DIGI*TRAC™ Systems

Design & Installation Guide

HIRSCH by IDENTIV

MAN001-1219

Rev. AJ, December 04, 2019
MAN001-1219

Version	Replaced Version and Summary of Changes:
MAN001-1219	MAN001-0319. Updated “About the Guide” section by including a new “Note”. Updated the cable capacitance in the following sections “ScramblePad/MATCH Inputs”, “SNIB2 Network Configuration Options Overview”, “SNIB2 Design”, “SNIB3 Design”, “SNIB2 Cabling”, “SNIB2 Network Configuration Options”, “Using Serial RS-485”, and “RS-485 Cabling for SNIB3s”. Under “Setup and Installation of Mx-1 Controller”, in section “Wiring Distance Limits” second row is removed from Table 9-15. In section “Wiring Distance Limits for an RREB” second row is removed from Table 2-12. In Section “Before You call” new content is included under the fourth list item. Added new sections “RREB Power rating” and “SNIB3 Power Rating”.
MAN001-0319	MAN001-0818. Updates the “UL Requirements” topic to add information about the UL 294 (7th edition) rating achieved by some older DIGI*TRAC components, to add electrical safety information about the connectors on various products, and to remove information about discontinued products. Additional changes in this version include: Adds a new topic about “Power Limitation Board Installation” on page 7-305. Updates several illustrations to show Revision 2 of the Mx-1 controller, and updates “Mx-1 Controller Configurations” on page 9-6 to mention the Mx-1-W license for controlling wireless locks. Adds information for UL listing of the Mx-1-ME controller, which is documented in Chapter 9. Various other miscellaneous changes.
MAN001-0818	MAN001-0418. Changes for UL 294 listing of Revision 2 of the Mx-1 controller, which is documented in Chapter 9. (The primary product change is a different set of Wet or Dry Mode jumpers for the power to the Door Relay and Aux Relay terminals, which are explained in Table 9-2.) Additional changes in this version include: Updates “Velocity Features that Reduce Available Memory” on page 2-24. Updates Table 8-5 by changing the max current draw for all the Wiegand terminals on an Mx controller from 2.0 Amps to 1.7 Amps. Adds some more cross-references to the worksheets for the Mx and Mx-1 controllers. In Table 9-2, updates the descriptions for the Mx-1 controller’s Battery connector, Door Relay terminal, Aux. Relay terminal, and Wet or Dry Mode jumpers. In Table 9-3, updates the descriptions for Pin 4 (Tamper Output) of the Wiegand Reader terminals and Pin 2 (LO) of the Door Input or Aux. Input terminal. In Table 9-5, updates the descriptions for the Mx-1 controller's G7, G8, and Y8 status LEDs (for CCM/CCMx firmware version 7.6.20). Adds Table 9-7, which explains the Mx-1-ME’s status LEDs for CCM/CCMx firmware version 7.6.20. In Table 9-10, updates the descriptions for the Mx-1 controller’s Door relay and Aux. relay terminals, and the Total Power available. Updates “Wiring for the Door” on page 9-37 to include some basic wiring diagrams for a normally closed electric door strike in either Wet mode or Dry mode. Updates “Interpreting the System Power Status Information” on page 9-50 (for CCM/CCMx firmware version 7.6.20). Various other miscellaneous changes.
MAN001-0418	MAN001-0118. Updates the “UL Requirements” topic to add information about the Identiv TS readers which were tested by UL with the Mx-1 controller (to meet the UL 1076 standard). Also includes a few other minor changes.
MAN001-0118	MAN001-1017. Updates the “UL Requirements” topic to add information about the Mx-1 and Mx-1-ME controllers. Updates the “Features of the Mx-1 Controller” topic and Table 9-2 to note some features which were not tested by UL. Enhances Explanatory Note 3 at the end of Table 9-1 to mention that the Mx-1 does not support any expansion boards. At several places in Chapter 9, adds a NOTE to see the table about “Standby Power Requirements for Various UL Standards” on page vi. Changes the value of the maximum simultaneous current draw for the Mx-1's Alarm Relay and Door Relay from 1.0 Amps to 0.75 Amps.

MAN001-1017	MAN001-0117. Adds Chapter 9 about the new Mx-1 controller. Adds new topic about "Connecting Exit Readers to Unused Wiegand Terminals on Mx-2 or Mx-4 Controllers" on page 8-22. Updates the Index.
MAN001-0117	MAN001-0916. Adds information about the RS-485 Readers Expansion Board (RREB). Also adds a new topic about "Velocity Features that Reduce Available Memory" on page 2-24, and adds references to that topic before Table 1-1, before Table 2-10, and after Table 8-2.
MAN001-0916	MAN001-0716. Updates the "UL Requirements" topic to add information about the extended voltage range of Mx controllers. Renames the "ScramblePad/MATCH Power Requirements" topic to be "Power Requirements for Various Devices" on page 2-17, and added information about other devices. Adds a new topic about the "SPSH-1: Heated Back Cover for a DS47L ScramblePad" on page 2-56, and adds a sentence between Table 2-5 and Table 2-6 about reduced wiring distances. Updates Figure 7-18 on page 7-30 to identify the J1 jumper on the CCM, and adds a Note explaining that it enables updating the CCM's firmware. Repeated a Warning that removing a memory expansion board from the controller will lose all codes, in a couple of other locations. Updates the four topics about installing a SNIB3, within "Installing and Configuring the SNIB3" starting on page 7-72. Updates Table 7-16 on page 7-136 with information about more MATCH board custom settings.
MAN001-0716	MAN001-0616. Updates information about providing surge protection for a master SNIB3 using an external surge protective device, which is only necessary for the initial version of the SNIB3 board (with a serial number of the form SNIB3**-S**-nnnnn). Also updates the "HIRSCH by IDENTIV" logo.
MAN001-0616	MAN001-1015. Adds information about the SNIB3 communications expansion board. Deletes duplicated topics about the SNIB2 board. Includes various other editorial improvements to some of the topics about the SNIB, the SNIB2, or the Mx controller. Updates numerous topics to explain that the Mx-2 controller now ships with just a 1.3 Ah standby battery.

MAN001-1015	MAN001-0314. Includes the following changes required to achieve UL listing for the Mx controller: Updates the “UL Requirements” topic. Adds topic about “General Safety Precautions”. Updates the “Controller Battery Standby Capacity” topic to correct the capacity of the Mx controller’s standby battery. Updates the “Upgrading the CCM” topic to explain how to use the Controller Properties dialog in Velocity to determine the CCM firmware version. Deletes information about obsolete S*NAP software. In the “Removing and Replacing the CCM” topic and in the “Hardware Cold Start Procedure” topic, added a step about disconnecting the main power to the controller before removing the AC fuse. Updates the “Standby Battery” topic to include the dimensions of the 7.2 Ah battery pack. Adds topic about “Replaceable Parts of the Mx Controller”. Adds topic about “Electrical Ratings”. Adds topic about “Separation of Circuits”, with Figure 8-3: Cable Inlets of the Mx Controller’s Enclosure. Updates the Mx controller’s “Controller Battery Standby Capacity” topic to reflect the capacity increase from 7.0 Ah to 7.2 Ah. Updates the “Typical Connections” topic to state the basic requirements for interconnecting devices. Updates the “Wiring for a Door” topic to state that its diagrams shown the logic of the typical wiring, and an installer should refer to the wiring diagram provided with a specific reader. Adds wiring diagrams for the TS-8010 and TS-8110 card readers. Updates the “Setup and Installation of an Mx Controller” topic to state the general operating conditions and location requirements. Adds topic about “Performing Periodic Maintenance”. Adds topic about “Gathering Diagnostic Information”. Adds topic about “Interpreting the System Power Status Information”. Adds topic about “Replacing the Memory Battery”. Updates the Index. Includes the following additional changes: Updates Identiv’s contact information in the “Getting Help” topic and in the “Before You Call” topic. Corrects some information in Table 2-9: Expansion Boards and in Table 8-1: Expansion Boards for the Mx Controller. Adds topic about “Data Capacity of an Mx Controller”. Updates the “Wiring for a Door” topic to add a Caution instructing the user to power off an Mx controller before adding or removing a reader connected to a 6-pin Wiegand terminal. Updates Identiv’s logo within Figure 8-6: Mx Controller Worksheet.
MAN001-0314	MAN001-0114. Updates the tables for Step 6 in “Installing the SNIB2” to explain that DIP switches S2-S3 in Switch Bank 2 are set to ON when resetting a SNIB2 to its factory default settings; repeated this info in the Switch Bank 2 table in “Setting Up the SNIB2”. Adds topic about “Resetting the SNIB2 to its Factory Default Values”. Replaces the black-and-white symbols in “Controller and SNIB2 LED Diagnostics” with new colored symbols. Updates company information and logo. Includes a few other minor editorial improvements.
MAN001-0114	MAN001-0813. Updates the “UL Requirements” topic to include the Mx controller and remove the discontinued DS37L and DS37L-HI ScramblePads. Corrects the Mx controller’s door relay pinouts in Figure 8-5 and Figure 8-6.
MAN001-0813	MAN001-0512. Adds chapter with Mx Controller information. Expands TOC to include entries for the List of Figures, the List of Tables, commands, and application examples. Updates company information and logo. Includes various other minor corrections and editorial improvements.
MAN001-0512	MAN001-0212. Update MATCH2 information, correct minor errors.
MAN001-0212	MAN001-1011. Reinsert MATCH-compliant reader wiring information. Update company name.
MAN001-1011	MAN001-0411. Updates. MATCH 2 reinsertion. Memory board qualification.
MAN001-0411	MAN001-0610. Updates SNIB2 documentation. Other modifications.
MAN001-0610	MAN001-0210. New readers and mounting boxes. Other modifications.
MAN001-0210	MAN001-0508. Readers placed into separate document. Many modifications.
MAN001-0508	MAN001-0305. Adds RUU-210 Verification Station and additional readers.
MAN001-0305	MAN001-1103. Updates MEB, Readers, SNIB2, LAN devices, etc.

MAN001-1103	MAN001-0303.
MAN001-0303	MAN001-0802. Updates Commands, Readers, DTLMs, etc.
MAN001-0802	MAN001-0702. Unifies CCM 6.x and 7.x into a single guide.
MAN001-0702	MAN001-0901.
MAN001-0901	MAN001-0501. Updates to expansion boards, XBox, MATCH2, DT Annunciator, command supplements, commands (including CCM 7.1).
MAN001-0501	MAN001-1100.
MAN001-1100	MAN001-0800.
MAN001-0800	MAN001-0300.
MAN001-0300	MAN001-0100.
MAN001-0100	MAN001-1199.
MAN001-1199	MAN001-899.
MAN001-899	MAN001-1298.
MAN001-1298	MAN001-698.
MAN001-698	MAN001-997.
MAN001-997	DT-W-4392 DIGI*TRAC Installation Guide, UMK-1NS1, ScramblePad Installation Guide, DIGI*TRAC End Of Line Module Technology Guide, AEB8, REB8, MEB/BE, MEB/CE, SNIB, and SCIB Installation Notes, PS2 Installation Guide, M-IN-0393 MATCH Addendum, DIGI*TRAC Programming Guide, Remote Site Management Information Guide, NET*MUX4 Application & Installation Guide, and Application Guide.

Identiv
1900-B Carnegie Avenue
Santa Ana, CA 92705-5520

Phone: 949-250-8888 or 888-809-8880 (toll-free)
Fax: 949-250-7372
Web: www.identiv.com

HIRSCH by IDENTIV

Getting Help

If you encounter a problem that is not discussed in this guide and you need technical support, do the following:

1. Contact your local dealer or the provider of this product.

2. If your dealer is not available, contact Technical Support directly. This can be done in a number of ways:

   Internet: https://support.identiv.com/contact/

   Email: support@identiv.com

   Phone: 877-447-7249 toll-free

   Mail: Identiv
   1900-B Carnegie Avenue
   Santa Ana, CA 92705-5520

   Attn: Technical Support

Whenever you contact your local dealer or Identiv, be sure to have your registration material, serial number, and software version numbers available.

For future reference, record these numbers here.

Serial Number: _____

Version Number: _____

Dealer: _____

Dealer Phone #: _____

CCM Firmware Version #: _____

SNIB2 or SNIB3 Firmware Version #: _____

UL Requirements

UL is an independent safety science company that develops safety-related standards, and tests products to determine whether they meet a specific standard so they can be certified as UL-listed. There are various UL standards related to security systems or their components, such as UL 294, the Standard for Access Control System Units, and UL 1076, the Standard for Proprietary Burglar Alarm Units and Systems.

Velocity is flexible software that can control a wide variety of hardware components, enabling you to design a custom system that meets your particular security needs. This topic provides information about designing a security system using Velocity software and DIGI*TRAC hardware that meets certain UL standards.

GENERAL INFORMATION

The UL-listed Velocity System may be comprised of the following components: Central Supervisory Station, M1N, M2, M8, M16, Mx, Mx-1, DS47L, DS47L-HI, DS47L-SPX, DS47L-SPX-HI, Power Limitation Board (CL2), PS2, DTLM1, DTLM2, DTLM3, MELM1, MELM2, and MELM3. The M2, M8, M16, and Mx controllers may employ the following expansion boards: MEB/BE, AEB, REB8, SNIB, SNIB2, and SNIB3. (NOTE: The SNIB3 board has not been evaluated with the M16 controller.)

UL 1076 compliance requires use of a listed reader. UL has verified compatibility of the following Identiv TS readers with the Mx-1 controller: 8210, 8230, 8330, and 8336.

Wiring methods shall be in accordance with the National Electrical Code (ANSI/NFPA70), Canadian Electrical Code (C22.1), local codes, and the authorities having jurisdiction. All cabling and wire used must be Listed or Recognized AWM wire, suitable for the application. Class 2 or 3 conductors must be segregated from electric light, power, Class 1 conductors, non-Class 2 or 3 signaling conductors, battery backup, and medium-power network-powered broadband communications-circuit conductors.

When using the initial version of the SNIB3 communications board (which has a serial number of the form SNIB3-**S**-nnnnn), surge protection must be provided for the master SNIB3 in each chain of connected controllers, using the Sankosha Guardian Net LAN-CAT5e-P+ surge protection device. For details, see “Providing Surge Protection for a Master SNIB3” starting on page 7-72.

The system shall not be installed in the fail-secure mode unless permitted by the local authority having jurisdiction, and it shall not interfere with the operation of Listed panic hardware. The use of panic hardware has not been evaluated by UL.

For proprietary burglary system use, all status changes at the protected premise must be programmed to cause both an audible and a visual annunciation at the central receiving station, and an acknowledgement signal and local annunciation must be programmed from the central receiving station to the protected premise.

UL terms that are applicable to this application can be found in Appendix B, “Glossary”.

Summary of UL 294 Performance Levels for Access Control Features:

Feature	Level I	Level II	Level III	Level IV
Destructive Attack	No attack test	Withstand attack test for 2 minutes	Withstand attack test for 5 minutes, or generate an alarm event in 2 minutes	Withstand attack test for 5 minutes, or generate an alarm in 2 minutes which cannot be silenced for 2 minutes
Line Security	No line security	Standard line security	Encrypted line security 128 bits	Encrypted line security 256 bits
Endurance	1,000 cycles	25,000 cycles	50,000 cycles	100,000 cycles
Standby Power	No secondary power source	Can maintain normal operations for a minimum of 30 minutes	Can maintain normal operation for a minimum of 2 hours	Can maintain normal operation for a minimum of 4 hours

UL 294 Rating Achieved by DIGI*TRAC Controllers:

Feature	M1N Rating	M2 Rating	M8 Rating	M16 Rating
Destructive Attack	Level I	Level I	Level I	Level I
Line Security	Level I	Level I	Level I	Level I
Endurance	Level IV	Level IV	Level IV	Level IV
Standby Power	Level IV (with supplied 1.2 Ah battery)	Level IV (with supplied 1.3 Ah battery)	Level IV (with supplied 7.0 Ah battery)	Level IV (with supplied 1.3 Ah battery)

UL 294 Rating Achieved by Other DIGI*TRAC Components:

Feature	Rating for the DS47L line of readers	Rating for the MATCH2 Reader Interface Board	Rating for the Power Limitation Board	Rating for the PS2 power supply
Destructive Attack	Level I	Level I	Level I	Level I
Line Security	Level I	Level I	Level I	Level I
Endurance	Level IV	Level IV	Level IV	Level IV
Standby Power	Level I	Level I	Level I	Level IV

UL 294 Rating Achieved by the Different Models of Mx Series Controllers:

Feature	Mx-1 Rating	Mx-1-ME Rating	Mx-2 Rating	Mx-4 or Mx-8 Rating
Destructive Attack	Level I	Level I	Level I	Level I
Line Security	Level IV	Level IV	Level IV when using XNET3 (with a SNIB3 and optionally an RREB); Level III when using XNET2 (with a SNIB2, or a SNIB3 and optionally an RREB)	Level IV when using XNET3 (with a SNIB3 and optionally an RREB); Level III when using XNET2 (with a SNIB2, or a SNIB3 and optionally an RREB)
Endurance	Level IV	Level IV	Level IV	Level IV
Standby Power	Level I	Level IV (with supplied 7.2 Ah battery)	Level II with 1.3 Ah battery; Level IV with 7.2 Ah battery	Level IV (with supplied 7.2 Ah battery)

Standby Power Requirements for Various UL Standards:

UL Standard	UL 294	UL 1076	CAN/ULC-S319-05
Required Duration of Standby Power	30 minutes for Access Control Performance Level II; 4 hours for Access Control Performance Level IV	24 hours, or 4 hours if the controller signals that it is operating on standby power	30 minutes for Class I equipment

When the available controller power is insufficient, an external power supply can be used to power attached devices such as a ScramblePad or MATCH2 interface. That power supply must be a UL-listed low-voltage Class 2 power-limited power supply, which is capable of providing standby power for the duration required by the UL standard your physical access control system must meet:

- UL 294 Access Control Performance Level I: not applicable
- UL 294 Access Control Performance Level II: 30 minutes
- UL 294 Access Control Performance Level III: 2 hours
- UL 294 Access Control Performance Level IV: 4 hours
- UL 1076: 24 hours, or 4 hours if the controller sends a signal to the central supervising station indicating that it is operating on standby power
- CAN/ULC-S319-05: 30 minutes (for Class I equipment)

A Velocity system with Mx controllers meets the requirements of CAN/ULC-S319-05 Equipment Class I. The Mx-1-ME controller meets the UL 294 Access Control Performance Level IV for standby power, and the UL 1076 requirement of 4 hours with a signal sent to the central supervising station.

ELECTRICAL SAFETY INFORMATION

To prevent electric shock, you must observe common-sense precautions when working with the high-voltage AC input power connections and the standby battery pack connections to a DIGI*TRAC or Mx controller. (For example, see “General Safety Precautions” on page xx.)

No special precautions are required when working with the Class 2 limited-power connections which supply low-voltage power to other devices such as readers. (When you create these connections, you are not working directly with bare live wires. Instead, the ends of the wires are attached to plastic terminal blocks on the controller, MATCH board, or reader.) However, when routing the wires for the Class 2 limited-power connectors, make sure that you maintain a safe separation of at least 0.25 inches from the wires for a controller’s AC input power and the standby battery pack. For an illustration of this principle, see Figure 8-3, “Cable Inlets of the Mx Controller’s Enclosure”, on page 8-14.

To improve the safety of some older DIGI*TRAC controllers (such as the M2, M8, or M16), you can install a Power Limitation Board between the controller’s main board and the controller’s power supply and standby battery pack. (A Power Limitation Board is not needed for newer controllers such as the Mx or the Mx-1.) For more information, see “Power Limitation Board Installation” on page 7-305.

Most of the controllers (except for the M1N and the Mx-1) support the addition of optional expansion boards, which are easily connected using a flexible EBIC5 ribbon cable. For more information, see “Connecting Expansion Boards” (and its subtopics) starting on page 7-13.

M1N Controller

The M1N controller is a 1-door controller which can power one ScramblePad and/or MATCH interface from the ScramblePad/MATCH terminal block associated with the supervised doors. (This controller does not include an expansion board connector.)

The M1N controller’s main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the lower left corner):

- ❑ One 4-wire S*NET RS-232 terminal block and one 5-wire RS-485 terminal block (along the lower left side) which are used for secure communication with the Velocity server on a private network. These connectors are the same as those on the SNIB expansion board; for more information, see “SNIB” on page 2-33.
- ❑ Four 3-wire INPUT terminal blocks (along the upper left side) which are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.
- ❑ One 5-wire KEYPADS terminal block (in the upper right corner) which is used for connecting the wiring from ScramblePad keypads or readers (through a MATCH2 Reader Interface). This is a *digital* circuit which supports daisy-chain connections to multiple devices on the same circuit.
- ❑ Three 3-wire Control Relay terminal blocks labeled RELAY2, RELAY3, and RELAY4 (along the middle of the right side) which are rated 24VDC at 2 Amps, resistive for externally-powered devices. NOTE: RELAY1 is a heavy-duty door relay rated 24VDC at 10 Amps, resistive for externally-powered devices.
- ❑ The 3-wire BOX TAMPER connector attaches to the corresponding connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open.

For more information about the wiring for this device, see the **M1N Quick Installation Guide** sticker on the inside of the controller enclosure's door, "Model 1N Design" on page 2-4, "Connecting Wires to the Controller Boards" on page 7-12, and Figure 7-8, "M1N Controller Board", on page 7-18.

M2 Controller

The M2 controller has two heavy-duty door relays, each with associated line module inputs for supervision and door functions. It also has two heavy-duty door relays for unsupervised doors.

The M2 controller's main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the upper left side):

- ❑ The Expansion Board Connector (in the upper left) is used to link any expansion boards mounted in the controller's enclosure to the controller's main board (using a flexible EBIC5 ribbon cable).
- ❑ Two 3-wire line module input terminal blocks (for DOOR 1 and DOOR2 in the top middle) are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.
- ❑ Two 5-wire MATCH terminal blocks (for DOOR 1 and DOOR2 in the top middle) are used for connecting the wiring from ScramblePad keypads or readers (through the MATCH2 Reader Interface). These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit.
- ❑ The 3-wire ALARM Relay terminal block (on the lower right side) is rated 24VDC at 2 Amps, resistive for externally-powered devices. NOTE: This connector will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The 3-wire BOX TAMPER connector attaches to the corresponding connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open.

For more information about the wiring for this device, see the **M2 Quick Installation Guide** sticker on the inside of the controller enclosure's door, "Model 2 Design" on page 2-5, "Connecting Wires to the Controller Boards" on page 7-12, and Figure 7-9, "M2 Controller Board", on page 7-18.

M8 Controller

The M8 controller has connectors for eight supervised doors. It also has four dedicated alarm relays.

The M8 controller's main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the upper left side):

- ❑ The Expansion Board Connector (in the upper left) is used to link any expansion boards mounted in the controller's enclosure to the controller's main board (using a flexible EBIC5 ribbon cable).
- ❑ Eight 3-wire line module input terminal blocks (for DOOR 1 through DOOR 8 along the top) are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.
- ❑ Eight 5-wire MATCH terminal blocks (for DOOR 1 through DOOR 8 along the top) are used for connecting the wiring from ScramblePad keypads or readers (through the MATCH2 Reader Interface). These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit.

- ❑ Four 3-wire ALARM Relay terminal blocks (along the middle of the right side) are rated 24VDC at 2 Amps, resistive for externally-powered devices. NOTE: These connectors will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The 3-wire tamper switch connector (on the lower right side) attaches to the corresponding connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open.

For more information about the wiring for this device, see the **M8 Quick Installation Guide** sticker on the inside of the controller enclosure's door, "Model 8 Design" on page 2-6, "Connecting Wires to the Controller Boards" on page 7-12, and Figure 7-10, "M8 Controller Board", on page 7-19.

M16 Controller

The M16 controller provides 16 line module inputs. Although it supports relays or additional inputs through the use of REB or AEB expansion boards, the M16 is not designed for supervised door access control; its primary function is to monitor and report the status of door contacts, motion detectors, alarm sensors, or other detection devices.

The M16 controller's main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the upper left side):

- ❑ The Expansion Board Connector (in the upper left) is used to link any expansion boards mounted in the controller's enclosure to the controller's main board (using a flexible EBIC5 ribbon cable).
- ❑ Two 5-wire KEYPADS terminal blocks (near the upper left corner) which can be used to power ScramblePads and MATCH reader interfaces.
- ❑ Sixteen 3-wire line module input terminal blocks (XA1 through XA16 along the top) which are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.
- ❑ The 3-wire ALARM Relay terminal block (on the lower right side) is rated 24VDC at 2 Amps, resistive for externally-powered devices. NOTE: This connector will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The 3-wire BOX TAMPER connector attaches to the corresponding connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open.

For more information about the wiring for this device, see the **M16 Quick Installation Guide** sticker on the inside of the controller enclosure's door, "Model 16 Design" on page 2-7, "Connecting Wires to the Controller Boards" on page 7-12, and Figure 7-11, "M16 Controller Board", on page 7-19.

Mx Controller

The Mx controller can be configured to control either 2, 4, or 8 doors, depending on which model of the Command and Control Module (CCMx) is installed.

The Mx controller's main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the lower left side):

- ❑ The four 3-wire alarm relay terminals generate different types of alarms (1 = General alarm, 2 = Duress alarm, 3 = Tamper alarm, and 4 = Trouble alarm), which can be handled separately to meet your specific needs. NOTE: These connectors will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The Ethernet connector (and its associated DIP switches) enables you to connect to a LAN/WAN and securely communicate with the Velocity server.
- ❑ The Expansion Board Connector is used to link any expansion boards mounted in the controller's enclosure to the controller's main board (using a flexible EBIC5 ribbon cable).
- ❑ The 3-wire Door Relay terminal blocks (one for each door) are rated 30VDC at 5 Amps, and are used to control externally powered door access devices such as magnetic locks and electric strikes. NOTE: These connectors will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The 3-wire Door Input terminal blocks (one for each door) are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.
- ❑ The 5-wire MATCH terminal blocks (one for each door) are used for connecting the wiring from ScramblePad keypads or readers (through the MATCH2 Reader Interface Board). These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit.
- ❑ The 6-wire Wiegand terminal blocks (one for each door) are used for connecting the wiring from a 12VDC keypad or reader with a Wiegand interface. These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials. For more information, see "Connecting Exit Readers to Unused Wiegand Terminals on Mx-2 or Mx-4 Controllers" on page 8-22.
- ❑ The 5-wire SNIB2 RS485 Terminal (and its associated DIP switches) enables you to securely communicate with downstream controllers on a private network (which is managed by the same Velocity server).
- ❑ The 3-pin Tamper Switch connector attaches to the corresponding 5-sided connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open.

For more information about the wiring for this device, see the **Mx Quick Installation Guide** sticker on the inside of the controller enclosure's door, Figure 8-2 on page 8-6, and "Separation of Circuits" on page 8-14.

Mx-1 Controller

The Mx-1 controller is a 1-door controller which is packaged in a compact plastic case, and can be powered by either PoE+ or DC power from an external power supply. (Its light weight and small size provides more flexibility when deciding where to install it.)

The Mx-1 controller's main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the middle of the left side):

- ❑ One 6-pin RS-485 Controller Bus terminal block which can be used to create a chain of controllers, where the first (master) controller communicates directly with the Velocity Server using its Ethernet connector, and the other (downstream) controllers communicate along the chain using RS-485 wiring. Otherwise, an Mx-1 controller can communicate directly with the Velocity Server across a network using its POE+ Ethernet connector.
- ❑ One Expansion Board Connector (which is used to link any expansion boards mounted in the controller's enclosure to the controller's main board, using a flexible EBIC5 ribbon cable).

  NOTE: Expansion boards cannot be used within the Mx-1 controller's compact plastic case. If you require expansion boards, you should choose a different controller.
- ❑ Two 8-wire terminal blocks (for connecting the wiring from a 12 VDC keypad or reader with a Wiegand interface). These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.
- ❑ One 5-wire terminal block (for connecting the wiring from a 12 VDC keypad or reader with an OSDP RS-485 interface).
- ❑ Two 3-wire analog Door Input and Aux. Input terminal blocks (for the line modules used to supervise doors, tamper circuits, and RQE devices).
- ❑ Two 3-wire Door Relay and Aux. Relay terminal blocks are used to control the door's access device (such as a magnetic lock or an electric strike) and an external alarm or auxiliary device. NOTE: These connectors will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The Ethernet / POE+ connector (and its associated DIP switches) provides up to Gigabit data connectivity for secure communication with the Velocity server, and can be used to power the controller (and some attached devices) through Power Over Ethernet Plus with a nominal 25.5 Watts of input power. The POE+ power source should be UL 294 listed. NOTE: If the Mx-1 controller will be part of an access control system which must meet a particular UL standard, you must use a UL-listed power source or backup battery which provides the required duration of standby power for that standard. For more information, see the table about "Standby Power Requirements for Various UL Standards:" on page ix.

For more information about the wiring for this device, see the **Mx-1 Quick Installation Guide** provided with the controller, Figure 9-2 on page 9-8, and "Separation of Circuits" starting on page 9-32.

Mx-1-ME Controller

The Mx-1-ME controller is a 1-door controller which is packaged in a traditional metal enclosure (with a locking door, a tamper switch, a power supply, a standby battery, and room for up to five optional expansion boards).

The Mx-1-ME controller's main board has the following Class 2 limited-power connectors (listed here in clockwise order starting from the middle of the left side):

- ❑ One Expansion Board Connector (which is used to link any expansion boards mounted in the controller's enclosure to the controller's main board, using a flexible EBIC5 ribbon cable).

- ❑ Two 8-wire terminal blocks (for connecting the wiring from a 12 VDC keypad or reader with a Wiegand interface). These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.
- ❑ One 5-wire terminal block (for connecting the wiring from a 12 VDC keypad or reader with an OSDP RS-485 interface).
- ❑ Two 3-wire analog Door Input and Aux. Input terminal blocks (for the line modules used to supervise doors, tamper circuits, and RQE devices).
- ❑ Two 3-wire Door Relay and Aux. Relay terminal blocks are used to control the door's access device (such as a magnetic lock or an electric strike) and an external alarm or auxiliary device. NOTE: These connectors will be Class 2 power-limited if the attached device's external power source is Class 2 power-limited.
- ❑ The Ethernet connector (and its associated DIP switches) provides up to Gigabit data connectivity for secure communication with the Velocity server. NOTE: Because the Mx-1-ME controller includes a power supply, its Ethernet connector does not include POE capability.
- ❑ One 6-pin RS-485 Controller Bus terminal block which can be used to create a chain of controllers, where the first (master) controller communicates directly with the Velocity Server using its Ethernet connector, and the other (downstream) controllers communicate along the chain using RS-485 wiring. Otherwise, an Mx-1-ME controller can communicate directly with the Velocity Server across a network using its Ethernet connector.
- ❑ The 3-pin Door Tamper connector attaches to the corresponding 5-sided connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open.

For more information about the wiring for this device, see the **Mx-1-ME Quick Installation Guide** sticker on the inside of the controller enclosure's door, Figure 9-2 on page 9-8, and "Separation of Circuits" starting on page 9-32.

MATCH2 Reader Interface Board

The MATCH2 Reader Interface Board (MRIB) enables a large number of reader technologies to communicate successfully with a DIGI*TRAC controller. It has the following Class 2 limited-power connectors (listed here in clockwise order starting from the upper right side):

- ❑ Two 6-wire reader terminal blocks (on the upper right) enable you to connect readers which have the Wiegand interface.
- ❑ Two 3-wire P1 and P2 connectors (along the bottom) each provide 250 mA at 5VDC to power additional devices. NOTE: These connectors will be Class 2 power-limited if the MATCH2 Reader Interface Board's power source is Class 2 power-limited.
- ❑ The 5-wire D*TRAC terminal block (on the left side) is used to connect to a DIGI*TRAC or Mx controller. (The Mx-1 controller does not have a MATCH connector.)
- ❑ The 5-wire KEYPADS terminal block (on the left side) is used to connect to one or two ScramblePads. This provides a *digital* circuit which enables you to daisy-chain multiple devices (such as a required entry reader and an optional exit reader for a door). NOTE: If a reader requires more than 5VDC or more than 250 mA, it must be separately powered by a UL 294 listed power supply with Class 2 power-limited output.

For more information about the wiring for this device, see “MATCH Reader Interface” starting on page 2-59, Figure 2-44, “MATCH Connections (MATCH2 Shown)”, on page 2-61, and “Connecting ScramblePad and MATCH Interfaces” starting on page 7-24.

DS47L Line of Readers

The DS47L line of readers includes many different models with a variety of features. For more information, see Table 2-16, “ScramblePad Types”, on page 2-48.

Models that include an integrated MATCH2 interface have the same Class 2 limited-power connectors as the MATCH2 Reader Interface Board (which are explained in the previous list).

For more information about the wiring for these devices, see “DS47L ScramblePad/ ScrambleProx Setup” on page 7-116, and “Wiring the ScramblePad” on page 7-117.

PS2 Power Supply

The PS2 Power Supply can power one or two heavy-duty locks/strikes or other powered devices. (Power to these devices is triggered by outputs from a controller, which are connected to inputs on the PS2.) It also includes a power connector for locally powering one or two ScramblePads at the door being controlled.

The PS2 has the following Class 2 limited-power connectors (listed here in clockwise order starting from the upper left corner):

- ❑ The 3-wire INPUT 1 and INPUT 2 terminal blocks are used to connect to door relay terminals on a controller.
- ❑ The 3-wire POWER 1 and POWER 2 terminal blocks are used to power a 24VDC electric lock or strike which secures a door. NOTE: Because the PS2 includes multiple 24VDC battery packs, these connectors will be Class 2 power-limited only if a CL2 Power Limitation Board is added to the PS2. For more information, see “Power Limitation Board Installation” starting on page 7-305.
- ❑ The 3-wire unpowered RELAY 1 and RELAY 2 terminal blocks can be used to connect to other devices, so they are also controlled by INPUT 1 and INPUT 2. NOTE: These connectors will be Class 2 power-limited if the attached device’s external power source is Class 2 power-limited.

For more information about the wiring for this device, see “Using the PS2 Power Supply” on page 2-44, and “Wiring the PS2” on page 7-308.

Power Limitation Board

The **Power Limitation Board** does not have any Class 2 limited-power connectors. For more information about this device, see “Power Limitation Board Installation” starting on page 7-305.

VELOCITY

1. For the software requirements and minimum hardware requirements of Velocity servers, clients, and standalone workstations, see the “System Requirements” topic in the *Velocity Installation Guide* (MAN004).
2. For burglary use, all status changes at the protected premise must be programmed to cause both an audible and a visual annunciation at the central receiving station, and an acknowledgement signal and local annunciation must be programmed from the central receiving station to the protected premise.
3. If Alarm Priority levels are assigned by the user, then the following priority must be assigned for UL applications:
   a. Fire alarm and industrial supervision where a risk of injury to persons, or damage to or destruction of property may be involved.
   b. Hold-up or panic alarm.
   c. Burglar alarm.
   d. Watchman tour.
   e. Fire-alarm supervision.
   f. Burglar-alarm supervision.
   g. Industrial supervision where a risk of injury to persons, or damage to or destruction of property will not be involved.
   h. Other supervisory services.

   Items (b) and (c) may have equal priority; items (e) and (f) may have equal priority; and items (g) and (h) may have equal priority.
4. The Alarm Stacking feature is not to be used for UL applications.
5. The Return to Normal feature is not to be used for UL applications.
6. The Video capability of the Velocity software has not been evaluated by UL.

CENTRAL SUPERVISORY STATION

The Central Supervisory Station may be employed in the following way:

1. The data processing equipment and office appliance and business equipment used as central supervisory station equipment shall be listed under Office Appliances and Business Equipment (UL 114), or Information Processing and Business Equipment (UL 478), or Part 1: General Requirements of Information Technology Equipment (UL 60950-1).
2. A redundant server configuration should be employed, where the servers and workstations are networked via a dedicated Ethernet LAN.
3. A “panel logged off” event may be a compromise attempt on the system.
4. Supply line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330V will be used on Central Monitoring Station equipment.
5. Signal line transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with maximum marked rating of 50V will be used on communication circuits extending more than 25 feet from the computer systems.

6. Communication circuits and network components connected to the telecommunications network shall be protected by secondary protectors for communication circuits. These protectors shall comply with the Standard for Secondary Protectors For Communication Circuits, UL 497A. These protectors shall be used only in the protected side of the telecommunications network.
7. The Central Monitoring Station equipment will be installed in a temperature-controlled environment. A temperature-controlled environment is defined as one that can be maintained between 13 – 35° C (55 – 95° F) by the HVAC system. Twenty-four hours of standby power will be provided for the HVAC system. The standby power for the HVAC system can be supplied by an engine-driven generator alone. A standby battery is not required.
8. In addition to the main power supply and secondary power supply that are required to be provided at the Central Supervisory Station, the system will be provided with an uninterruptible power supply (UPS) with sufficient capacity to operate the computer equipment for a minimum of 15 minutes. If more than 15 minutes is required for the secondary power supply to supply the UPS input power, the UPS will be capable of providing input power for at least that amount of time.
9. The UPS will comply with the Standard for Uninterruptible Power Supply Equipment, UL 1778, or the Standard for Fire Protective Signal Devices, UL 1481.
10. In order to perform maintenance and repair service, a means for disconnecting the input to the UPS while maintaining continuity of power to the automation system will be provided.
11. The alarm system's network settings will be designed such that the maximum time lapse from the initiation of an initiating device circuit until it is annunciated at the central supervising station will not exceed 90 seconds.
12. The alarm system's network settings will be designed such that the maximum time for the central supervising station to annunciate a single break, single ground, wire-to-wire short, loss of signal, or any combination of these will not exceed 200 seconds.
13. The alarm system configuration will be designed such that the number of signals on a single channel will be limited to 1000.

UL-LISTED DIGI*TRAC COMPONENTS

The following DIGI*TRAC components are UL-listed:

M1N

1. Input rating of the M1N is 120VAC, 50/60 Hz, 500mA.
2. The Alarm/Control Relay contact rating is 24VDC, 1A, resistive.

M2

1. UL has verified compatibility of the Hirsch DS47L, DS47L-HI, DS47L-SPX, and DS47L-SPX-HI with the M2.
2. The Alarm/Control Relay contact rating is 24VDC, 1A, resistive.

M8

1. UL has verified compatibility of the Hirsch DS47L, DS47L-HI, DS47L-SPX, and DS47L-SPX-HI with the M8.
2. The Alarm/Control Relay contact rating is 24VDC, 1A, resistive.

M16

1. Input rating of the M16 is 120VAC, 50/60 Hz, 1A.
2. UL has verified compatibility of the Hirsch DS-47L-SPX with the M16.
3. The Alarm/Control Relay contact rating is 24VDC, 1A, resistive.

Mx

1. Input rating of the Mx is 110-240VAC, 50/60 Hz, 2A.
2. UL has verified compatibility of the Hirsch DS47L, DS47L-HI, DS47L-SPX, and DS47L-SPX-HI with the Mx.
3. The Alarm/Control Relay contact rating is 24VDC, 1A, resistive.
4. The Ethernet cable connecting the SNIB2 or SNIB3 board's communications port to an external network must be shielded.

Mx-1

1. When using an external power supply (via the Power terminal), the input rating of the Mx-1 controller is 24-28 VDC, 2 Amps. When using POE+ (via the Ethernet jack), the input rating of the Mx-1 is 44-57 VDC, and the maximum output power is 25.5 W.
2. The Mx-1 supports both a UL-listed entry reader and an optional exit reader, each with audible feedback capability, which can be connected using either the 8-pin Wiegand terminals or the 5-pin RS-485/OSDP terminal. For more information, see "Wiring for the Door" starting on page 9-37.
3. The Ethernet cable connecting the Mx-1's communications port to an external network must be shielded.
4. UL has not tested the Mx-1 in a chain of controllers connected using RS-485 wiring.
5. The Mx-1 controller does not require a Power Limitation Board (CL2).
6. UL has verified compatibility of the following Identiv TS readers with the Mx-1 controller: 8210, 8230, 8330, and 8336.
7. For UL applications, the Mx-1 needs to be powered by either a UL 294, UL 1076, and ULC-S319 power supply or POE+, with the appropriate required standby power.
8. Revision 1 of the Mx-1 controller has the model number of Mx-1 026-0000121-P, and is described in Chapter 9 of a previous version (Revision AH dated April 17, 2018) of this document. Revision 2 of the Mx-1 controller has the model number of Mx-1 026-0000121-P**-2**, and is described in Chapter 9 of later versions of this document.

NOTE: There is an **Mx-1-W** license for an Mx-1 or Mx-1-ME controller that is specifically configured to manage up to eight wireless locks. (These can be either ASSA-ABLOY's Aperio brand of wireless locks, or Allegion's Schlage brand of wireless locks.) For more information, see the DIGI*TRAC Hardware Configuration > Wireless Locks > **Wireless Locks – Overview** topic in the Velocity online help. This functionality has not been evaluated by UL.

Mx-1-ME

1. The input rating of the Mx-1-ME is 110-240VAC, 50/60 Hz, 2A. It uses the Sinpro model R/C (QQGQ2, QQGQ8) power supply (part number SBU150-109).
2. The Mx-1-ME supports both a UL-listed entry reader and an optional exit reader, each with audible feedback capability, which can be connected using either the 8-pin Wiegand terminals or the 5-pin RS-485/OSDP terminal. For more information, see "Wiring for the Door" starting on page 9-37.

3. The Ethernet cable connecting the Mx-1-ME's communications port to an external network must be shielded.
4. UL has not tested the Mx-1-ME in a chain of controllers connected using RS-485 wiring.
5. UL has verified compatibility of the following Identiv TS readers with the Mx-1-ME controller: 8210, 8230, 8330, and 8336.

PS2 Power Supply

1. The PS2's KEYPAD POWER connector cannot be used for UL installations.
2. Do not use 12V batteries (instead of the supplied 24 VDC battery packs).
3. Because the PS2 includes multiple 24VDC battery packs, its POWER 1 and POWER 2 terminal blocks will be Class 2 power-limited only if a CL2 Power Limitation Board is added to the PS2. For more information, see "Power Limitation Board Installation" starting on page 7-305.
4. Use compatible UL-listed locking devices. If installation or occupancy requirements call for fail-safe operation of door locking devices, use UL-listed panic exit hardware or UL-listed fail-safe locks. (A fail-safe lock should be connected to the 24VDC N.C. and Ground terminals of a powered relay, or to the N.C. and Common terminals of an unpowered relay.)
5. The cables powering the locking devices should be separated from the other cables, and if they are carrying 8 or more Amps, they must be insulated by conduit.
6. Do not exceed the relay contact ratings which are listed in the **PS2 Quick Installation Guide** or in "Using the PS2 Power Supply" starting on page 2-44. For switching larger loads, use UL-listed external relays.
7. Do not use higher rated fuses than those listed in the **PS2 Quick Installation Guide**.

RREB

1. Information about the RREB is provided in "RS-485 Readers Expansion Board (RREB)" starting on page 2-28 (and its subtopics), and in "RS-485 Readers Expansion Board (RREB) Installation" starting on page 7-35.
2. UL has verified compatibility of the RREB with the Mx-8 controller.
3. Shielded cable must be used when connecting RS-485 readers to the RREB.

General Safety Precautions

Be sure to observe the following common-sense precautions when working with the high-voltage AC input power connections and the standby battery pack connections to a DIGI*TRAC or Mx controller:

- ❑ Before removing or replacing fuses, turn off the main power leading into the controller.
- ❑ Before working on the power supply connections of a controller, turn off the main power leading into the controller.

NOTE: Identiv sells its controllers to licensed dealers (known as Identiv Channel Alliance Network partners), who employ trained installers who have been certified by the Identiv Academy. For more information, visit **https://academy.identiv.com/**.

Table of Contents

List of Figures

List of Tables

Introduction & Overview

1

About This Guide

Planning security for a facility is never easy, but it can be made less difficult and time-consuming if you know what your options are. This guide provides you with information about what those options are, and detailed instructions about how to design a secure environment for your requirements.

The job of adapting Hirsch security apparatus to a facility involves a number of tasks:

- ❑ Determining the security needs of the facility consistent with business objectives of management.
- ❑ Choosing the best locations to place security accessways and the DIGI*TRAC controller(s).
- ❑ Selecting the right security equipment for each accessway. This should take into account all architectural, electrical, and physical requirements, as well as local building codes.
- ❑ Configuring the equipment to meet specific needs.

Note: Identiv recommends that all physical installations and cabling meet the specifications published in the appropriate electrical standard to ensure proper operation of all Identiv devices connected. When determining the required power delivery for connected devices, Installers should calculate cabling needs based on the power specifications of each connected device, the operational output of the power source and the voltage drop relative to the length of the cable. Identiv does not specify cable types or gauges due to the wide variance of available cable configurations, and similar wide variance in installation types and environmental conditions. All examples provided throughout this installation document are designed to provide guidance only and should be verified by a certified low voltage electrician or contractor on a per site basis.

Who Should Read This Guide

This guide is intended for several audiences:

- ❑ Systems/Design engineers responsible for
  - Selecting and configuring hardware components
  - Preparing submittals and installation drawings
  - Ordering equipment

  Chapters 1, 2, and 6 will prove most useful for them.
- ❑ Programmers responsible for configuring DIGI*TRAC software for a specific site or application. Chapters 1, 3, 4, and 5 will prove most useful to them.
- ❑ Technicians responsible for setting up and installing Hirsch equipment at the specific site. Chapters 2, 5, 6 and 7 should prove most useful to them.
- ❑ Operators responsible for adding and deleting users, generating reports on standalone panels, or programming the Hirsch system onsite using the Hirsch ScramblePad. Chapters 1, 3, 4, and 5 will prove most helpful for them.

*Note: This guide focuses on the standalone configuration – using a local ScramblePad to program and operate a DIGI*TRAC controller. For instructions on programming and operating the DIGI*TRAC controller from a host PC, refer to the appropriate S*NAP, SAM, MOMENTUM, or Velocity manual.*

What's In This Guide

The following topics are included in this guide:

- ❑ Chapter 1, *Introduction & Overview*—describes the purpose of this guide and introduces you to the Hirsch DIGI*TRAC family of access control panels.
- ❑ Chapter 2, *Design Considerations*—provides more information on each component within the Hirsch access control system, plus information about common building features for which the components are used, such as doors, HVAC, turnstiles, gates, and elevators.
- ❑ Chapter 3, *Basic Programming*—an introduction to the DIGI*TRAC Control Language which explains some of the fundamental commands and basic routines used to configure the system.
- ❑ Chapter 4, *Command Reference*—the detailed explanation of all commands in the DIGI*TRAC Control Language, with syntax and examples for each.
- ❑ Chapter 5, *Factory Setup and Printout Guide*—provides detailed information on factory defaults for the DIGI*TRAC Control Language, and an explanation of printouts.
- ❑ Chapter 6, *Application Examples*—describes ways in which you can use Hirsch devices and programs to outfit any building with the most up-to-date security. Provides many door and network plans as examples of possible configurations.
- ❑ Chapter 7, *Setup and Installation*—provides detailed instructions on how to set up, wire, and install a Hirsch security system. This chapter includes specific information on cabling distances, power requirements, component dimensions, and connections.
- ❑ Chapter 8, *Mx Controller*—provides information about Hirsch Mx Controllers.
- ❑ Chapter 9, *Mx-1 Controller*—provides information about Hirsch Mx-1 Controllers
- ❑ Appendix A, *Worksheets*—provides forms that help you plan both the hardware configuration for the DIGI*TRAC system and programming requirements.
- ❑ Appendix B, *Glossary*—provides a glossary of frequently-used terms.
- ❑ Index

System Overview

A DIGI*TRAC system consists of three types of devices:

- Controllers (including optional expansion boards)
- Remote Components
- Communications Devices

Controllers are the security control/monitoring equipment in the middle which take signals from input devices—such as keypads and readers—then decide how these devices should respond.

