit, 192 Bit or 256 Bit.
2. In the Data Encryption Key field, accurately enter the encryption key.



3. Select the Reverse Network Setup button.
4. Enter the port number in the Reverse Network Port Number field of the router, end point or the computer with the reverse network communication manager at the host location.



5. Select the radio button – Static Local Port or Dynamic Local Port (50,000 – 59,999), depending on whether the inbound port on the router/end point is assigned to a static port or a range of dynamic ports at the remote location.

- Static Local Port configures the outbound communication port number as entered in the Reverse Network Port Number field
- Dynamic Local Port configures the outbound communication port number dynamically between 50,000 – 59,000

6. Select Save.
7. Allow several minutes for the connection, after completing programming. If the CA150 is unable to establish communication, verify all the settings are correct and the host location has a valid path to the computer with the reverse network communication manager from the Internet and that the correct port settings are specified.

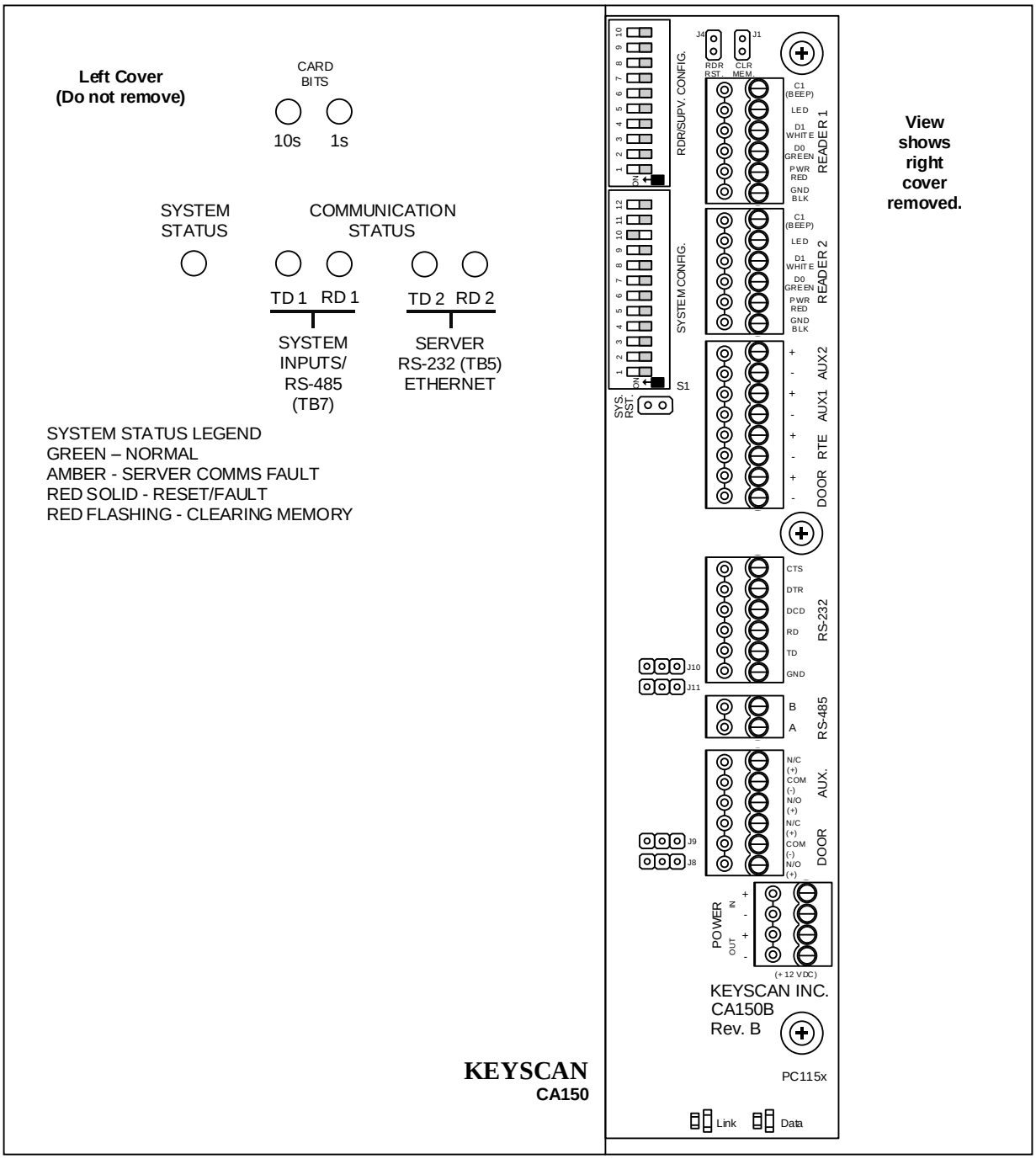
Reverse Network ACU Connection Summary

The ACU will attempt to connect to the computer with the Keyscan reverse network communication manager under the following circumstances:

- If Carrier Detect is passive, the ACU will attempt to connect every 60 seconds
- If Carrier Detect is asserted, but the communication data is corrupt or no data has been detected for 15 minutes, the ACU will disconnect, reset the NETCOM, and attempt to re-connect
- If Carrier Detect remains asserted, disconnect, reset, and re-connect attempts will occur every 2 minutes

CA150B Quick Reference

Figure 70 – CA150B Control Board



KI-00382E-11-15

Table 18 – CA150B Quick Reference

Function	Location	Instructions/Notes	Additional Reference
Power	PoE - Ethernet terminal	Maximum current load for all devices = 680 mA	See page 58.
	12 VDC – Power In (+) & (-) terminals		See page 58
Reader 1 and 2	Data 0, Data 1	Wiegand signal	
DIP Switches & Jumpers	J1 – Clear Memory	Resets board to factory defaults	See page 48.
	S1.1 to S1.12 – System Configuration	For communication and system settings	See page 36.
	S2.1 to S2.6 – Reader Configuration	Sets system to specific reader format/type	See page 40.