Remote Components are all the components found outside the controller's enclosure. They are usually located at the doors or accessways requiring access control, and include:

- **Keypads and Readers** which allow access to a secure area.
- **Input devices** are those remote devices—such as door contacts, request-to-exit devices, and motion detectors—which send alarms or other security information to a controller for interpretation and response.
- **Output devices** are those remote devices—such as magnetic locks, electric strikes, and audible signals—which are operated by relays in the controller.
- **Printers** which produce real-time event logs, user lists, and system setups/status documents.
- **Power Supplies** which provide power to output devices such as electric locks.

Communications Devices—such as network boards and modems—link a DIGI*TRAC controller to a local or remote PC. You can use DIGI*TRAC controllers either as stand-alone systems, or as part of a network of controllers with the addition of these devices.

Figure 1-1 illustrates some of the components used with the DIGI*TRAC controller:

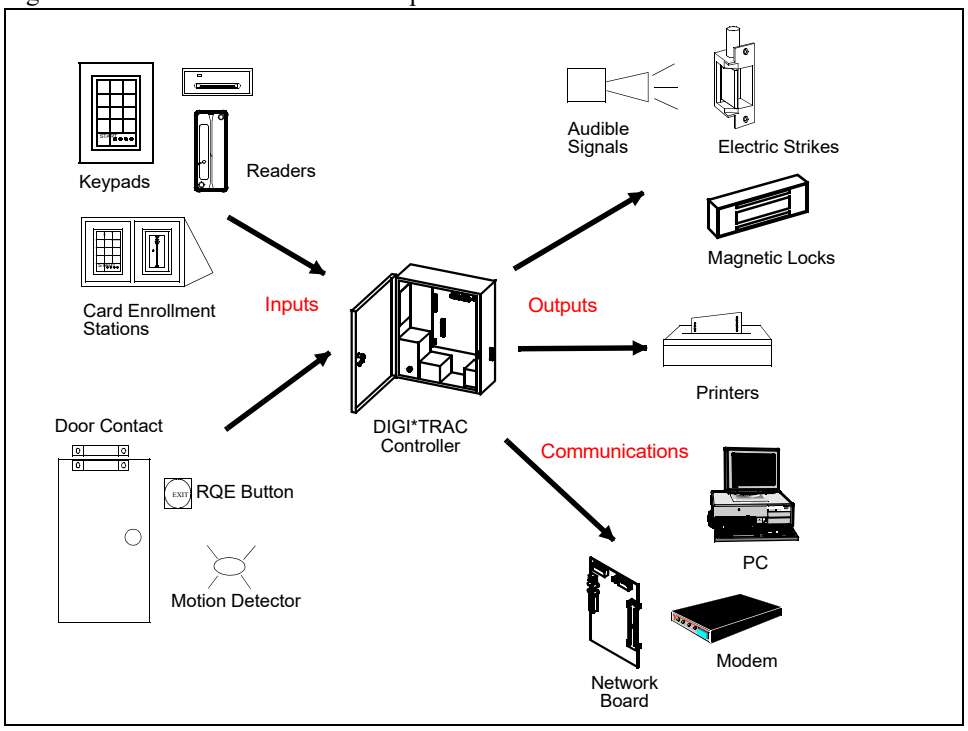


*Figure 1-1: Components of the DIGI*TRAC System*

The following sections provide some insight into how all these devices are used together.

Typical Door

A typical door diagram will help explain the major elements of a standalone DIGI*TRAC system:

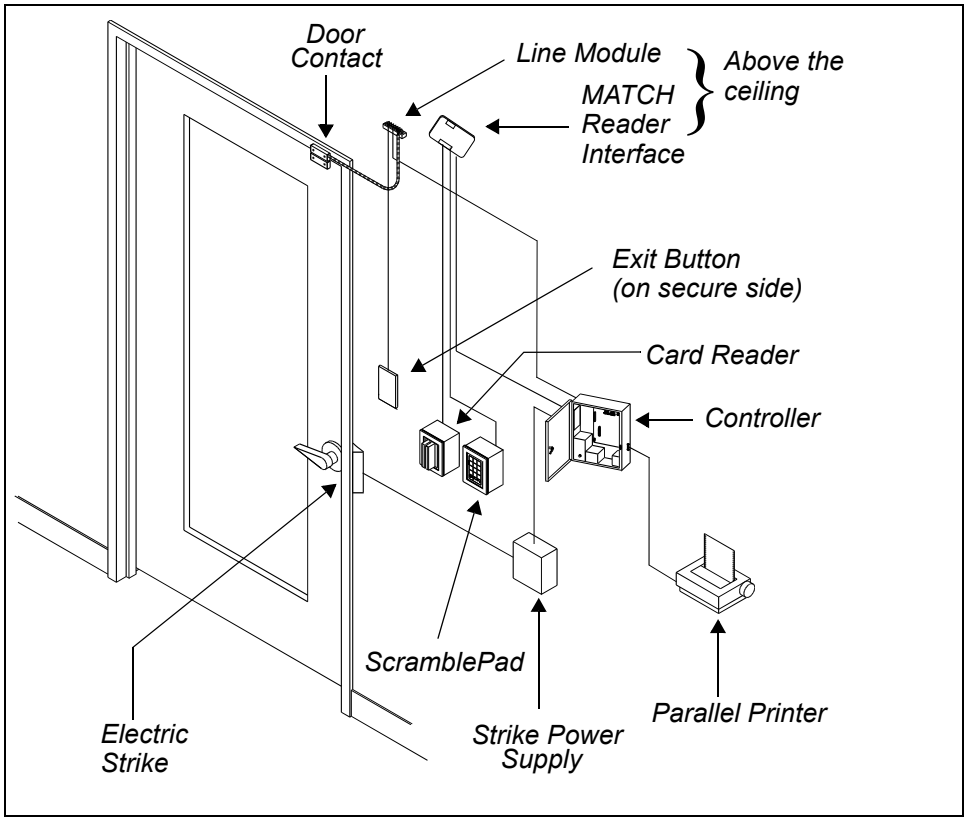


Figure 1-2: Typical Door Example

In this example, both a card reader and a ScramblePad keypad are used to secure entry. Here is the sequence this array will follow:

1. A card is passed through the card reader and the attached MATCH board sends the card code to the controller. If the card is enrolled in the system, the ScramblePad's first yellow LED flashes.

Note: Doors are identified to the controller by IDs which are configured through DIP switch settings on the MATCH Interface and ScramblePad.

2. A code is entered at the ScramblePad and this is sent to the attached MATCH which then sends the code to the controller.

   If a reader and a ScramblePad are installed on the same side of the same door (as shown in Figure 1-2), the ScramblePad must be wired through the MATCH so that the reader and ScramblePad signals are combined and sent to the controller through common wiring. If you use a DS47 ScramblePad, a MATCH is already built into the ScramblePad keypad; this means you can attach any standard 26-bit card reader to the DS47.

Note: Where only a ScramblePad is used (no dual technology), a MATCH is not required and data is sent from the ScramblePad directly to the controller.

3. The Controller determines whether the code and card are authorized for that door at that time. If they are, the controller triggers the door relay to unlock the door. Depending on the application, the door relay will allow electrical current from the power supply to energize or de-energize the locking device.
4. After a designated number of seconds, the door is relocked.

Note: The door can be programmed for 'Auto Relock' which will relock the door upon opening or closing, to minimize tailgating.

5. A Door Contact continuously monitors the door for open or closed status. The Door Contact is wired to a Line Module which provides supervision and information so the controller can produce an alarm if unauthorized door opening or tampering occurs.
6. An authorized code and card will temporarily 'mask' the alarm for a predetermined interval while the individual passes through the door.
7. From the other side, the employee can request exit from the room by pushing the Request-to-Exit (RQE) button. This sends a signal to a Line Module which sends the message to the Controller.
8. The RQE also masks the alarm from the Door Contact and can unlock the door (if required) for a specified amount of time. After that interval, the Door Contact is unmasked (normal alarm monitoring).
9. If the Door Contact detects that the door is opened beyond a prescribed number of seconds, the controller records a Door-Open-Too-Long (DOTL) alarm condition and responds to the condition as dictated by its program.

   This response can take the form of an audible alarm, a printed alarm, the activation of a videocamera to record the intruder, or any number of other responses.
10. When the Door closes, the Door Contact sends a signal through the Line Module to the Controller. If this signal arrives before the specified time duration is up, then no DOTL alarm condition is recorded.
11. All conditions and events may be recorded by a printer connected to the Controller, or sent to a PC.

Note: Mx Controllers do not include a printer port; all activity is recorded and managed by the Velocity software. For more information, refer to Chapter 8, "Mx Controller".

Typical DIGI*TRAC Controller

At the center of a Hirsch system is the DIGI*TRAC Controller, as shown in the following example:

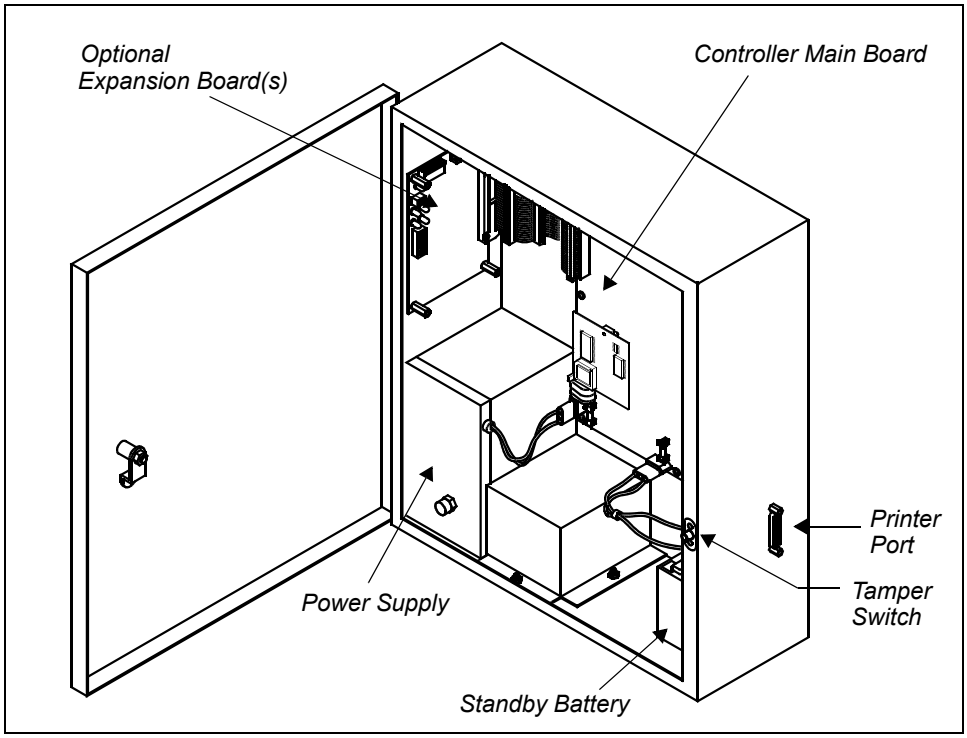


Figure 1-3: Typical Controller Components (in Secure Enclosure)

The Controller enclosure contains the following components:

- ❑ Controller main board
- ❑ Power supply
- ❑ Standby battery
- ❑ Printer port
- ❑ Tamper switch
- ❑ Optional expansion boards

Each of these components is explained briefly.

Controller Main Board

The Controller Main Board contains the main connectors to the surrounding system. Through it, you can connect to ScramblePads and MATCH reader interfaces, input devices, output devices, and power sources.

Certain items are common to all DIGI*TRAC controller boards and define the functionality of the board as shown in this sample.

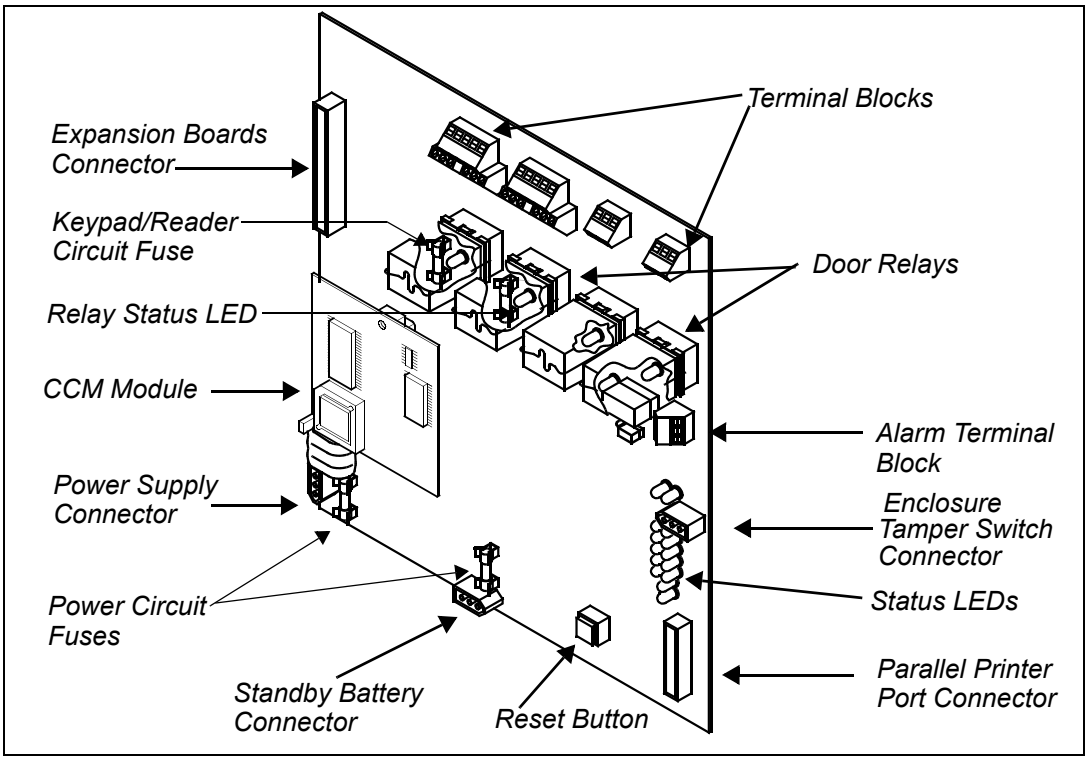


Figure 1-4: Typical Controller Main Board Connectors and Components (Model 2 Shown)

Relays come in two sizes:

- ❑ Heavy-duty (10 amp, Form C) relays for controlling door access devices, such as magnetic locks and electric strikes, and
- ❑ Smaller (2 amp, Form C) relays for executing various types of alarm events.

Terminal Blocks are the green plastic components into which wires are inserted from input/output devices. As you can see, some terminal blocks have five slots or terminals, while others have three. The terminal blocks with five terminals are used for connecting the wiring from ScramblePad keypads or readers (through the MATCH Reader Interface Board). These are *digital* circuits and support daisy-chain connections to multiple devices on the same circuit. The smaller terminal blocks are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes. While each DIGI*TRAC Controller provides a certain number of terminal blocks—and through them connections to input/output devices—the M2, M8, M16, and MSP model controllers can be increased by adding optional expansion boards.

Fuses are mounted wherever power circuits are located. All power circuits are fused.

Expansion Board Connector links any expansion boards mounted in the Controller enclosure to the Controller Main Board.

Status LEDs provide quick diagnostics on the current operation of the Controller Main Board.

Parallel Printer Port provides a link to any printer with a parallel interface. A parallel printer port is located on the right side of the Controller enclosure. If you require a serial interface, Hirsch provides an expansion board, the Serial Communication Interface Board (SCIB), for this purpose.

Reset Button performs three types of reset depending on how long you hold down the button, as shown in Table 7-3, "Reset Switch Functions", on page 7-26.

Command and Control Module (CCM) contains all of the logical instructions the Controller Board uses to process its information including the DIGI*TRAC Control Language. So flexible is the CCM firmware that it enables you to configure the Controller and the system it supports in almost any manner you require. And because of the CCM's modular design, you can upgrade the firmware just by downloading it from Velocity (or by replacing the CCM). For more about the extraordinary capabilities of the system, refer to Chapters 3 and 4 which deal with the DIGI*TRAC Control Language and programming.

Note: Because each Controller in the Hirsch family (except for the Mx) contains the same CCM, each one can provide the same level of firmware functionality.

Power Supply Connector provides cable connection to the Internal Power Supply.

Standby Battery Connector provides cable connection to the backup battery.

Enclosure Tamper Switch Connector provides a cable connection to the Tamper Switch on the Controller enclosure. Whenever the enclosure door is opened, the tamper switch alarm is activated.

Internal Power Supply

The Internal Power Supply can use either a 110 or 240 VAC supply (or 100 VAC for Japan) to provide DC power to the Controller Main Board and attached Expansion Boards. Depending on your controller, this means support for up to 16 ScramblePads or combination of ScramblePads and readers. For input and output devices requiring power – such as electric strikes and magnetic locks, motion detectors, retinal scanners, and surveillance cameras – auxiliary power supplies must be used.

Standby Battery

This component supplies 24 VDC of backup power to the Controller Board even if primary AC power fails. This battery is capable of supplying power to the Controller Board for several hours. The standby time is dependent on the connected devices and can be calculated by using the formula found in "Controller Battery Standby Capacity" starting on page 2-10.

Expansion Boards

Optional expansion boards increase the capabilities of DIGI*TRAC Controllers. For example, the MEB series increases the Controller's available memory, expanding the number of alarm and event buffers or codes the controller can hold. Communications boards provide any Controller with the ability to communicate with printers or a PC. The Relay Expansion Board extends the number of control outputs that a Controller can accommodate, and the Alarm Expansion Board increases the number of line module inputs that the controller can accept.

Table 1-1 provides an overview of available expansion boards. Note that your system's actual capacity could be less, as explained in "Velocity Features that Reduce Available Memory" on page 2-24.

Model #	Description	Comments
MEB/CE4	Memory Expansion Board - Code Expansion	Expands code memory to 5,000. *Note:If you are using CCM6, your code memory range is 1,000–4,000.*
MEB/CE16	Memory Expansion Board - Code Expansion	Expands code memory from 4,000 to 8,000. *Note:If you are using CCM6, your code memory range is 1,000–16,000.*
MEB/BE	Memory Expansion Board - Buffer Expansion	Expands internal buffered history log from 100 events and 100 alarms to 20,000 events and 2,000 alarms.
MEB/CB64	Memory Expansion Board - Code/Buffer Expansion	Expands code memory from 1,000 to 65,000 codes, expands standard buffer up to 130,000 events and 13,000 alarms, or any combination of users and events.
MEB/CB128	Memory Expansion Board - Code/Buffer Expansion	Expands code memory from 1,000 to 128,000 codes, expands the alarm and event buffers up to 260,000 events and 26,000 alarms, or provides a combination of both users and buffers.
AEB8	Alarm Expansion Board	High Security Line Module Inputs. Up to 4 AEB8 cards can be installed per controller.
REB8	Relay Expansion Board	2 Amp Form C Relays. Up to 5 REB8s can be installed per controller. (Not available for the M64.)
RREB	RS-485 Readers Expansion Board	Adds eight independent RS-485 communication ports, for fast processing of PIV or PIV-I credentials at FICAM-compliant smart card readers (which are part of a physical access control system) using the bi-directional Open Supervised Device Protocol (OSDP). Each port is capable of supporting a door with both an entry reader and an exit reader.
SNIB, SNIB2, or SNIB3	Secure Network Interface Board	Networks DIGI*TRAC (or Mx) controllers to the Host PC. Optically isolated RS-232 port on SNIB or SNIB2; optically isolated RS-485 port on SNIB, SNIB2, or SNIB3; RJ-45 Ethernet port on SNIB2 or SNIB3. *Note:The SNIB3 is backwards compatible with the SNIB2, but not with the original SNIB.*
SCIB	Serial Communications Interface Board	Optically isolated RS-232 and RS-485 ports for serial printer.

Table 1-1: Expansion Boards

*Note: The addition of alarm or relay expansion boards does not increase the door capacity of a DIGI*TRAC Controller.*

DIGI*TRAC Controller Models

There are several DIGI*TRAC or Mx Controller models. Some of the more important similarities and differences between these controllers are highlighted here:

- ❑ The M1N can control one door with two ScramblePads. It can also support four line modules and four outputs. It includes a SNIB network board as an integrated part of its controller board.
- ❑ The M2 can control four doors; however, only two doors support line modules and the associated supervised door contacts and RQE feature. The other two doors are suitable for parking gates, elevators, and similar 'unsupervised' applications.
- ❑ The M8 controls up to 8 doors, all of which support line modules, associated supervised door contacts, and the RQE feature.
- ❑ The M16 monitors up to 16 line module inputs.
- ❑ The MSP-8R is a modular relay control system which solves many control applications, such as HVAC (heating, ventilation, air conditioning), lighting, CCTV and interlock control as well as elevator control. The MSP-8R combines an SP controller board with an REB8 expansion board.
- ❑ The M64 (previously called the MSP-64R) provides 64 programmable relays for applications such as tenant after-hours HVAC and lighting control, as well as CCTV and interlock control. It is also used for elevator control. The M64 combines an SP board (mounted on the door) with an M64 board.
- ❑ The Mx controller can be configured to control either 2, 4, or 8 doors, depending on which model of the Command and Control Module (CCM) is installed. It includes SNIB2 capability and provides an RJ-45 Ethernet connector and an RS-485 terminal. In addition to the 5-wire terminal block used for connecting the wiring from card readers or ScramblePad keypads through a MATCH2 Reader Interface Board, each door provides an alternative 6-pin Wiegand terminal which enables you to directly connect an industry-standard Wiegand card reader (without a separate MATCH2 board). For more information, see Chapter 8, "Mx Controller".
- ❑ The Mx-1 is a single-door controller in a compact plastic case, which does not support any expansion boards. It can be powered by POE+, and the functionality of the CCM and the SNIB3 are built onto its main board. For more information, see Chapter 9, "Mx-1 Controller".

Note: Expansion boards can greatly extend the capabilities of most controllers. Currently the M2, M8, M16, MSP-8R, and Mx controllers can accommodate up to 5 expansion boards. The M64 can support 4 expansion boards. The M1N and the Mx-1 cannot support any expansion boards.

- ❑ All controllers except the Mx or the Mx-1 support ScramblePads for programming. All controllers also support ScramblePads and/or MATCH interfaces to initiate logic sequences and other control functions. However, only the Model 2, Model 8, Mx, and Mx-1 controllers support door access control applications.
- ❑ The number of readers and ScramblePads the controller can support is determined by:
  - The number of addresses available (16 maximum) for ScramblePads and MATCH interfaces
  - The total power required by ScramblePads and MATCH interfaces attached to the controller. This cannot exceed the power capacity of the controller. To calculate this capacity, see "Maximum Current Draw Per Controller" on page 2-19.

Note: An external power supply can be used to power ScramblePads and MATCH interfaces when available controller power is insufficient. That power supply must be a UL-listed low-voltage Class 2 power limited power supply, which is capable of providing standby power for the duration required by the UL standard your physical access control system must meet. For more information, see "UL Requirements" starting on page vii.

Table 1-2 provides the main features of the DIGI*TRAC controllers:

Feature	M1N	M2	M8	M16	MSP-8R	M64	Mx2, Mx4, or Mx8
Door Relays (Supervised)[1]	1	2	8	0	0	0	2, 4, or 8
Door Relays (Unsupervised)[1]	0	2	0	0	0	0	0
Base Expansion Relays[2]	0	0	0	0	8	64	0
Max. Expansion Relays[3]	0	32	32	32	32	64	32
Base Line Module Inputs[2]	1	2	8	16	0	0	2, 4, or 8
Max. General Purpose Line Module Inputs[3]	3	32	32	32	32	32	32
Max. Line Module Inputs (Door/Gen'l Purpose)[3]	4	34	40	32	32	32	40
Base Alarm Relays[2]	3	1	4	1	4	4	4
ScramblePad/Reader Terminals[4]	1	2	8	2	1	1	2, 4, or 8
Max. Expansion Boards[3]	0	5	5	5	5	4	5
Base Users	4,000	4,000	4,000	4,000	4,000	4,000	4,000
Max. Users[3]	4,000	132,000	132,000	132,000	132,000	132,000	132,000
Enclosure Height in. (cm)	12 (30.5)	15.25 (38.7)	20 (50.8)	15 (38.1)	15 (38.1)	20 (50.8)	15.25 (38.7)
Enclosure Width in. (cm)	12 (30.5)	18 (45.7)	22 (55.8)	18 (45.1)	18 (45.1)	22 (55.8)	18 (45.7)
Enclosure Depth in. (cm)	4 (9.8)	5.5 (14.0)	6 (15.2)	5.5 (14.0)	5.5 (14.0)	6 (15.2)	5.5 (14.0)
Shipping Weight lbs. (kg)	18 (8.17)	30 (13.6)	60 (27.2)	30 (13.6)	30 (13.6)	60 (27.2)	30 (13.6)

Table 1-2: Controller Comparison Table

[1] Unused 'Door' relays may be reconfigured to serve as 'Control' relays.

[2] 'Base' refers to what is included within the controller for the model number shown.

[3] 'Maximum' refers to the sum of what is available in the base model plus associated expansion boards. Since a mix of expansion boards can be installed, all maximums are not concurrently available.

[4] An Mx controller provides both a 5-pin MATCH terminal and a 6-pin Wiegand terminal for each door, but only one of them can be used.

Most controllers possess internal 115/230 VAC power supplies, relays, status LEDs, and a command/control module (CCM). The Mx controller's configuration can be easily changed in the field to support either 2, 4, or 8 doors by replacing its CCM.

Remote Components

As a general rule, all those components in a system which do not physically reside in the Controller are considered remote components. Some remote components, like ScramblePads and readers, initiate entry/exit access while others, like audible annunciators and magnetic locks, respond to access requests and logic sequences. Remote components fall into five categories:

- ScramblePads and MATCH Readers
- Input Devices
- Output Devices
- Printers
- Power Supplies

Each type is briefly discussed on the following pages.

ScramblePads and MATCH Readers

This category includes:

- Keypads/ScramblePads
- MATCH Reader Interface
- Readers

These devices are discussed briefly in this section.

ScramblePads

ScramblePads are Hirsch's answer to prying eyes. A unique, patented feature – scrambling digits – eliminates pattern recognition. ScramblePad numbers are randomly redisplayed each time the START button is pressed so a nearby observer cannot learn the code by memorizing which buttons are pressed. The numbers are illuminated displays located behind transparent pushbuttons. Slats, or viewing restrictors, are located between the lights and the pushbuttons. Vertical viewing restriction (up and down) is ±26° and the horizontal viewing restriction (side to side) is ±4°. On the high intensity display versions of the keypads (such as the DS47L-HI), horizontal viewing restriction is increased to ±20°.

Note: Viewing restriction is less on the high-intensity display models.

This means that if the ScramblePad is mounted at the recommended height, 58 inches (147 centimeters), any person between 4-feet 2-inches (127 cm) and 6-feet 2-inches (188 cm) in height can view the numbers, but only the user can see the numbers clearly. Anyone more than 4° to either left or right of the ScramblePad won't be able to see the numbers.

Note: ADA or local codes may require different mounting heights.

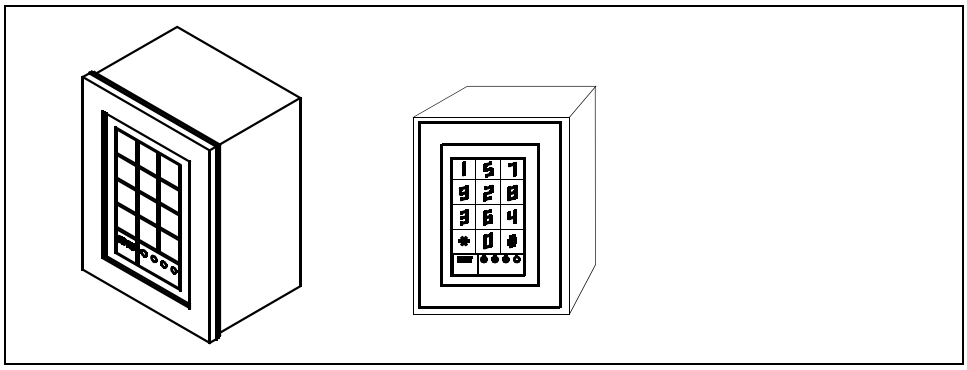


Figure 1-5: Two Views of the Hirsch ScramblePad

For detailed information on the ScramblePad, see “ScramblePads” on page 2-48.

MATCH Reader Interface

The MATCH Reader Interface is the necessary option for all Hirsch DIGI*TRAC systems when you plan to use a reader or keypad other than the ScramblePad. (For basic access control applications that only need an entry reader on a door, the Mx controller provides a 6-pin Wiegand terminal for each door that enables you to directly connect an industry-standard Wiegand card reader.) The MATCH (**M**ultiple **A**ccess **T**echnology **C**ontrol by **H**irsch) enables a large range of magnetic stripe, proximity, and other reader technologies to communicate with DIGI*TRAC controllers.

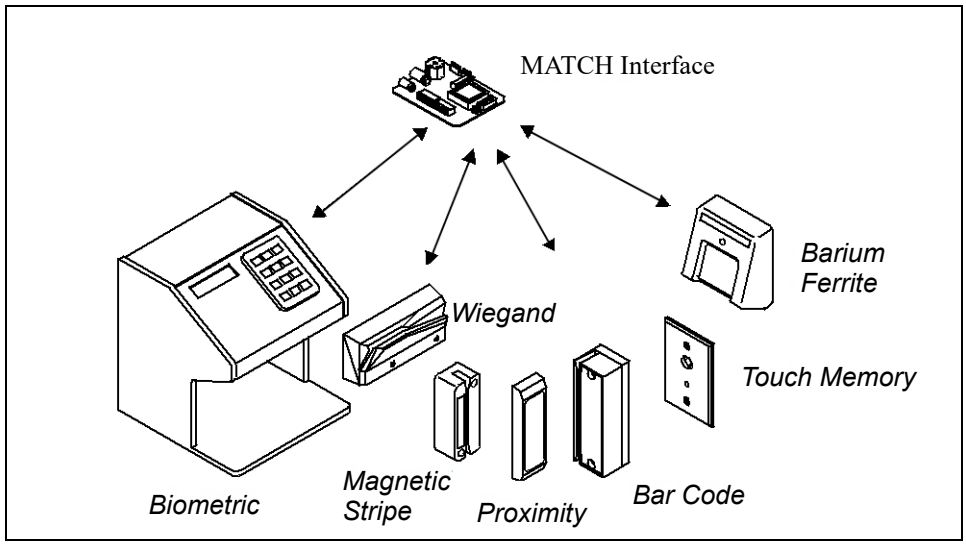


Figure 1-6: MATCH Communicates with Many Different Readers

MATCH can also be used for dual technology combining ScramblePads and readers at a door, then passing the combined signals along to a controller. The MATCH should be located at the door. Each MATCH can accommodate up to 2 readers and 2 ScramblePads for dual technology entry and dual technology exit door applications.

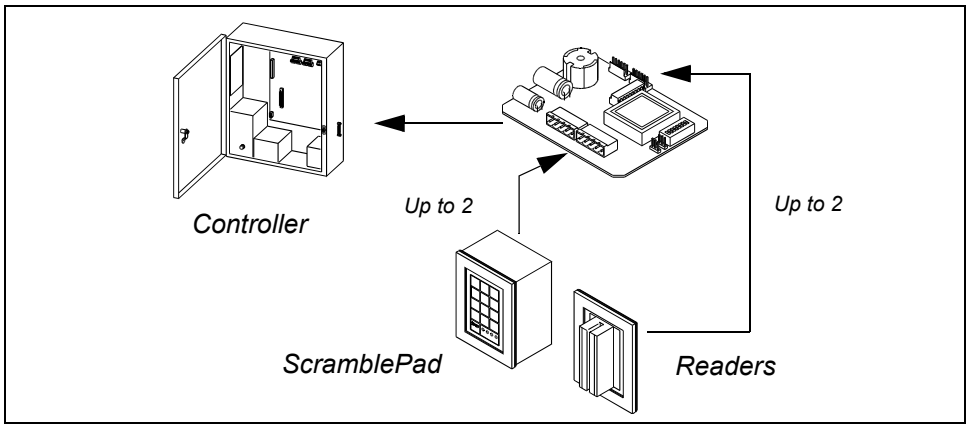


Figure 1-7: MATCH Functionality

The Hirsch DS47L ScramblePad includes both a keypad and MATCH board, thereby eliminating the need for installing a separate MATCH at the location. The DS47L's built-in MATCH only supports standard 26-bit readers; no custom settings are supported.

The Hirsch ScrambleProx (DS47L-SPX) includes a keypad, MATCH, and reader in one package. This eliminates the need for installing both a separate MATCH and reader at the required location. For more on the ScrambleProx, refer to "ScramblePads" on page 2-48.

For more information on configuring and dimensions, see "MATCH Reader Interface" on page 2-59.

MATCH-Compatible Readers

Readers and non-ScramblePad keypads connect to the Controller through the MATCH Reader Interface. For more on these readers, see "MATCH-Compatible Readers" on page 2-63.

Input Devices

Aside from keypads and readers, all other input devices must be connected to the Controller through Line Modules.

Line Modules

Line Modules are the devices which collect signals from Request-to-Exit (RQE) devices and alarm sensors (such as door contacts) and send them to the Controller using supervised circuits. Alarm Sensors are used for a variety of security monitoring functions. In access control systems, they typically monitor doors for open or closed status, enabling the controller to generate 'forced open' or 'door open too long' alarm conditions. In intrusion detection applications, they normally monitor sensors which can have either normally open (NO) or normally closed (NC) contacts.

Line Module inputs include:

- ❑ RQE Devices
- ❑ Door Contacts
- ❑ Device Tamper Switches
- ❑ Interior Motion Sensors
- ❑ Perimeter and Fence Alarms
- ❑ Break Glass Window Sensors

- ❑ Capacitance Duct Sensors
- ❑ Above-Ceiling Motion Sensors

While sensors can help the controller identify intruders, there must also be a mechanism which enables the controller to detect when the sensor itself is being tampered with or has been compromised. This can be done by monitoring the circuits which connect the alarm sensors, indicating when an alarm circuit is shorted, opened, noisy and/or out of spec. These conditions are considered attempts to breach the system and are monitored and reported on an input-by-input basis.

Through line modules, the Controller digitally processes the analog measurement of an alarm circuit's resistance at 100 times per second. With the appropriate line module, the system measures any 2% variation in the alarm circuit's condition and reports the appropriate alarm condition upon detection.

Line modules come in two types: DTLM and MELM. The DIGI*TRAC Line Module (DTLM) is a device with a screw terminal designed for easy inclusion in a junction box. The Miniature Embedded Line Module (MELM) is a device with flying leads which is much smaller than the DTLM and can fit in tighter, more confined spaces. The MELM may be installed within the sensor's housing or its mounting box.

For exact dimensions and cabling information, see "Line Modules" on page 2-75.

Output Devices

Output devices include:

- ❑ Magnetic Locks/Electric Strikes
- ❑ Turnstiles
- ❑ Parking Gates
- ❑ Elevators
- ❑ Heating/Ventilation/Air Conditioning (HVAC)
- ❑ Lighting Control
- ❑ Audible Signals

Although these devices are not manufactured by Hirsch, they can all connect to Hirsch DIGI*TRAC Controllers through either Door/Control Relays or Alarm Relays.

Wires from relay terminals to output devices must comply with Form C standards and are labeled as NO (Normally Open), NC (Normally Closed), and C (Common).

Door/Control Relay Connections

There are three types of relays used by the DIGI*TRAC Controller:

- ❑ Door Relays
- ❑ Control Relays
- ❑ Alarm Relays

Door Relays are the large heavy-duty relays found on the M2 and M8 controllers. These are normally used to switch power to output devices requiring a lot of electricity such as electric locks, electric strikes, and electric turnstiles.

Control Relays are smaller, lighter-duty relays and are normally used for auxiliary control applications or operation of remote heavy-duty relays. These are used to switch equipment on or off – either directly, or indirectly using intermediate relays – such as power or light-

ing circuits. In some cases, such as elevator control, control relays enable/disable floor buttons by providing discrete signals to the elevator control panel. For more about Door and Control Relays, see “Door Contacts” on page 2-80.

Alarm Relays are dedicated response relays which indicate:

- ❑ System alarm conditions
- ❑ Duress alarms present
- ❑ Tamper conditions present
- ❑ Trouble conditions present

Locks

Electric strikes normally operate on the principle: locked without power, unlocked with power. Conversely, magnetic locks are locked with power on and unlocked when power is momentarily turned off.

Consider what this means when using a magnetic lock as the only lock on an exterior entrance. If power fails and the standby battery wears down, a magnetic lock will unlock the door, leaving the building unsecured. Local building codes dictate requirements for using locking devices on fire exit doors, such as the main entrance. Refer to your local building codes.

There are two primary strategies for locking devices:

- ❑ **Fail Safe Lock** – If power fails, it fails open, or unlocked. These locks provide the safety feature of granting entry or exit in case of emergency conditions. However, they do not maintain security during power outages.
- ❑ **Fail Secure Lock** – If power fails, it fails locked. Fail Secure locks are a better choice for most high-security access control applications since doors remain locked during times of power outages. Doors equipped with fail secure locks may include a mechanical key override with limited distribution of the key. This enables entrance to and exit from a door even under conditions of no lock power or overall access control system failure. Most electric strikes are Fail Secure.

Note: Fail Secure Locks are usually not permitted for fire exit doors.

Alarm Relay Connections

Alarm Relays are dedicated relays that interface with local alarm annunciators or remote monitoring stations (perhaps through digital communicators). A DIGI*TRAC alarm output relay can report a variety of alarm conditions as shown in Table 1-3:

Alarm Relay	Description	Alarms Conditions Reported
1	General Alarms	Door Forced Open, Door Open Too Long, Input Alarm
2	Duress Alarms	User Under Duress At Keypad
3	Tamper Alarms	Controller Enclosure Tamper, ScramblePad Physical Tamper, Code Tamper (multiple invalid codes) at ScramblePad
4	Trouble Alarms	AC Fail, UPS Fail, parallel printer off-line, printer out of paper, line out of spec, keypad off-line

Table 1-3: Alarm Types

There is one dedicated Alarm Relay available on the M2 and M16 controllers. This one

relay is a composite of the four alarm types. The M8, MSP-8R, M64, and Mx controllers have four dedicated alarm relays – one for each alarm type, and each alarm relay is fully programmable.

Note: Any unused door or control relay can be reconfigured as an alarm relay.

For more information about Alarm Relays, see "Alarm Relays" on page 2-83.

Printers

When the DIGI*TRAC controller is used as a standalone system (without Velocity security management software), a printer provides an audit trail as well as user lists, setup data, and status information. Each time an alarm is triggered, a command is entered, or a security event occurs, it is immediately printed out and can then be read by the on-duty security personnel. Normally, the printer is connected to a DIGI*TRAC Controller using the standard parallel printer port. Optionally, a serial port is available with the Serial Communications Interface Board (SCIB). The security manager can determine what events/alarms should be printed using the DIGI*TRAC Control Language.

If the Controller is networked to a PC, the operator can choose to view events on the screen and print them out from the PC when necessary. For more information, see "Printers" on page 2-91.

Note: Mx Controllers do not include a printer port; all activity is recorded and managed by the Velocity software. For more information, refer to Chapter 8, "Mx Controller".

Power Supplies

DIGI*TRAC Controllers can power a number of ScramblePads, MATCH interfaces, and 5VDC readers (as determined by a formula found on page 2-19). Auxiliary power may be required to support the maximum number addressable.

Within a DIGI*TRAC Controller, no lock power or auxiliary power is available. Power for locks and all outputs must be supplied through additional power sources (such as Hirsch's PS2). In addition, each controller possesses backup power which can support all controller functions (memory and relay operation) for a period of time determined by the formula found on page 2-10.

For more information on using the devices described in this overview, refer to Chapter 2, "Design Considerations." For detailed instructions on setting up and installing each component, refer to Chapter 7, "Set Up and Installation."

Communication Devices

Communication Devices consist of expansion boards and external devices which provide communications to a printer or a PC using Hirsch's secure protocol, SCRAMBLE*NET. SCRAMBLE*NET is a network protocol which allows multiple DIGI*TRAC Controllers to communicate to a single PC or server.

Intermediate devices may reside on the SCRAMBLE*NET communications path which support long distances, telephone pathways, fiber optic pathways, electrical isolation strategies, large numbers of controllers, and other installation requirements.

Some of the devices supported are:

- ❑ Serial Communications Interface Board (SCIB) – For connecting a serial printer to the controller.
- ❑ Secure Network Interface Boards (SNIB, SNIB2, or SNIB3) – For connecting a controller to a local PC on RS-232 (using an original SNIB or a SNIB2), or connecting a network of controllers to a PC over longer distances on either RS-485 (using a SNIB, a SNIB2, or a SNIB3)or Ethernet (using a SNIB2 or a SNIB3).
- ❑ Telephone Modems – For operation over Leased or Dial-Up phone lines.
- ❑ Fiber Optic Transceivers – For long distance or non-electric, highly-secure operation over glass fibers.
- ❑ NET*MUX4 Multiplexor – Providing electrical isolation and power for up to 4 channels of 16 controllers each.
- ❑ SCRAMBLE*NET Gateway (X-Box) – For connecting the SCRAMBLE*NET Network to a PC.

For information about the SCIB, see “Serial Communications Interface Board (SCIB)” on page 2-32. For information about the SNIB, see “Secure Network Interface Board (SNIB, SNIB2, or SNIB3)” on page 2-33.

For more information about network devices such as the modems, transceivers, NET*MUX4, and X-Box, see “Network Components” on page 2-96.

Design Considerations

2

Introduction

This chapter discusses the considerations you may face while designing and configuring Hirsch security components. These topics are discussed:

- ❑ Requirements and limitations of each component
- ❑ System-wide considerations
- ❑ Power concerns for each device
- ❑ Wiring concerns for each device

DIGI*TRAC systems are designed and manufactured with the highest quality standards. To ensure the DIGI*TRAC system operates at its full potential, it is recommended that you select electric locks, door contacts, alarm sensors, cable, and other accessories and components of high quality.

After you've read this chapter, see Chapter 6 for examples of how these components are used to create a complete system. Then, turn to Appendix A for worksheets which aid you in planning your own system.

DIGI*TRAC Controllers

Each DIGI*TRAC controller is specified in this section and the procedures for mounting, configuring, wiring, and powering each are detailed. As a general rule, locate the Controller in a safe and secure area. It is often installed in electrical rooms, telephone equipment rooms, closets, or the security operations office. An environmentally managed room is not required as long as the temperature ranges don't exceed the Controller's specifications.

In addition to monitoring, reporting, and controlling a variety of devices, each controller can power a specific number of ScramblePads, MATCH interfaces, and attached readers. Other devices, such as interior motion sensors and some readers, may require power from a separate power supply.

Information about the Mx controller (which an be configured to control either 2, 4, or 8 doors) is provided in Chapter 8. Information about the Mx-1 controller is provided in Chapter 9.

Model 1N Design

The M1N has one heavy-duty door relay with associated line module input for supervision and door functions. This relay is capable of powering two keypads. The M1N also has three additional inputs for door contacts and alarm sensoring and four control relays to monitor and activate various relay circuits. Relay 4 can double as an alarm relay but it is not dedicated to that task.

In addition, the M1N includes an integrated SNIB for direct connection via either RS-232 or RS-485 to a SCRAMBLE*NET network, a keypad connector, and a printer port.

The M1N is shown in Figure 2-1:

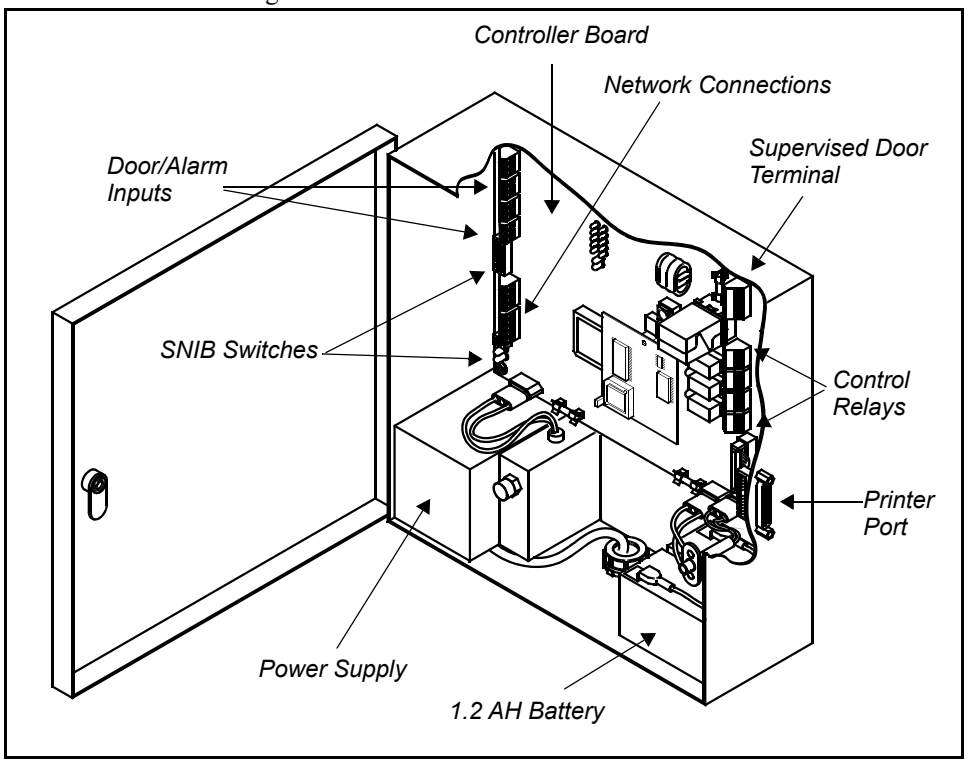


Figure 2-1: Model 1N Controller

The M1N is essentially a one door DIGI*TRAC controller. It can power one ScramblePad and/or MATCH interface from the ScramblePad/MATCH terminal block associated with the supervised doors. The M1N does not include any expansion board connectors.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller. The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

Dimension:	12"H x 12"W x 4"D (30.5cm x 30.5cm x 10cm)
Shipping Weight:	15 lbs (7 kg)

Model 2 Design

The M2 has two heavy-duty door relays, each with associated line module inputs for supervision and door functions. It also has two heavy-duty door relays for unsupervised doors, each without a line module input, auto-relock support, door status reporting, or RQE devices support.

The Model 2 is shown in Figure 2-2:

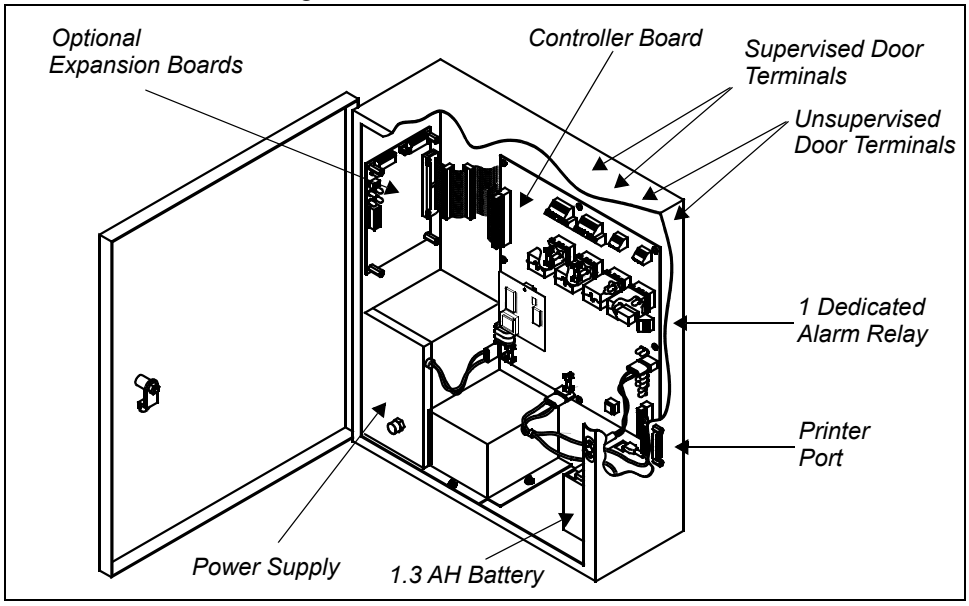


Figure 2-2: Model 2 Controller

The M2 can power ScramblePads and MATCH interfaces from the two ScramblePad/MATCH terminal blocks associated with the supervised doors. The Model 2 supports expansion boards as discussed later in this chapter.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller. The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

Dimension:	18"H x 15.25"W x 5.5"D (45.7cm x 38.7cm x 14cm)
Shipping Weight:	30 lbs (13.6 kg)

Model 8 Design

The M8 provides for eight supervised doors: this includes eight heavy-duty door relays with eight line module inputs. Each door is represented by a ScramblePad/MATCH terminal block, a relay terminal block, and a line module terminal block. The M8 can power ScramblePads and MATCH interfaces from the ScramblePad/MATCH terminal blocks.

The Model 8 is shown in Figure 2-3:

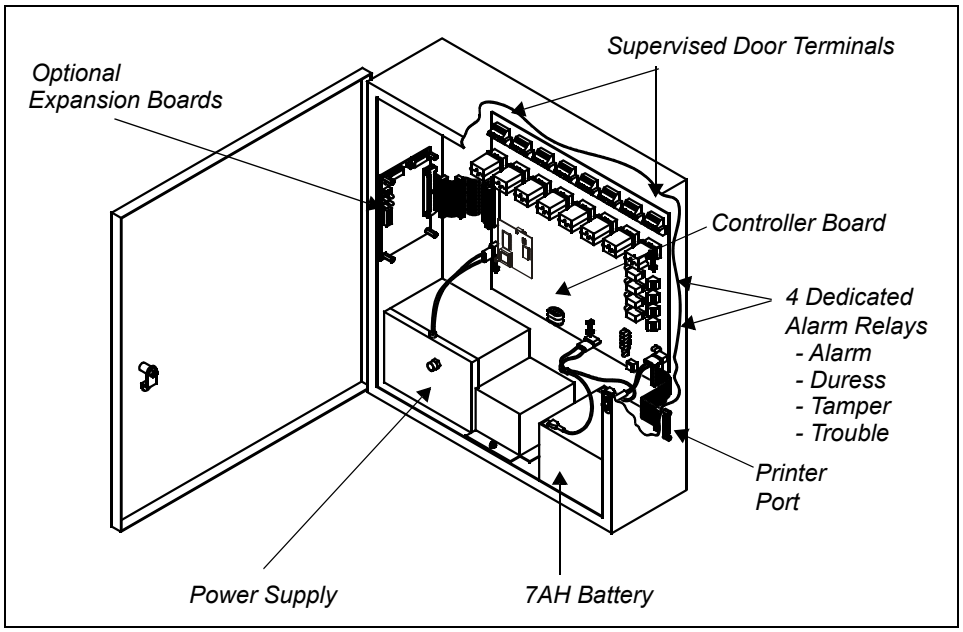


Figure 2-3: Model 8 Controller

The M8 supports expansion boards, as discussed later in this chapter.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller.

The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

Dimension:	22"H x 20"W x 6.25"D (55.9cm x 51cm x 15.9cm)
Shipping Weight:	60 lbs (27.2 kg)

Model 16 Design

The M16 provides 16 line module inputs. Though it supports relays or additional inputs through the addition of one or more REB or AEB expansion boards, its primary function is to monitor and report the status of door contacts, motion detectors, alarm sensors, or other detection devices.

The M16 can power ScramblePads and MATCH interfaces from the two ScramblePad/ MATCH terminals on the controller board.

The M16 is shown in Figure 2-4:

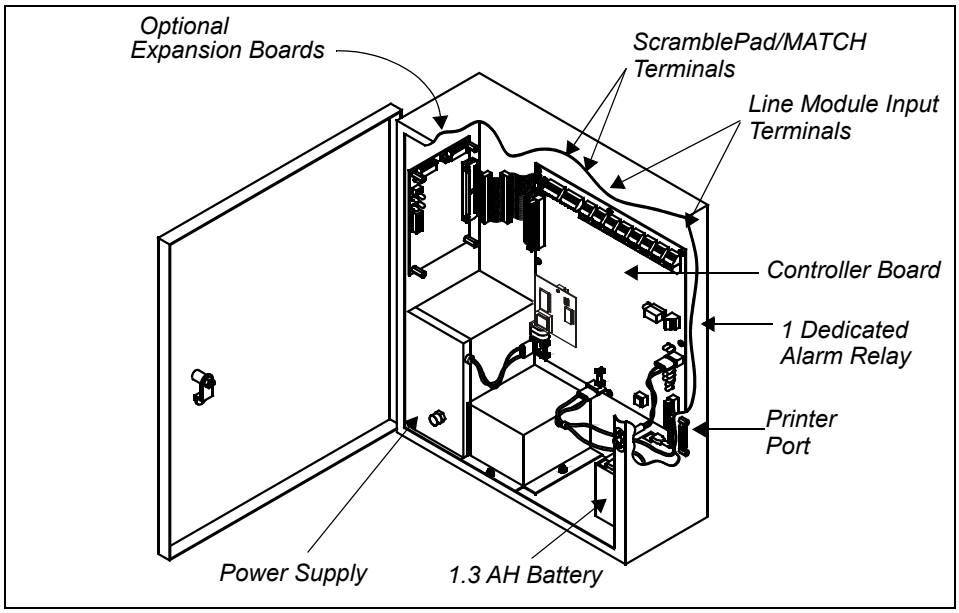


Figure 2-4: Model 16 Controller

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller.

The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

The M16 is not designed for door access control. If you require this capability, select the M2 or M8.

Dimension:	18"H x 15.25"W x 5.5"D (45.7cm x 38.7cm x 14cm)
Shipping Weight:	30 lbs (13.6 kg)

Model SP-8R Design

The MSP-8R comes with an SP controller board and an REB8 expansion board. Additional REB8s may be mounted in the expansion board area. The MSP-8R can power ScramblePads and MATCH interfaces from the two ScramblePad/MATCH terminals on the SP board.

The MSP-8R enclosure is shown in Figure 2-5:

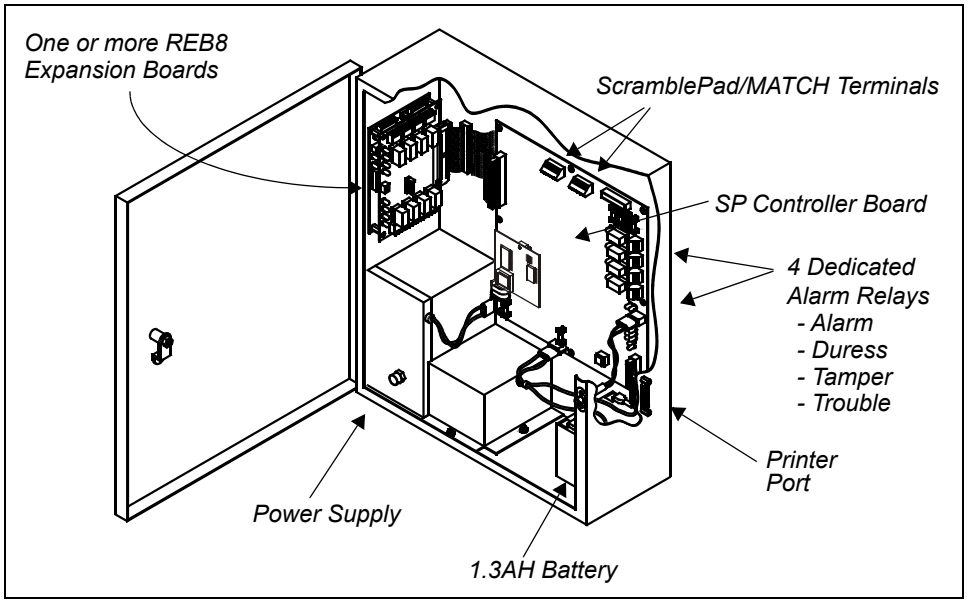


Figure 2-5: Model SP-8R Controller

The MSP-8R Controller is often used for elevator control, HVAC and lighting control, and interlocking function applications.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller.

The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

The MSP-8R is not designed for door access control. If you require this capability, select the M2 or M8.

Dimension:	18"H x 15.25"W x 5.5"D (45.7cm x 38.7cm x 14cm)
Shipping Weight:	30 lbs (13.6 kg)

Model 64 Design

The M64 Controller comes with a door-mounted SP Controller Board and a special 64-relay expansion board (M64) mounted in the enclosure. The M64 can power ScramblePads and MATCH interfaces from the two ScramblePad/MATCH terminals located on the SP Board or from the four ScramblePad/MATCH terminals located on the M64 Relay Board. The M64 is shown in Figure 2-6:

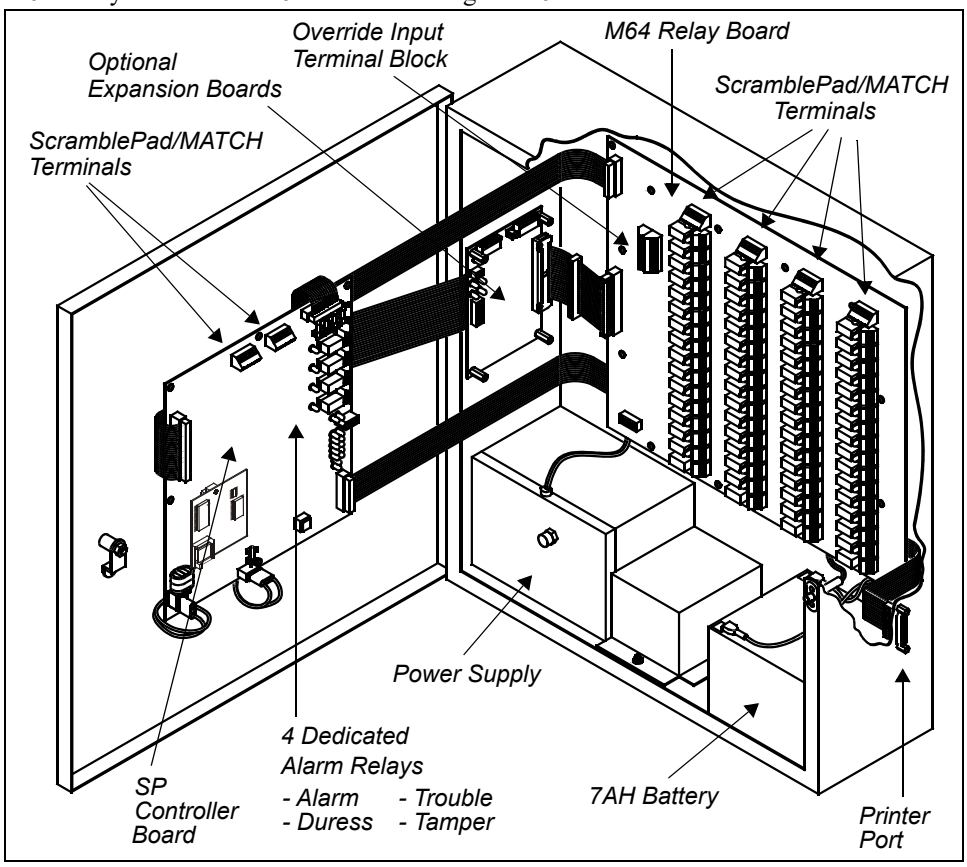


Figure 2-6: Model 64 Controller

The M64 Controller is often used for HVAC and lighting control as well as elevator access control. This requires the controller to be located near the elevator control equipment, either in the penthouse or in the basement. Interface between the M64 control relays and the elevator control inputs is usually done by the elevator service company.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller. The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage and void manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

The M64 is not designed for door access control. If you require that capability, select an M2, M8, or Mx controller.

Dimension:	22"H x 20"W x 6.25"D (55.9cm x 51cm x 15.9cm)
Shipping Weight:	60 lbs (27.2 kg)

Controller Battery Standby Capacity

The M8 and M64 come factory-equipped with a 24V 7.0 Ah battery. The Mx-2 comes factory-equipped with a 24V 1.3Ah battery, while the Mx-4 and Mx-8 come factory-equipped with a 24V 7.2 Ah battery. The M1N comes factory-equipped with a 24V 1.2Ah battery. The M2, M16, and MSP-8R come factory-equipped with a 24V 1.3Ah battery; however, the M2 controller can also be reconfigured with a 7.0 Ah battery, to comply with the standby power requirements of UL 1076 Section 40 that requires that each M2 or M8 Controller include an approved 24V DC 7Ah standby battery. The M16 and MSP-8R can be reconfigured with a 7.0 Ah battery. Each DIGI*TRAC battery kit consists of two 12-volt batteries connected in series for a full 24-volt standby unit.

If still more backup power is required, the DIGI*TRAC internal standby battery can be replaced by larger-capacity external 24VDC batteries (up to a limit of 14 amp-hours), or by a charger and batteries (such as those made by AlarmSafe). A 120/240VAC UPS can also be tied into the main power, providing the controller with both surge protection and emergency power.

When using either external batteries or a charger and batteries, remember:

- ❑ When using an external battery pack, remove the controller's internal battery and connect the new power line into the unused standby battery input on the controller board. Remember: connecting two similar batteries in series doubles the voltage.
- ❑ When using a UPS, connect the UPS into the AC power line.

To determine how much backup battery power a particular controller requires, use this formula:

$$(I_{Devices} + I_{Controller}) \text{ x hours} = \text{Battery Life Required}$$

This is the sum of the load at 24VDC of all the attached devices plus the load at 24VDC of the controller itself multiplied by the hours of battery operation required. Table 2-1 provides the extended standby battery requirements (current draw in amps) for typical DIGI*TRAC components, based on quiescent (idle) conditions:

Controller/ Attached Devices	**Requirements @ 24VDC (Amps)**
M1N	0.50
M2	0.60
M8	0.80
M16	0.50
MSP-8R/M64	1.20
DS37L (non-illuminated value)	0.07
DS37L-HI (non-illuminated value)	0.10
DS47L (non-illuminated value)	0.04
DS47L-HI (non-illuminated value)	0.04
DS47L-SPX/DS47L-SPX-HI (non-illuminated value)	0.05
MATCH (readers powered separately)	0.07
MATCH (powering 1 or 2 readers)	0.20

*Table 2-1: Quiescent Current Draw for Various DIGI*TRAC Components*

For example, suppose an M2 is connected via MATCH Interfaces to two doors, each of which is using dual technology: 4 ScramblePads – 2 regular for interior and 2 high intensity for exterior – together with 4 CR11L mag stripe readers.

The installed example system is itemized:

1 M2	x	0.60 =	0.60A
2 DS47L	x	0.04 =	0.08
2 DS47L-HI	x	0.04 =	0.08
2 MRIB	x	0.20 =	0.40
Total		**=**	**1.16A**

A factory-installed 1.3 AH battery could support this configuration for more than an hour. However, by using a 7.0 AH battery, the M2 could support this configuration for:

$$\frac{\text{7.0 Amp-Hours}}{\text{1.16A}} = \textbf{6.03} \text{ hours}$$

However, if you specify that the extended standby battery backup requirement must be at least 8 hours of operation without primary power:

1.16A x 8 hours = 9.28 amp-hours

Obviously a 7 AH battery is not sufficient for this system. This DIGI*TRAC system will require either an external battery with at least a 10 AH capacity or a front-end UPS in order to operate for a full 8 hours.

Typical Connections

The controller can connect to a number of input and output devices:

- ❑ Typical Line Module Inputs
- ❑ Typical Door Relay Outputs
- ❑ ScramblePad/MATCH Inputs

Typical Line Module Inputs

The Line Module is an intermediate connection between Door Contacts (or Alarm Sensors), RQE devices, and the controller's input terminal blocks.

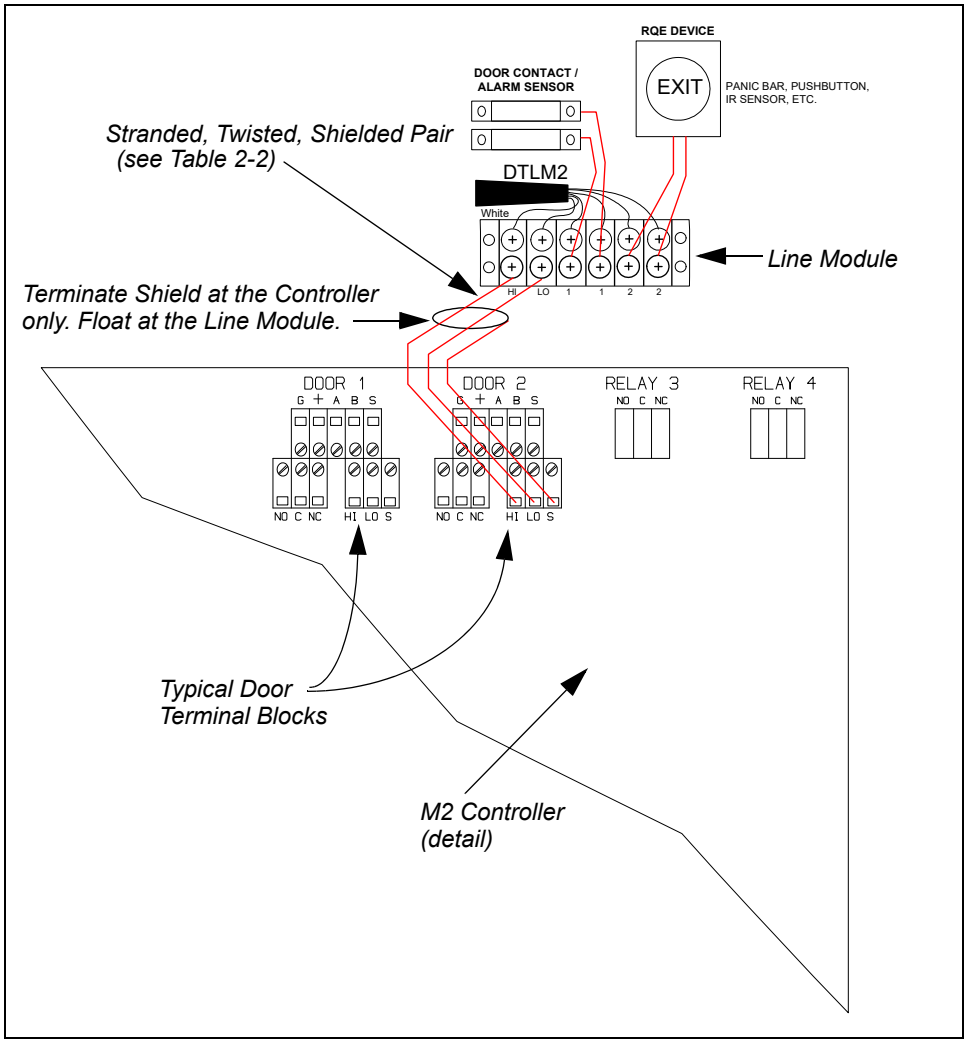


Figure 2-7: Typical Line Module Input Connection

The recommended gauge and maximum distances for a cable between the Controller and the Line Module are shown in Table 2-2:

Wire (AWG)	DTLM/MELM 1 Feet	Meters	DTLM/MELM 2 Feet	Meters	DTLM/MELM 3 Feet	Meters	Belden Ref. No.
22	5,200	(1,575)	2,500	(750)	900	(275)	8761
20	8500	(2,500)	4,500	(1,375)	1,200	(350)	8762
18	13,000	(3,975)	7,500	(2,275)	2,000	(600)	8760
16	20,000	(6,100)	11,500	(3,500)	3,100	(950)	8719
14	32,000	(9,750)	18,000	(5,500)	5,000	(1,525)	8720
12	50,000	(15,250)	28,000	(8,550)	8,000	(2,450)	8718

Table 2-2: Controller to Line Module Wiring Recommendations in Feet (Meters)

For wiring requirements between the Line Module and alarm devices, see “Line Modules” on page 2-75.

Typical Door Relay Outputs

The typical door relay output terminal block provides the connection between a door lock and the controller.

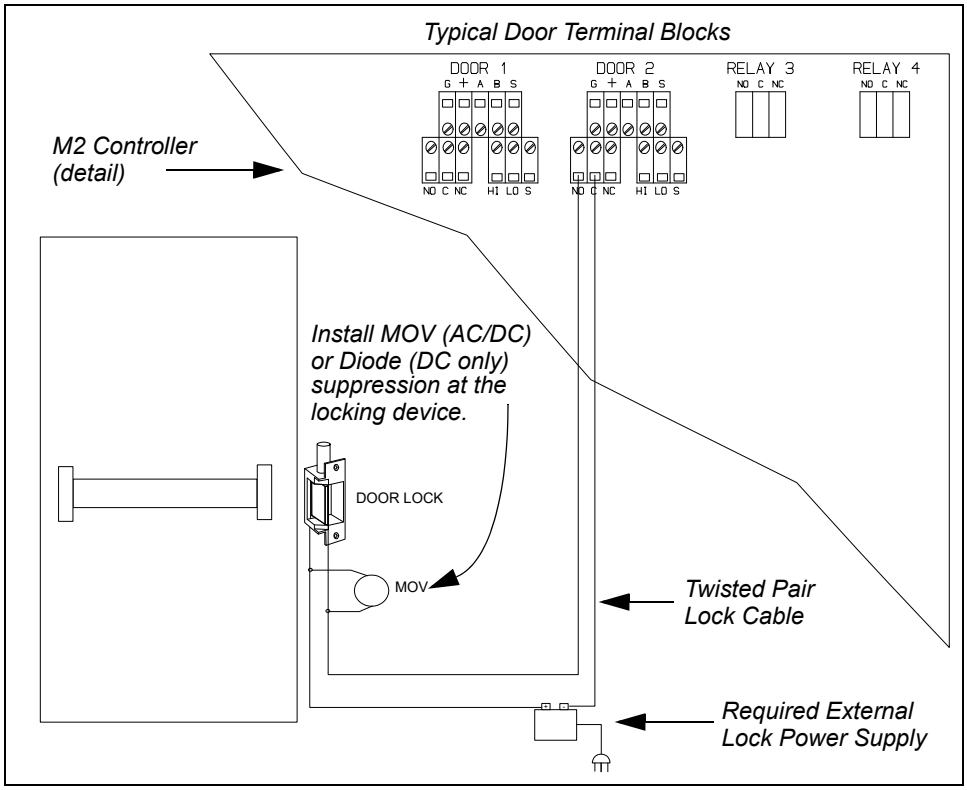


Figure 2-8: Typical Door Relay Connection

Cable runs for electric and magnetic locks must be separated by at least 6 inches (15cm) from ScramblePad and DTLM circuits, unless you use twisted-pair cable for all circuits. Zip cord is <u>not</u> acceptable.

All electronic locks induce electrical noise or interference on their control lines. These lines, when connected to the relays inside the controller, can interfere with normal controller function.

Surges, spikes, and noise produced by the lock can be suppressed by adding either an MOV or diode near the locking device. Some door locks include suppression. However, in many cases, you must install a Metal Oxide Varistor (MOV) or Diode at the lock. You can use an MOV with either AC or DC locks. An MOV is available from Hirsch as Part No. MOV35 (Thomson VE09M00250K, GE V39ZA1 or equivalent). Use a diode with DC locks only. The diode required is a 1A, 400V diode and is available from Hirsch as Part No. DIODE. Since a diode has a cathode and anode side, it is polarity-sensitive. Make sure to connect the cathode side of the diode to the positive (striped) side of the locking device.

When connecting to a door lock or some other output device requiring more than the Contact Ratings of the controller's relays, an intermediate relay is required. The Relay Contact Ratings are shown in this table:

Relay Type	Ratings
Door Relays	24V DC, 10A, resistive
Alarm/Control Relays	24V DC, 2A, resistive

Table 2-3: Relay Contact Ratings

The maximum length for lock power runs (in feet and meters) depends on this formula and the wire gauge table associated with it:

$$W \times \frac{V_L}{I_L} = \textit{maximum distance (in feet and meters)}$$

where:

W = Cable Impedance Multiplier
V_L = Lock Voltage
I_L = Lock Current

W, the *Cable Impedance Multiplier*, is calculated using Table 2-4:

Wire Gauge (AWG)	Cable Impedance Multiplier	
	Feet	Meters
22	5	1.52
20	9	2.74
18	14	4.27
16	22	6.70
14	35	10.67

Table 2-4: Cable Impedance Multiplier

The lock cable can be run in the same conduit with ScramblePad/MATCH circuits or line module input circuits, but the lock cable must always be a twisted pair.

For example, if the lock voltage is 24 VDC and the lock current is .125 Amps, and the lock is connected to the controller with 18 AWG cable, then the maximum allowed distance is:

$$14 \times \frac{24}{.125} = 2688 \text{ feet}$$

ScramblePad/MATCH Inputs

The typical ScramblePad or MATCH input terminal block provides the connection between the controller and a ScramblePad or MATCH Interface.

An example of such a connection is shown in Figure 2-9.

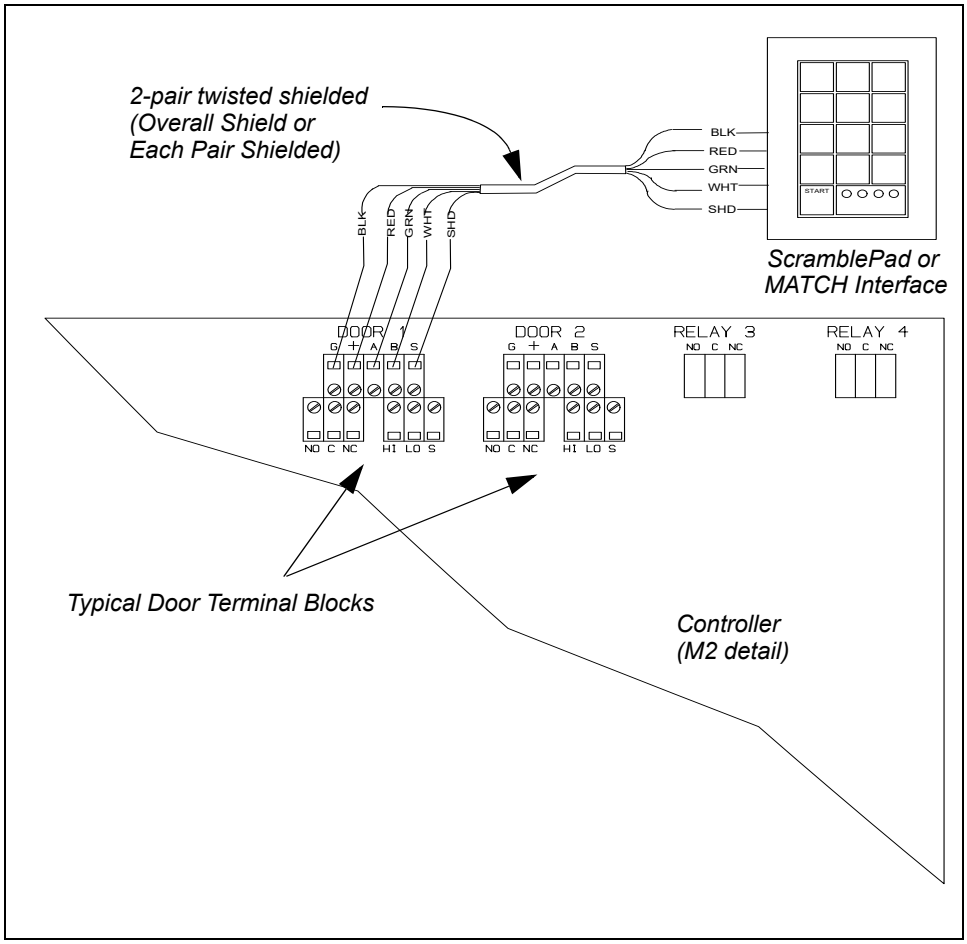


Figure 2-9: ScramblePad/MATCH Inputs

Table 2-5 shows absolute maximum cable distances allowed in feet and meters between the controller and any one or two ScramblePad combinations according to wire gauge:

Cable Gauge (AWG)	Maximum Distance in feet (meters) from Controller to:									
	1 L		1 H		2 L		L + H		2 H	
22	750	(228.6)	500	(152)	375	(114)	280	(85)	230	(70)
20	1,200	(366)*	800	(244)	600	(183)	460	(140)	375	(114)
18	1,800	(549)*	1,200	(366)*	935	(285)*	720	(219)	585	(178)
16	3,000	(914)*	1,875	(571)*	1,500	(457)*	1,150	(350)*	935	(285)*

Table 2-5: Maximum Cable Distances Between Controller and ScramblePad

In Table 2-5, the DS37L/DS47L/DS47L-SPX keypads are abbreviated as L and the DS37L-HI/DS47L-HI (or weatherized versions, DS37L-HW/DS47L-HW) are abbreviated as H. The MATCH Interface is abbreviated as M. Items followed by asterisks (*) indicate cable capacitance must not exceed a total of 100,000 pf.

NOTE: Use half of these distances when the controller is supplying power to a ScramblePad with an SPSH-1 heated back cover.

Table 2-6 shows absolute maximum cable distances in feet and meters between the controller and any MATCH and/or 1 or 2 ScramblePad combinations according to wire gauge:

Cable Gauge (AWG)	Maximum Distance (feet/meters) from Controller to:					
	M	M + L	M+H	M+2L	M+L+H	M+H+H
22	1875 (572)*	535 (183)	375 (114)	310 (94)	250 (76)	205 (62)
20	3000 (914)*	860 (262)	600 (183)	500 (152)	400 (122)	330 (100)
18	4500 (1371)*	1340 (408)*	935 (285)	780 (238)	625 (190)	515 (157)
16	7500 (2286)*	2150 (655)*	1500 (457)*	1250 (381)*	1000 (305)	825 (251)

Table 2-6: Maximum Cable Distances Between Controller and MATCH

In Table 2-6, the DS37L/DS47L/DS47L-SPX keypads are abbreviated as L and the DS37L-HI/DS47L-HI (or weatherized versions, DS37L-HW/DS47L-HW) are abbreviated as H. The MATCH Interface is abbreviated as M. Items followed by asterisks (*) indicate cable capacitance must not exceed a total of 100,000 pf.

Table 2-6 is applicable for MATCH-powered 5VDC readers, as allowed by the MATCH Interface's 28V/5V switch power supply efficiency. A reader drawing 200 mA at 5VDC translates to only about 40 mA at the MATCH Interfaces's 24VDC input side. Since the MATCH uses a switching power supply, the load presented by two 5VDC readers is no greater than that for one 5 VDC reader. Therefore, this table is valid whether one or two readers are powered by the MATCH Interface.

Overall shield or individual shielded pairs are acceptable. Color coded cable – black, red, green, white – is recommended. Pair one, the black and red wires, provides power to the ScramblePad or the MATCH Interface; pair two provides data communications between the Controller and the ScramblePad or MATCH Interface.

If two ScramblePads are installed at the same door – one for entry and the other for exit – they can share the same cable run. Connect the second ScramblePad to the removable connector of the first ScramblePad. For longer cable runs, provide a local auxiliary power supply to the ScramblePad or MATCH Interface.

Power Requirements for Various Devices

To determine how many ScramblePads and MATCH interfaces a DIGI*TRAC controller can power, you must figure both the current draw of the ScramblePads and MATCH Interfaces and compare it to the maximum current draw available from the controller.

The MATCH powers one or two readers, while the controller powers ScramblePads and the MATCH. The controller cannot power readers directly.

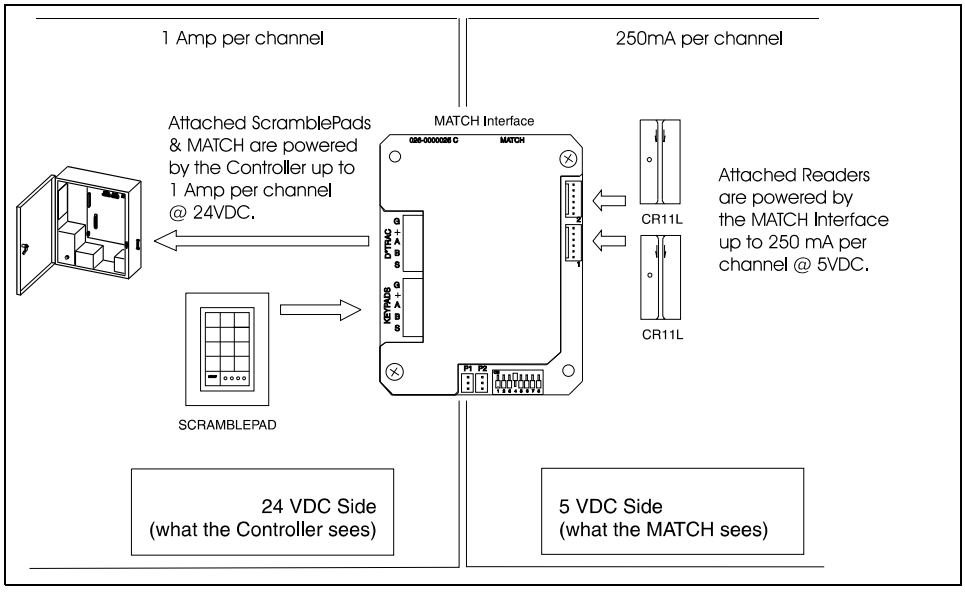


Figure 2-10: Current Draw Orientation

As shown in Figure 2-10, voltage from the Controller to the MATCH and ScramblePads is 24VDC while voltage from the MATCH to its connected readers is 5VDC. (While ScramblePads may be connected through the MATCH to the controller, the ScramblePads are powered by the controller, not the MATCH.)

In order to determine how many ScramblePads and MATCH interfaces the controller can power, use this procedure:

1. Determine what devices you will be using. For example, an M2, DS-37L ScramblePads, an MRIB MATCH Interface, and MATCH-compatible readers.
2. Determine the quantity of each device you'll need. For example, 1 M2, 1 DS37L and 1 DS37L-HI ScramblePads, 1 MRIB, and 2 CR31L readers.
3. Determine whether the MATCH Interface will be able to power the connected readers. Make sure the readers' 5VDC draw does not exceed the MATCH's 250mA at 5VDC limit. If the MATCH powers readers, it draws more current from the controller than if the readers were separately powered.
4. To determine the current draw of each attached device on the controller at 24VDC, multiply the number of devices by the current draw for each device, then add the total for each device to calculate the Total Current Draw required from the controller using the values shown in Table 2-7:

Device	Draw per Device (Amps) @ 24VDC
DS37L ScramblePad (illuminated)	0.15A
DS37L-HI / DS47L-HI ScramblePad (illuminated)	0.25A; 0.04A
DS47L ScramblePad (illuminated; non-illuminated)	0.125A; 0.04A
DS47L-SPX-H / DS47L-SPX-I ScrambleProx (illuminated; non-illuminated)	0.135A; 0.05A
DS47L-SPX-H-HI / DS47L-SPX-I-HI ScrambleProx (illuminated; non-illuminated)	0.25A; 0.05A
DS47L-SSP-HID (illuminated; non-illuminated)	0.205A; 0.12A
DS47L-SSP-HID-HI (illuminated; non-illuminated)	0.32A; 0.12A
MATCH Interface (powering 1 or 2 readers @ 5VDC; readers powered separately) date code 010327 or later	0.20A; 0.07A
NetMux4	0.15A
SNIB or SNIB2	0.125A
AEB8	0.08A
REB8 (all relays on; standby)	0.135A; 0.12A
Memory Expansion Board (MEB/BE, MEB/CE16, MEB/CE32, MEB/CE64, or MEB/CE128)	0.08A

Table 2-7: Current Draw of Various Devices

Note: Do not include the reader's 5VDC current draw in the calculation.

As shown in Table 2-7, it doesn't matter to the controller whether a MATCH is powering one or two readers, because the MATCH is using a switching power supply. The MATCH can provide up to 250 mA @ 5VDC to each of two readers and present a load to the controller of only 200 mA @ 24VDC. If readers attached to a MATCH are self-powered, the MATCH presents a load to the controller of only 70 mA.

For this example, given both entry and exit dual technology – 1 DS47L-HI ScramblePad and 1 CR31L Wiegand Swipe Reader on the entry side and a DS47L ScramblePad and CR31L on the exit side – tied into a MATCH interface, the following calculations would result:

1 DS47L x 0.125A = 0.125A
1 DS37L-HI x 0.25A = 0.250A
1 MRIB x 0.20A = 0.200A
Total Current Draw = 0.525A

5. Determine whether a controller can power the ScramblePads/MATCHs connected to it by comparing the Total Current Draw required against this table:

Controller	Max. Current Draw per Controller (Amps)	Max. Current Draw per Channel (Amps)	Controller's Own Current / Power Draw
M1N	0.125A*	0.125A	0.28A (92 BTU)
M2	1.05A	1.0A	0.60A (215 BTU)
M8	2.90A	1.0A	0.80A (425 BTU)
M16	1.15A	1.0A	0.60A (215 BTU)
Mx	2.90A	1.0A	0.53A (186 BTU)
MSP-8R	1.25A	1.0A	
M64	2.15A	1.0A	

Table 2-8: Maximum Current Draw Per Controller

* maximum *peak* current draw per M1N controller is 0.50 A.

6. Verify that the current from any one DIGI*TRAC ScramblePad/MATCH terminal block does not exceed 1.0 Amp.

   The preceding total of 0.60A is well within the M2's 1A per channel limit and 1.05A total capacity limit.

When the total current draw required exceeds a controller's limits, you can either purchase another controller or use a remote power supply for one or more of the attached devices.

The PS2 power supply's current draw depends on its load. For example:

- 0.11 A when driving normally OFF door strikes
- 0.17 A when driving one magnetic lock (or crash bar)
- 0.22 A when driving a pair of magnetic locks

Here is another data point: an M64N2 controller (at 110VAC) with 2 AEB8 expansion boards draws 0.32 A (0.43 A when all 64 relays are ON).

Expansion Board Options

A family of expansion boards is available for DIGI*TRAC controllers. Expansion boards are used to enhance or expand the controller's capabilities.

Model #	Description	Comments
MEB/CE4	Memory Expansion Board - Code Expansion	Expands code memory to 5,000. *Note:If you are using CCM6, your code memory range is 1,000–4,000.*
MEB/CE16	Memory Expansion Board - Code Expansion	Expands code memory from 4,000 to 8,000. *Note:If you are using CCM6, your code memory range is 1,000–16,000.*
MEB/BE	Memory Expansion Board - Buffer Expansion	Expands internal buffered history log from 100 events and 100 alarms to 20,000 events and 2,000 alarms.
MEB/CB64	Memory Expansion Board - Code/Buffer Expansion	Expands code memory from 1,000 to 65,000 codes, expands standard buffer up to 130,000 events and 13,000 alarms, or any combination of users and events.
MEB/CB128	Memory Expansion Board - Code/Buffer Expansion	Expands code memory from 1,000 to 130,000 codes, expands standard buffer up to 260,000 events and 26,000 alarms, or any combination of users and events
AEB8	Alarm Expansion Board	High Security Line Module Inputs. Up to 4 AEB8 cards can be installed per controller. (Not available for the M16.)
REB8	Relay Expansion Board	2 Amp Form C Relays. Up to 5 REB8s can be installed per controller. (Not available for the M64.)
RREB	RS-485 Readers Expansion Board	Adds eight independent RS-485 communication ports, for fast processing of PIV or PIV-I credentials at FICAM-compliant smart card readers (which are part of a physical access control system) using the bi-directional Open Supervised Device Protocol (OSDP). Each port is capable of supporting a door with both an entry reader and an exit reader.
SCIB	Serial Communications Interface Board	Optically isolated RS-232 and RS-485 ports for serial printer.
SNIB, SNIB2, or SNIB3	Secure Network Interface Board	Networks DIGI*TRAC (or Mx) controllers to the Host PC. • An optically isolated RS-232 port is provided on the original SNIB and the SNIB2. • An optically isolated RS-485 port is provided on the SNIB, the SNIB2, and the SNIB3. • An RJ-45 Ethernet port (which requires a host-to-master controller TCP/IP connection) is provided on the SNIB2 and the SNIB3. *Note:The SNIB3 is backwards compatible with the SNIB2, but not with the original SNIB.*

Table 2-9: Expansion Boards

NOTE: For information about the expansion boards available for the Mx controller, see “Expansion Boards” starting on page 8-8. For the Mx-1-ME controller, see “Expansion Boards for an Mx-1-ME Controller” on page 9-25.

M2, M8, M16, and MSP-8R controllers can accept up to 5 Expansion Boards. The M64 can accept up to 4 Expansion Boards. The M1N controller possesses no expansion board connectors but includes complete SNIB function on its main board. The ribbon cable used to connect these boards to the Controller board is the EBIC5, which can link up to five expansion boards.

All expansion boards have the same dimensions and shipping weight:

Dimension:	6”H x 4.25”W x 0.75”D (15.2cm x 10.8cm x 1.9cm)
Shipping Weight:	1 lb (0.5 kg)

For detailed information on setup and installation of expansion boards, see “Expansion Board Installation” on page 7-31.

Memory Expansion Boards

There are five types of memory expansion boards available for Hirsch controllers: MEB/CE4, MEB/CE16, MEB/CE32, MEB/CB64, and MEB/CB128.

The MEB/CE4 increases onboard memory to accommodate memory for up to 5,000 user records. Installing the MEB/CE16 increases onboard memory to handle up to 8,000 users. Installing the MEB/CE32 increases onboard memory to handle up to 32,000 users. Installing the MEB/CB64 increases the memory capacity to more than 64,000 users; it also acts as a buffer expansion board to increase buffer size.

The MEB/CB64 supports 64,000 user records, expands the alarm and event buffers, or provides a combination of both records and buffers. This means that a portion of memory can be allocated to storing users while the remainder is used for buffering events. Normally, it takes twice as much space to store a user profile as it does to store an event (for example, the board can store two users or four events). Hirsch's Velocity security management program supports an option to allocate 20% of the board to alarm/event buffer usage. This option is irreversible.

Hirsch's latest memory expansion board, the MEB/CB128, supports up to 128,000 users, expands the alarm and event buffers, or provides a combination of both users and buffers.

Install only one Memory Expansion Board type for code expansion in a controller at a time. Don't mix MEB/CE4s, MEB/CE16s, MEB/CE32s, MEB/CB64s, or MEB/CB128s.

Equipping a controller with an optional Buffer Expansion Board (MEB/BE) increases the buffer size from the standard 100 events and 100 alarms to 20,000 events and 2,000 alarms in battery protected internal memory. Once the buffer fills with events and alarms, it automatically deletes and replaces the oldest events and alarms with newer ones as they arrive.

Note: When a local printer is connected (with or without an MEB/BE), the alarms and events are automatically output to the printer. If the Host PC is used, a local printer should not be used because it may empty the buffer to the printer before the Host can retrieve the information.

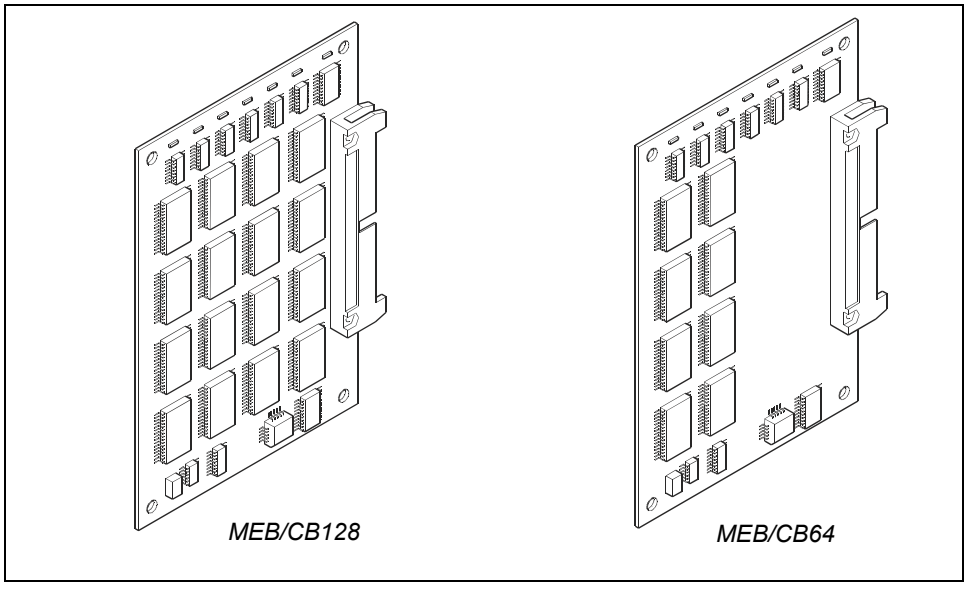


Figure 2-11: Memory Board Examples (MEB/CB128 and MEB/CB64)

The newer CCM V7.0 can diminish the number of events that an expansion board can successfully buffer, since the event string is up to four times longer. For example, a buffer that could comfortably store 4,000 events with the previous CCM (V6.6 and earlier) now buffers only 1,000 events using the V7.0 CCM.

CCM 7.0 now supports increased User and Alarm/Event capacity for up 132,000 user records. To achieve these capacities, two new Expansion Boards are now available—the MEB/CB64 and MEB/CB128. With CCM 7.0, the capacities of the Expansion Boards are additive, rather than in lieu of the base memory.

Note: Neither the MEB/CB64 nor the MEB/CB128 are supported by CCM 6.x. They must be installed in controllers equipped with CCM 7 boards.

Older boards—the MEB/CE4, MEB/CE16, MEB/CE32, and MEB/BE—still work with CCM 7.0, but at reduced capacities. If a controller has one of these boards and is upgraded to CCM 7.0, it might also be necessary to upgrade the memory expansion boards. Upgrading memory boards can provide the added benefit of increasing expansion board capacity, since the Code Expansion (CE) and Buffer Expansion (BE) can now reside on a single board—the MEB/CB64 or the MEB/CB128.

Table 2-10 describes the maximum user capacities for each memory board type as a function of both IDF and CCM version. Note that your system's actual capacity could be less, as explained in "Velocity Features that Reduce Available Memory" on page 2-24.

Maximum User Capacities	CCM 6.6 IDFs 1, 2, 3	CCM 6.6 IDFs 4, 5, 6	CCM 6.6 IDF 7	CCM 7.0 All IDFs
Base Controller	1,000	500	250	4,000
With CE4	4,000	2,000	1,000	5,000
With CE16	16,000	8,000	4,000	8,000
With CE32	32,000	16,000	8,000	20,000
With CB64	N/A	N/A	N/A	68,000
With CB128	N/A	N/A	N/A	132,000

Table 2-10: Memory Board User Capacities

The *allocated user memory* is the memory that is currently dedicated to users. The *projected maximum user capacity* is the amount of memory the CCM can auto-allocate to users as additional users are enrolled. 1024 is the base allocated user memory. If you add more than 1024 users, more memory is allocated in units of 256. So, if you add 1025 users, it increases the total memory to 1280; if you add 1281 users, it increases it to 1536, and so on.

There is a feature in Velocity that enables the operator to allocate 20% of MEB/CB expansion memory to the buffer. If the operator selects this setting, the host buffers increase the capacity and the projected maximum user capacity is slightly lower. The minimums are then 1560 buffer events and 1024 users. These values do not decrease, no matter how much extra memory is allocated.

For information on setup and installation of the memory expansion boards, see "Memory Expansion Boards Installation" on page 7-31.