	S2.7 to S2.8 – Supervision Mode	Sets the input supervision type	See page 47.
	S2.9 to S2.10 – System Software Mode	Sets the board for the Keyscan system software application	See page 39
	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	See page 50.
	J10 to J11 – Aux Output Relay Powered/Unpowered	Sets Aux relay with power from control board or as a dry contact	See page 50.
Wiegand LED Card Bits	10s, 1s	10s counts first binary digit 1s counts the second binary digit	See page 46.
Communication	RS-232	For direct RS-232 serial communication, connect to RS-232 (TB5) terminal block S1.10 & S1.11 – switches OFF	See page 51.
	Ethernet - Operation Mode (Network TCP/IP)	For network communication, connect network cable to on-board Ethernet terminal S1.10 – switch ON / S1.11 – switch OFF	See page 51.
	Ethernet - Program Mode (Network TCP/IP)	Ethernet program mode uses RS-232 via TB5 at 9600 BPS. S1.10 – Switch ON / S1.11 – switch ON	
	RS-485	For future use	
Control Board Test Voltages			See Table 9 on page 62.
Communication Test Voltages			See Table 10 on page 63.

CA150B Specifications

The CA150 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 CA150 does not support global functions. The table below outlines CA150B specifications.

Table 19 - CA150B 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	PoE (Class 0) +12V DC independent power supply
CA150 Current	170 mA to maximum 200 mA
Communication	Ethernet (TCP/IP) RS-232
PTC Resettable Fuses	Reader port 1 – 500 mA Reader port 2 – 500 mA Door output – 500 mA Aux/Accessibility output – 500 mA RTE port – 300 mA Maximum current for all connected devices with PoE is 680 mA.
PoE	IEEE 802.3af Class 0
Software Requirements	Aurora – 1.0.1.0 or higher System VII – 7.0.14 or higher Vantage – 8.1.13 or higher NETCOM Program Utility – version 6.0.18 or higher for programming on-board Ethernet module for network communication
Cable	RS-232 – 5 conductor 22 AWG shielded cable - maximum 20 ft (6m) PoE – CAT 5 or CAT 6 – maximum 328 ft (100 m)
Applications	Indoor installations only

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:**

This page is intentionally blank.

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 Keyscan. 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.

Index

dormakaba Canada Inc.
901 Burns St., E
Whitby, Ontario
Canada L1N0E6
T: 888-539-7226
eadorders.ca@dormakaba.com

www.dormakaba.us