Warning: Once installed, removing a memory expansion board from the controller will lose all codes.

Velocity Features that Reduce Available Memory

There are several places in this document which list the capacity of the various controllers and memory expansion boards to support user records or alarms and events. These capacities assume that you are running a version of Velocity which only uses data structures of a certain size. Your system's capacity could be reduced by up to 50% when using any of the following features (which require larger data structures):

Feature	Initially Released in
timed anti-passback	Velocity 3.1 and CCM firmware 7.4.25
multiple access zones	Velocity 3.6 and CCM firmware 7.5.28
PIV, PIV-I, or PIV-C cards	Velocity 3.6 SP2 and CCM firmware 7.5.64

Alarm Expansion Boards (AEB8)

In order to expand the line module input capacity of the controller, use the Alarm Expansion Board (AEB8). These provide an additional 8 line module inputs per board.

Expansion line module inputs are used for a variety of security monitoring functions. In intrusion detection applications, they normally monitor interior motion sensors, perimeter doors and windows for forced entry or intrusion into a protected area; however, they are generally not employed for door access control applications.

Note: Each line module input, whether connecting to a base alarm on the controller board or an expansion alarm on an AEB8, must be routed through a line module.

In the newest version of the AEB8, up to four AEB8s can be installed in the M2, M8, M16, M64, MSP-8R, or M64. The M1N cannot accommodate an AEB8 (or any other expansion board).

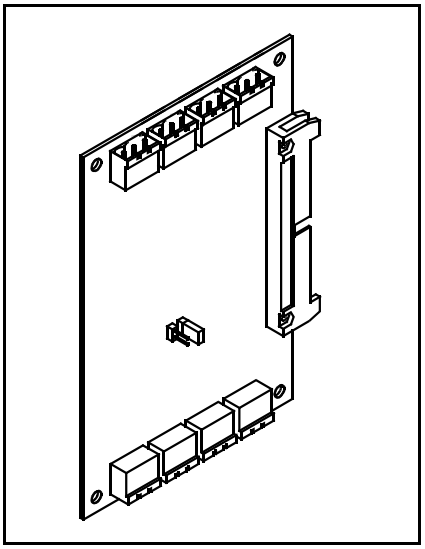


Figure 2-12: Sample AEB8 Board

One or two AEB8 boards work with older versions of the CCM (earlier than V7.0). For CCM V7.0 and later, you can use up to four of the newer AEB8 boards.

Existing AEB8's are not obsolete; however, they can only be used for addresses 1–16. The new AEB8 can be used with all existing CCMs for addresses 1 through 16.

The wiring and settings of the AEB8 are shown in Figure 2-13.

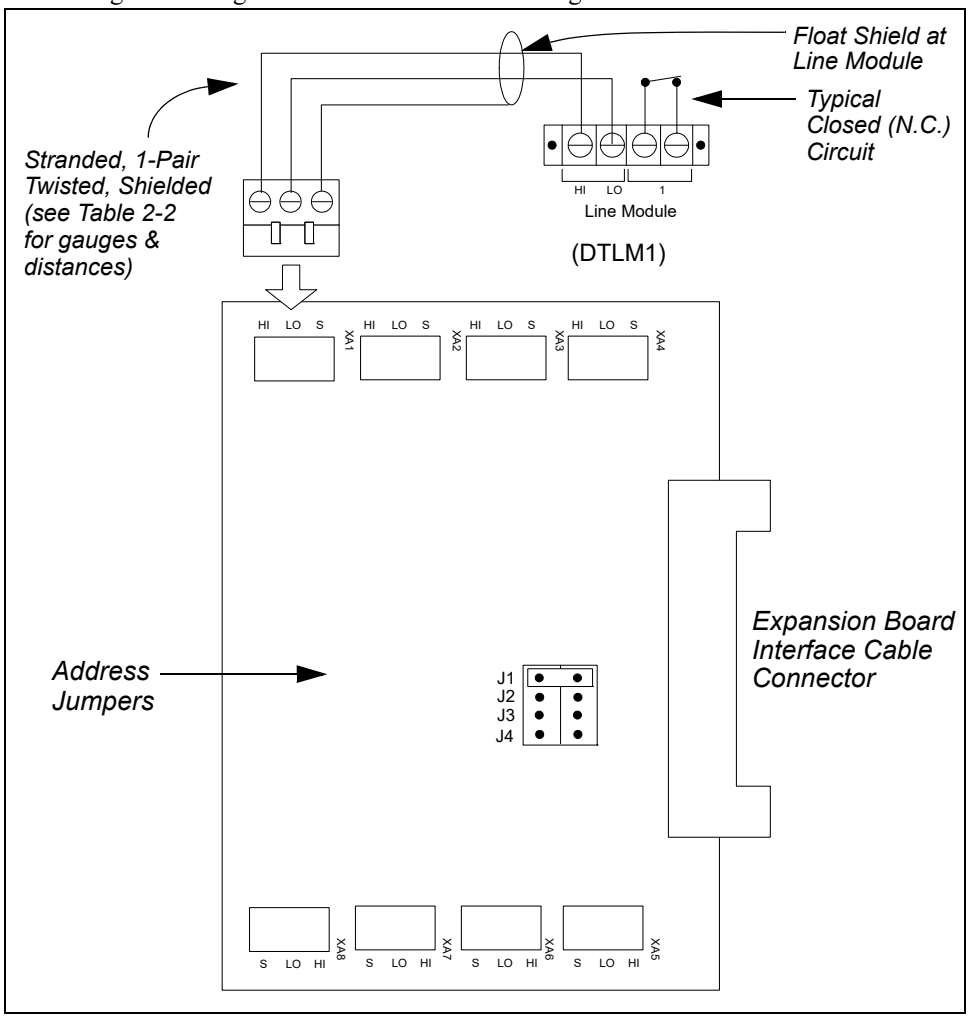


Figure 2-13: Alarm Expansion Board (AEB8)

As Figure 2-13 shows, the shield should be floated at the line module. Also, it is recommended that line module inputs be wired NC.

The AEB8 has four address jumpers where the previous AEB8 only possessed two. Each jumper allocates a range of eight addresses. This addressing scheme enables up to four AEB8's to reside in one controller. For the M16, which has 16 inputs on the base controller board, two additional AEB8's can be added to the controller for 32 inputs as well.

Note: If you are using an older AEB8 board, the jumper block is located in a different location on the board, between the XA2 and XA7 connectors.

For more about line module inputs, see “Request-To-Exit Devices (RQE)” on page 2-80. For more information about DTLM, MELM, and SBMS3, see “Line Modules” on page 2-75. For information about setup and installation of the AEB8, see “Alarm Expansion Board (AEB8) Installation” on page 7-33.

Relay Expansion Board (REB8)

In order to expand the control relay capacity of the controller, use the Relay Expansion Board (REB8). This provides eight additional 2 Amp Form C dry relay outputs, rated for 24VDC. These relays are socketed and removable.

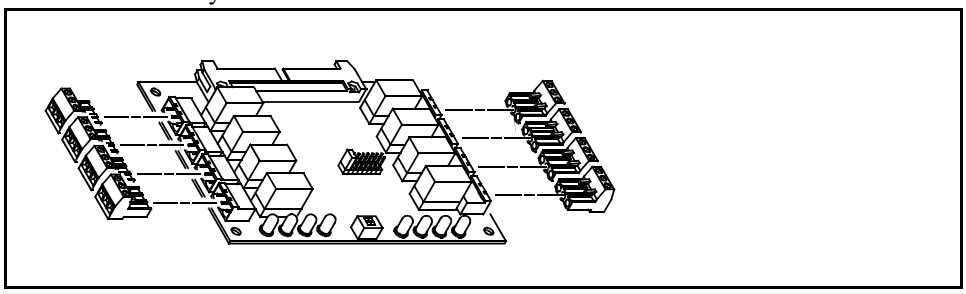


Figure 2-14: Relay Expansion Board (Physical View)

In the newest version of the REB8, up to five REB8s can be installed in an M2, M8, M16, or MSP-8R. The REB8 cannot be installed in an M64 or M1N.

The wiring and settings of the REB8 are shown in Figure 2-15.

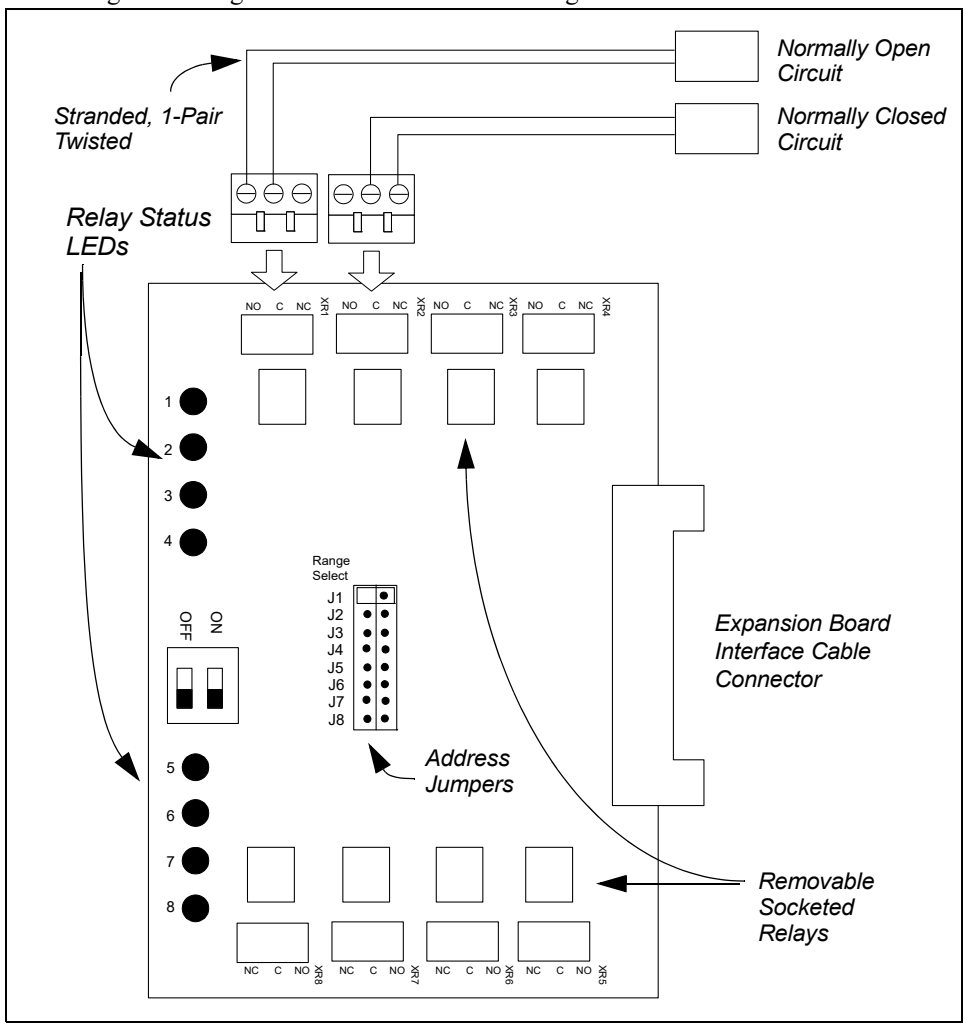


Figure 2-15: Relay Expansion Board (REB8)

Unlike the large heavy-duty door relays used to switch electric lock or strike power at 10 Amp loads, the expansion relays are normally used for signal level switching or pilot duty. Such switches, when closed, provide an input to a low-voltage sensing circuit like the one shown in Figure 2-16:

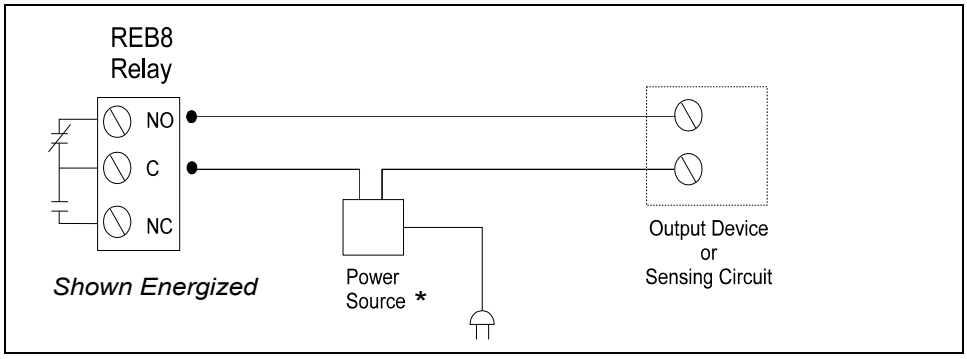


Figure 2-16: Alarm or Pilot Relay Circuit For Low-Power Switching

Note: Some sensing circuit terminals also provide a power source. In this case, a separate power source (marked by an asterisk in Figure 2-16) is not required.

However, the switch can also be used to activate the coils of a remote heavy-duty relay like this:

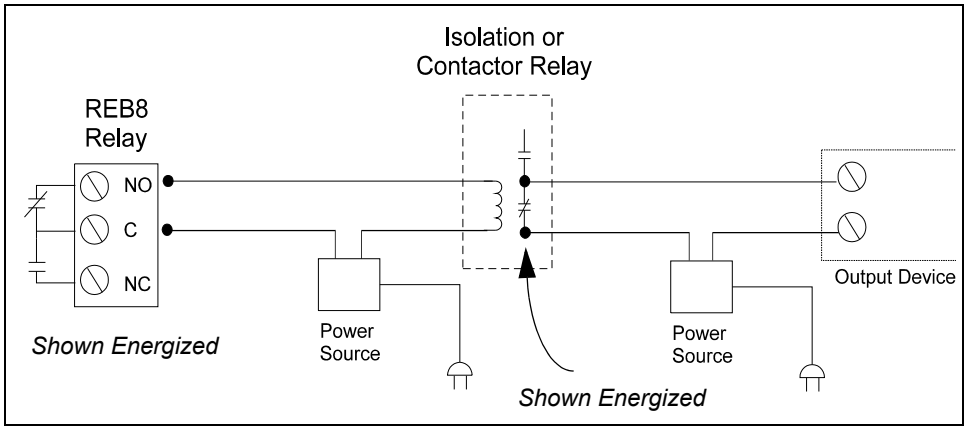


Figure 2-17: Remote Relay Circuit for Heavy-Duty Output Device]

The examples above connect across the NO and C terminals so no power is consumed when the device is in the normal state. This is the case in applications like elevator control where the control relays provide a contact closure to elevator control equipment only. There is almost no distance limitation for the cable between the REB8's terminal block and an isolation relay. If a powered device is being activated or energized, use the ScramblePad distance limitations as a good measure of distance capability (Table 2-5 on page 2-16). However, for accuracy, voltage drop calculations should be made for the specific load, cable, and distances involved, similar to lock calculations on page 2-14.

The REB8 is equipped with a Master Relay Override DIP switch. This switch can override all relays ON or all relays OFF. In the OFF position, relays cannot be activated by the controller until the Master Override OFF is returned to the normal operating position.

For information on setup and installation of the REB8, see "Relay Expansion Board (REB8) Installation" on page 7-37.

RS-485 Readers Expansion Board (RREB)

The RS-485 Readers Expansion Board (RREB) is the component of Identiv's end-to-end FICAM solution which provides eight independent RS-485 communication ports, for fast processing of PIV or PIV-I credentials at FICAM-compliant smart card readers (which are part of a physical access control system) using the bi-directional Open Supervised Device Protocol (OSDP). Each port is capable of supporting a door with both an entry reader and an exit reader. The following figure shows an RREB, and identifies its connections.

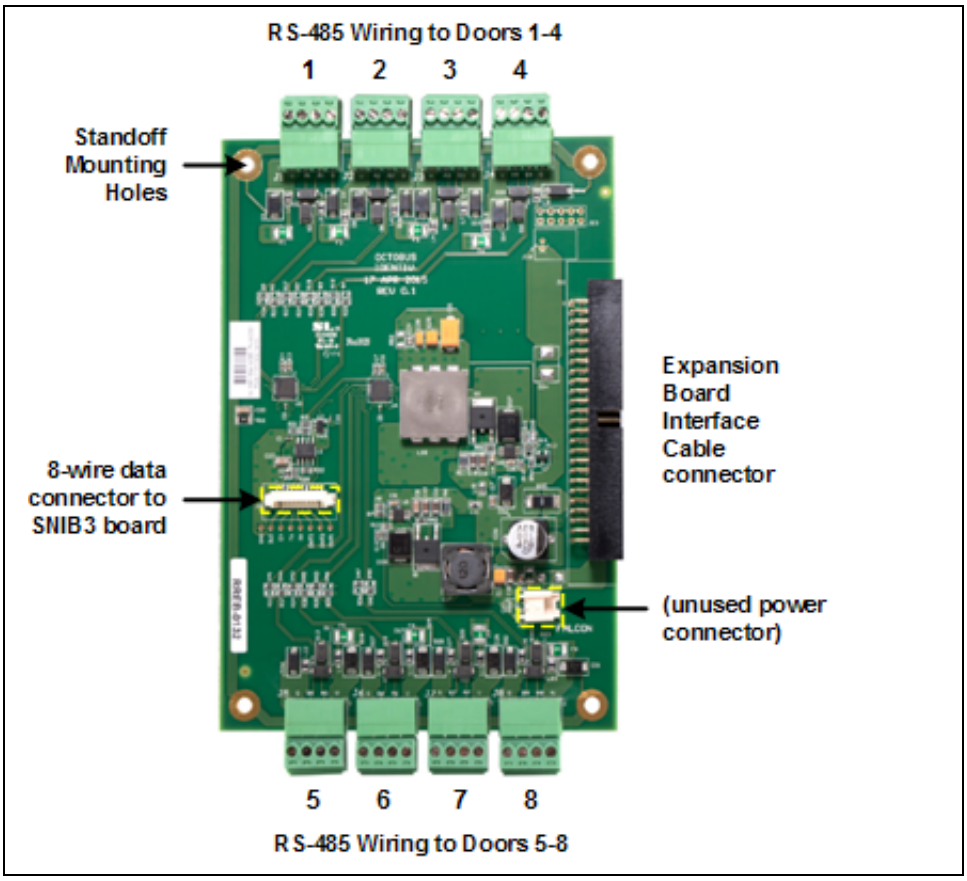


Figure 2-18: Connections on the RS-485 Readers Expansion Board (RREB)

Government agencies transitioning from a traditional PACS to FICAM will need to replace their old readers and upgrade their version of the Velocity software, but the RREB (in conjunction with the SNIB3) enables them to reuse their existing wires and door controllers (including the M2, M8, and Mx). The RREB:

- ❑ provides the necessary connections to FICAM-compliant smart card readers (which are part of a physical access control system), for two-way communication with the SNIB3 communications expansion board
- ❑ uses standard RS-485 wiring (two-pair stranded and twisted 18 AWG wires, with an overall shield) to readers
- ❑ has the same form factor as other boards, and draws power through the controller's EBIC5 ribbon cable

Example Wiring Diagram for an RREB

The following figure shows an example wiring diagram for an RREB and a pair of Identiv's uTrust TS Government Readers, which are the entry reader and the optional exit reader for a door. Note that:

- The exit reader is wired through the entry reader for a door, so it shares an RS-485 port on the RREB.
- On the exit reader, a jumper wire is needed between P1.1 and P1.4 (or between the orange and the black wires on the pigtail model) to designate that it is the exit reader.
- All of these readers have a default OSDP Address of 0, which is the correct value when they are used as the entry reader for a door. If a door also requires an exit reader, then adding a jumper wire between P1.1 and P1.4 (or between the orange and the black wires on the pigtail model) changes the default OSDP Address to 1, which is the correct value for an exit reader. Be sure that you specify the correct OSDP Address when you configure each reader in a FICAM-capable version of the Velocity software.
- The diagram shows power being supplied to the readers from the RREB. But depending on the types and quantity of readers being used, you might need to power some of the remotely located readers from an external power supply. For more information, see “Power Provided at the RS-485 Terminal Blocks” on page 2-31.

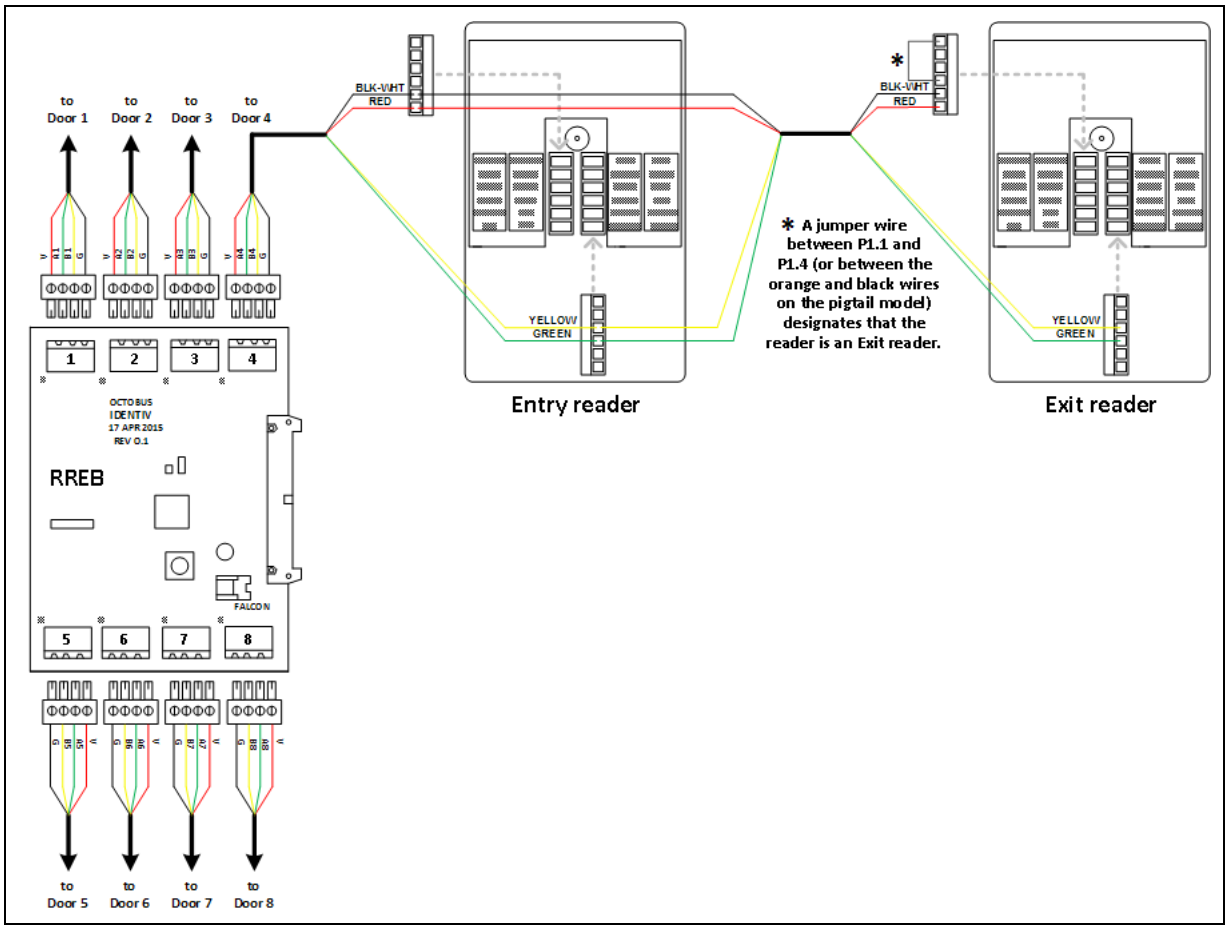


Figure 2-19: Example Wiring Diagram for an RS-485 Readers Expansion Board (RREB)

The following table lists Identiv's FICAM-capable High Frequency TS readers (which appear in the **Readers > uTrust TouchSecure > Government FICAM** category of the Product Catalog for Hirsch by Identiv Physical Access Control Solutions).

Form Factor	Model Number	Wiring	Ethernet?
Mullion: 	8002ABPFF00	Pigtail	No
	8002ABTFF00	Terminal	No
	8032ABPFF00	Pigtail	Yes
	8032ABTFF00	Terminal	Yes
Wall Mount: 	8102ABPFF00	Pigtail	No
	8102ABTFF00	Terminal	No
	8132ABPFF00	Pigtail	Yes
	8132ABTFF00	Terminal	Yes
Keypad: 	8202ABTFF00	Terminal	No
	8232ABTFF00	Terminal	Yes
TS ScramblePad: 	8332ABTFF00	Terminal	Yes

For information about installing the RREB, see "RS-485 Readers Expansion Board (RREB) Installation" on page 7-35.

Power Provided at the RS-485 Terminal Blocks

An RS-485 Readers Expansion Board (RREB) draws its power from the EBIC5 cable connecting a controller to its expansion boards. The following table shows the power provided at the RS-485 terminal blocks of an RREB.

Voltage	Max. Current Draw per RS-485 Port	Max. Current Draw per Controller
12 VDC	0.5 A	4.0 A

Table 2-11: Voltage and Maximum Current Draws for an RREB's RS-485 Terminals

Because each RS-485 port is fuse-limited to a maximum of 0.5 Amps, you will need to use an external power supply when the combined requirements for the entry reader and the exit reader of a door exceed that limit.

RREB Power Rating

- ❑ The RREB is powered by the 28V rail from the EBIC5 cable from the control panel.
- ❑ The quiescent current draw of the RREB is 10mA @ 28V.
- ❑ The RREB converts the 28V into two power rails 5V and 12V. The 5V rail can power the SNIB3 and the 12V rail powers the readers.
- ❑ Max Rating of 5V rail on RREB - 3A
- ❑ Max Rating of 12V rail on RREB - 4A
- ❑ Each of the 8 reader ports on the RREB is fused at 500mA.

NOTE:The overall power rating of the RREB is 2.2A @ 28V (when the Reader ports are loaded at its max rating of 500mA per port and SNIB3 power port is loaded to max rating of 1.35A).

Wiring Distance Limits for an RREB

The following table shows the wiring distance limits between an RS-485 Readers Expansion Board (RREB) and a FICAM-compliant smart card reader (which is part of a physical access control system). Note that the wires must be stranded and pair twisted, with an overall shield.

Type of Wired Connection	Maximum Distance
RS-485 data only using 22 gauge wires (power supplied separately)	4,000 feet (1,220 meters)

Table 2-12: Wiring Distance Limits Between an RREB and a FICAM-compliant Smart Card Reader

Serial Communications Interface Board (SCIB)

The Serial Communications Interface Board enables the Controller to connect to a serial printer which can be located a greater distance from the controller than the default parallel printer.

Note: A parallel printer port is standard and ready-to-use for instant connection to a parallel printer. Use this board only if you need to move the printer more than10 feet from the controller.

The wiring and settings of the SCIB are shown in Figure 2-20.

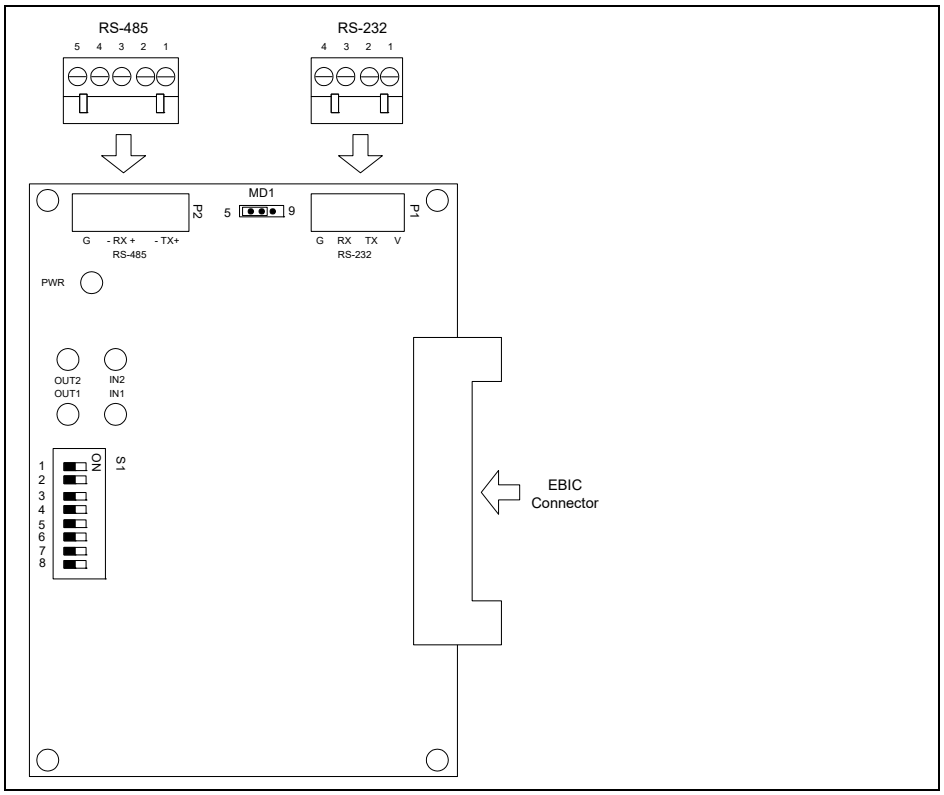


Figure 2-20: Serial Communication Interface (SCIB) Board

The SCIB provides both RS-232 and RS-485 ports. The power and data lines should be fully isolated from the controller, providing immunity from transients and common-mode ground voltages between the controller and the remote terminal or printer.

*Note: The SCIB does not use SCRAMBLE*NET Protocol.*

Maximum SCIB cabling lengths are shown in this table:

Port Type	Maximum Cable Length (feet/meters)
RS-485	4000 (1220)
RS-232	50 (15)

Table 2-13: SCIB Cabling Distances

For information on setup and installation of the SCIB, see “Serial Communications Interface Board (SCIB) Installation” on page 7-39.

Secure Network Interface Board (SNIB, SNIB2, or SNIB3)

When installed, the SNIB, SNIB2, or SNIB3 expansion board enables a DIGI*TRAC or Mx controller to be programmed, monitored, and controlled from a properly-configured IBM-compatible host PC running the Velocity software. Communication is secured by Hirsch's proprietary Hirsch Encrypted Standard (HES) protocol SCRAMBLE*NET network. The SNIB, SNIB2, and SNIB3 boards are shown in Figure 2-21:

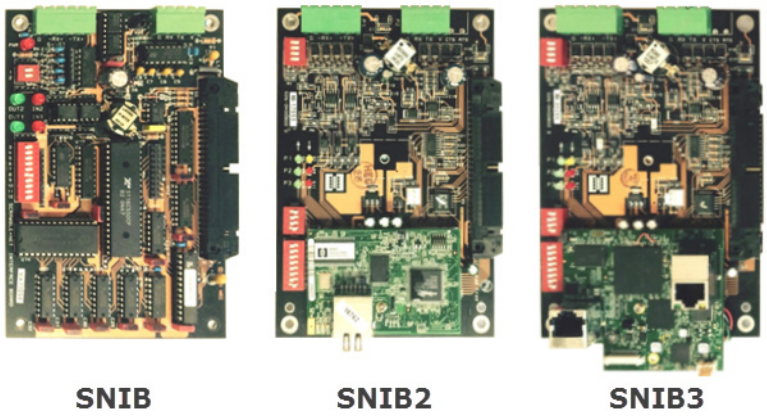


Figure 2-21: SNIB, SNIB2, and SNIB3

NOTE: The SNIB3 is compatible with the SNIB2, but not with the original SNIB.

SNIB

The SNIB provides both RS-232 and RS-485 SCRAMBLE*NET ports. If you need to connect the host to the master SNIB via RS-485, you can only use the SNIB; otherwise, you have a choice of either SNIB or SNIB2. An example of the SNIB is shown in Figure 2-22.

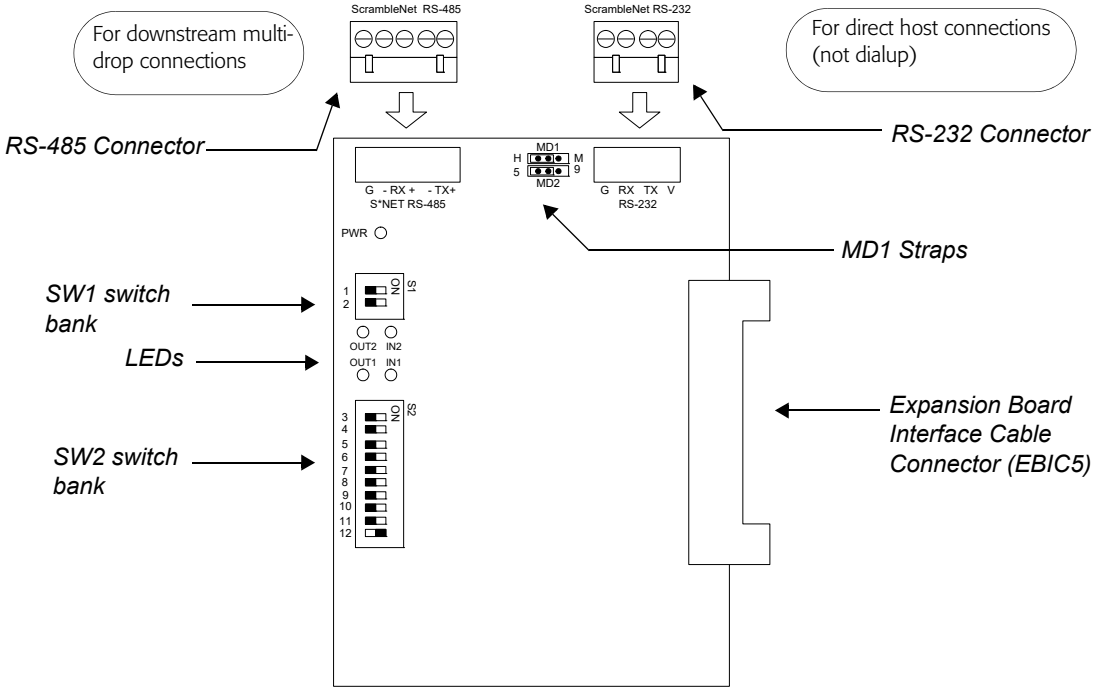


Figure 2-22: SNIB Board

An example of the possible SNIB connections is shown in Figure 2-23.

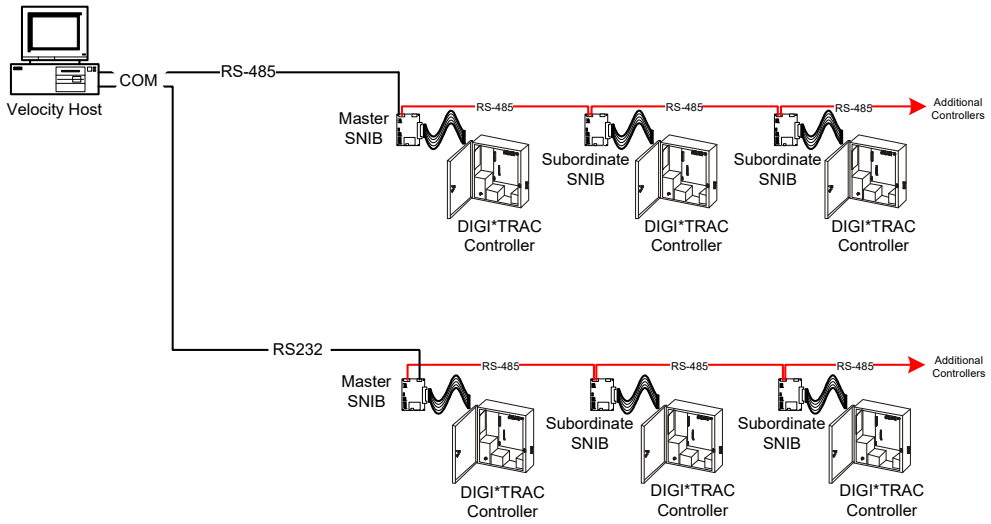


Figure 2-23: SNIB Connections

The power and data lines are fully isolated from the controller, providing immunity from transients and common-mode ground voltages between the SNIB-connected controller(s) and a host PC. Maximum SNIB cabling lengths are shown in Table 2-14:

Port Type	Maximum Cable Length in feet (meters)
Ethernet (CAT5, CAT6)	328 (100)
RS-485	4000 (1220)
RS-232	50 (15)

Table 2-14: SNIB Cabling Distances

For a single controller network, connect to the S*NET via either an RS-485 or RS-232 port. If connecting more than one controller on the network and the first controller is within 50 feet (15 meters) of the Host PC, connect the PC to the first controller via the RS-232 connector and the rest of the controllers to the RS-485 S*NET connector on the first controller.

Alternatively, simply connect to the RS-485 connector and daisy-chain the wire to the multiple controllers. The M1N does not require a SNIB to network because SNIB circuitry with both RS-232 and RS-485 connectors is embedded on the controller board.

SNIB2

The SNIB2 is a high-security encryption Secure Network Interface Board.

The main components of the SNIB2 are shown in Figure 2-24.

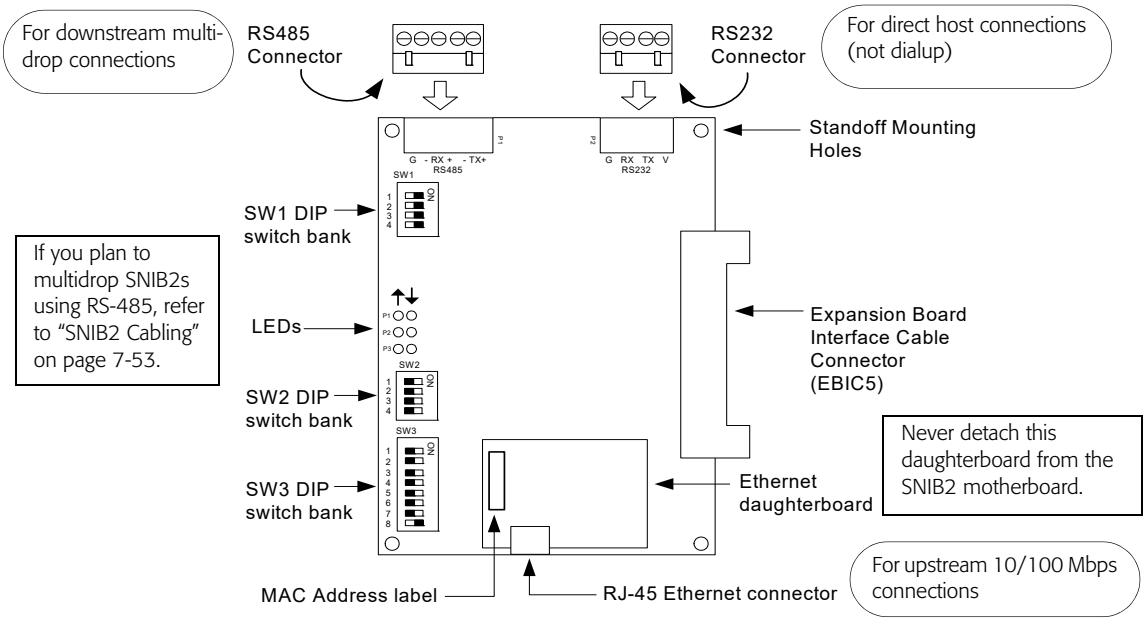


Figure 2-24: SNIB2 Board

The SNIB2 includes an RS-232 and RS-485 as well as an Ethernet port. In addition, SNIB2 supports full encryption from the host to the last downstream controller. The SNIB2 also offers XBox functionality with support for global I/O from the master SNIB2 downstream to all attached slave SNIB2s. The SNIB2 supports both an Ethernet or RS-232 connection between the host PC and the master SNIB2. Downstream connections from the master SNIB2 to slave SNIB2s must be RS-485.

The SNIB2 is a controller-resident communication board that enables a host PC running Velocity (version 2.6 SP2 or higher) to program, monitor, and control up to 63 SNIB2-resident controllers per SNIB2 Ethernet port. A NET*MUX4 is required whenever there are more than 16 controllers. Additional NET*MUX4s may be required to ensure that there are never more than 16 controllers per port.

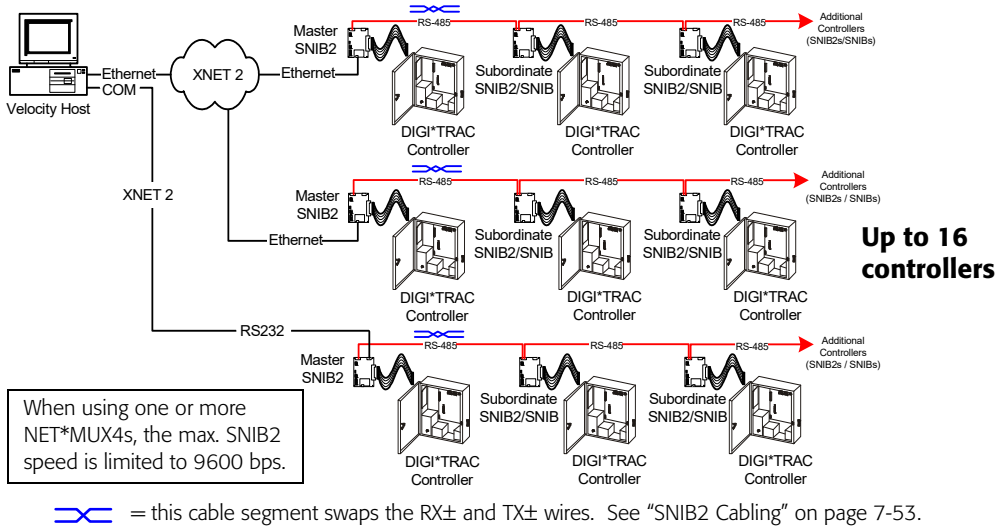


Figure 2-25: SNIB2 Connections

Each connected controller must have its own SNIB2 or SNIB board installed. The SNIB2 provides RS-485, RS-232, and 10/100BaseT Ethernet ports. The SNIB2 supports the XNET2 protocol.

Note: An Mx controller's main board provides built-in SNIB2 capability, and it includes an Ethernet connector and an RS-485 connector (but not an RS-232 connector).

Physically, the SNIB2 board differs from the original SNIB in three obvious respects. The SNIB2 has:

- three switch banks (SW1, SW2, and SW3)
- an Ethernet RJ-45 connector with its accompanying daughterboard
- three pairs of status LEDs (see "Controller and SNIB2 LED Diagnostics" on page 7-69)

With the SNIB2 board, a host PC running Velocity can program, monitor, and control up to 63 controllers with NET*MUX4 (as shown in Figure 2-26), or up to 16 without NET*MUX4. Each connected controller must have its own SNIB2 or SNIB board installed. The SNIB2 provides a downstream/multi-drop RS-485 port as well as an upstream 10/100 Mbps Ethernet port and an RS-232 port for direct host connections (not dial-up).

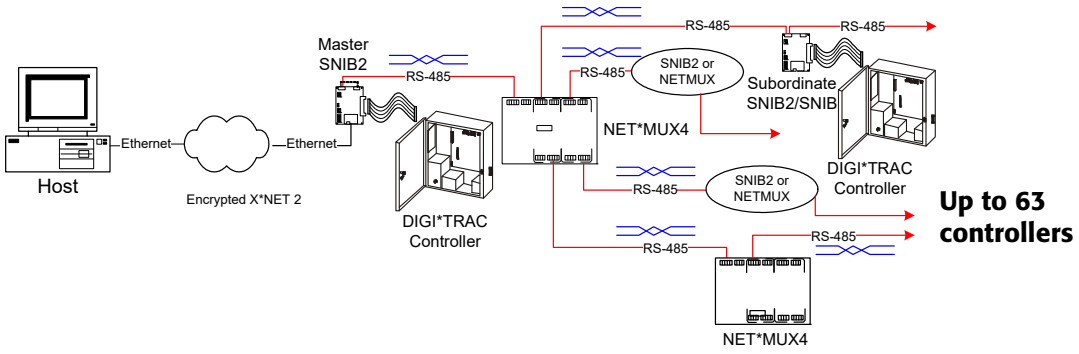


*Figure 2-26: SNIB2 to Controller Using a NET*MUX4*

If required, you can add a second level of NET*MUX4s to create additional controller runs; however, Hirsch does not support more than two levels of NET*MUX4s.

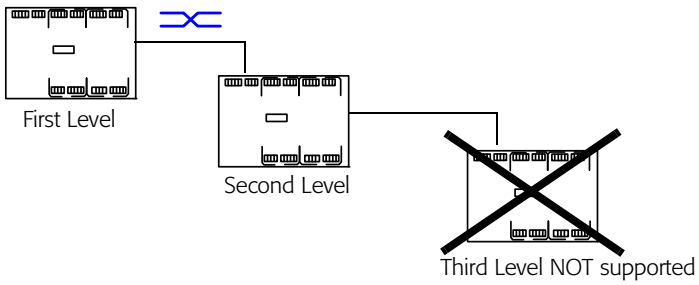


*Figure 2-27: NET*MUX4 Second Level Support*

*Note: NET*MUX4 speeds are dictated by wire gauge and distance. We recommend using Cat5/Cat6 cable.*

Benefits of the SNIB2

The SNIB2 provides these functional advantages over the original SNIB:

- AES encryption
- Ethernet connectivity (if required)
- XBox functionality
- Higher serial communication speeds

Each of these features is explained below.

❑ AES Encryption

The SNIB2 employs AES-Rijndael asymmetric 128-bit block data encryption.

The National Institute of Standards and Technology (NIST) has awarded the SNIB2 AES Certificate #280.

❑ Ethernet Connectivity

A standard RJ-45 Ethernet port is included on the SNIB2. This enables the connected controller installed with a SNIB2 to communicate with the server using TCP/IP over 10BaseT or 100BaseT Ethernet networks. This eliminates the need for external device servers for LAN connectivity.

❑ XBox Functionality

The SNIB2 also incorporates full XBox gateway functionality, thereby eliminating the need for an XBox. This enables the SNIB2 to function as a gateway for up to 63 controllers (with inclusion of the NET*MUX4), and provides the ability to globalize certain features.

Globalizing is the task of connecting two or more controllers in order to share credential user management and control zone information amongst all connected controllers. Globalization can only be performed within a local XBox node. One SNIB2 acting as an XBox cannot talk to and share information with another XBox or another master SNIB2.

❑ **Higher Serial Communication Speeds**

Communications between multidropped SNIB2s are now supported at speeds up to 115,200 bps with Cat5/Cat6 cable.

When using one or more NET*MUX4s, the maximum SNIB2 speed is limited to 9600 bps. When combining SNIBs and SNIB2s, the maximum speed is limited to the lower SNIB speed – that is, the lowest speed that all connected devices have in common.

Communications become less robust as baud rates increase, wire gauge decreases, and distances increase. Most tables for wire gauge and distance in this document are based on 9600 bps.

At higher baud rates, maximum distances are decreased and minimum wire gauge is increased. It may not be possible to implement the higher baud rates supported by the SNIB2 if you have long wire runs or small wire gauges.

In order to use the SNIB2, your controller must be running CCM 7.3.08 or higher; use Vn. 7.4.00 or higher if your computer has Velocity 3.0.

You can install the SNIB2 board in any Hirsch DIGI*TRAC controller except the M1N. (The Mx controller includes SNIB2 capability.)

For more information about setup and wiring of any SNIB board, see “Secure Network Interface Boards (SNIB, SNIB2, or SNIB3)” on page 2-96. For installation instructions, see “Secure Network Interface Board (SNIB, SNIB2, or SNIB3) Installation” on page 7-42.

SNIB2 Network Configuration Options Overview

The SNIB2’s Ethernet port provides high-speed TCP/IP communication over an Ethernet network between the host computer and the controller as shown in Figure 2-28.

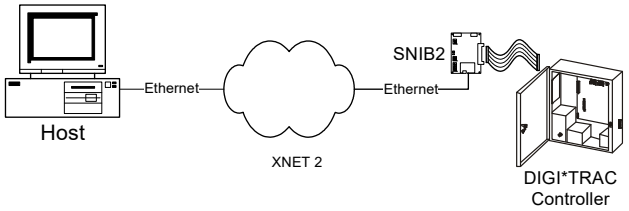


Figure 2-28: SNIB2 Ethernet Connection Using XNET2

In a multiple controller sequence, the configuration can look like Figure 2-29.

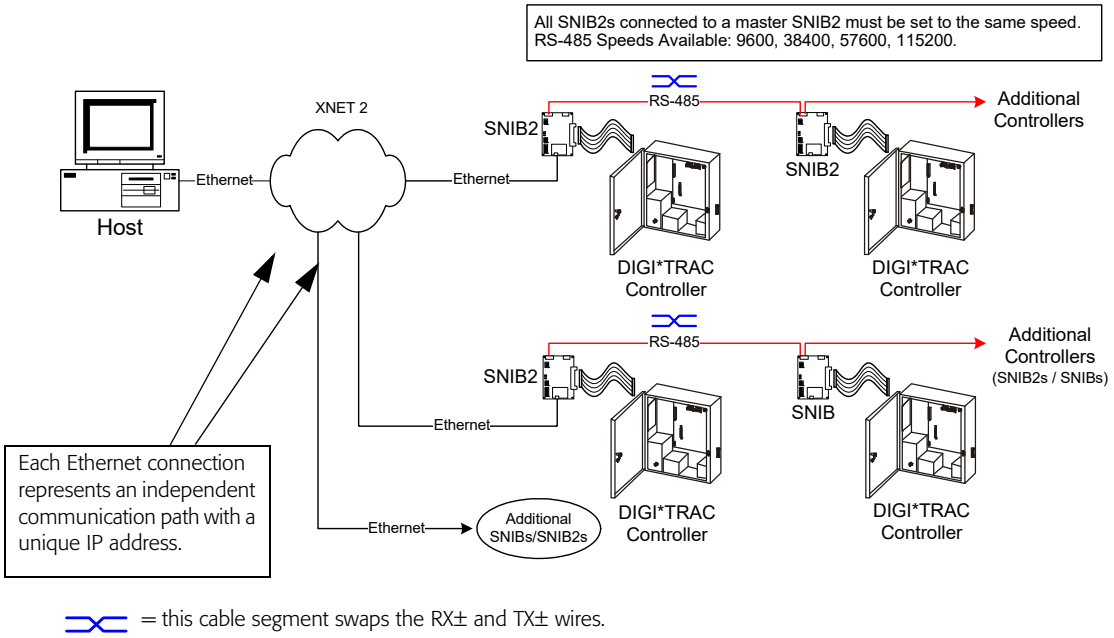


Figure 2-29: Multiple Controller Sequence Using SNIB2

This enables communication between the controller with the master SNIB2 and host PC at 10/100BaseT. Speeds between the master SNIB2 and other connected downstream SNIB2s range up to 115200 bps when using Cat5/Cat6 cable. Speeds between a master SNIB2 and downstream SNIBs are limited by the top speed of the older SNIBs (38400 bps).

Higher baud rates are also more dependent on the number of twists per foot, so capacitance specifications must be strictly followed: total wire run per port is not to exceed a total of 100,000 p*f*.

Before the Velocity server can communicate over Ethernet with a SNIB2, you must first configure the SNIB2 through Velocity. For more on this, refer to “Configuring a Master SNIB2 in a Different Subnet” on page 7-64.

Whenever an Ethernet connection is employed between the host and the SNIB2, Velocity views the SNIB2 as an XNET port because the SNIB2 includes XBox functionality. The host communicates with the Ethernet-connected SNIB2 using AES-encrypted XNET 2.

Controller-to-controller speeds range from 9600 to 115200 bps. For each string of controllers, the first (master) SNIB2 with the Ethernet connection must be assigned the same address as the XBox port.

For more on this, refer to “Configuring a Master SNIB2 in a Different Subnet” on page 7-64.

*Note: When the host is connected to a SNIB2 using Ethernet, Velocity views the first (master) SNIB2 as both a DIGI*TRAC controller and an XBox residing on an XNET port. Subsequent multidropped controllers in the sequence do not appear as XBox controllers.*

SNIB3

The Secure Network Interface Board v3 (SNIB3) is an update to the SNIB2 board currently used with the Mx, M2, M8, M16, M64, and MSP controllers. The SNIB3 is based on a new, more powerful hardware platform that supports IPv6 as well as IPv4.

The SNIB3 also supports more robust encryption (with a 256-bit key length) through the XNET3 protocol. For compatibility with older SNIB2-equipped controllers, the SNIB3 can run in XNET2 mode using 128-bit AES encryption. (If you are using SNIB2 boards in some of your controllers, you cannot use the XNET3 protocol, and those controllers must be downstream slaves to a master SNIB3, connected using the RS-485 port, as shown in Figure 2-32.)

The SNIB3 includes one available RJ-45 Ethernet port (connector 1) that is used to connect the Velocity host to this board. When the SNIB3 is in a master configuration, it supports RS-485 serial connectivity to downstream SNIB2 or SNIB3 slave controllers.

The main components of the SNIB3 are shown in Figure 2-30.

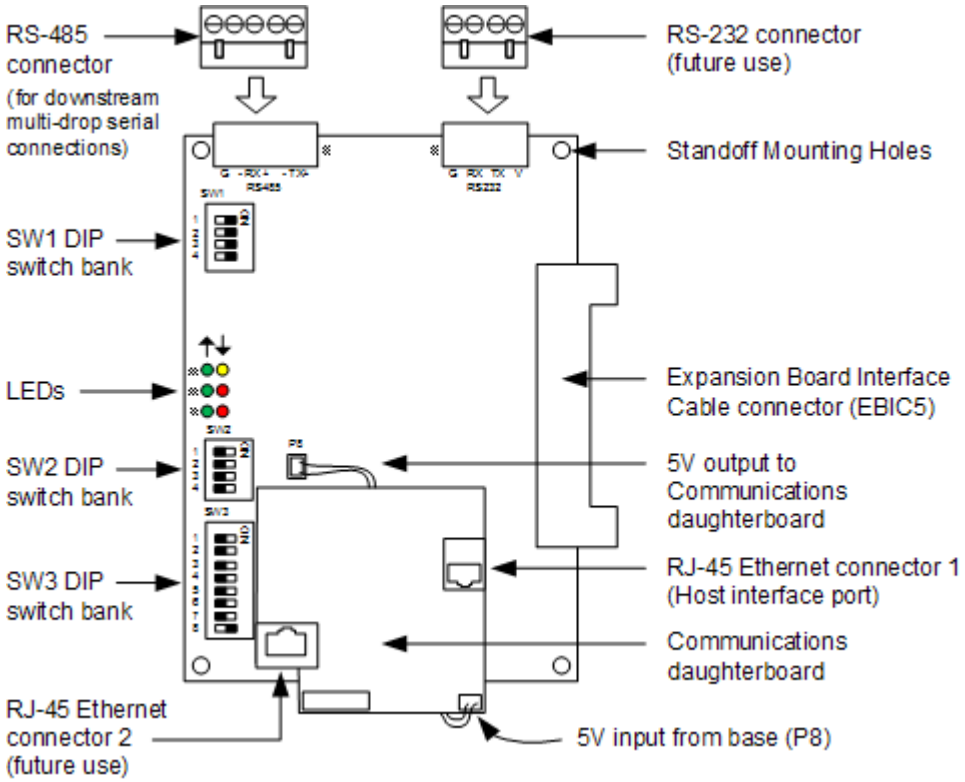


Figure 2-30: Main Components of the SNIB3 Board

NOTE: If you want to use the SNIB3 with an Mx controller, you must first remove the SNIB2 daughterboard from the controller's main board. For more information, see "Preparing an Mx Controller to Use a SNIB3" on page 7-75.

Benefits of the SNIB3

The SNIB3 provides these functional advantages over the previous SNIB2:

❑ **Faster Ethernet Speed**

The standard RJ-45 Ethernet port included on the SNIB2 enables the connected controller to communicate with the Velocity host using TCP/IP over 10BaseT or 100BaseT Ethernet networks. The SNIB3's RJ-45 Ethernet port is capable of 10BaseT, 100BaseT, or 1000BaseT (gigabit) speeds.

❑ **IPv6 Addressing**

The SNIB3 supports version 6 of the Internet Protocol, which uses 128-bit addresses to identify and locate devices on the Internet. (The previous IPv4 used 32-bit addresses.)

❑ **AES Encryption with 256-bit key length**

The SNIB3 supports more robust encryption (with a 256-bit key length) through the XNET3 protocol. For compatibility with older SNIB2-equipped controllers, the SNIB3 can run in XNET2 mode using 128-bit AES-Rijndael asymmetric data encryption.

❑ **FIPS 140-2 Certification**

The SNIB3's cryptographic modules use the **OpenSSL library**, which has been certified by the National Institute of Standards and Technology (NIST) to meet their Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules. (The Velocity software uses Microsoft's BCRYPTPRIMITIVES library, which also has been certified by NIST to meet FIPS 140-2.)

❑ **Hardware Security Authentication Module (SAM)**

The SNIB3 has a Security Authentication Module (SAM) for securely storing keys. One application for this module is to secure firmware downloads, using a TRN format as used on Touch Secure readers. In this method the firmware is first verified for authenticity by using the SAM keys before downloads are allowed.

SNIB3 Power Rating

❑ Peak current draw: 1.35A @ 3.3V

❑ Normal current draw: 850mA @ 3.3V

SNIB3 Network Configuration Options Overview

Be aware that the SNIB3 is backwards compatible with the SNIB2, but not with the original SNIB. Each connected DIGI*TRAC or Mx controller must have its own SNIB2 or SNIB3 board installed.

The SNIB3 provides both an RS-485 port and a 10/100/1000BaseT RJ-45 Ethernet port.

If you are using only SNIB3 boards in all of your controllers, you can use either the XNET2 or the XNET3 protocol, and the downstream controllers in your security network can either be connected directly using the RJ-45 Ethernet port, or be connected to a master

SNIB3 using the RS-485 port. These options are shown in Figure 2-31.

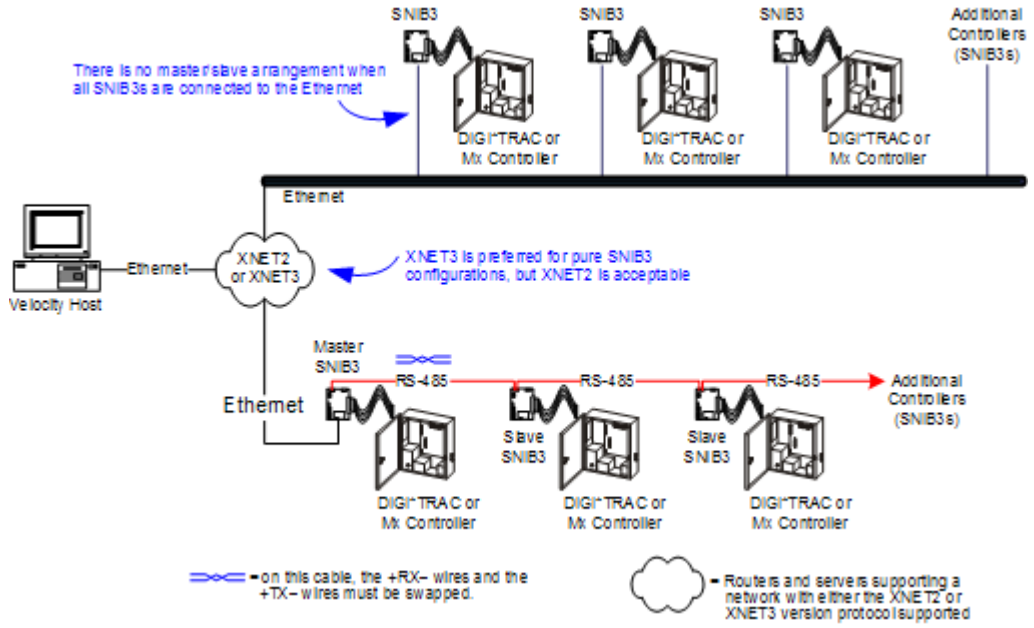


Figure 2-31: Example Network Configurations Using Only SNIB3 Boards

If you are using SNIB2 boards in some of your controllers, you cannot use the XNET3 protocol, and those controllers must be downstream slaves to a master SNIB3, connected using the RS-485 port, as shown in Figure 2-32.

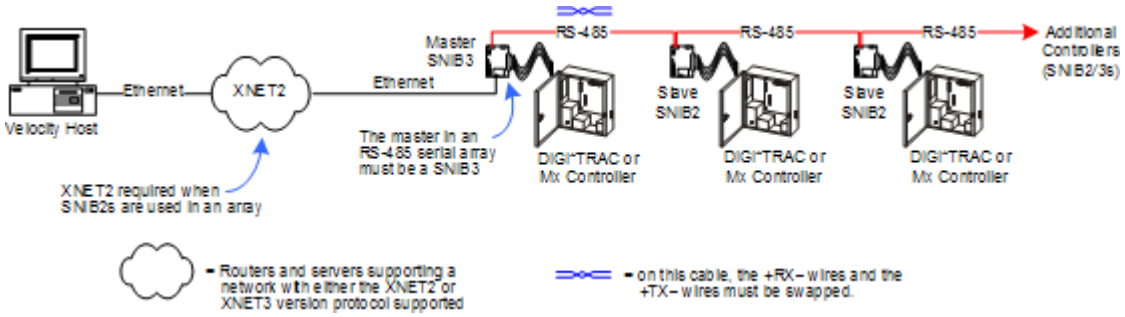


Figure 2-32: Example Network Configuration Using SNIB2 and SNIB3 Boards

The SNIB3 also supports connections to the NET*MUX4, as explained in “Using NET*MUX4s with SNIB3s” on page 7-81. This enables more controllers to be managed through a single network port, but it limits the data communication speed to 9600 baud.

Power Supplies

Locks and other output devices require separate power supplies to function. While DIGI*TRAC controllers can power a number of ScramblePads and MATCH interfaces (see “ScramblePad/MATCH Inputs” on page 2-15 for more information), a separate power supply can be used to power ScramblePads and MATCH interfaces which require more current than the controller can provide.

Specific information is provided here for Hirsch’s own PS2 Power Supply; however if you want to substitute another power supply, you can use the wiring and connection information in this section for that device as well.

Powering ScramblePads/MATCH Interfaces Locally

Ordinarily the controller provides sufficient power to operate attached ScramblePads and/or MATCH interfaces; however, there are conditions which require more power than the controller can supply. This usually occurs when readers connected to the MATCH draw more current or require a different voltage than the MATCH can supply, or if the wire run between the Controller and the MATCH is more than 1800 feet (549 meters).

When this happens, connect a local 24V DC power supply to the ScramblePad or MATCH’s connector as follows:

- ❑ Use the black wire from the controller. Do *not* use the red wire.
- ❑ Wire from the power supply to the respective G and + terminals on the ScramblePad or MATCH.

Figure 2-33 provides a view of this arrangement:

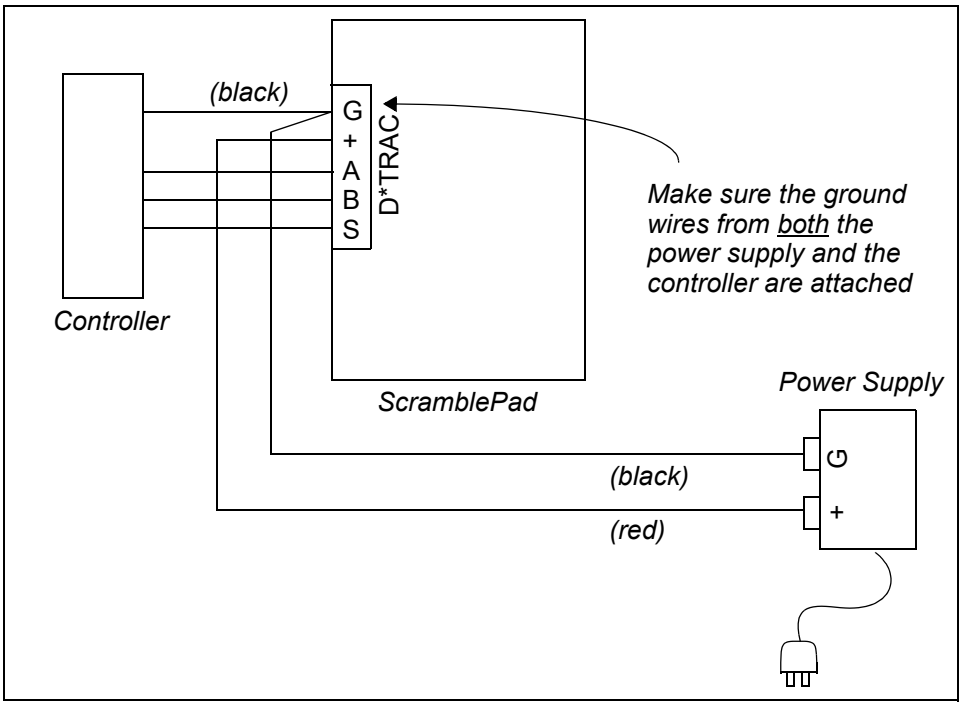


Figure 2-33: Powering the ScramblePad Locally

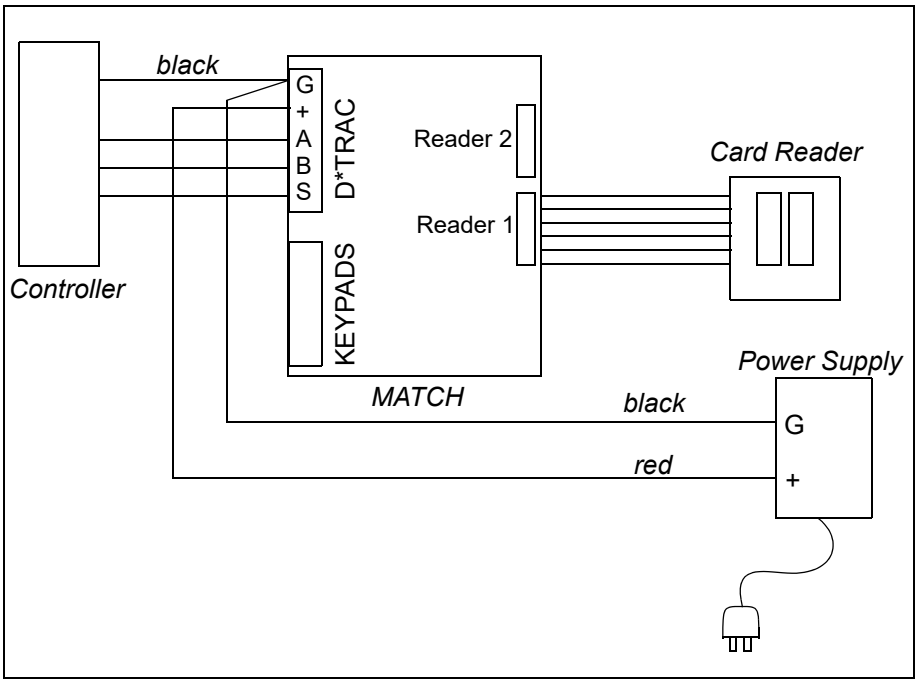


Figure 2-34: Powering the MATCH Locally

When powering locks and other output devices, always read the device's manual before proceeding.

For using power supplies to power locks, see "Locks/Strikes" on page 2-82. For information on powering other output devices, see "Remote Output Components" on page 2-82.

For more detailed information on local power, see "Powering the ScramblePad Locally" on page 7-125 and see "Powering the MATCH Locally" on page 7-143.

Using the PS2 Power Supply

The PS2 power supply is a companion product to the DIGI*TRAC Controllers. It is designed to power electrified locks or magnetic locks and provide auxiliary power to ScramblePads and MATCH interfaces. The PS2 incorporates several unique features:

- ❑ High inrush capacity, up to 16 Amps current on each of its two powered outputs. This enables the PS2 to be used to power the Von Duprin electrified Panic Devices as well as other electrified locking hardware with heavy surge requirements.
- ❑ Continuous duty holding current capacity is limited to 500 mA total or 250 mA from each powered output. This covers most 24V DC locks on the market.
- ❑ Dual battery standby packs – one for the controller and one for the locks. Both batteries must be installed to operate surge locks. Both batteries share the responsibility of unlocking locks and operating controllers during AC power failure. They are float charged by a unique circuit that balances power demand between controller operation and lock operation to maximize the charge rates at all times.
- ❑ Power connector for locally powering ScramblePads or MATCHs at the controlled door. PS2-supplied keypad power is 500mA @ 28VDC.

The optional PS2H adds high security supervision on a lock relay cable run. This prevents bypassing of the access control system by shorting the lock cable to cause the lock to actuate, or by jumping the cable with a battery strong enough to unlock the lock. If you use a PS2 power supply, see “PS2 Power Supply Installation” on page 7-307 for complete instructions on how to configure and install the PS2.

Figure 2-35 provides an illustration of the basic PS2 wiring plan.

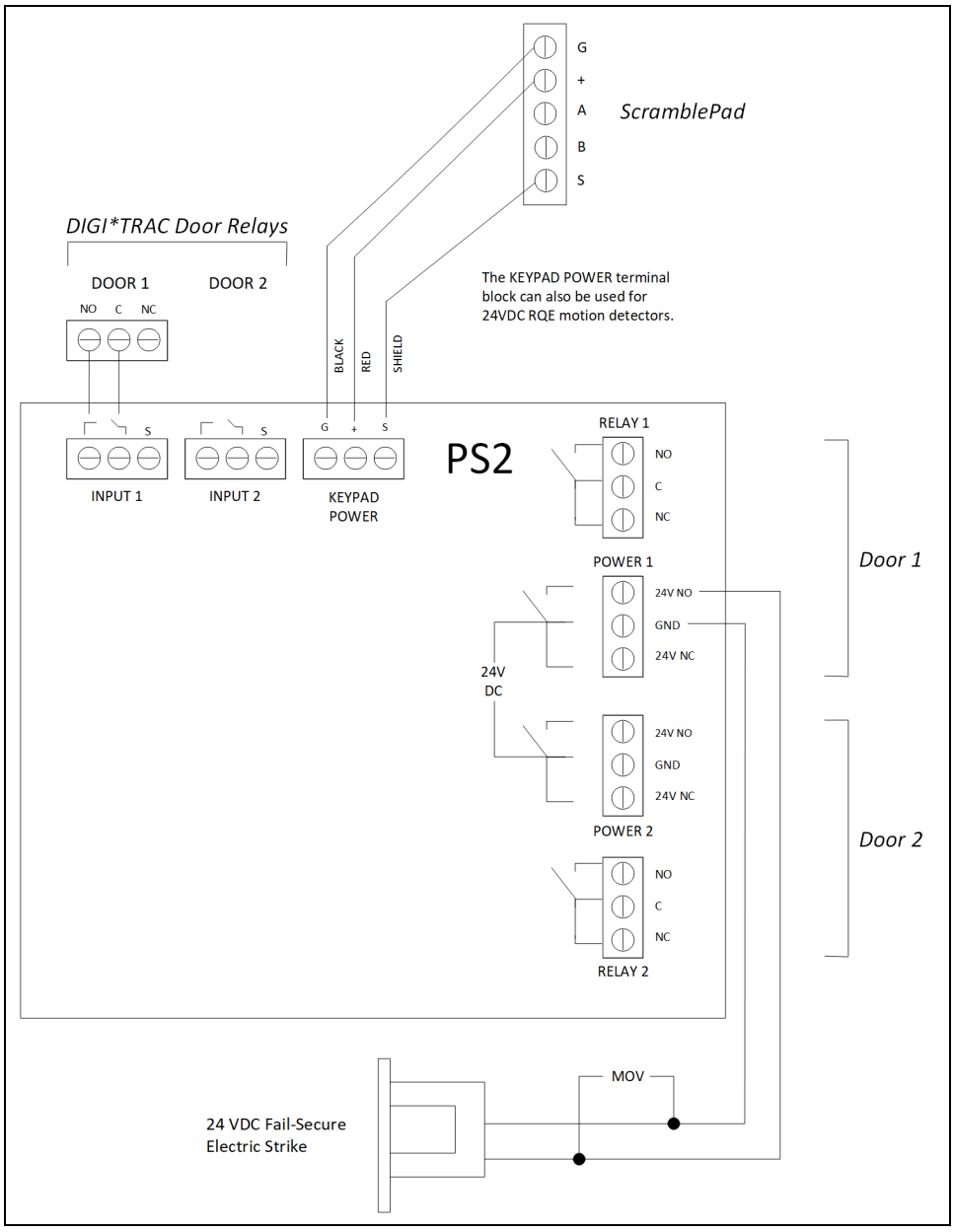


Figure 2-35: PS2 Power Locking System

As shown in this diagram, when a valid code is entered or an RQE device is activated, the DIGI*TRAC controller's door relay trips, completing the circuit to the input on the PS2. Whenever the PS2 input sees a circuit closed, it simultaneously trips the associated power and dry relay contact. The power relay is allocated for a 24 VDC lock and the dry relay can be used for alarm shunting, camera call-up, and other uses.

The maximum distance (in feet) for the lock power cable is a function of the wire gauge and lock current:

$$DISTANCE = \frac{WGV}{LockInrushCurrent}$$

where:

WGV, the Wire Gauge Value, can be calculated using this table:

Wire Gauge	22	20	18	16	14	12
WGV	123	198	312	500	794	1258

and the *LockInrushCurrent* can be calculated using this formula:

$$LockInrushCurrent = \frac{LockVoltage}{ImpedanceofLockCoil} = \frac{24V}{\Omega_{LockCoil}}$$

Obtain the *Impedance of the Lock Coil* from the lock or strike manufacturer's data.

This will provide you with the maximum cable distance between a lock/strike and the PS2.

Note: Always calculate cable distance based on Lock Inrush Current, not lock holding current.

If the necessary wiring distance is longer than the calculated maximum, either:

- ❑ Choose a larger wire gauge and recalculate
- ❑ Install the PS2 closer to the lock.

For example, if you are using a 24 VDC lock with a lock coil impedance of 10 ohms connected to the controller by 18 AWG lock cable, then maximum distance would be calculated in this manner:

$$LockInrushCurrent = \frac{24V}{10\Omega} = 2.40$$

$$DISTANCE = \frac{312}{2.40} = 130feet$$

There is also a keypad power connection for powering ScramblePads and MATCH interfaces locally instead of directly from the DIGI*TRAC Controller. If ScramblePads are powered by the PS2, these are the maximum cable lengths allowed in feet (and meters):

AWG	**DS37L DS47L**	**DS37L-HI DS47L-HI**	**2 DS37L 2 DS47L**	**DS37L + DS37L-HI DS47L + DS47L-HI**	**2 DS37L-HI 2 DS47L-HI**
22	750 (230)	450 (138)	375 (115)	275 (84)	225 (69)
18	1800 (549)	1150 (350)	925 (282)	700 (213)	575 (175)

Table 2-15: PS2-to-ScramblePad Cable Distances

*Note: The ScramblePad must be powered by the DIGI*TRAC Controller for UL294 installations.*

The relay contact ratings for RELAY 1 and RELAY 2 are as follows:

Powered Contacts	24V DC unregulated (18V-27V), 16A Inrush current for 0.5 second, 0.3A continuous holding current
Unpowered Contacts	10A resistive at 24V DC

PS2 Enclosure

The PS2 is housed in a key-locked metal enclosure. This box is mounted in the same way as the DIGI*TRAC controller and includes a cord and plug for line power.

Dimension:	12”H x 12”W x 4”D (30.5cm x 30.5cm x 10cm)
Shipping Weight:	16.3 lbs (7.4 kg)

For instructions on mounting and wiring the PS2, see “PS2 Power Supply Installation” on page 7-307.

Remote Input Components

This section includes design notes on the following devices:

- ScramblePads
- Verification Stations
- MATCH Reader Interface
- Readers
- Line Modules
- RQE Devices
- Door Contacts
- Surveillance Cameras

ScramblePads

In addition to access control, the ScramblePad is used to:

- Enter codes to program the controller
- Unlock doors
- Mask alarms
- Trigger relays for equipment or process control

Pull cable runs from the controller to ScramblePads for each door. Make sure you select the correct ScramblePad mounting box for the applications and conditions specific to each door. Pay special attention to the specified mounting height for the ScramblePad. If it's not right, the ScramblePad will be difficult to use properly.

Table 2-16 shows the many types of ScramblePads that are available:

ScramblePad	Description
DS37L	Industry standard for keypad entry with the patented scrambling key design. This version is no longer sold.
DS37L-HI	High-intensity version of the ScramblePad for outdoor locations.
DS37L-HW	Weatherized, environmentally-sealed version of the ScramblePad.
DS47L	Combines the ScramblePad with a MATCH reader interface.
DS47L-HI	High-intensity version of the DS47L.
DS47L-SPX	ScrambleProx. All-in-one ScramblePad/MATCH reader interface with built-in HID proximity reader. Use HID cards.
DS47L-SPX-HI	High-intensity version of the DS47L-SPX ScrambleProx. Use HID cards.
DS47L-SPX-I	DS47L-SPX ScrambleProx with built-in Indala reader. Use Indala 26-bit cards.

Table 2-16: ScramblePad Types

ScramblePad	Description
DS47L-SPX-I-HI	High-intensity version of the DS47L-SPX ScrambleProx with built-in Indala reader. Use Indala 26-bit cards.
BQT Readers	
DS47L-SS-BT	ScrambleSmart which incorporates a ScramblePad with an integrated MIFARE smart card reader.
DS47L-SS-BT-HI	High-intensity display version of ScrambleSmart.
DS47L-SS-BT-DF	Same as ScrambleSmart but with integrated MIFARE DESfire smart card reader.
DS47L-SS-BT-HI-DF	High-intensity display version of the ScrambleSmart with integrated MIFARE DESfire smart card reader.
HID Readers	
DS47L-SS-HID	DS47L ScramblePad with embedded 13.56MHz, ISO 14443-4 A&B contactless smart card reader and antenna. Reads PIV II End Point, DESFire (with CHUID only), and iCLASS. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, DESFire with FASC-N encoding, or iCLASS cards.
DS47L-SS-HID-HI	High-intensity display version of DS47L-SS-HID.
DS47L-SS-HID-SN	Same as DS47L-SS-HID but reads MIFARE/DESFire Serial Numbers, and iCLASS. Use MIFARE, DESFire, or iCLASS cards.
DS47L-SS-HID-SN-HI	High-intensity display version of DS47L-SS-HID-SN.
DS47L-SSP-HID	DS47L ScramblePad with embedded 125kHz proximity and 13.56MHz, ISO 14443A&B contactless smart card readers and antennae. Reads PIV II End Point, DESFire (with CHUID only), iCLASS, and HID 125kHz proximity. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, DESFire with FASC-N encoding, iCLASS cards., or HID 125kHZ cards.
DS47L-SSP-HID-HI	High-intensity display version of DS47L-SSP-HID.
DS47L-SSP-HID-SN	Same as DS47L-SSP-HID but reads MIFARE/DESFire serial numbers, iCLASS, and HID 125kHz proximity. Includes MATCH2 functionality. Use MIFARE, DESFire, iCLASS, or HID 125kHZ cards.
DS47L-SSP-HID-SN-HI	High-intensity display version of DS47L-SSP-HID-SN.

Table 2-16: ScramblePad Types (Continued)

ScramblePad	Description
Integrated Engineering Readers	
DS47L-SSDM-IE	DS47L ScramblePad with embedded 13.56MHz, ISO 14443-4A contactless smart card reader and antenna. Reads DESFire file system and MIFARE sector cards. PIV II Transition Compliant. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV, IE MIFARE or DESFire cards.
DS47L-SSDM-IE-HI	High-intensity display version of DS47L-SSDM-IE.
DS47L-SS-IE	DS47L ScramblePad with embedded 13.56MHz, ISO 14443-4 A&B contactless smart card reader and antenna. Reads PIV II End Point and PIV II Transitional cards including FRAC (SmartMX), DoD alpha & beta, DESFire PIV (V0.6 only), TWIC V1, MMAC, DESFire SN (1st 4bytes), and MIFARE SN. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, MIFARE, or DESFire cards.
DS47L-SS-IE-HI	High intensity display version of DS47L-SS-IE.
DS47L-SSP-IE	DS47L ScramblePad with embedded 125kHz proximity and 13.56MHz, ISO 14443A&B contactless smart card readers and antennae. Reads PIV II End Point and PIV II Transitional cards including FRAC (SmartMX), DoD alpha & beta, DESFire PIV (V0.6 only), TWIC V1, and MMAC.. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, DESFire with FASC-N encoding, or HID 125kHZ cards.
DS47L-SSP-IE-HI	High-intensity display version of DS47L-SSP-IE.

Table 2-16: ScramblePad Types (Continued)

The DS47L can be used in any application where a DS37L is used. It can also be used in applications where a DS37L + MRIB or an MRIA is used since it has the same bezel and physical tamper switch. The DS47L-SPX ScrambleProx provides a single device for card and code entry. The ScrambleProx also has a second reader port which can be used to connect a second reader to the other side of the door. This means that the ScrambleProx can be used to place dual technology on one side of the door and card access on the other side.

If you plan to use either the DS47L or the DS47L-SPX, you have several different configurations possible at the door site. Figure 2-36 through Figure 2-39 provide examples of several keypad configurations.

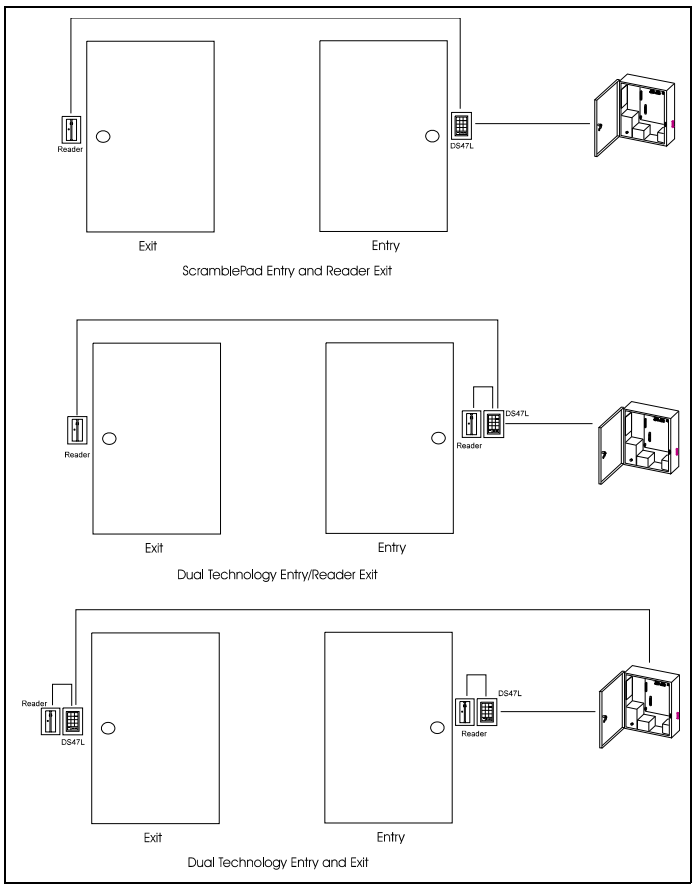


Figure 2-36: Possible DS47L Configurations

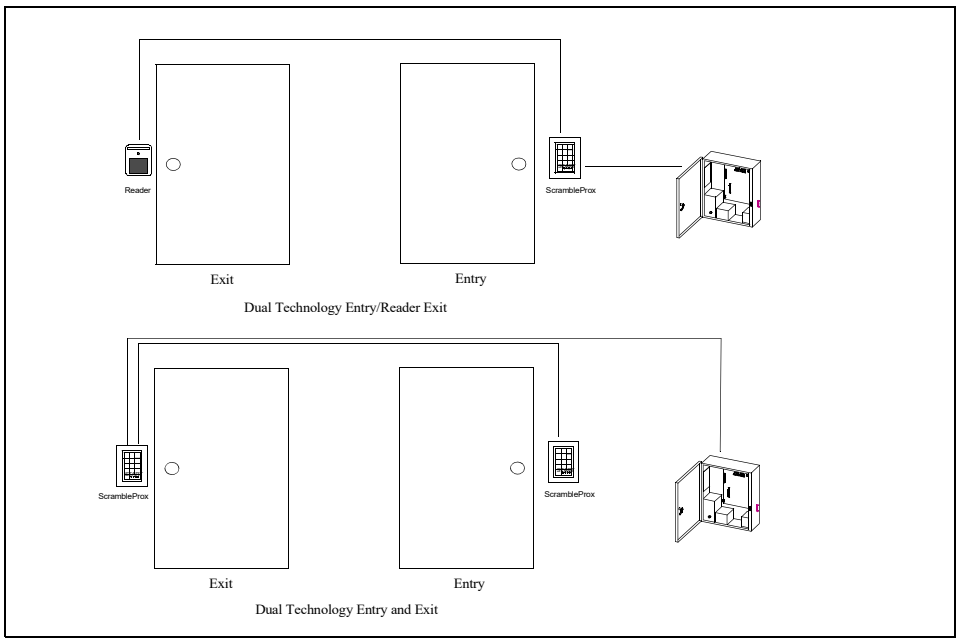


Figure 2-37: Possible ScrambleProx Configurations

Figure 2-38 and Figure 2-39 show the typical ScramblePad-to-Controller connections for both DS37L and DS47L-series ScramblePads.

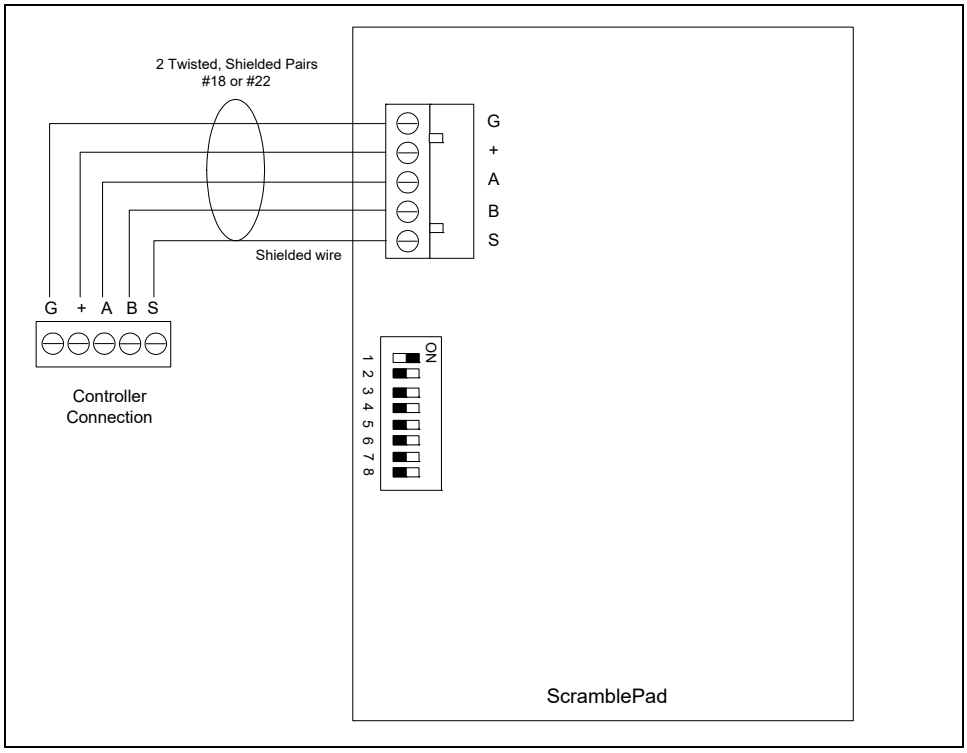


Figure 2-38: Typical ScramblePad to Controller Connection

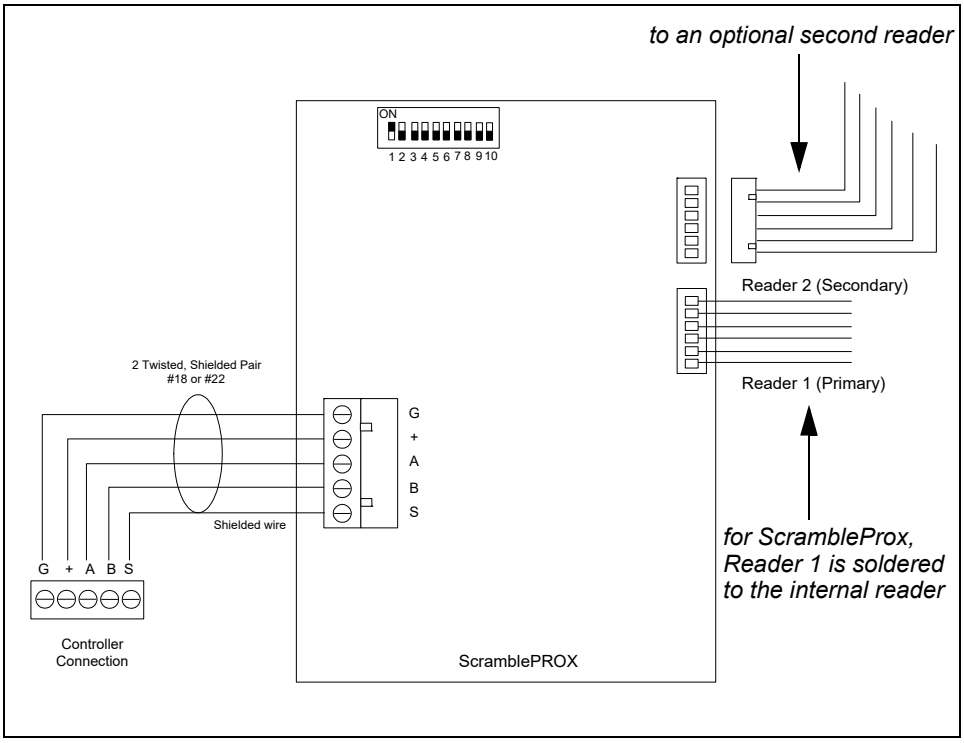


Figure 2-39: DS47L ScramblePad/DS47L-SPX ScrambleProx Connections to Controller/Reader

ScramblePad Mounting

The DS37L or DS47L are ideal for normal lighting, such as interior walls and doorways. Mounting boxes for these keypads come in two main types: surface-mounted and flush-mounted. Surface mounted boxes project from the wall on which they are mounted. Flush boxes are set into the wall so that they are flush with the wall.

Hirsch offers several varieties of each mounting box as shown in Figure 2-40. The dimensions for each of these boxes is shown in Table 2-17 on page 2-55.

In addition, the Universal Mounting Kit (UMK) can be used with the MB2 and MBS2S to position the face at three different aspects: flush, semi-flush, and tilted (for handicapped). For more information about installing mounting boxes, see “Installing the Mounting Box” on page 7-97.

When ScramblePads must be installed on exterior walls or on gate posts, select the MB5 Exterior Mounting Box.

For exterior locations, consider one of these ScramblePad model options:

- ❑ DS37L-HI
- ❑ DS47L-HI
- ❑ DS47L-SPX-HI

In high-ambient light conditions (which may occur indoors as well as outdoors), use the DS37L-HI, DS47L-HI, or DS47L-SPX-HI. The standard ScramblePad uses Red LEDs which become unreadable in bright or direct sunlight. When ScramblePads are installed on east- or west-facing walls or gates, the display washes out in the morning or afternoon hours.

The high-intensity DS37L-HI, DS47L-HI, or DS47L-SPX-HI uses the same off-white incandescent display used in commercial aircraft instrumentation. They are readable even in direct sunlight and highly reliable. The viewing restriction on the DS37L-HI, DS47L-HI, or DS47L-SPX-HI is less restrictive: approximately 12° horizontally (as opposed to 4° for the DS37L) to help see the display or when installed in the MB5. Occasionally, the DS37L-HI is selected for users who are color-blind to red.

Figure 2-40 shows the ScramblePad and its available mounting boxes. For directions on mounting the ScramblePad, see “ScramblePad Installation” on page 7-97.

Dimension (Face):	5.75”H x 4.37”W (14.6cm x 11.11cm)
Dimension (Body):	4.5”H x 3.5”W x 2.25”D (11.43cm x 8.89cm x 5.71cm)
Shipping Weight:	2 lbs (0.9 kg)

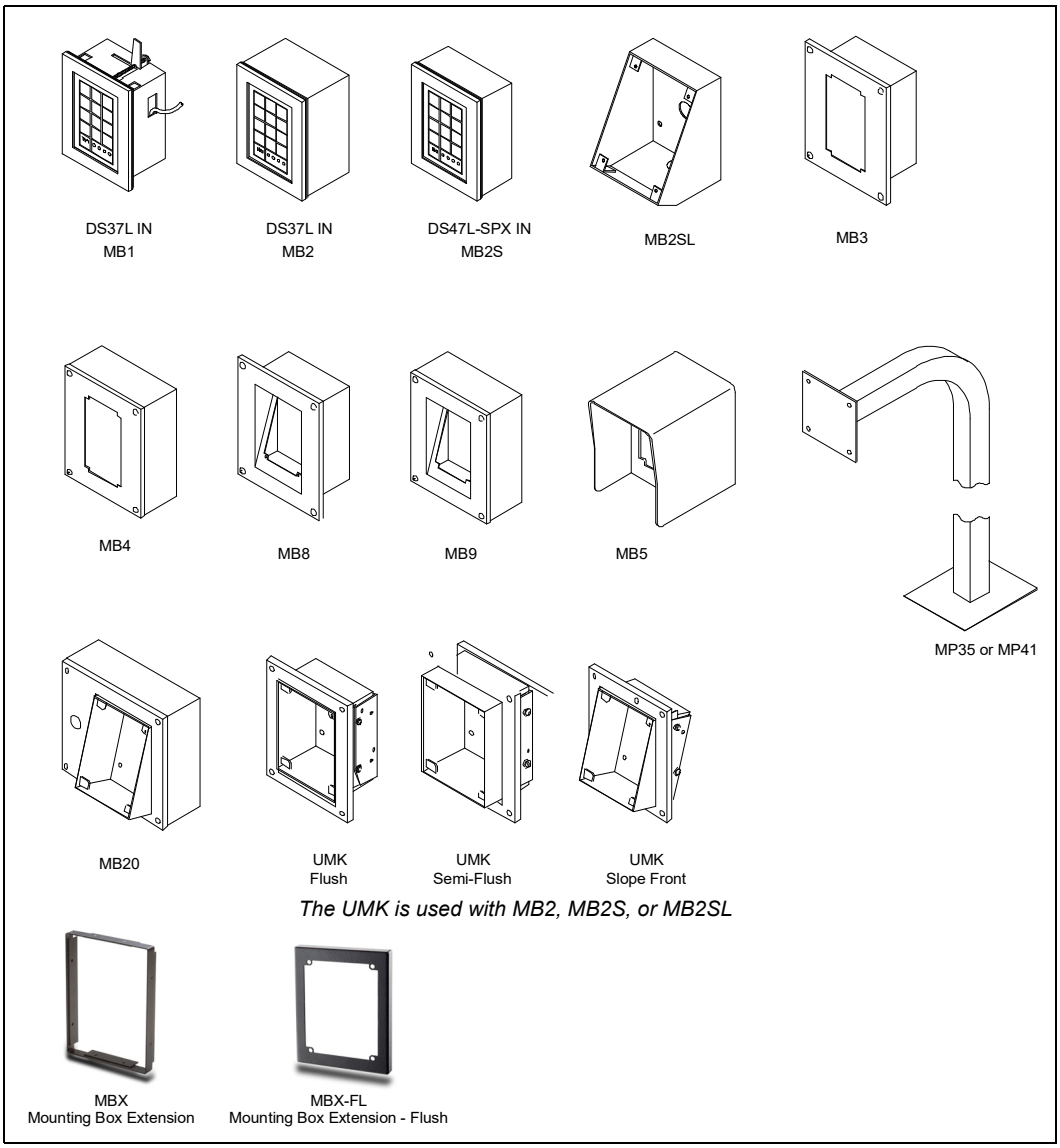


Figure 2-40: ScramblePads and Mountings

The mounting height for each of these boxes is shown in Table 2-17 as measured from ground or floor level to the middle (centerline) of the ScramblePad in inches (and meters).

Box	Specifications	Mounting Height
MB1	Flush: standard	56 - 58 (1.42-1.46)
MB2	Surface: standard	56 - 58 (1.42-1.46)
MB2S	Flush: shallow for DS47L and DS47L-SPX	56 - 58 (1.42-1.46)
MB2SL	Surface: slope-front for DS47L and DS47L-SPX	56 - 58 (1.42-1.46)
MB3	Flush: heavy duty	56 - 58 (1.42-1.46)
MB4	Surface: heavy duty	56 - 58 (1.42-1.46)
MB5	Surface or Post: heavy duty exterior	56 - 58 (1.42-1.46)
MB8	Flush: heavy Duty slope front	46 - 48 (1.17 - 1.22)
MB9	Surface: heavy Duty slope front	46 - 48 (1.17 - 1.22)
MB20	Surface: slope-front keypad with magstripe reader mounted side-by-side	46 - 48 (1.17 - 1.22)
MP35	Curb mounting post for MB5	35 (0.89)
MP41	Street mounting post for MB5	44 1/8 (1.12)
MBX	Mounting Box Extension	½-inch (.012)
MBX-FL	Mounting Box Extension – Flush	½-inch (.012)
UMK	Universal Mounting Kit: Flush, Semi-Flush, or Slope Front (requires MB2)	dependent on box/post

Table 2-17: Mounting Heights for ScramblePads and Mounting Boxes

Most states require strict compliance with ADA (Americans with Disabilities Act) in addition to many local and regional code requirements. Consult your local codes for exact height requirements.

Select a mounting box which provides a convenient viewing angle for personnel confined to wheelchairs. The UMK provides several angles. The MB8, MB9, and MB20 are also tiltable for easy reading. To accommodate state and federal disabilities statutes, a tilted box may prove necessary. For information about installing mounting boxes, see “Installing the Mounting Box” on page 7-97.

See Figure 7-35 through Figure 7-40 for close-ups of ScramblePad Mounting Box types and dimensions.

Mounting Extensions

Hirsch mounting boxes can be fitted with two extensions:

- ❑ MBX – A ½- inch extension for surface-mounted boxes used with ScramblePad or bezel-mounted reader assemblies in cases where the mounting box depth is too shallow for the electronics, as with some of the ScrambleSmart products. The MBX package includes four extra long screws and is suitable for use with the MB2, MB2S, MB2SL, or UMK/MB2 (either sloped or semi-flush).

- MBX-FL – A ½-inch extension for flush-mounted boxes used with ScramblePad or bezel-mounted reader assemblies in cases where the mounting box depth is too shallow for the electronics, as with some of the ScrambleSmart products. The MBX-FL includes four extra long screws and is suitable for use with the MB1.

Firestops for Mounting Boxes

Many installers are concerned about fire rating for their mounting boxes, particularly the MB2. The MB2 is not fire-rated; however, the box and its contents can be made fire-resistant using a *hole-plug-type firestop*. The firestop restores the wall's fire rating.

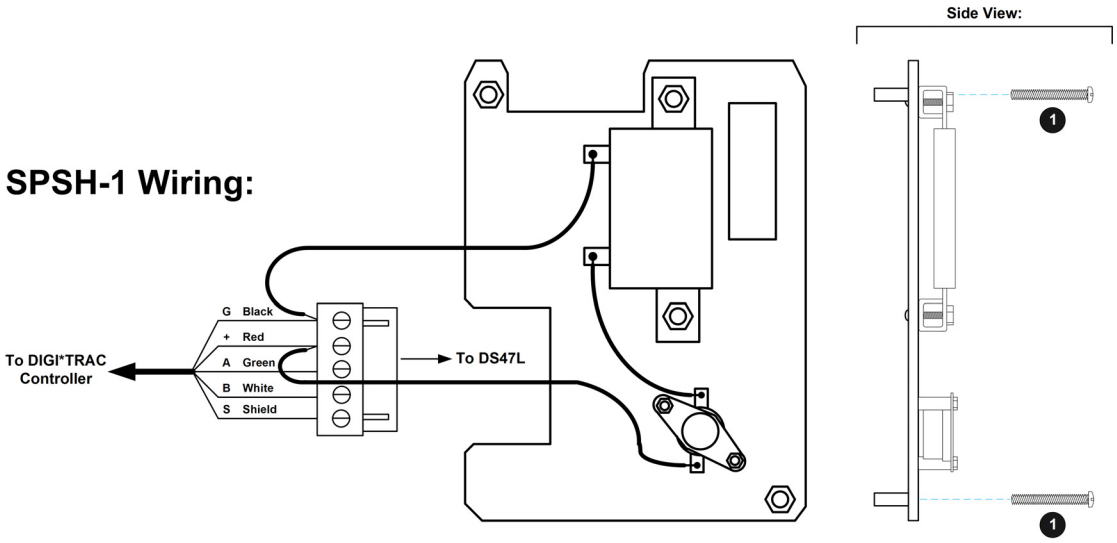
To install it, simply mount the MB2 over a firestop. Firestops are available in many sizes and shapes and can be purchased from many suppliers. You can find most firestop manufacturers listed in the Thomas Register or through its webpage, *www.thomasregister.com*.

SPSH-1: Heated Back Cover for a DS47L ScramblePad

If you are using a DS47L ScramblePad in an environment where the temperature may drop below freezing or where condensation may be an issue, you can replace the reader's standard back cover with the SPSH-1 heated back cover. For example, an SPSH-1 is recommended for outdoor applications (such as controlling access to a restricted parking area) in cold climates where a DS47L ScramblePad is enclosed in an MB5 mounting box and mounted on a pole.

The SPSH-1 draws its power from the **G** and the **+** connections of the DS47L (as shown in the following diagram), and it consumes 0.33 Amps at 28VDC.

SPSH-1 Wiring:



1 NOTE: 2 mounting screws (part number 038-0001008) are provided to mount the SPSH-1 heater onto the back of a DS47L-XX ScramblePad.

When the DS47L is powered by a DIGI*TRAC controller:

- there can be only one DS47L with an SPSH-1 per door,
- there can be no more than two DS47Ls with an SPSH-1 per controller, and
- the maximum cabling distance between the controller and a DS47L with an SPSH-1 is half of the values shown in Table 2-5 on page 2-16.

If you need to have more than two DS47Ls with an SPSH-1 connected to a controller, then you must provide separate power for the additional SPSH-1s.

Verification Stations

The Hirsch RUU-201 Verification Station™ combines an array of smart card reader technologies to provide a complete access solution. Currently, the RUU Verification Station supports these smart card platforms:

- ❑ PIV
- ❑ CAC
- ❑ General purpose

The following functions are included in this reader:

- ❑ ScramblePad keypad
- ❑ Prox (contactless) card reader
- ❑ Magstripe card reader
- ❑ Contact Smart card reader
- ❑ Biometric fingerprint reader

An LED display is included that informs the user of access status.

The RUU-201 also incorporates enrollment functions that enable a qualified operator to enroll both cards and codes, including the writing of biometric parameters to Smart Cards.

The front view of this reader looks like Figure 2-41:

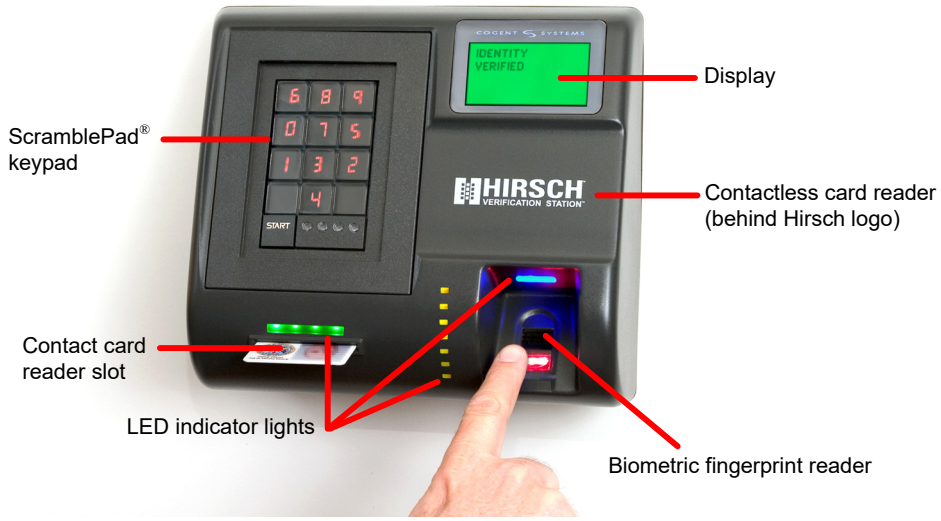


Figure 2-41: RUU-201 Verification Station

The Verification Station can be used for:

- ❑ a card-code access point
- ❑ in its general purpose configuration, a card writing station
- ❑ when attached to a Velocity server, an enrollment station

Table 2-18 shows the types of Verification Stations now available:

Verification Station	Description
RUU-201	Basic wall mount version of the PIV Verification Station.
RUU-201-HI	High-intensity wall mount version of the PIV Verification Station for outdoor locations.
RUU-201-DT	Desktop version of the PIV Verification Station.
RUU-CAC	Basic wall mount version of the CAC Verification Station.
RUU-CAC-HI	High-intensity wall mount version of the CAC Verification Station for outdoor locations.
RUU-CAC-DT	Desktop version of the CAC Verification Station.
RUU-GEN	Basic wall mount version of the general purpose Verification Station.
RUU-GEN-HI	High-intensity wall mount version of the general purpose Verification Station for outdoor locations.
RUU-GEN-DT	Desktop version of the general purpose Verification Station.

Table 2-18: Verification Station Types

Dimensions: 8.46”H x 9.45”W x 4.63”D. (214.88mm x 239.97mm x 117.6mm).

Shipping weight: 2 lb. (0.9kg).

For information on installing the Verification Station, refer to “Verification Station Installation” on page 7-128.

For additional information, refer to these documents:

- ❑ *Verification Station Quick Installation Guide*
- ❑ *Verification Station Configuration Guide*

MATCH Reader Interface

The MATCH Reader Interface is required by all DIGI*TRAC controllers if you plan to attach any readers, unless one of these conditions exists:

- ❑ You are only using a ScramblePad without a reader.
- ❑ You are using a DS47L-SPX ScrambleProx which includes both a reader and a MATCH.
- ❑ You are using a DS47L-series ScramblePad which includes a MATCH and a standard 26-bit card reader.
- ❑ You are only using an industry-standard Wiegand card reader which is directly wired to a Wiegand terminal on an Mx controller.

The MATCH Reader Interface enables a large number of reader technologies to communicate successfully with any DIGI*TRAC controller.

Hirsch provides three MATCH Reader Interface configurations:

- ❑ MATCH2 Reader Interface Board (MRIB)
- ❑ MATCH2 Reader Interface Assembly (MRIA)
- ❑ DS47L-series ScramblePad with integrated MATCH

Note: The MATCH2 replaces the older MATCH reader models. All drawings that follow apply to MATCH2 specifications.

The new MATCH2 board has fewer components than the old MATCH, but includes more functionality. The MATCH2 provides a second switch bank which can be programmed to accept a large selection of custom readers.

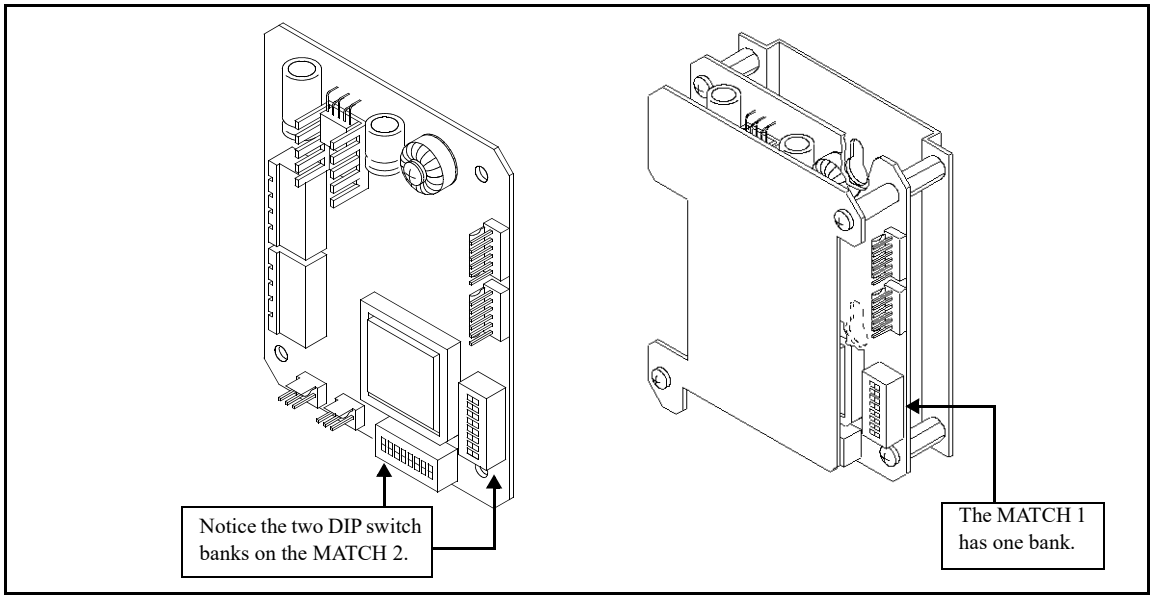


Figure 2-42: MATCH2 Board and Package

The MRIB consists of a printed circuit board mounted between two protective metal plates with keyhole mounting slots. The MRIA includes the MRIB which is attached to a mounting base and bezel. The bezel is the same as the one included with a ScramblePad and includes a physical tamper switch. The MRIA is designed for installation on a Hirsch mounting box. For a description of available mounting boxes, see “MRIA/MRIB Mounting” on page 2-63.

The MATCH is also integrated into the DS47L-series ScramblePads. These keypads can be used in much the same manner as a MATCH. But there are differences: while a DS47L ScramblePad can support one or two readers for dual entry or dual entry-card only exit, a MATCH can support two readers and two ScramblePads for dual entry and dual exit. Another and often better solution is to use DS47L ScramblePads, each with an associated reader.

The MRIB is normally located in close proximity to the readers it will connect to, as shown in Figure 2-43. The MRIB is usually installed above the ceiling line. A junction box (J-box) is often used to house and protect the board above the ceiling line. An MRIA in a Hirsch mounting box can also be used.

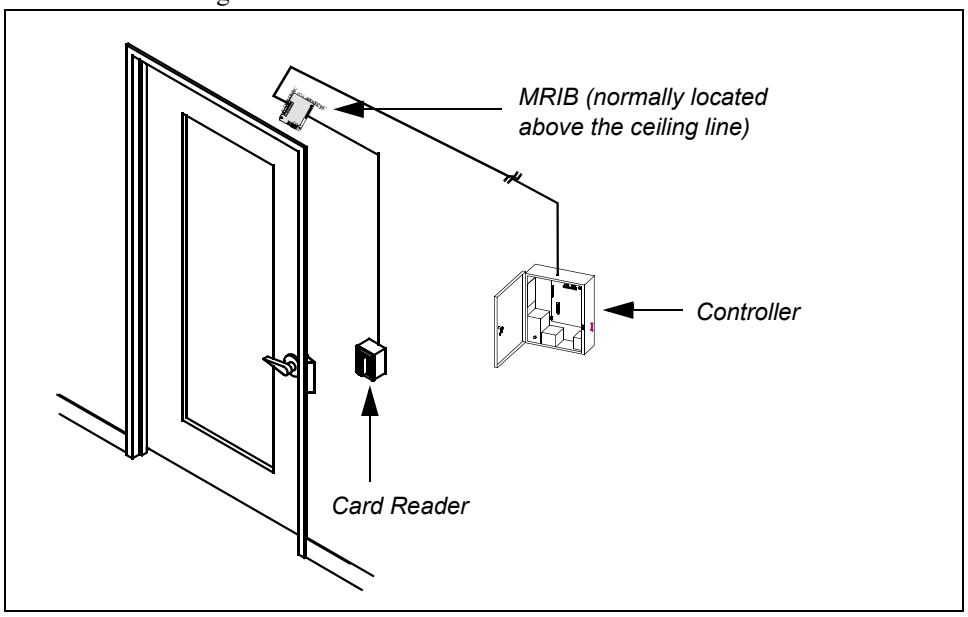


Figure 2-43: MATCH Location Example

Whether integrated or separate, the MATCH can supply 250mA to each reader using 5VDC. Readers which require more than 250 mA current (or other voltage levels) must always use a separate power supply. In addition, one or two ScramblePads can be connected to each MATCH. The MATCH should be located at the door or control location. Each MATCH includes two reader connectors with 12-inch flying leads.

The allowed maximum distance between the MATCH and a connected reader varies according to the reader. For example, the Hirsch CR11L Mag Stripe Card Reader can be located up to 500 feet (152 meters) from the MATCH to which it is connected. For maximum allowed distances between the MATCH and your selected reader(s), see “MATCH Reader Installation” on page 7-145 or refer to the literature shipped with your reader(s).

To increase the length beyond the prescribed maximum, the MATCH or attached reader must be powered locally. This eliminates the need for power from the controller and increases the allowed wire length. For more on powering a MATCH or reader, see “Powering the MATCH Locally (Schematic)” on page 7-144.

The dimensions and weight of the MATCH board and assembly are listed below:

Dimension (MRIA): 5.75”H x 4.5”W x 2”D (14.6cm x 11.4cm x 5.1cm)

Dimension (MRIB): 4.5”H x 3.5”W x 1.75”D (11.4cm x 8.9cm x 4.4cm)

Shipping Weight: 2 lbs (0.9 kg)

Figure 2-44 provides an example of the connections between the MATCH, the reader, the ScramblePad, and the DIGI*TRAC Controller:

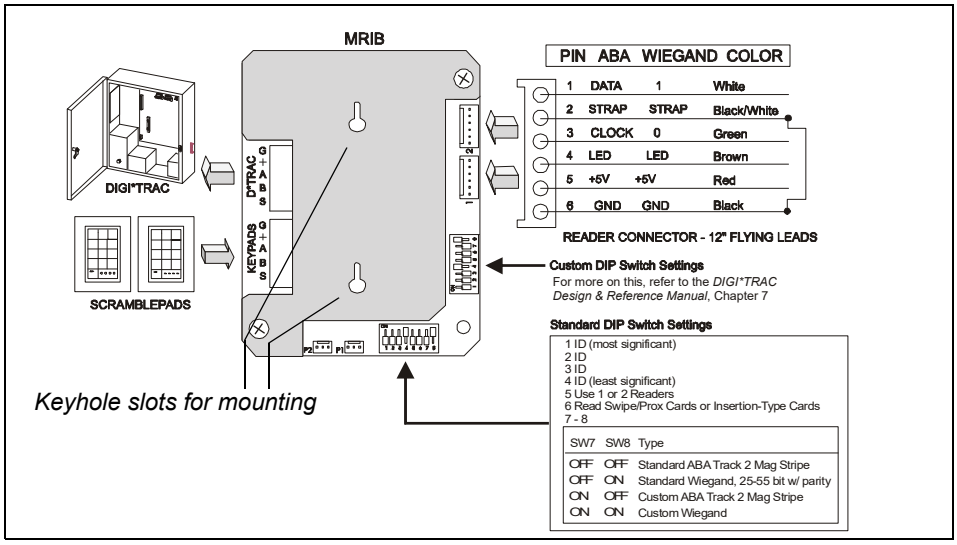


Figure 2-44: MATCH Connections (MATCH2 Shown)

The flying lead which connects the reader to the MATCH through one of two connectors on the board must conform to the wiring standards shown in Figure 2-44.

With a DS47L-series ScramblePad, a reader can be connected at a door without using an additional MATCH. The reader connects to the DS47L (and its integrated MATCH) and

the ScramblePad then connects to the controller, as shown in Figure 2-45.

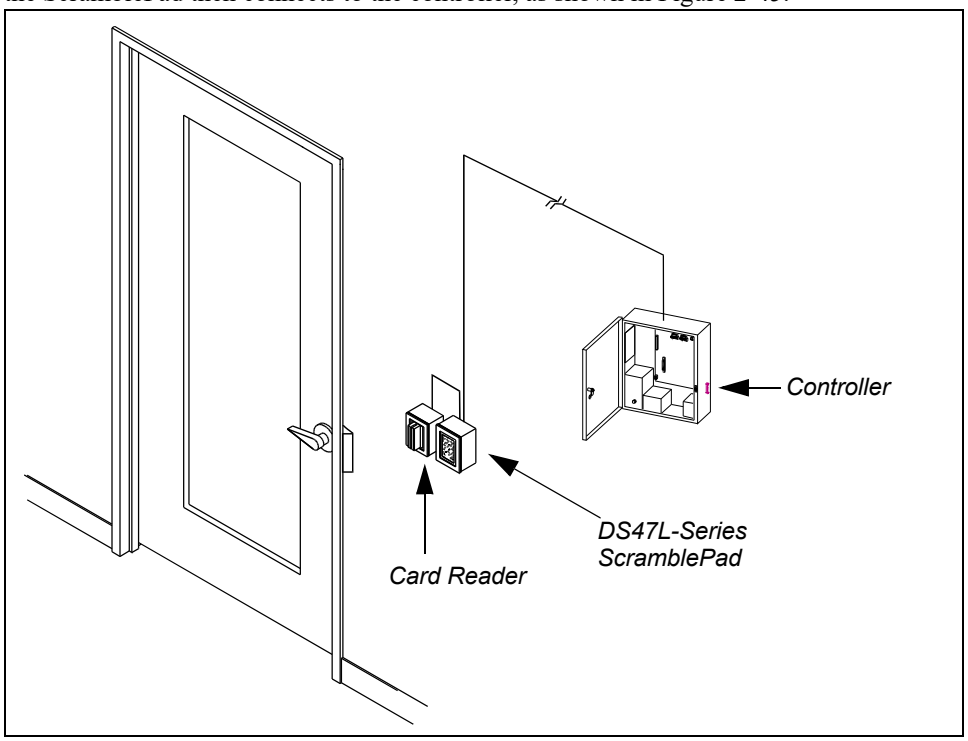


Figure 2-45: Using a DS47L-Series ScramblePad Instead of a Separate MATCH

For more about setting up the MATCH and installing it, see “MATCH Reader Installation” on page 7-145.

When installing a DIGI*TRAC MATCH Enrollment Station (DMES)—which consists of a MATCH Reader Assembly (to connect to an appropriate reader), a DS37L ScramblePad, and an ES2 Enrollment Stand—locate the ScramblePad/Reader tandem close to the controller and its printer. The maximum distance allowed between the DMES and the controller can be figured using Table 2-6 on page 2-16 (refer to the maximums for a MATCH and ScramblePad).

For more on the DMES and SMES Enrollment Stations, see “Enrollment Station Installation” on page 7-325.

MRIA/MRIB Mounting

There are four mounting boxes available for the MRIA: the MB1, MB2, MB3 and MB4. The MRIB is usually mounted in a separate J-Box using the keyhole slots (see Figure 2-44 on page 2-61). Choose the box that fits system requirements.

Note: The MRIA in a Hirsch mounting box supports physical tamper monitoring.

Figure 2-46 shows the available MRIA mounting boxes. For directions on mounting the MRIA in an MB1, MB2, MB3, or MB4 mounting box, see "Installing the Mounting Box" on page 7-97. For instructions on mounting the MRIB, see "MATCH Interface Installation" on page 7-134.

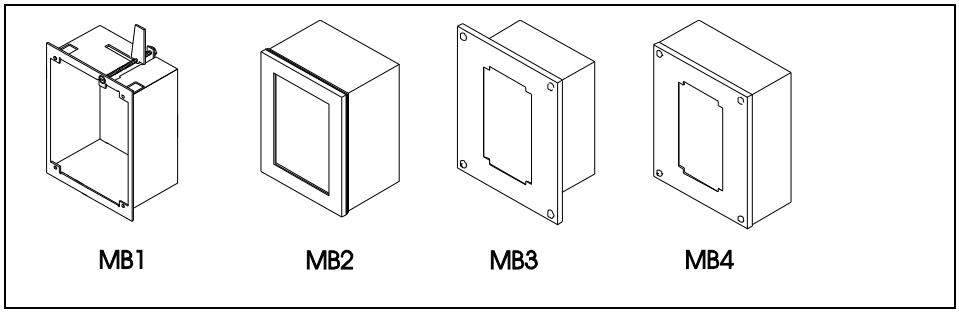


Figure 2-46: Available MRIA Mounting Boxes

MATCH-Compatible Readers

Readers are a general category of access control devices that include:

- ❑ Mag Stripe Card Readers (insertion and swipe)
- ❑ Proximity Card Readers
- ❑ Wiegand Card Readers
- ❑ Biometric Readers (e.g. Hand Geometry, Retinal Scanner)
- ❑ Barcode Readers
- ❑ Infrared Readers
- ❑ Wiegand-Compliant Keypads

When used in conjunction with the MATCH Reader Interface, most readers can communicate with Hirsch DIGI*TRAC controllers. Hirsch's MR11LA includes an MRIA. The MR11LA consists of a CR11L magnetic stripe card reader mounted on an MRIA. The CR11L is small enough to fit within the MRIA bezel.

An example of how an MR11LA might work at a door is shown in Figure 2-47.

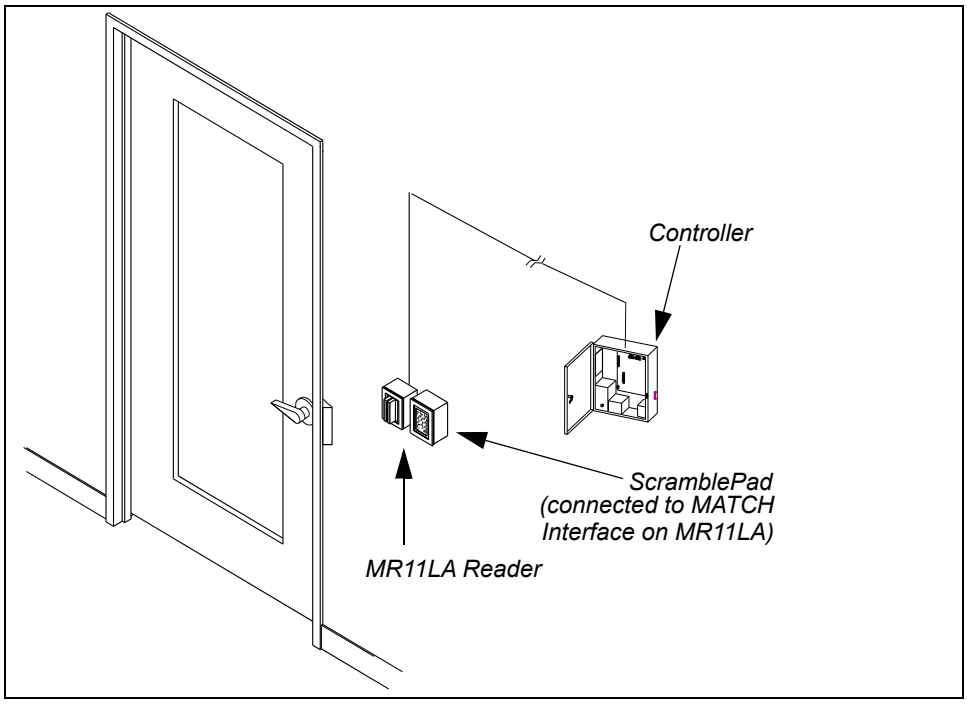


Figure 2-47: MR11LA Example

In addition, the DS47L family of ScramblePads includes an integrated MATCH which can support one or two readers (the D47L-SPX ScrambleProx also includes a built-in proximity reader). All other readers require the purchase of a separate MATCH and the connection of the reader to the MATCH Interface.

A complete list of ScramblePad DS47L readers with the MATCH already installed is shown in Table 2-19.

ScramblePad	**Description**
DS47L	Combines the ScramblePad with a MATCH reader interface.
DS47L-HI	High-intensity version of the DS47L.
DS47L-SPX	ScrambleProx. All-in-one ScramblePad/MATCH reader interface with built-in HID proximity reader. Use HID cards.
DS47L-SPX-HI	High-intensity version of the DS47L-SPX ScrambleProx. Use HID cards.
DS47L-SPX-I	DS47L-SPX ScrambleProx with built-in Indala reader. Use Indala 26-bit cards.
DS47L-SPX-I-HI	High-intensity version of the DS47L-SPX ScrambleProx with built-in Indala reader. Use Indala 26-bit cards.
BQT Readers	
DS47L-SS-BT	ScrambleSmart which incorporates a ScramblePad with an integrated MIFARE smart card reader.
DS47L-SS-BT-HI	High-intensity display version of ScrambleSmart.

Table 2-19: DS47L ScramblePad Types

ScramblePad	Description
DS47L-SS-BT-DF	Same as ScrambleSmart but with integrated MIFARE DESfire smart card reader.
DS47L-SS-BT-HI-DF	High-intensity display version of the ScrambleSmart with integrated MIFARE DESfire smart card reader.
HID Readers	
DS47L-SS-HID	DS47L ScramblePad with embedded 13.56MHz, ISO 14443-4 A&B contactless smart card reader and antenna. Reads PIV II End Point, DESFire (with CHUID only), and iCLASS. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, DESFire with FASC-N encoding, or iCLASS cards.
DS47L-SS-HID-HI	High-intensity display version of DS47L-SS-HID.
DS47L-SS-HID-SN	Same as DS47L-SS-HID but reads MIFARE/DESFire Serial Numbers, and iCLASS. Use MIFARE, DESFire, or iCLASS cards.
DS47L-SS-HID-SN-HI	High-intensity display version of DS47L-SS-HID-SN.
DS47L-SSP-HID	DS47L ScramblePad with embedded 125kHz proximity and 13.56MHz, ISO 14443A&B contactless smart card readers and antennae. Reads PIV II End Point, DESFire (with CHUID only), iCLASS, and HID 125kHz proximity. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, DESFire with FASC-N encoding, iCLASS cards., or HID 125kHZ cards.
DS47L-SSP-HID-HI	High-intensity display version of DS47L-SSP-HID.
DS47L-SSP-HID-SN	Same as DS47L-SSP-HID but reads MIFARE/DESFire serial numbers, iCLASS, and HID 125kHz proximity. Includes MATCH2 functionality. Use MIFARE, DESFire, iCLASS, or HID 125kHZ cards.
DS47L-SSP-HID-SN-HI	High-intensity display version of DS47L-SSP-HID-SN.
Integrated Engineering Readers	
DS47L-SSDM-IE	DS47L ScramblePad with embedded 13.56MHz, ISO 14443-4A contactless smart card reader and antenna. Reads DESFire file system and MIFARE sector cards. PIV II Transition Compliant. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV, IE MIFARE or DESFire cards.
DS47L-SSDM-IE-HI	High-intensity display version of DS47L-SSDM-IE.

Table 2-19: DS47L ScramblePad Types (Continued)

ScramblePad	Description
DS47L-SS-IE	DS47L ScramblePad with embedded 13.56MHz, ISO 14443-4 A&B contactless smart card reader and antenna. Reads PIV II End Point and PIV II Transitional cards including FRAC (SmartMX), DoD alpha & beta, DESFire PIV (V0.6 only), TWIC V1, MMAC, DESFire SN (1st 4bytes), and MIFARE SN. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, MIFARE, or DESFire cards.
DS47L-SS-IE-HI	High intensity display version of DS47L-SS-IE.
DS47L-SSP-IE	DS47L ScramblePad with embedded 125kHz proximity and 13.56MHz, ISO 14443A&B contactless smart card readers and antennae. Reads PIV II End Point and PIV II Transitional cards including FRAC (SmartMX), DoD alpha & beta, DESFire PIV (V0.6 only), TWIC V1, and MMAC.. Includes MATCH2 functionality. One MATCH connector with 6-inch pigtail. Installs in Hirsch mounting boxes (MB2 or deeper). Use PIV II, DESFire with FASC-N encoding, or HID 125kHZ cards.
DS47L-SSP-IE-HI	High-intensity display version of DS47L-SSP-IE.

Table 2-19: DS47L ScramblePad Types (Continued)

All other readers require the purchase of a separate MATCH and the connection of the reader to the MATCH Interface.

Table 2-20 provides a partial list of MATCH-compatible readers. This table also includes the required output type for each reader, the reader manufacturer, the Hirsch model number (where appropriate), and recommended Hirsch cards used with each Hirsch reader.

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
Mag Stripe Readers					
Dorado	512 Insert		32-bit Wiegand		
	512 Insert		ABA		
	612 Swipe		34-bit Wiegand		
	612 Swipe		ABA		
Interflex	Magstripe insertion reader		ABA		
Magtek	21050002 Track 2 Swipe		ABA		
	21050005 Track 3 Swipe		ABA		
	210650004 Track 2 Insert		ABA		

Table 2-20: MATCH-Compatible Readers

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
Mercury	MR10 #36002 Weather Resistant	CR12L	ABA	IDC10	
	30001-0010 Weather Resistant	CR12L-T	ABA	IDC10	
	30001-0010 Weather Resistant	CR12L-T1-28	ABA	ICD10	
	30001-10 Weather Resistant	CR12LLADC-TWC	ABA	IDC10	
MSC	3002-0001-MR-10 Track 2, Swipe		26-bit Wiegand		
Neuron	MCR-570-1R-0902 Track 2, Swipe		ABA		
Omron	3S4YR-HSR4 Track 2, Swipe	CR11L	ABA	IDC10	
	3D4YR-HSR4H Track 2, Swipe, Assembly	CR11LA	ABA	IDC10	
	SBR Track 2, Insertion		ABA		
XICO	3890SD Weather Resistant Swipe		ABA		
Identec Ltd	SR1 10R Weather Resistant Swipe		ABA		
Proximity Readers					
AWID	SR-2400 Prox Reader		26-bit Wiegand		
Casi-Rusco	940 ProxPerfect				
	971 Prox plus keyboard				
	972 ProxLite				
	973 ProxLite				
Checkpoint	Mirage		33-bit Wiegand		1, 2
Cotag	3511 Single Zone		26-bit Wiegand		1
Deister	PRX5		33-bit Wiegand		1
Deister	PRX10		33-bit Wiegand		1
GE	T-520 Contactless				

Table 2-20: MATCH-Compatible Readers (Continued)

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
HID	SS53001N Single Channel Reader/Scanner		26-bit Wiegand		1
	5320-H1N Thin-Line Reader/Scanner		26-bit Wiegand		1
	Short Range ProxPoint - Beige	CR20L-BG			
	Short Range ProxPoint - Black	CR20L-BL			
	Short Range 6005 ProxPoint	CR20L-125			
	5365 BGNOO Short Range Mullion	CR21L-125	26-bit Wiegand	IDC20, 21	1
	5355 AGNBOO Medium Range	CR22L-125	26-bit Wiegand	IDC20, 21, C2K	1
	5455 Medium Range	CR22L-2	26-bit Wiegand		
	5355 AKNOO Long Range	CR23L-125	26-bit Wiegand	IDC20, 21	1
	5375 AKNOO Long Range	CR23L-125D	26-bit Wiegand		
	5385 AGBOO Thinline	CR24L-125	26-bit Wiegand	IDC20, 21	1
	Prox Thinline (Euro-Asian)	CR24L-EA	26-bit Wiegand		
	Multi-Prox reader plug	CR28L			
	230 Prox/Mag Stripe Reader				
Identec Ltd	RL1-AAG Indoor		26-bit Wiegand		1
Indala	PR-10 Indoor		26-bit Wiegand		1
	PR-3 Mullion		26-bit Wiegand		1
	ASR-110 Indoor	CR-ASR-110 BG	26-bit Wiegand	IDC20, CPM-H[a]	1
	ASR-110 Outdoor	CR-ASR-110 BL	26-bit Wiegand	IDC20, CPM-H	1
	ASR-112 Indoor	CR-ASR-112	26-bit Wiegand	IDC20, CPM-H	1
	ASR-120 Indoor	CR-ASR-120 BG	26-bit Wiegand	IDC20, CPM-H	1
	ASR-124 26-Bit Extended Range	CR-ASR-124	26-bit Wiegand	IDC20, CPM-H	1
	ASR-136 26-Bit Extended Range	CR-ASR-136	26-bit Wiegand	IDC20, CPM-H	1
	ASR-500 ValueProx	CR-ASR-500	26-bit Wiegand	IDC20, CPM-H	1
	ASR-503 Slimline	CR-ASR-503	26-bit Wiegand	IDC20, CPM-H	1
	ASR-505 WallSwitch	CR-ASR-505	26-bit Wiegand	IDC20, CPM-H	1
	ASR-605 Arch	CR-ASR-605	26-bit Wiegand	IDC20, CPM-H	1
	ASR-620-BL	CR-ASR-620-BL	26-bit Wiegand		
	ASR-650	CR-ASR-650	26-bit Wiegand	IDC20, CPM-H	
	FlexPass Wave Mid-Range	CR-FP1231A	26-bit Wiegand		
	FlexPass Wave Slim	CR-FP1511A	26-bit Wiegand		
	FlexPass Wave Wall-Switch	CR-FP1520A	26-bit Wiegand		
	FlexPass Curve Mid-Range	CR-FP2231A	26-bit Wiegand	IDC20	
	FlexPass Curve Slim	CR-FP2511A	26-bit Wiegand	IDC20	
	FlexPass Curve Wall-Switch	CR-FP2521A	26-bit Wiegand		

Table 2-20: MATCH-Compatible Readers (Continued)

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
Indala (cont.)	FlexPass Arch Mid-Range	CR-FP3231A	26-bit Wiegand		
	FlexPass Arch Slim	CR-FP3511A	26-bit Wiegand		
	FlexPass Arch Wallswitch	CR-FP3521A	26-bit Wiegand		
	FlexPass Linear Slim (Black)	CR-FP4511A			
	FlexPass Linear Slim (White)	CR-FP4516A			
	FlexPass Linear Wall-Switch (Black)	CR-FP4521A			
	FlexPass Linear Wall-Switch (White)	CR-FP4526A			
	FlexPass Linear Wall-Switch (Beige)	CR-FP4527A			
	FlexPass Linear Magstripe Style	CR-FP4551A	26-bit Wiegand	IDC20, CPM-H	
Keri	MCR-403 InStar Prox Reader		26-bit Wiegand		
Motorola	FlexPass Linear Magstripe Style	CR-FP4551A	26-bit Wiegand	IDC20, CPM-H	
	FlexPass Arch Wallswitch DSX-2L	CR-FP3521A 33	35-bit Wiegand		
Pyramid	P-600 Prox/Keypad Reader				
Rosslare	AY-K12B Prox Reader		26-bit Wiegand		
Transition	XCEED FX-2100-B Contactless				
Wiegand Readers					
Cardkey	L40-G Swipe				2, 3
eSecure	iWiegand Reader		26-bit Wiegand		
Hirsch/ Sensor	3100990 Swipe	CR31L		IDC30,33	
	3121260 Insertion	CR32L		IDC30,33	
	3130180 Key Swipe	CR33L		IDC30,33	
	3140190 Turnstile	CR34L		IDC30,33	
	30387 Swipe				
	32005 Key				
	31880 Insert				
	Reader Module Swipe				
Barcode Swipe Card Readers					
ABR	TAGIT Button Tag	CR-BR61L	26-bit Wiegand	IDC80	4
Barcode Automation	BA-200 Barcode Swipe		26-bit Wiegand		
	BAI Vehicle Barcode Reader	CR-VBC			
IBC	SSLOT1 Barcode Swipe		26-bit Wiegand		
ICI	8035 Barcode Swipe		26-bit Wiegand		
	8035-SMT Barcode Swipe		26-bit Wiegand		5
Jantek	MK-2000 Barium Ferrite Swipe		26-bit Wiegand		
RCSI	RF Commercial Receiver		26-bit Wiegand		1, 6

Table 2-20: MATCH-Compatible Readers (Continued)

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
Securitron	IRC Infrared Receiver & IRT-1 Single Button Transmitter		26-bit Wiegand		1
Sentex	CR26 RF Radio Receiver	CR91L	26-bit Wiegand	IDC90	1
Time Keeping Systems	TKS-ACM-110 Barcode Swipe	CR51L	26-bit Wiegand	IDC50	
	TKS-ACM-VL110 Visual Light Barcode Swipe	CR51L-VL	26-bit Wiegand	IDC50	
	AC MIL-DOD	CR51L-DOD	26-bit Wiegand	IDC50	
Biometric Readers					
BioScrypt	VeriFlex Fingerprint	CR-BIO-VF	26-bit Wiegand		
	VeriProx Fingerprint Prox	CR-BIO-VFP	26-bit Wiegand		
	VeriPass Fingerprint Local	CR-BIO-VP	26-bit Wiegand		
Cogent	Local Bio Reader	CR-BIO-CG-L			
	External Bio Reader	CR-BIO-CG-LEXT			
EyeDentify	8.5 Retina Scan Biometric		26-bit Wiegand		1
Indentix	Touchlock Finger Print		26-bit Wiegand		1
LG	MIB 4000 Iris Recognition		26-bit Wiegand		
Panasonic	BM-ET300 Iris Reader				
Recognition Systems	ID3D-R HK Hand Key Reader		ABA		1
	Infrared HK-2 Hand Key Reader		26-bit Wiegand		
Sagem	MA100 Fingerprint Reader	CR-BIO-MA100	26-bit Wiegand		1
	MA110 Fingerprint Reader	CR-BIO-MA110			
	MA120 MIFARE Fingerprint	CR-BIO-MA120			
	MA120 PIV Fingerprint	CR-BIO-MA120W			
	MA521T TWIC Fingerprint	CR-BIO-MA521T			
	MA521T-O TWIC Fingerprint	CR-BIO-MA521TO			
Schlage	HK-2 Hand Reader	CR-BIO-HAND			

Table 2-20: MATCH-Compatible Readers (Continued)

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
SmartCard Readers					
BQT	E/A MIFARE	CR-BT815W	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	E/A DESFire	CR-BT815W-DF	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	DESFire/MIFARE	CR-BT815W-SN	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	SmartCard Reader - DESFire	CR-BT900W	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	SmartCard Reader - DESFire	CR-BT900W-DF	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	DESFire/MIFARE	CR-BT900W-SN	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	BioSmart SmartCard - MIFARE	CR-BT910W	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	BioSmart SmartCard - PIV	CR-BT910W-DF	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	BioSmart SmartCard - MIFARE/ MIFARE	CR-BT910W-SN	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
	SmartCard Biometric	CR-BT910X	36-bit Wiegand	IDC100-BT/IC, PVC-CS series	
Cogent	MIFARE Fingerprint SmartCard	CR-BIO-CG-M			
	MIFARE External Fingerprint SC	CR-BIO-CG-MEXT			
HID	FlexSmart Series 6075		Wiegand		
	iClass - Mullion MIFARE	CR-ICR10	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Mullion PIV/DESFire	CR-ICR10PIV	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass -Mullion MIFARE/DESFire	CR-ICR15	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Mullion PIV/DESFire	CR-ICR15PIV	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Mullion MIFARE/DESFire Prox	CR-ICRP15	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Mullion MIFARE/DESFire Indala Prox	CR-ICRP15-I	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Mullion PIV/DESFire Prox	CR-ICRP15-PIV	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Mullion PIV/DESFire Indala Prox	CR-ICRP15-PIV-I	Wiegand	IDC100-AT/ IC, PVC-CS-IC	

Table 2-20: MATCH-Compatible Readers (Continued)

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
HID (cont.)	iClass - E/A MIFARE/DESFire	CR-ICR30	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - E/A PIV/DESFire	CR-ICR30PIV	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Wallswitch MIFARE/DESFire	CR-ICR40	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Wallswitch PIV/DESFire	CR-ICR40PIV	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Wallswitch Keypad Smart-Card Reader	CR-ICRK40	Wiegand		
	iClass - Wallswitch MIFARE/DES-Fire Prox	CR-ICRP40	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Wallswitch MIFARE/DES-Fire Indala Prox	CR-ICRP40-I	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Wallswitch PIV/DESFire Prox	CR-ICRP15-PIV	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - Wallswitch PIV/DESFire Indala Prox	CR-ICRP15-PIV-I	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	iClass - R90 Long-range SmartCard	CR-ICR90	Wiegand	IDC100-AT/ IC, PVC-CS-IC	
	G2 DESFire/MIFARE SmartProx	CR-G2SP-M			
	G2 Single-Gang CP SmartCard	CR-G2S-SGCP			
	G2 MIFARE SSN SmartCard	CR-G2SSN	34-bit SMF SN		
Hirsch	RUU PIV Biometric SmartCard	CR-BIO-RUU-PIV			
	RUU CAC Biometric SmartCard	CR-BIO-RUU-CAC			
	RUU GEN Biometric SmartCard	CR-BIO-RUU-GEN			
Integrated Engineering	SmartID DESFire Card Reader	CR-IEM-DF75	Wiegand ABA		
	SmartReader, SmartID, SmartID Pro, SmartLogin		Wiegand		
LG	ICU-4000 SmartCard Reader	CR-BIO-ICU4000-W	Wiegand		
	ICU-4300 SmartCard Reader	CR-BIO-ICU4300-W	Wiegand		
Transcore	SmartPass AI-1620				

Table 2-20: MATCH-Compatible Readers (Continued)

Company	Model Name/No.	Hirsch Model	Output	Cards	Notes
MATCH-Compliant (Non-ScramblePad Keypads)					
Essex	KTP-163 ruggedized keypad (dual reader)		26-Wiegand		2
HID	HID 5355 keypad (dual reader)		26-Wiegand		2
	HID 240 prox/magstripe/keypad				
	iCLASS RK40 smart card keypad				
	iCLASS RP/RPK40 smart card readers with keypad		75-bit & 64-bit FASCN/PIV		
IEI	SSWFX Wiegand keypad		26-Wiegand		
Piezo	PiezoProx Keypad Prox Reader		26-Wiegand		
SCM	Contact/Contactless MIFARE/ DESFire/PIV	CR-SCM-CCL	34-bit Wiegand		
	Contact/Contactless MIFARE/ DESFire/PIV with keypad	CR-SCM-CCLK	36-bit Wiegand		
	Contact/Contactless MIFARE/ DESFire/PIV with MRIA	DS47L-MRIA-SCM-CCL	34-bit Wiegand		
Infrared and Long-Range Readers					
Hirsch	RF Receiver Long Range	CR91L	26-bit Wiegand		
Nedap	Transit AVI Long Range (EurAsian)	CR-NMR	26-bit Wiegand	IDC-PP, CR-N*x*	
	Transit AVI Long Range (U.S.)	CR-NMRU	26-bit Wiegand	IDC-PP, CR-N*x*	
	PS-70 Transit Long Range			IDC-PP, CR-N*x*	
Miscellaneous Readers and Devices					
Secura Key	SK-034WK Barium Ferrite Slotless Touch Card Reader		31-bit Wiegand	IDC40	1
	SK-034W Barium Ferrite Slotless Touch Card Reader		30-bit Wiegand	IDC40	1
	SK-028C Barium Ferrite Slotless Touch Card Reader		27-bit Wiegand	IDC40	1
	SK-029W Barium Ferrite Touch	CR41L	27-bit Wiegand	IDC40	1
	SK-038W Barium Ferrite Slotless Touch Card Reader		47-bit Wiegand	IDC40	1
BQT	AEB Encryption Extenders	ENC-M4			

Table 2-20: MATCH-Compatible Readers (Continued)

a. The Indala IDC21 has been replaced by the HID PVC CPM-H.

Note Codes

1. Requires separate power supply.
2. Requires unique ROM configuration. Consult Hirsch for details.
3. Requires an interface board
4. Comes with switchplate.
5. Available only from Hirsch.
6. Single and dual button transmitters.

For an up-to-the-minute list of all readers compatible with the MATCH and DIGI*TRAC

controllers, refer to Hirsch's website, **www.hirschelectronics.com**.

Which Reader or Keypad Is Right?

The keypads/readers shown in the previous section are designed for many different conditions and environments. To select the keypad or reader that is correct for a specific location, use Table 2-21.

Reader Types	Security	Cost	Ease of Use	User Throughput	User Acceptance	Weather Resistance	Vandal Resistance
Keypad (Generic)	Low	Low	Easy	Moderate	Moderate	Moderate	Moderate
ScramblePad™	High	Moderate	Moderate	Moderate	High	Moderate	Moderate
Magnetic Stripe	Low	Low	Moderate	Moderate	Moderate	Poor	Poor
Bar Code	Low	Low	Low	Moderate	Moderate	Poor	Poor
Wiegand	High	Moderate	Moderate	Moderate	Moderate	Good	Good
Proximity	High	High	Easy	Fast	High	Moderate	Moderate
Touch Memory	High	Moderate	Moderate	Moderate	Moderate	Poor	Good
Radio Frequency	Moderate	High	Easy	Fast	Moderate	Moderate	Poor
Finger Print	High	High	Difficult	Slow	Low	Poor	Poor
Hand Geometry	High	High	Difficult	Slow	Low	Poor	Poor
Retinal Scan	High	High	Difficult	Slow	Low	Poor	Poor

Table 2-21: Reader Technology Selection

where:

'Security' refers to resistance to unauthorized duplication or creation.

'Cost' includes installation and cards or tokens, where applicable.

Note: The selection criteria ratings by reader are for general applications. Specific mounting, use, and other factors can vary the ratings slightly, but the relative ratings for a specific application are usually consistent.

For a complete list of Hirsch-compatible reader wiring diagrams, refer to the Hirsch Reader Library (Hirsch # 020**)**.

Line Modules

Line Modules are a necessary component of the line module input circuits from the controller. In addition to providing supervision of the wiring from a controller, the line module also supports a request to exit (RQE) input and a tamper input.

Line Modules provide supervision by indicating when a circuit is shorted, opened, noisy and/or out-of-spec. These conditions are usually considered attempts to breach the security of the system and are therefore monitored and reported on an input-by-input basis at all times for enabled inputs. The controller digitally processes the analog measurement of the circuit resistance at an effective 100 times per second rate. The circuit measures variation in conditions (±2% with the DTLM3 Line Module and ±4% with the DTLM1/2 Line Modules) then reports any appropriate alarms upon detection.

Hirsch provides two types of line modules:

- ❏ DTLM (Screw Terminals)
- ❏ MELM (Flying Leads)

There is also a door contact with integral line module:

- ❏ SBMS3-2707A

Each line module type is explained in this section. For detailed information on setup, mounting, and installation of line modules, see “Line Module Installation” on page 7-313.

DTLM

The DIGI*TRAC line module (DTLM) provides terminal block connections. It is recommended that DTLMs be limited to a single sensor per input. The DTLM is used for the RQE, Auto-Relock, Door Forced, and Door Open Too Long (DOTL) functions. There are three types of DTLM:

- ❏ The DTLM1 has one input and is used for alarm applications with ±4% sensitivity.
- ❏ The DLTM2 has two inputs and is used when an RQE device is required to mask the line module input and, optionally, trigger the door lock with ±4% sensitivity.
- ❏ The DTLM3 has three inputs and is used in high security applications where alarm, RQE, and tamper detection are required with ±2% sensitivity.

DTLM inputs are labeled 1, 2, and 3 for simplicity in which 1 normally connects to the door contact or alarm sensor, 2 connects to the RQE, and 3 monitors a Tamper switch.

Model	Terminals & Functions			
	HI LO	INPUT 1	INPUT 2	INPUT 3
DTLM1	DIGI*TRAC	Alarm		
DTLM2	DIGI*TRAC	Alarm	RQE	
DTLM3	DIGI*TRAC	Alarm	RQE	Tamper

Table 2-22: DTLM Wiring

As shown in Figure 2-48, the default configuration for line module input circuits is normally closed. For a closed circuit, the controller instantly reports an alarm for any attempt to tamper with or cut the circuit. For a normally open circuit, the circuit cannot be monitored and tampering goes undetected. All input devices must be isolated ‘dry contact’ types. (A dry contact is a switch or relay which provides no power to the circuit.)

Figure 2-48 provides a representation of the DTLM wiring:

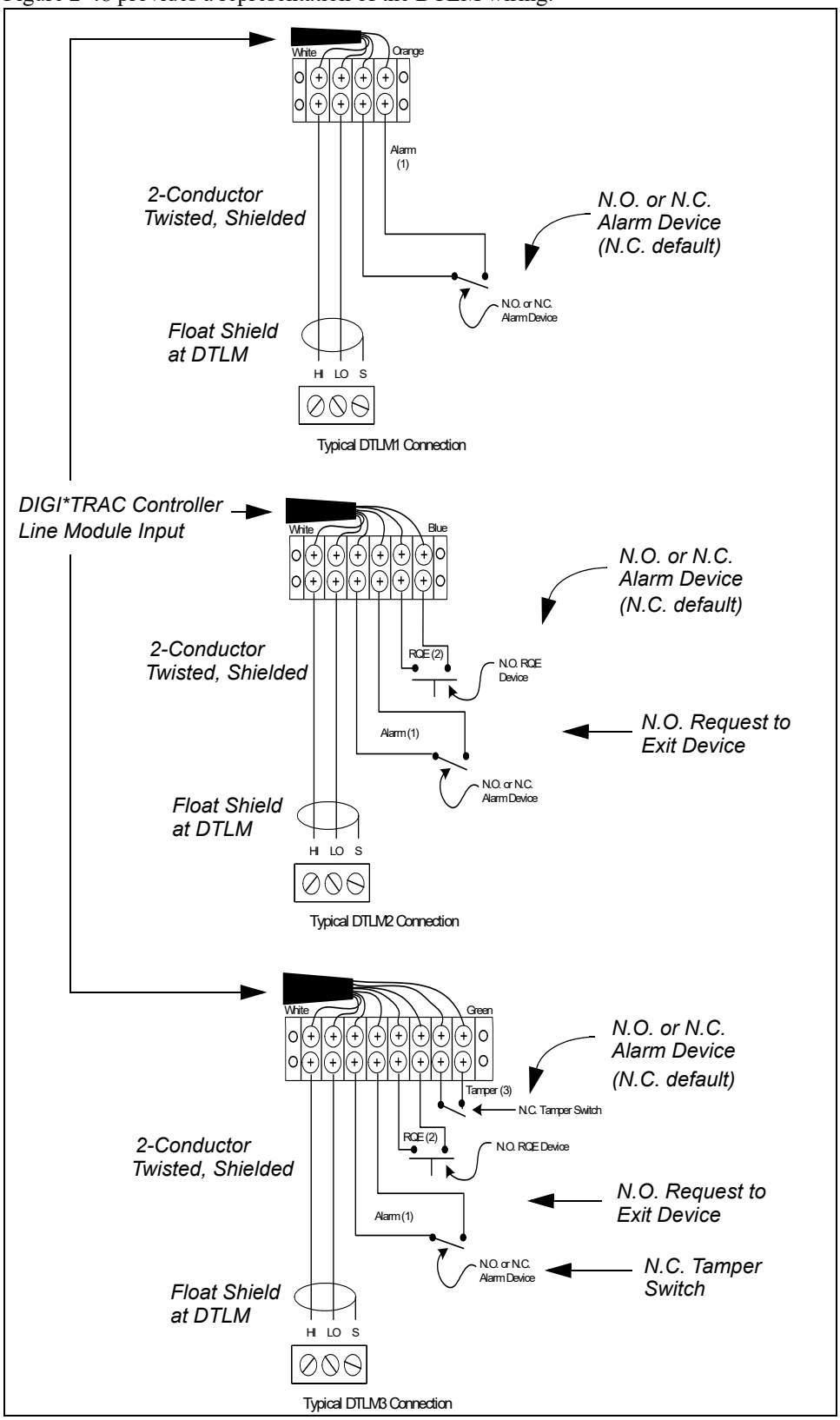


Figure 2-48: DTLM Wiring

Confirm the polarity of the HI / LO terminals at both ends of the DTLM cable run. HI must be linked to HI; LO must be linked to LO. Connect the shield at the controller terminal and let it float (don't connect it) at the DTLM end.

A separate cable is required from the controller to the DTLM. ScramblePad/MATCH reader cable (2-pair stranded, twisted overall shield) and DTLM cable (1-pair stranded, twisted, overall shield) can be run together in the same conduit; however, each pair *must be individually shielded*.

It is recommended that the DTLM should be as close to the sensor(s) it connects as possible for optimum performance.

The dimensions and shipping weight for each DTLM is shown in Table 2-23:

Model	Dimensions (Length x Width x Height) for each
DTLM1	2-1/8" x 1-3/8" x 3/8" (5.5cm x 3.5cm x 1.1cm)
DTLM2	2-7/8" x 1-1/2" x 3/8" (7.5cm x 3.7cm x 1.1cm)
DTLM3	3-5/8" x 1-1/2" x 3/8" (9.3cm x 3.7cm x 1.1cm)
Shipping Weight: 1 lb (0.45 kg)	

Table 2-23: DTLM Dimensions

For maximum cable lengths between the controller and each DTLM module, see "Typical Line Module Inputs" on page 2-12. For detailed information on installation of DTLM, see "Wiring the DTLM Line Module" on page 7-315.

MELM

The MELM (Miniature Embedded Line Module) performs the same functions as a DTLM, except it is much smaller and has flying leads instead of terminal connections. It is ideal for installation inside the RQE or alarm device housing. MELMs provide a pair of flying leads per input:

- ❑ The MELM1 has one input and is used for alarm applications.
- ❑ The MELM2 has two inputs and is used when an RQE device is required to mask the line module input and, optionally, trigger the door lock.
- ❑ The MELM3 has three inputs and is used in high security applications where alarm, RQE, and tamper detection are required with ±2% sensitivity.

Instead of marked terminals, the MELM has colored wires (flying leads) as shown in Table 2-24.

Model	Wire Pair Colors & Functions			
	HI (white) LO (black)	**Orange**	**Blue**	**Green**
MELM1	DIGI*TRAC	Alarm		
MELM2	DIGI*TRAC	Alarm	RQE	
MELM3	DIGI*TRAC	Alarm	RQE	Tamper

Table 2-24: MELM Wiring

As shown in Figure 2-49 on page 2-79, the default configuration for line module input circuits is normally closed. For a closed circuit, the controller instantly reports an alarm for

any attempt to tamper with or cut the circuit. For a normally open circuit, the circuit cannot be monitored and tampering goes undetected.

The dimensions and shipping weight for the MELM is shown in Table 2-25:

Model	Dimensions (Length x Diameter) for each
MELM1–3	1” x 1/2” (2.5cm x 1.3cm)
Shipping Weight: 1 lb (0.45 kg)	

Table 2-25: MELM Dimensions

For maximum cable lengths between the controller and each MELM module, see “Typical Line Module Inputs” on page 2-12. For detailed information on installation of MELM, see “Wiring the MELM Line Module” on page 7-318.

Wiring for the MELM line modules is shown in Figure 2-49:

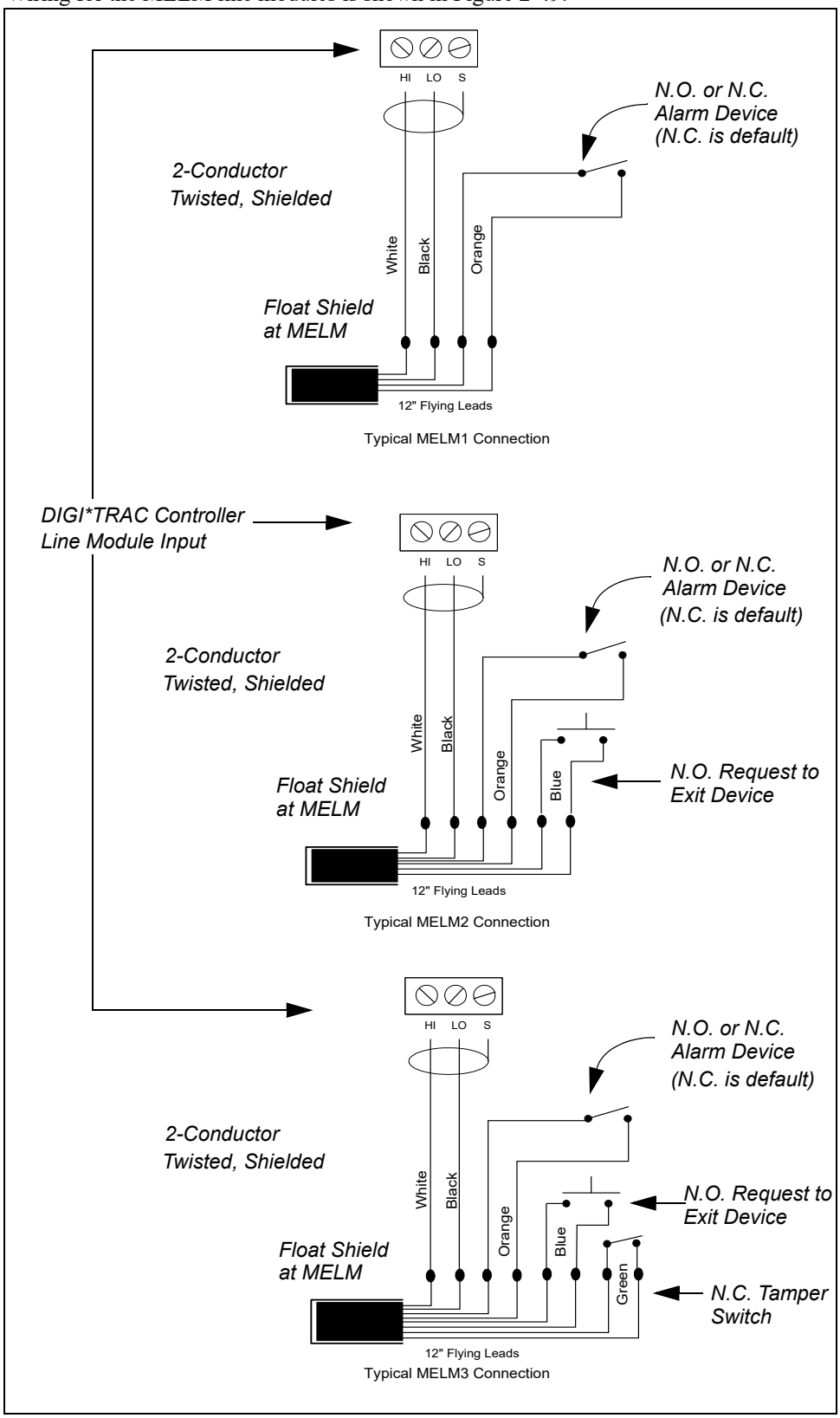


Figure 2-49: MELM Wiring

SBMS3

The SBMS3-2707A consists of a balanced magnetic switch (Sentrol Model #2707A-L14) with an MELM3 factory installed. This door contact is tamper protected and wiring is supervised all the way to the unit without an external line module. External wires are available for connecting the DIGI*TRAC controller and an RQE device.

For more on the SBMS3, see “Door Contacts” on page 2-80. For information on the setup and installation of SBMS3, see “Mounting and Wiring the SBMS3” on page 7-320.

Request-To-Exit Devices (RQE)

RQEs are for doors that are either:

1. Being monitored by the access control system, or
2. Equipped with a magnetic lock.

There are several types of RQE devices which include:

- ❑ Exit Bar with switches built into the door hardware
- ❑ Push Buttons
- ❑ Motion or Presence Sensors

The purpose of an RQE is to mask the alarm on an authorized exit and unlock the lock if required. They can be setup to trigger once only, or to continually retrigger while actuated (for use with motion detector RQE devices).

An RQE may also be used as a remote door release at a receptionist station permitting the entry of visitors requesting access.

Note: Make certain that the use of RQE devices are in compliance with local building safety codes.

An alternative to an RQE is a ScramblePad or Reader. A ScramblePad/Reader can be used as an exit device that logs users out of the secure area. It is slower than an exit bar or sensor, but provides an audit trail, recording the identity of the personnel who exits a room or facility. Exit ScramblePads or Readers are also required for specialized passback control as well as occupancy tracking and control applications.

For maximum cable lengths between the controller and each RQE, see “Typical Door Relay Outputs” on page 2-13.

Door Contacts

Door Contacts are devices which sense whether the door is open or closed. Most modern door contacts are two-piece magnetic devices, with one part installed on the door frame and the other part installed on the door itself. For normally closed contacts, when the door is closed, the contact is closed; when the door is open, the contact is open. Since the door contact is usually a simple circuit, any attempt to tamper with the contact will also produce an open condition and trigger the device.

All door contacts must be connected to line modules and may be either normally open or normally closed devices.

Hirsch provides a very secure door contact, the SBMS3, which includes an integrated MELM3 module. Because the line module is combined with the door contact, any attempt to tamper with the door contact will trigger the MELM3’s tamper alarm.

Figure 2-50 provides an illustration of the most common door contact.

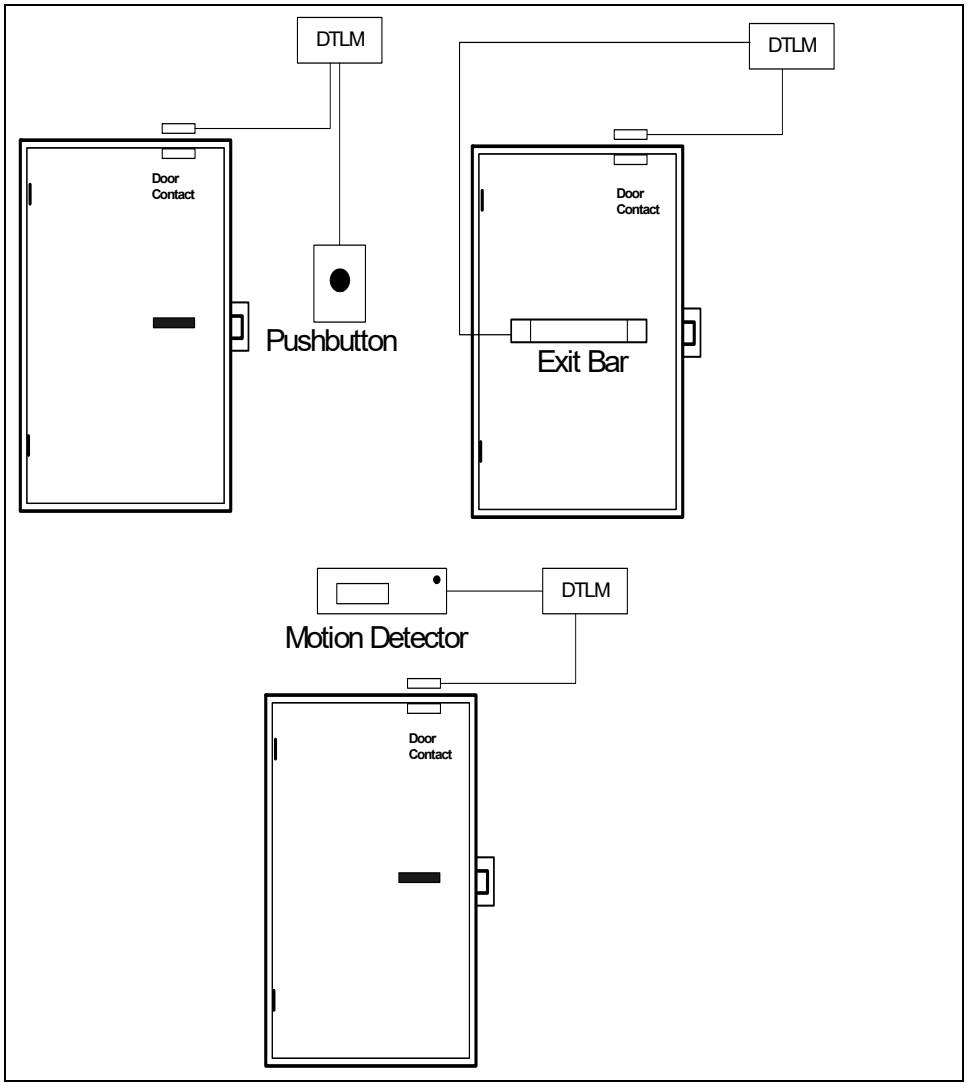


Figure 2-50: RQE and Door Contact Devices

For maximum cable lengths between the controller and each door contact, see “Typical Door Relay Outputs” on page 2-13.

Remote Output Components

This section includes design notes on the following devices:

- ❑ Locks/Strikes
- ❑ Doors
- ❑ Gates
- ❑ Turnstiles
- ❑ Elevators
- ❑ HVAC/Lighting
- ❑ Printers
- ❑ DIGI*TRAC Annunciator

Locks/Strikes

Installing electric strikes or magnetic locks requires specific training and skills. In new construction projects, electrified hardware is often supplied by hardware distributors and installed by the general contractor. Be aware that often these devices are not properly installed and checked out by the contractor. If these devices do not work properly, the entire security system will not be acceptable.

If you are not comfortable with installing a locking device, the best choice might be to subcontract the lock work to a qualified industrial locksmith. There are many choices in electrified hardware depending on door and frame conditions. It is possible to violate building and fire codes by substituting improper electric locks for existing mechanical hardware. If you have any doubts, get help.

For detailed information on installation of locks and strikes, see “Door Relay Installation: Strikes and Locks” on page 7-321.

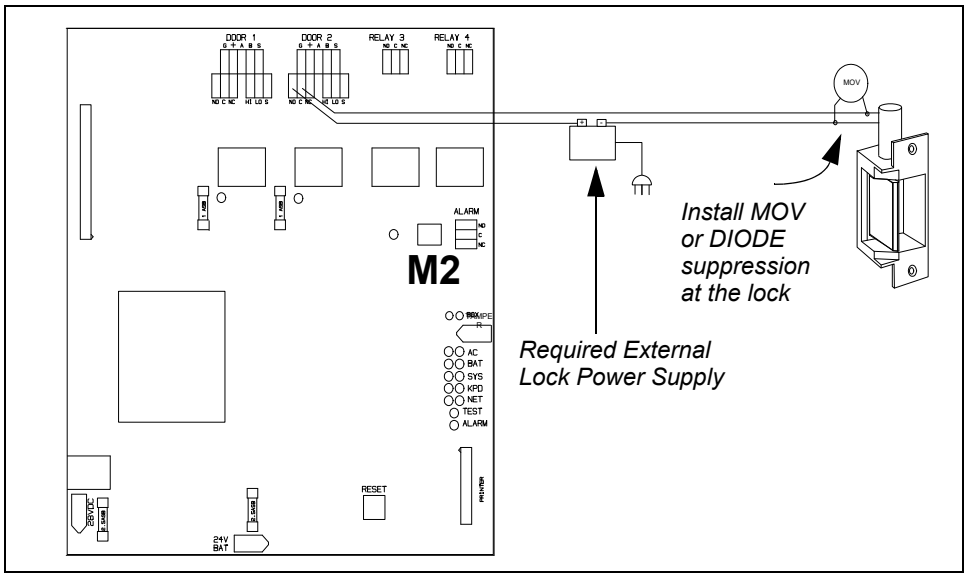


Figure 2-51: Lock-to-Controller Wiring

To determine the maximum distance for lock power cable in feet and (meters) for a particular application, see “Typical Door Relay Outputs” on page 2-13.

When using a PS2 power supply, the DIGI*TRAC relays used to unlock the door do not switch lock power through their contacts. The Hirsch PS2 electric lock power system provides a pair of isolation relays. This approach provides for greater distances between the controller and the locking device.

For the recommended distances between the PS2 and the locking device, use the distance formula and table described in “Using the PS2 Power Supply” on page 2-44.

Alarm Relays

Alarm relays are dedicated relays for interface to local alarm annunciators or remote monitoring stations through digital communicators.

M1N	The M1N uses control relay #4 for this purpose.
M2 **M16**	The M2 and M16 have one alarm relay. The four alarm types that can trigger this relay are: general alarms, duress alarms, tamper alarms and trouble alarms (see Table 1-3 on page 1-17 for alarm descriptions). All alarms are fully programmable.
M8 **MSP-8R** **M64**	The M8, MSP-8R, and M64 have four alarm relays—one each for general alarms, duress alarms, tamper alarms and trouble alarms.

When an alarm condition occurs, a DIGI*TRAC controller can activate the alarm relay for a programmable time based on default settings or operator-selected control settings, using the DIGI*TRAC Control Language.

For more about programming relays, refer to Commands 261, 262, and 263 starting on page 4-187.

In addition to routing alarm conditions to alarm relays, the user can also route alarm conditions to unused on-board door relays or expansion board relays, as required. For example, by using Command 262, an alarm condition can be programmed to trigger a control zone, thereby causing special control conditions or annunciation to take place.

Figure 2-52 shows the default alarm relay configurations for the DIGI*TRAC controllers.

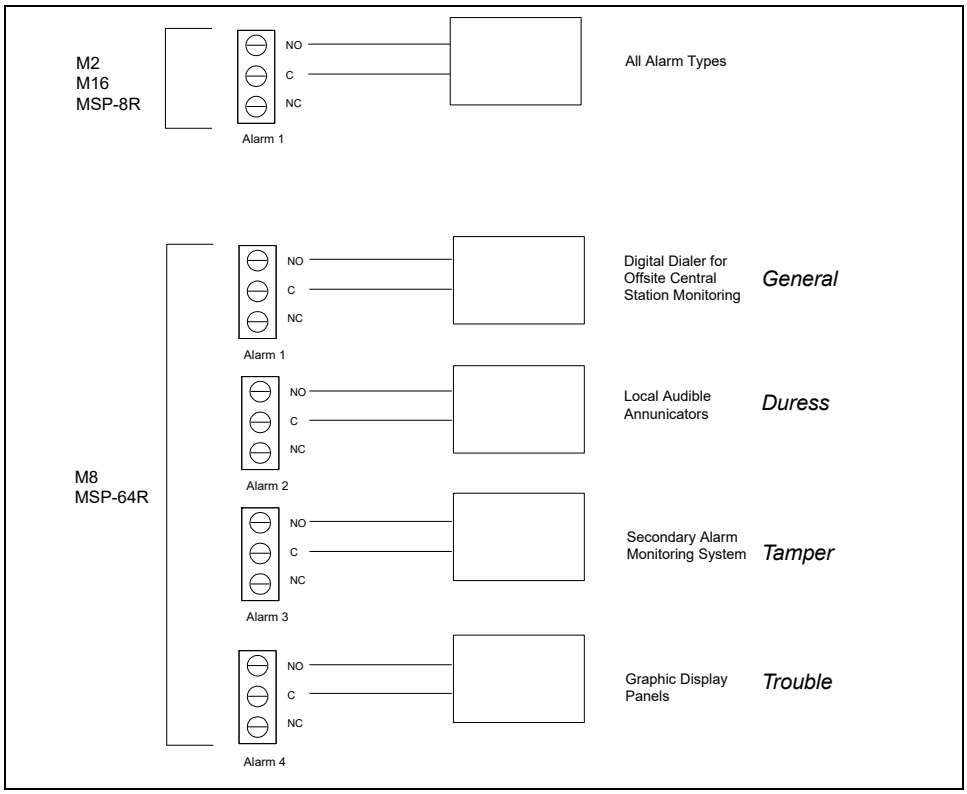


Figure 2-52: Alarm Relays

Doors

Doors can be thought of as a grouping of relays, alarm inputs, and readers\keypads. In most configurations, a door is comprised of one relay, one alarm input, and an entry and/or exit reader/keypad. When defining these three components for a door, make sure they are wired to the controller in a logical manner. For example, when connecting the components of Door 1 to the controller, make sure to wire the alarm input to Input 1 on the controller and the relay for that door to Relay 1 on the controller. You wouldn't want to connect the relay for Door 2 to Relay 1 on the controller anymore than you would want to connect Input 2 on the controller to the input on Door 1. Hirsch controller firmware makes certain assumptions about door logic, the most important being that relays, inputs, and readers are grouped by door. In fact, the concept of control zones does not work properly unless you have wired the components for each door to the controller in a logical manner.

The large heavy-duty socketed relays found on the M2 and M8 controller board are used to switch electric lock power and are rated for 24V DC, 10Amp loads. If a door must be kept locked, there are typically two types of locks utilized:

- ❏ Electric Strikes
- ❏ Magnetic Locks

Electric Strikes can be either 12- or 24-VDC and are either fail safe (unlocked when de-energized) or fail secure (locked when de-energized), though most are fail secure. Magnetic locks can also be either 12- or 24-VDC and are fail safe devices only. Both types require installation of either an MOV (for AC and DC) or diode (DC only) at the lock unless the lock provides its own power suppression. Figure 2-53 provides examples of Electric Strike and Magnetic Lock Doors.

For more about doors, see “Door Contacts” on page 2-80.

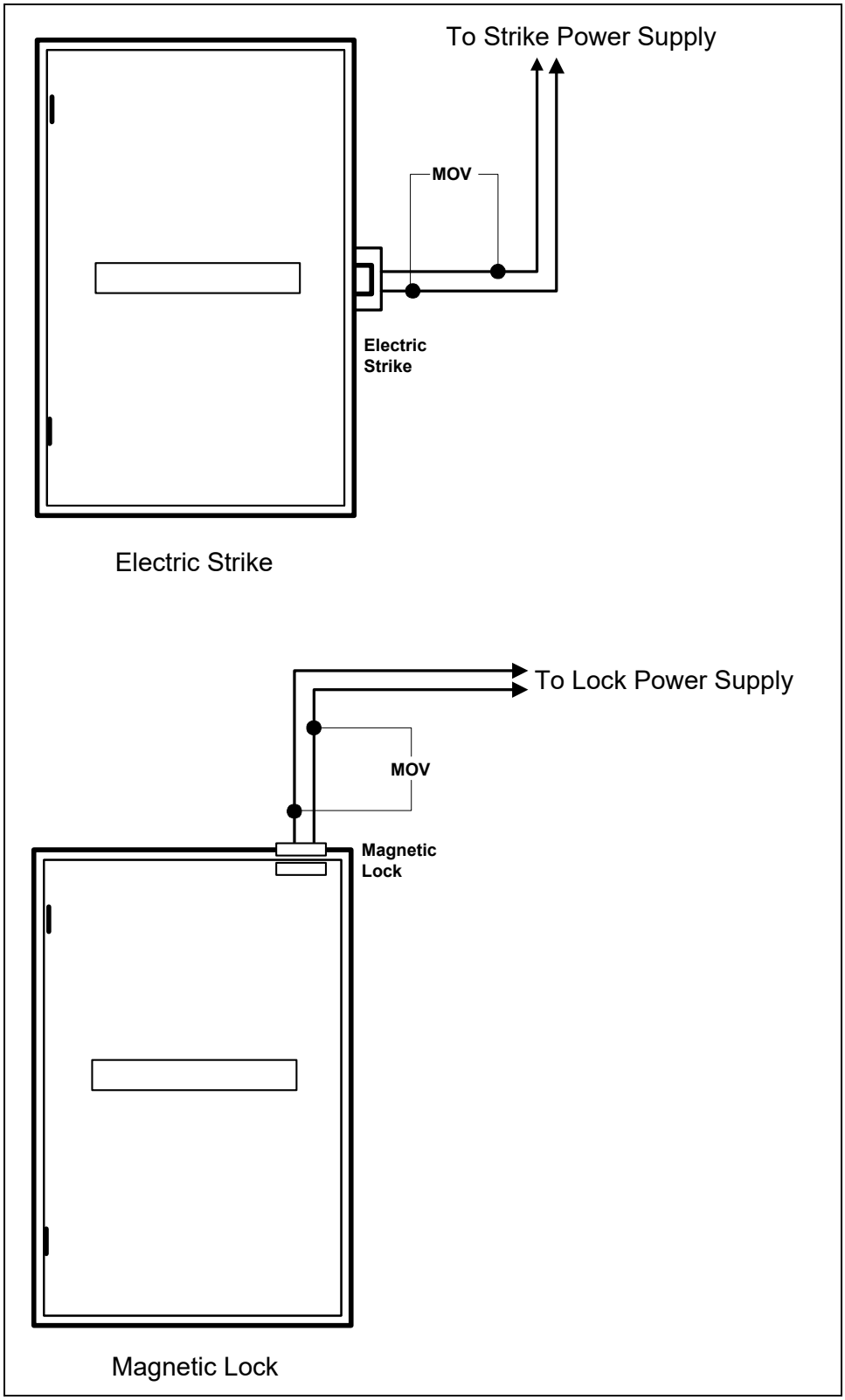


Figure 2-53: Electric and Magnetic Lock Wiring

Gates

The relay from the controller is normally tied into a self-powered input on the gate control system. Do not run gate motor voltages of 50V AC or higher through the relays in a DIGI*TRAC Controller. Instead, use an interposing relay when controlling the gate control system's gate motor directly.

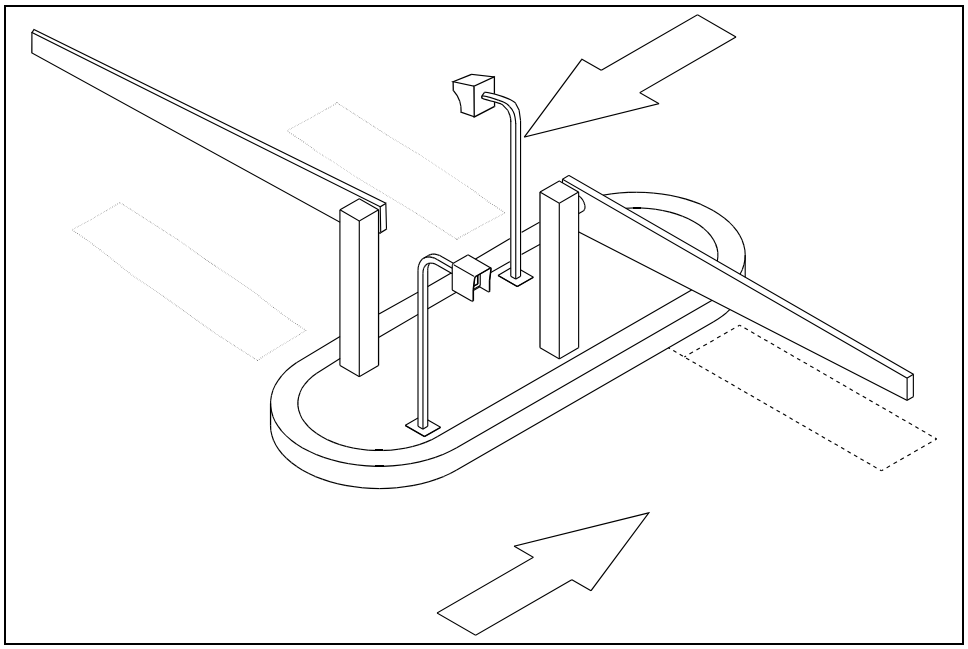


Figure 2-54: Typical Parking Gate

Entering Gates

For a vehicle gate entrance, choose the location for the ScramblePad or MATCH and Reader, keeping the following issues in mind:

- ❑ Does the location accommodate a Hirsch mounting post and MB5 mounting box?
- ❑ If the gate in question is used by both high cab trucks and passenger vehicles, you have the option to install double ScramblePads (or MATCHs and Readers) – one at normal vehicle height (curb or street mounting) and one at truck height. A custom mounting post would have to be fabricated for the truck height.
- ❑ An alternative to dual ScramblePads (or dual MATCHs and Readers) is one ScramblePad (or MATCH and Reader). This means truck drivers must get out of their vehicle to use it. This alternative can cause an inconvenience, especially to those in bad weather areas.
- ❑ The high-intensity version of the ScramblePad is always recommended for exterior gate control applications. It has less viewing restriction and a brighter display which makes viewing easier from a vehicle.

Exiting Gates

In most cases exiting from a controlled gate is automatic. The presence of the vehicle is detected by a magnetic loop buried in the asphalt or concrete on the approach side of the gate. This loop is tied into the gate controller and opens the gate for free exit. In other cases, where higher security is required, an exit ScramblePad (or MATCH and Reader) can be installed requiring a code (or card) for exit as well as for entry.

On personnel gates in fence lines, ScramblePads or MATCH readers are often mounted on fence posts adjacent to the personnel gate. The gates sometimes use special types of electrified hardware, although magnetic locks are being used more often in these applications. An RQE device or exit ScramblePad are normally used on personnel gates for exit control. They must be properly protected from someone reaching through the fence to unlock the gate to gain unauthorized entry.

Turnstiles

Turnstiles are used as alternatives to doors and gates. There are several types of turnstiles:

- ❑ Full Height Turnstile
- ❑ Half Height Turnstile
- ❑ Optical Turnstile

Turnstiles, Gates, and Doors share most of the same power and wiring specifications. Each is discussed in this section.

Full Height Turnstile

Full height turnstiles are for facilities that require single person access. They are usually installed outdoors or in lobbies of large facilities and are locked from rotation by a solenoid. A common access control application can have the turnstile locked for entry only and free for exit. In other applications, it is locked in both directions.

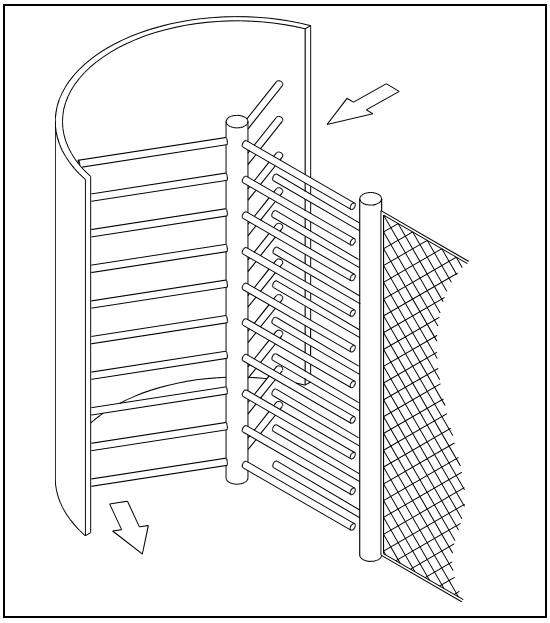


Figure 2-55: Full Height Turnstile

A ScramblePad/MATCH reader can be installed for entry and exit control. However, special mounting brackets may have to be fabricated to mount any of the ScramblePad mounting boxes.

If you're installing a turnstile outdoors with a ScramblePad, you have the option to use the DS47L-HI or the DS47L-SPX-HI along with the MB5 mounting box.

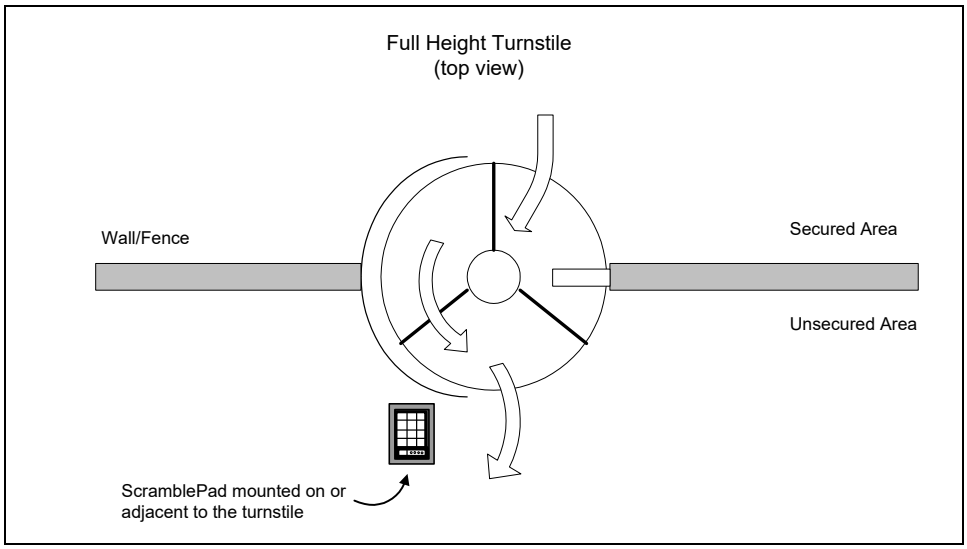


Figure 2-56: Full Height Turnstile Mounting

Half Height Turnstile

Half height turnstiles are typically used for two-way pedestrian control. However, it may be locked from rotation (by a solenoid) for entry only and free for exit. Other applications might have the turnstile locked in both directions.

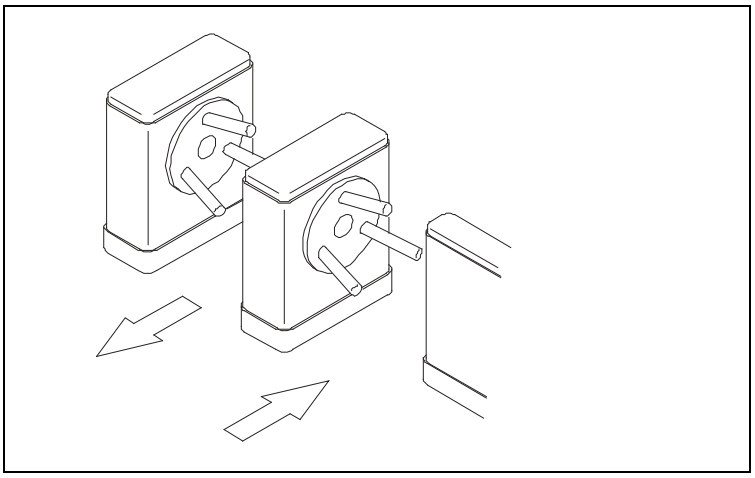


Figure 2-57: Half Height Turnstile

A ScramblePad/MATCH reader can be installed for entry and exit control. However, special mounting brackets may have to be fabricated to mount any of the ScramblePad mounting boxes.

If you're installing a turnstile outdoors with a ScramblePad, you have the option to use the DS47L-HI or the DS47L-SPX-HI along with the MB5 mounting box.

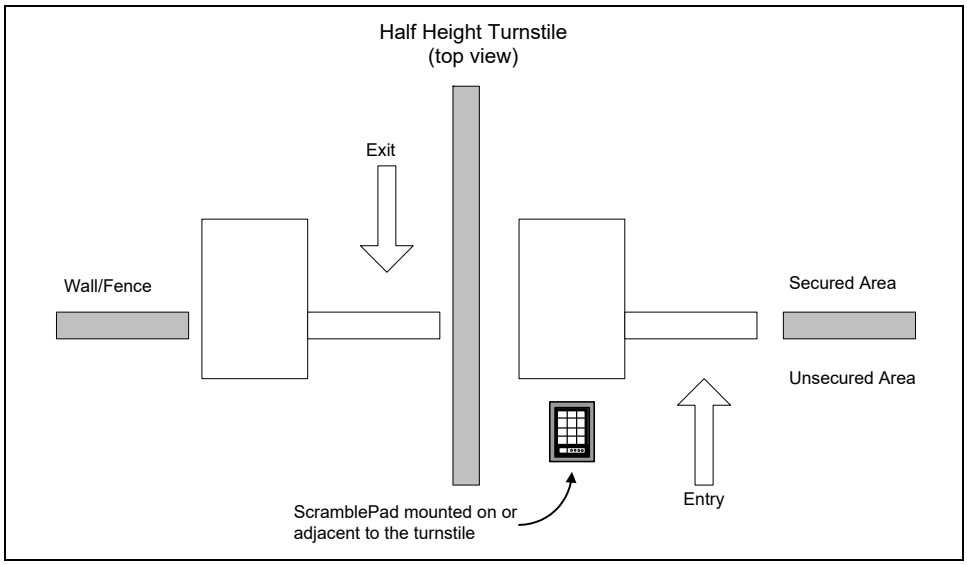


Figure 2-58: Half Height Turnstile Mounting

Optical Turnstile

A fairly new type of turnstile is the optical turnstile, or “passageway.” It is an attractive turnstile, used in lobby installations, and a little faster than traditional rotating devices. It does use more floor space, however, and is not designed for exterior use. An invisible barrier created by an infrared beam activates an audible and visual alarm when broken.

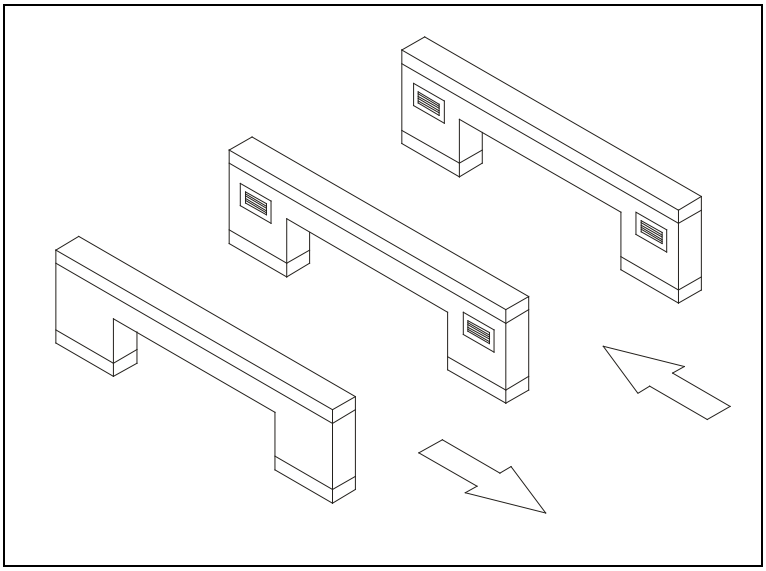


Figure 2-59: Optical Turnstile

The design allows a large number of authorized users into and out of a facility with little delay. Authorized users simply mask alarm detection when they enter their codes or present their cards, thus allowing free passage through the passageway.

If unauthorized users walk through an active passageway without entering a valid code, the alarm will not be masked when the beam is broken. Typically these turnstiles are under observation by guards so they can respond to the audible and visual alarms produced by

any unauthorized access attempts.

Installing ScramblePads/MATCH readers on passageways will require close cooperation between the passageway manufacturer, the system installer and owner to optimize the throughput for the controlled facility.

HVAC, Lighting, and Elevator Control

Heating, ventilation, air conditioning, lighting and elevator control are generally handled by the smaller 24 VDC, 2A relays found on expansion boards and MSP-8R or M64 controllers. The MSP-8R and M64, are specifically designed for this kind of control switching. One of the chief uses for the M64 is elevator control while the MSP-8R is used for many management and control applications, including HVAC, lighting, prison door control, interlock, and CCTV.

For more information about setting up and installing these components, see “HVAC, Lighting, and Elevator Control” on page 7-322.

Elevator Control

When controlling access to an elevator, there are typically two modes of operation:

- ❑ Day Mode (Free Access)
- ❑ Night Mode (Restricted Access)

The mode is usually controlled by a time schedule. There are three primary ways to control access to an elevator. Each way provides a different level of security, cost, and convenience:

- ❑ Hall Call Button Control
- ❑ Floor Restriction Control
- ❑ Automatic Floor Selection

Hall Call Button Control requires that you install a reader adjacent to the Hall Call Button (Up and Down Arrow buttons outside the cab). In Secure Mode, pressing either the Up or Down Arrow button will do nothing until a valid code or card is presented to the reader. The user will then have a limited period of time, usually 10 seconds, to press one of the buttons. Once the cab arrives, the user gets on and selects the floor they need. This option provides the lowest level of security, but is also the least expensive form of elevator control.

Floor Restriction Control enables the user to select the floor button they require. This option requires installation of a ScramblePad or reader in the elevator cab. During Night Mode, a user gets on the elevator, enters a valid code or presents a valid card to the reader. He/she then has a limited amount of time (usually 10 seconds) to press the button associated with the floor he/she wants. The DIGI*TRAC Control Language is used to define which floor(s) they are authorized to access and at what times. This option is usually selected when a user can access multiple floors in a building and needs to manually select which floor they are authorized to access and when. It provides a higher level of security but costs more in equipment and installation than the first option.

Automatic Floor Selection requires installation of a reader in the elevator cab. During Night Mode, a user gets on the elevator, enters a valid code or presents a valid card to the reader, and the floor button is automatically selected as defined by the user’s Control Zone. This should be used when the user only has access to one floor.

If a user has a requirement to access multiple floors, a modified version of the third option is possible. From a ScramblePad in the elevator cab, the user can enter his/her base code

followed by a 1- or 2-digit floor number they wish to access. Alternatively, users can also utilize previously-defined function groups for this purpose. (For more about function groups, see “Function Groups” on page 3-28.)

If authorized, the specific floor requested is selected. This option provides a higher degree of security than the first option and has the same security as the second option. As an added benefit, this option creates an audit trail—recording which people have accessed which floors.

Printers

In most installations, the printer is connected through the Host PC. However, there are occasions when only a single, standalone controller without a PC is being used. In order to program the system and printout events and configuration information, a printer must be installed. Also, a local printer is an excellent troubleshooting aid.

For more information about configuring and installing printers, see “Printer Installation for Standalone Controller” on page 7-323.

If you plan to install a printer at the controller location, make sure it’s installed in an easy-to-reach place. The standard parallel printer can only be located 12 feet (3.7m) or less from the controller enclosure. A printer shelf or table is also recommended for the location.

You can also choose to install a serial printer if the controller is located in an area unsuitable or inconvenient for placing a printer. With the addition of a SCIB expansion board and an NET*ADAPT (NA1) adaptor in the controller, you can locate a serial printer up to 4000 feet from the Controller.

For more about the NA1, see “NET*ADAPT Communications Adaptor (NA1)” on page 2-109.

Many installations also include badge printers. These are installed in the same fashion as paper printers through the host PC (using a serial connection) and are configured using software included with the printer package.

Card Enrollment Stations

Card Enrollment Stations are used to enroll a card into the controller’s database. Enrollment is the process of associating the unique number on each card with a user number in the controller. There are two steps involved:

1. The card is assigned to a specific employee, either by entering the required user number at a ScramblePad (DMES) or at a Host PC (SMES).
2. The new card is run through the reader. Information is read off the card by the reader and is sent to a database.

Note: When a MATCH code enrollment cross-reference list is provided and a PC with appropriate software is available, the code (as well as user name and other information) can be used to enter the numeric information by PC keyboard. An enrollment station is not required in this situation.

There are four types of Hirsch card enrollment stations now supported:

- ❑ DMES enrollment station
- ❑ SMES enrollment station
- ❑ nedap

- RUU Verification Station for Smart Cards

DMES Enrollment Station

The DMES and SMES share many features as shown in Figure 2-60.

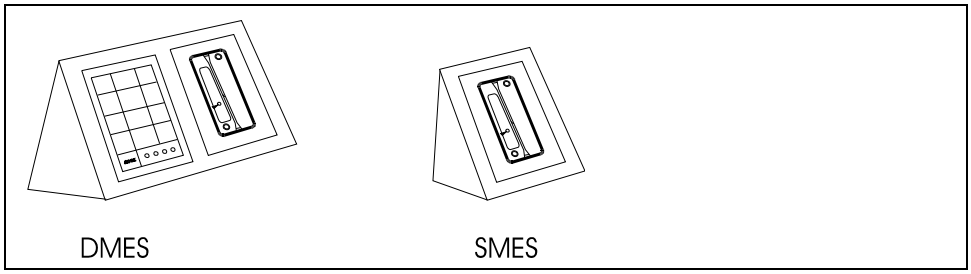


Figure 2-60: Enrollment Stations

However, the DMES includes a keypad as well as a reader whereas the SMES only has a reader. This means the DMES can enroll both cards and codes whereas the SMES is designed for codes alone.

The DMES series of enrollment stations include these three types:

- DMES-M—includes a DS47L ScramblePad programming station and a magstripe reader head mounted on an ES2 enrollment stand.
- DMES-H—includes a DS47L ScramblePad programming station and an HID prox reader head mounted on an ES2 enrollment stand.
- DMES-U—includes a DS47L ScramblePad programming station mounted on an ES2 stand. It is a universal version which can be connected to any compatible prox or magstripe reader head.

The DMES unit is connected to the controller via the integrated MATCH port on the back of the DMES as shown in Figure 2-61.

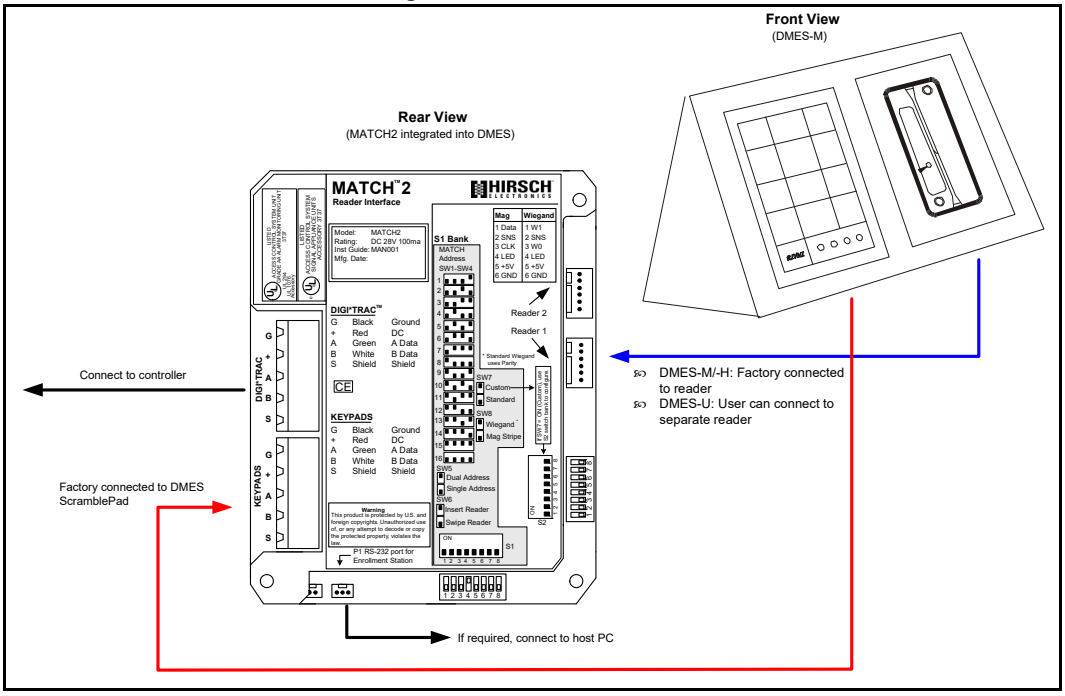


Figure 2-61: DMES-M Configuration

When the DMES enrollment station is connected to a controller, cards are enrolled using the attached ScramblePad by invoking Commands 310-315 (refer to page 4-210 through page 4-215).

Hint The DMES was developed for use with security systems that do not use security software on a connected PC to enroll users. In most modern installations, the inclusion of a ScramblePad for enrollment using keypad commands is no longer necessary. The software handles all of that. The SMES is a better choice for PC-operated security systems.

The DMES should be located adjacent to the controller printer to validate and record proper enrollment. The distance from the DMES to the controller should be no more than 1250 feet.

For DMES installation instructions, see “Enrollment Station Installation” on page 7-325.

SMES Enrollment Station

The SMES enrollment station enables cards to be enrolled through a Host PC using one of Hirsch’s software programs: SCRAMBLE*NET Access Manager (SAM), MOMENTUM, or Velocity.

The SMES series of enrollment stations include these three types:

- ❑ SMES-M—includes a MATCH2 board and magstripe card reader.
- ❑ SMES-H—includes a MATCH2 board and an HID prox reader mounted on an ES1 enrollment stand.
- ❑ SMES-U—includes a MATCH2 board mounted on an ES1 stand which can be connected to any compatible prox or magstripe reader head.

The SMES is connected to a Host PC and requires software such as Hirsch’s SCRAMBLE*NET Access Manager (SAM) or Velocity.

The SMES should be located adjacent to the host or client PC tasked with the job of validating and recording proper enrollment.

For SMES installation instructions, see “Enrollment Station Installation” on page 7-325.

Hirsch nedap AVI Enrollment Station

Hirsch supports and sells the nedap® AVI Long Range Identification Enrollment Station (Hirsch # CR-NES). This reader kit is provided for customers who need to enroll employees from/to TRANSIT AVI tags.

The Hirsch nedap kit includes the nedap Enrollment station, the Hirsch DMES-U, and a customized cable.

The following diagram shows the kit:

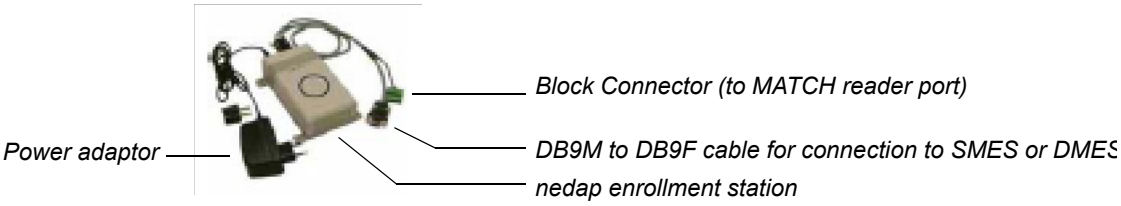


Figure 2-62: Hirsch nedap Enrollment Station Kit

Using the custom cable, the nedap Enrollment Station connects to the MATCH2 on the back of the DMES-U which is, in turn, connected to the controller and/or Host PC.

For more about connecting the nedap Enrollment Station, see “Hirsch nedap Enrollment Station Installation” on page 7-327.

Smart Card Enrollment Station

A new type of card enrollment has been ushered in with the introduction of the Smart Card. Because these cards incorporate both memory and circuitry, they can store far more employee information on a card than was ever possible before, including such memory-intensive identification data as fingerprints, retinal scans, and credit information.

Neither the Hirsch DMES nor SMES enrollment station are currently designed for enrolling smart cards. Instead, proprietary enrollment readers are now available from individual smart card vendors. These enrollment readers normally connect to the host PC through the Hirsch MATCH board.

The reader/enrollment station of choice for this card type is the RUU Verification Station. There are several smart card platforms that this station supports, including:

- ❏ PIV
- ❏ CAC
- ❏ General purpose
- ❏ TWIC

For more about installing these devices for use as enrollment stations, see “Verification Station Installation” on page 7-128.

DIGI*TRAC Annunciator

The DIGI*TRAC Annunciator (DTA) is used to monitor basic security functions—such as alarm, event, and device status—even when the guard or administrator is away from the main guard station.

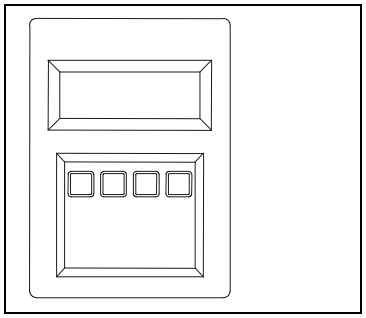


*Figure 2-63: DIGI*TRAC Annunciator – Front View*

The Annunciator includes an integral MATCH2 board so that it can communicate with the controller using the same digital channel as both the ScramblePad and MATCH.

The display is a four line, 20-character non-backlit LCD display with four status request buttons. The status request buttons are unlabeled smart keys that change their meaning based on the current dialog. Their dynamic labels are displayed in the LCD window above the keys. These keys are used for status requests only and cannot issue commands of any type. Status requests supported are:

- ❏ Alarm Log Display from the Controller's Alarm Buffer (holds last 256 alarms)

- ❑ Current Relay Status (to determine if a door is locked)
- ❑ Current Input Status (to determine is a door is closed or a device is secured)

This unit requires CCM 7.0 but does not require any host software support for setup or operation. It is ideal for lobbies, and other passages outside of the secured area where an individual can confirm that the protected area is secure, i.e. locked and ready to leave.

It is designed for

- ❑ through-the-door mounting in control panels
- ❑ mounting in cut-outs of custom sheet metal façades
- ❑ mounting in the cutout of a customer cover plate and back box.

The DTA comes pre-assembled with the MATCH2 conveniently installed in the back of the DTA (not shown). There are available optional cover plates as well as surface mount and flush mount back boxes.

The DTA communicates with the MATCH2 via its RS-232 port (P2) and draws its power from one of the MATCH2's reader channels (C2). The DTA is a secure annunciator and requires a ScramblePad code or card to activate the display. When a ScramblePad or ScrambleProx is used, it connects to the keypad port on the integrated MATCH2. When a reader is used, it connects to the unused reader channel (Channel 1) on the MATCH2.

For ScrambleProx, an extension cable must also be field fabricated so its proximity reader will connect to the MATCH2 reader channel instead of the ScrambleProx's onboard reader channel. The ScramblePad, ScrambleProx or Reader used to activate the DTA can also be used as a standard entry access device.

Since a MATCH2 is integrated with the Annunciator, the same power cable requirements apply to this unit as would apply to the MATCH2. For more on this, refer to “Powering ScramblePads/MATCH Interfaces Locally” on page 2-43.

If you are planning to connect the Annunciator to a ScrambleProx unit, you must first disconnect the data cable from the ScrambleProx’s native MATCH2 board and splice the cable into the Annunciator’s MATCH2 card.

Once connected, the operator accesses the Annunciator by either entering a special code into the connected ScramblePad or using a special card on the attached reader or ScrambleProx. A simple menu appears on the Annunciator LED. The operator then follows the menu to access the information they require.

For more on using the Annunciator, please refer to the *DIGI*TRAC Annunciator User’s Guide*.

For instructions on installing the Annunciator, see “DIGI*TRAC Annunciator Installation” on page 7-330.

Network Components

Although it is possible to program, control, and monitor a single DIGI*TRAC controller from a ScramblePad and printer, a network of controllers requires a different approach. It's often easier to run a single or multi-controller security system from a PC. This requires a variety of communications components to establish the network between the PC and one or more DIGI*TRAC controllers.

This section introduces you to these Hirsch network products:

- ❑ Secure Network Interface Boards (SNIB, SNIB2, or SNIB3)
- ❑ NET*MUX4 Network Multiplexor
- ❑ Adaptors and Connectors
  - NET*ADAPT Communications Adaptor (NA1) (External)
  - MODEM*ADAPT Communications Adaptor (MA1/MA2)
  - PC*CONNECT Network Connector (PC1)
  - MODEM*CONNECT Network Connector (MC1/MC2)
  - AT Adaptor Cable (AT-AC)
  - MODEM Cable (MC-PC)
  - NET*ADAPT-PC Communications Adaptor (NAPC) (Internal)
- ❑ Telecommunications: Modems/Transceivers
  - Dial-Up Modems
  - Leased-Line Modems or Short-Haul Modems
  - Fiber Optic Transceivers
- ❑ SCRAMBLE*NET Gateway (XBox)
- ❑ Network Communications: Device Servers

For descriptions and examples of different network configurations, refer to Chapter 6.

Secure Network Interface Boards (SNIB, SNIB2, or SNIB3)

There are now three generations of the Secure Network Interface Board:

- ❑ SNIB
- ❑ SNIB2
- ❑ SNIB3

Each is discussed in this section.

SNIB Design

When installed in a DIGI*TRAC Controller, the SNIB enables the Controller to be programmed, monitored, and controlled from a PC. For a one-controller network, you can connect to either the SNIB's RS-485 connector (up to 4000 feet/1220 meters) or the RS-232 connector (up to 50 feet/15 meters).

If you are connecting to more than one controller on the network and the first controller is within 50 feet (15 meters) of the Host PC, you can connect the PC to the first controller via the RS-232 connector and the rest of the controllers to the RS-485 S*NET connector on the first controller. Alternatively, simply connect to the RS-485 connector and daisy-chain the wire to the multiple controllers.

Note: A SNIB board must be installed in every controller you plan to connect to the network

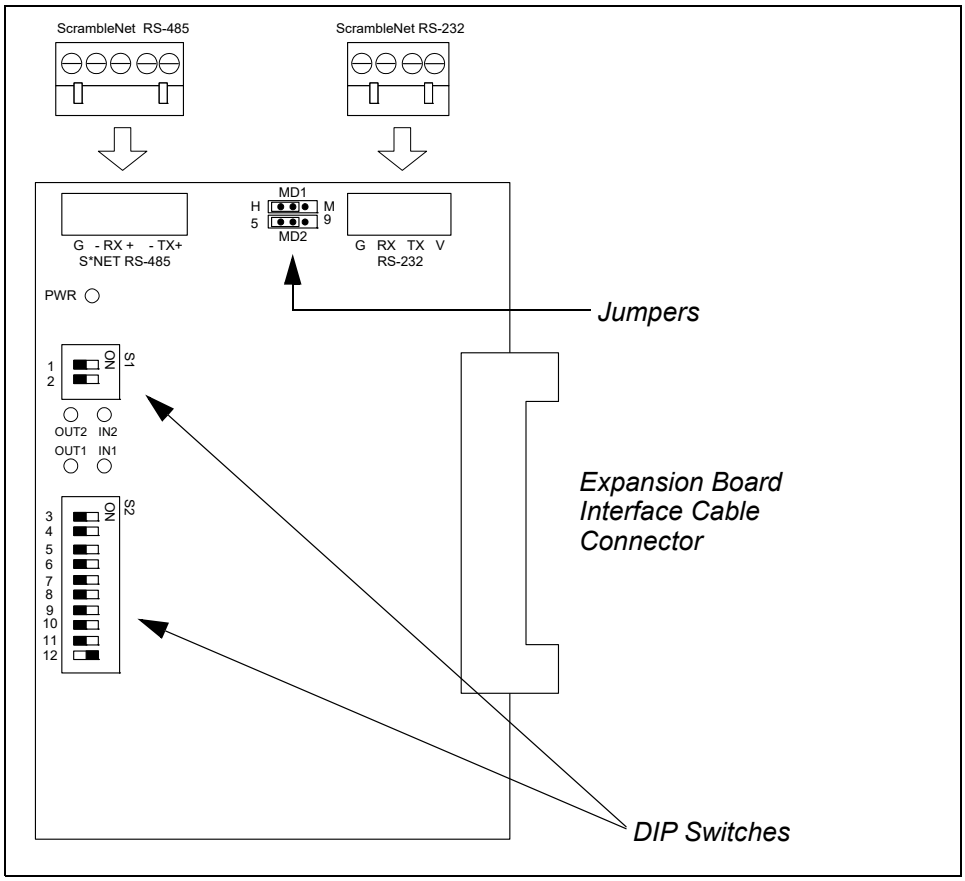


Figure 2-64: The Original Secure Network Interface Board (SNIB)

Figure 2-65 provides examples of how the SNIB can be used to connect two controllers to a host PC using either an RS-232 or RS-485 connection.

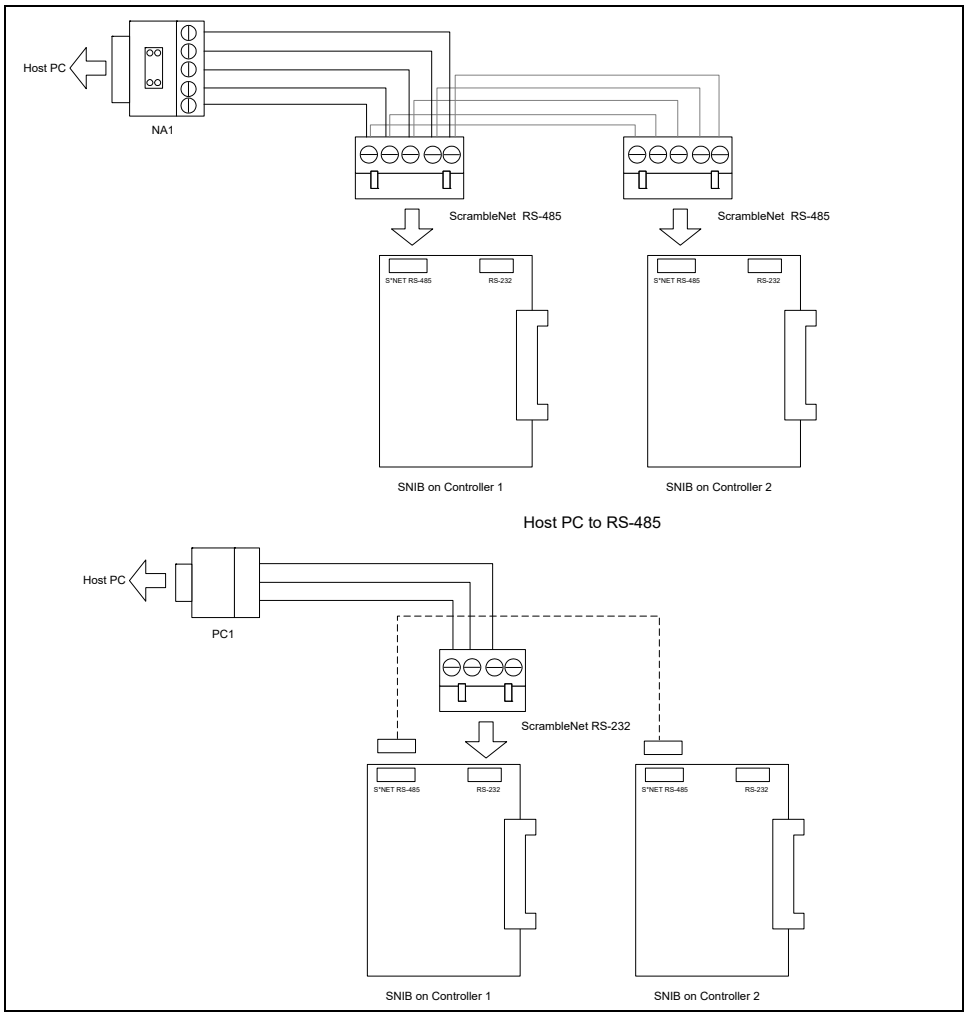


Figure 2-65: Host PC to SNIB Wiring Examples

For more on the use and installation of the SNIB, see “Secure Network Interface Board (SNIB, SNIB2, or SNIB3) Installation” on page 7-42.

SNIB2 Design

The SNIB2 is a drop-in replacement for the original SNIB. It is intended for those installations that require high security over Ethernet.

A call-out of the SNIB2 is shown in the Figure 2-66:

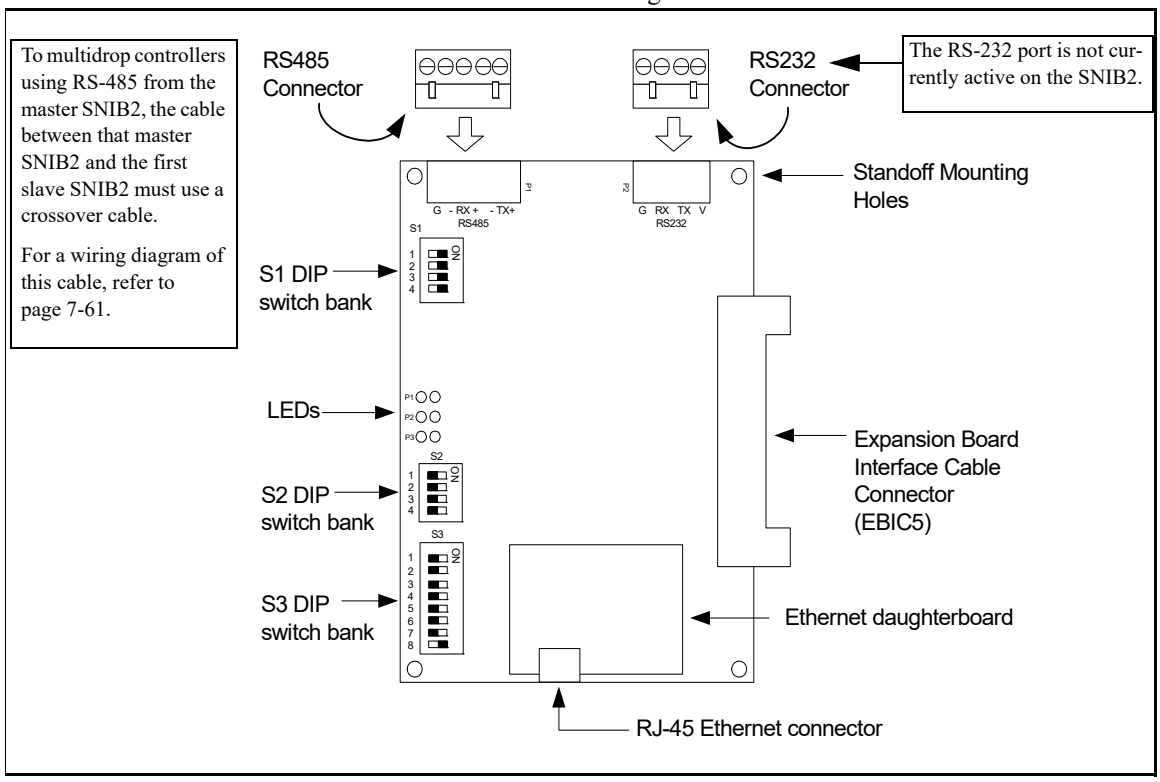


Figure 2-66: SNIB2 Call-Out

The SNIB2 is a controller-resident communication board that enables a host PC running Velocity to program, monitor, and control up to 63 SNIB2-resident controllers per SNIB2 Ethernet port. A NET*MUX4 is required whenever there are more than 16 controllers. Additional NET*MUX4s may be required to ensure that there are never more than 16 controllers on a single hard copper wire segment.

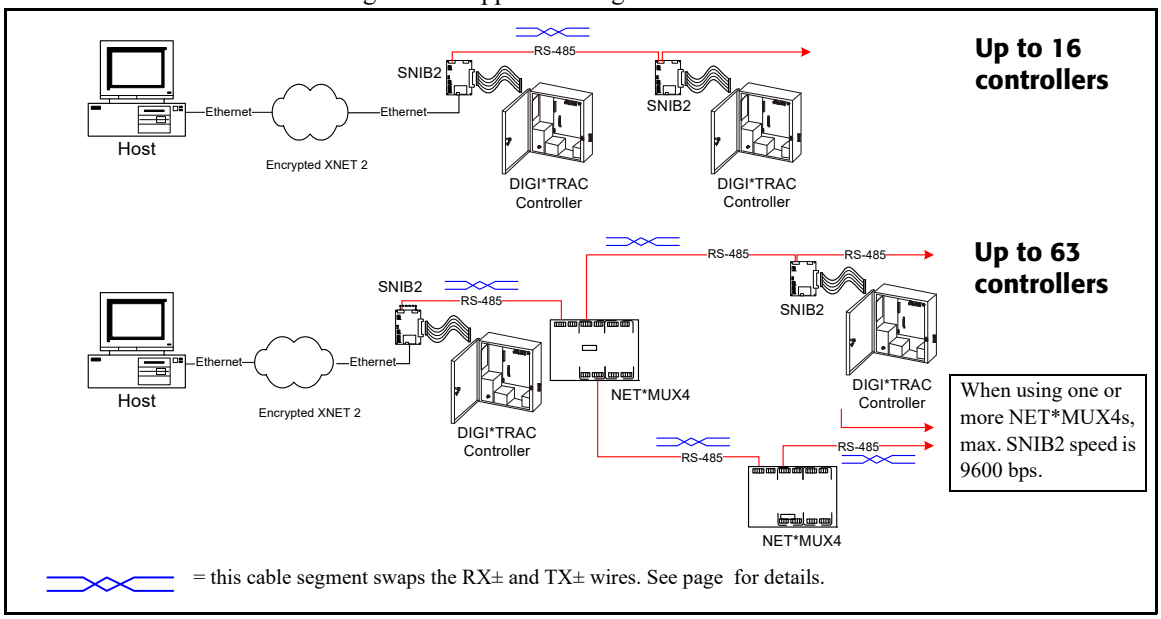


Figure 2-67: SNIB2 Controller Limits

*Note: When using one or more NET*MUX4s, maximum SNIB2 speed is 9600 bps.*

Each connected controller must have its own SNIB2 board installed. The SNIB2 provides an RS-485 port as well as a 10/100BaseT Ethernet port. The SNIB2 supports the XNET 2 protocol.

*Note: X*NET2 requires Velocity version 2.6 with Service Pack 1, or higher. CCM firmware version 7.3.0 or higher is also required.*

Physically, the SNIB2 board differs from the SNIB in three obvious respects. The SNIB2 has:

- ❑ three switch banks (SW1, SW2, and SW3)
- ❑ an Ethernet RJ-45 connector with its accompanying daughterboard
- ❑ three pairs of status LEDs

The SNIB2 provides these functional advantages over the SNIB:

- ❑ AES-Rijndael encryption
- ❑ Globalization functionality without an XBox
- ❑ Higher serial communication speeds
- ❑ Ethernet connectivity

Communications become less robust as baud rates increase, wire gauge decreases, and distances increase. Most tables in the *DIGI*TRAC Design and Installation Guide* for wire gauge and distance are based on 9600 baud. At higher baud rates, maximum distances are decreased and minimum wire gauge is increased.

It may not be possible to implement the higher baud rates supported by the SNIB2 if you have long wire runs or small wire gauges. Higher baud rates are also more dependent on the number of twists per foot, so capacitance specifications must be strictly followed: total wire run per port is not to exceed acceptable total capacitance of 100,000 p*f*.

! CAUTION **To use the SNIB2, your controller must be running CCM firmware version 7.3.08 or higher. (Also, you cannot install the SNIB2 board into the Hirsch M1N controller because it does not support any expansion boards.)**

The SNIB2's Ethernet port provides high-speed TCP/IP communication over an Ethernet network between the host computer and the controller.

Note: You can mix SNIBs and SNIB2s in your configuration; however, be aware that the speed of the network will be determined by the slowest of the network components.

The Ethernet connection enables communication between the controller with the master SNIB2 and host PC at 10/100BaseT. Speeds between the master SNIB2 and other connected downstream slave SNIB2s range up to 115200 bps.

Hint A multidropped run of controllers is only as fast as its slowest component. Therefore, if you set a SNIB2 in the run to 19200, the maximum speed for any other SNIB2 in the run is limited to 19200 and addresses 1- 31.

A simple configuration connecting a single SNIB2-installed controller to the host might look like the example in Figure 2-68.

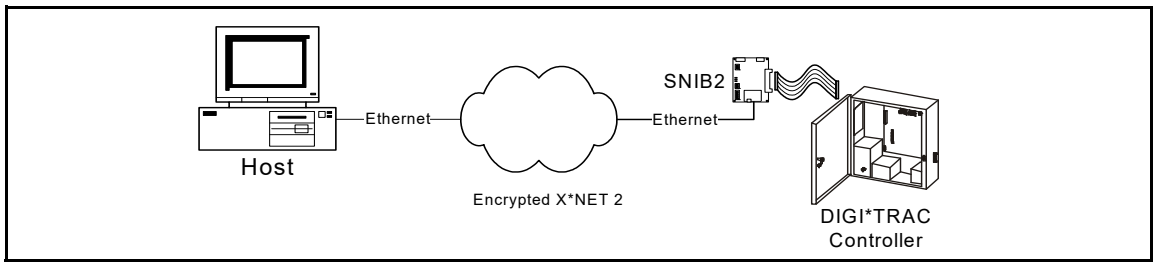


Figure 2-68: Host-to-Single SNIB2 Example

A more typical configuration that connects multiple controllers to the host, might look like the example in Figure 2-69:

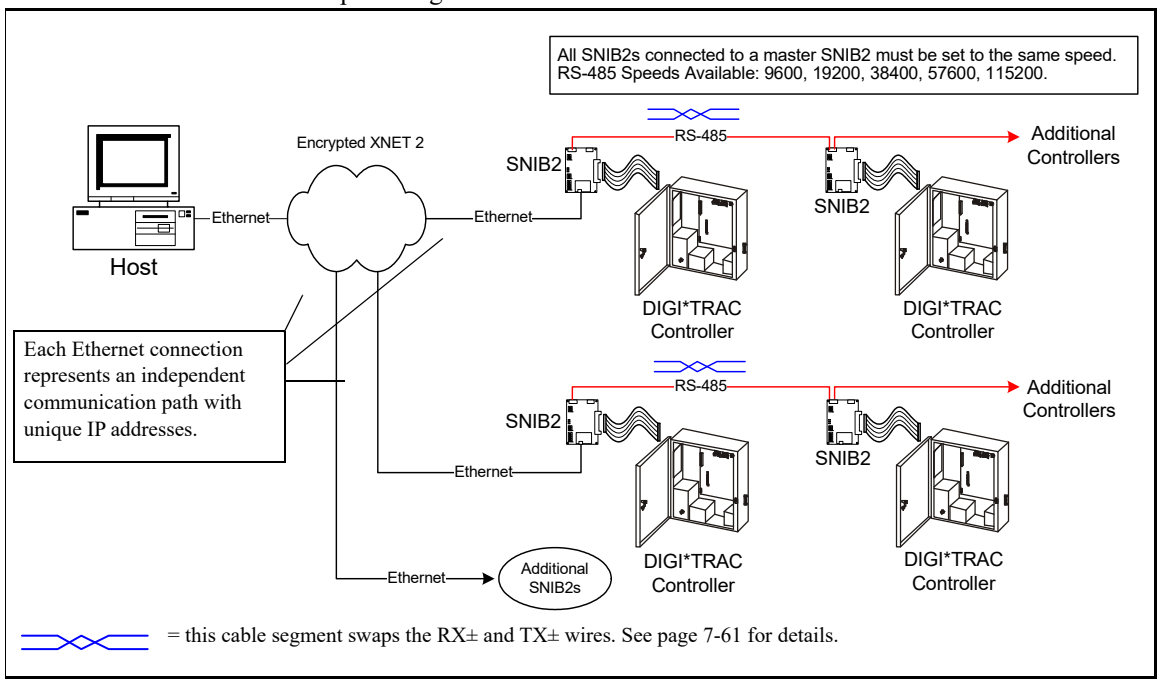


Figure 2-69: Host-to-Multiple SNIB2s Configuration Example

Before the Velocity server can communicate over Ethernet with a SNIB2, you must first configure the SNIB2 through Velocity.

Whenever an Ethernet connection is employed between the host and the SNIB2, Velocity views the SNIB2 as an XNET port since the SNIB2 includes XBox functionality. The host communicates with the Ethernet-connected SNIB2 using AES-encrypted XNET 2.

Controller-to-controller speeds range from 9600 to 115200 bps. For each string of controllers, the first (master) SNIB2 with the Ethernet connection must be assigned the same address as the XNET port. No matter how many master SNIB2s are assigned Address 1, Velocity will be able to identify them appropriately using the SNIB2's ROM ID and IP addresses assigned to them.

*Note: When the host is connected to a SNIB2 using Ethernet, Velocity views the first (master) SNIB2 as both a DIGI*TRAC controller and an XBox residing on an XNET port. Subsequent multidropped controllers in the sequence do not appear as XBox controllers.*

You can also use the SNIB2 with the NET*MUX4. The NET*MUX4 consists of a single

input for either RS-232 or RS-485 and four outputs to which a series of controllers or additional NETMUX4s can be wired as shown in Figure 2-70:

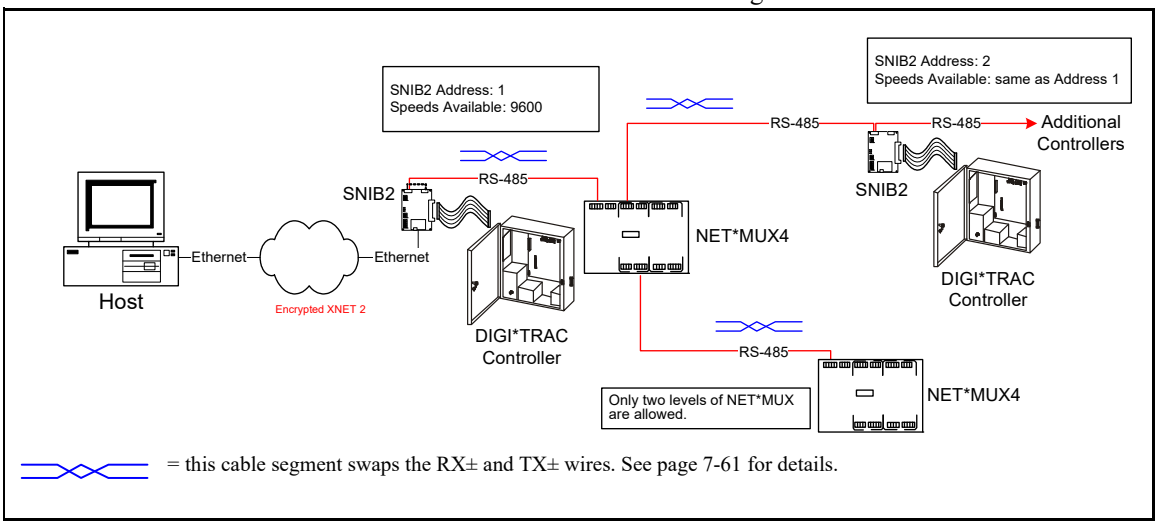
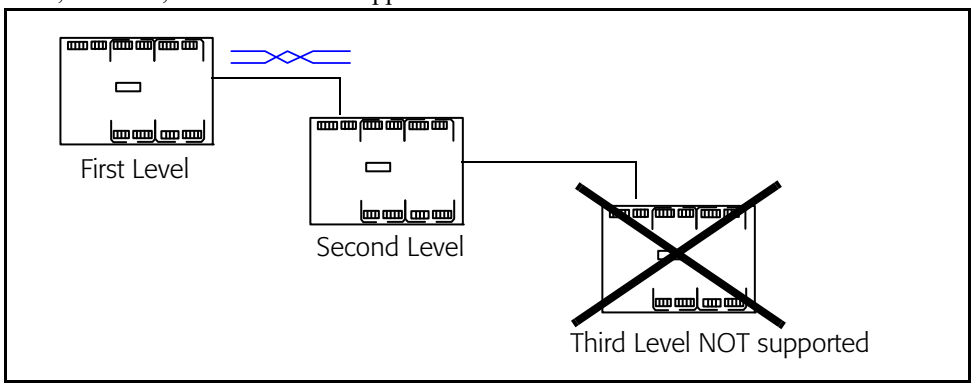


*Figure 2-70: Host-to-Multiple SNIB2s using NET*MUX4s*

If required, you can add a second level of NET*MUX4s to create additional controller runs; however, Hirsch does not support more than two levels of NET*MUX4s.



*Note: Any installation with cascaded NET*MUX4s cannot use SNIB2 speeds higher than 9600 bps, no matter what cable or distance is involved.*

For information on setting up and installing the SNIB2, refer to “Installing the SNIB2” on page 7-49.

SNIB3 Design

The Secure Network Interface Board v3 (SNIB3) is an update to the SNIB2 board currently used with the Mx, M2, M8, M16, M64, and MSP controllers. The main components of the SNIB3 are shown in Figure 2-30 on page 2-40.

The SNIB3 is based on a new, more powerful hardware platform that supports:

- faster Ethernet speeds. The SNIB3's RJ-45 Ethernet port is capable of 10BaseT, 100BaseT, or 1000BaseT (gigabit) speeds.
- version 6 of the Internet Protocol, which uses 128-bit addresses to identify and locate devices on the Internet. (The previous IPv4 used 32-bit addresses.)
- more robust encryption (with a 256-bit key length) through the XNET3 protocol. (For compatibility with older SNIB2-equipped controllers, the SNIB3 can run in XNET2 mode using 128-bit AES encryption.)

When installed in a DIGI*TRAC or Mx controller, the SNIB3 communications board enables a host PC running Velocity to program, monitor, and control up to 63 controllers per SNIB3 Ethernet port. Each controller must have its own SNIB2 or SNIB3 board.

The SNIB3 is not backwards compatible with the original SNIB. You cannot use the SNIB3 with the M1N controller, because it does not support any expansion boards. To use the SNIB3 with an Mx controller, you must first remove the SNIB2 daughterboard from the Mx controller's main board, as explained in "Preparing an Mx Controller to Use a SNIB3" on page 7-75.

The SNIB3 provides both an RS-485 port and a 10/100/1000BaseT RJ-45 Ethernet port, which enables you to choose the security network configuration that is most appropriate for your situation:

- If you are using only SNIB3 boards in all of your controllers, you can use either the XNET2 or the XNET3 protocol, and the downstream controllers in your security network can either be connected directly using the RJ-45 Ethernet port, or be connected to a master SNIB3 using the RS-485 port. (These options are shown in Figure 2-31 on page 2-42.)
- If you are using SNIB2 boards in some of your controllers, you cannot use the XNET3 protocol, and those controllers must be downstream slaves to a master SNIB3, connected using the RS-485 port. (This option is shown in Figure 2-32 on page 2-42.)
- The SNIB3 also supports connections to the NET*MUX4, as explained in "Using NET*MUX4s with SNIB3s" on page 7-81.

The SNIB3's RS-485 connector enables wire runs of up to 4000 feet (1220 meters). Higher baud rates are more dependent on the number of twists per foot, so capacitance specifications must be strictly followed: total wire run per port is not to exceed acceptable total capacitance of 11-17 p*f* and a total of 100,000 p*f* .

A NET*MUX4 is required whenever there are more than 16 controllers. Note that using a NET*MUX4 enables more controllers to be managed through a single network port, but it limits the data communication speed to 9600 baud.

Whenever an Ethernet connection is employed between the host and the SNIB3, Velocity views the SNIB3 as an XNET port because the SNIB3 includes XBox functionality. The host communicates with the Ethernet-connected SNIB3 using either XNET 2 or XNET 3. For each string of controllers, the first (master) SNIB3 with the Ethernet connection must be assigned the same address as the XBox port.

Prerequisites for the SNIB3

The SNIB3 board has the following prerequisites or dependencies:

- The CCM firmware must be version 7.5.37 (or later).
- The Velocity software must be version 3.6 SP1 (or later).
- If you want to use the SNIB3 with an Mx controller, you must first remove the SNIB2 daughterboard from the Mx controller's main board. For more information, see "Preparing an Mx Controller to Use a SNIB3" on page 7-75.
- Although the SNIB3 supports dynamic IP addressing using the Dynamic Host Configuration Protocol (DHCP) for both IPv4 and IPv6, Identiv strongly recommends using static or reserved IP addresses for your SNIB3 boards.
- IPv6 is generally not compatible with IPv4, so if you want to use IPv6 addressing for a SNIB3, it must be installed on a network which supports IPv6.
- Upgrading the firmware of downstream SNIB3s must be done one at a time. In a master-slave configuration, you must upgrade the master SNIB3 board's firmware first, and then upgrade each slave SNIB3 board's firmware in sequence. Don't start the download for the next SNIB3 board until the firmware upgrade for the previous SNIB3 board has completed.

NET*MUX4 Network Multiplexor

The NET*MUX4 is a multiplexor which enables you to segment the SCRAMBLE*NET circuitry into four discrete, electrically isolated segments for greater distance and survivability. The NET*MUX4 is installed in a separate locked enclosure with its own power supply and battery as shown in Figure 2-71.

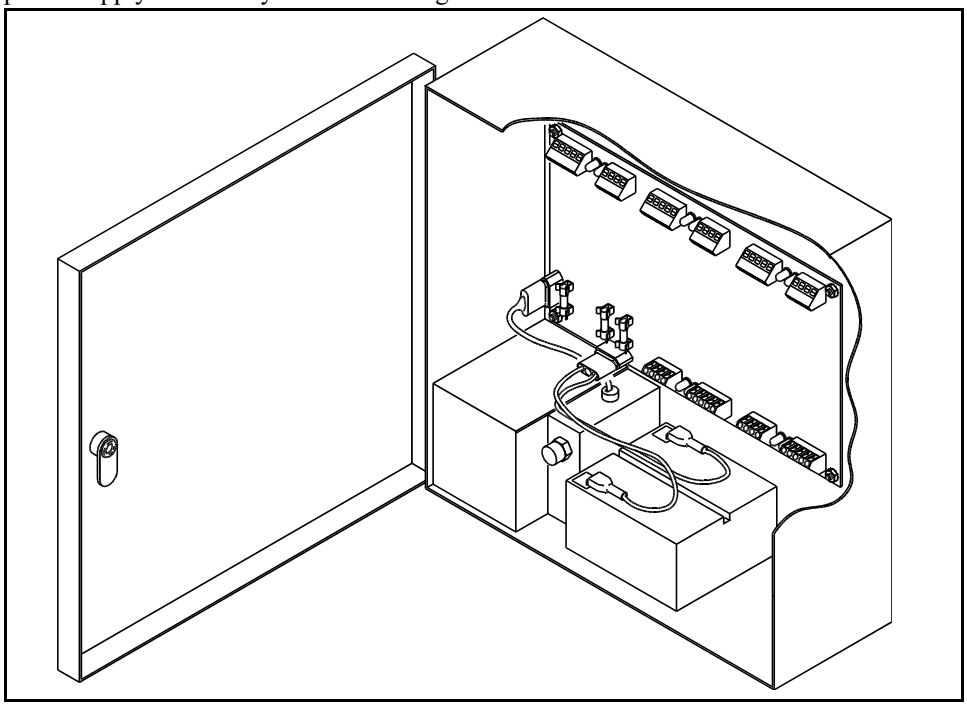


*Figure 2-71: NET*MUX4 Enclosure*

The NET*MUX4 can also be used for expanding SCRAMBLE*NET communications to multiple single-ended devices, such as leased phone lines. Additional NET*MUX4s can be cascaded for more than four isolated SCRAMBLE*NET circuits; however, all NET*MUX4s must be located between the Host PC and any controller.

There are five SCRAMBLE*NET ports (one IN, four OUT) on the NET*MUX4, each of which can be single-ended RS-232 or multi-drop RS-485 as shown in Figure 2-72.

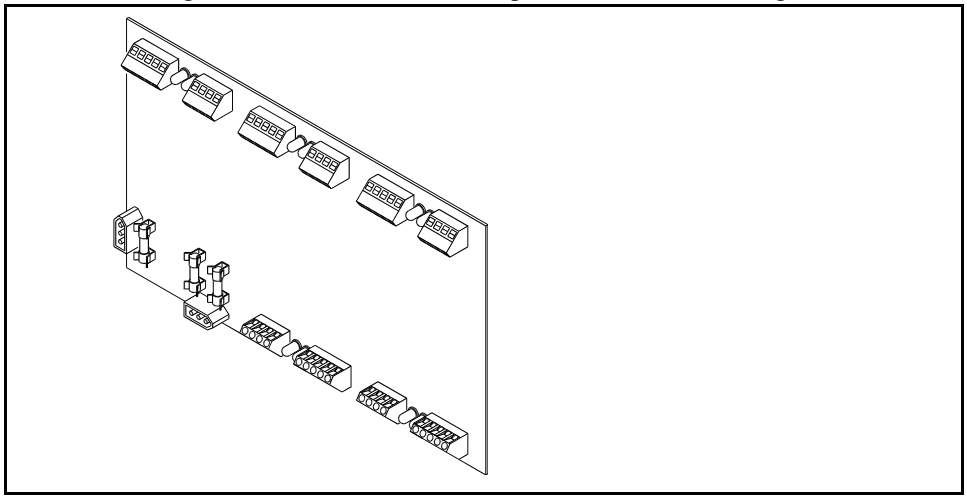


*Figure 2-72: NET*MUX4 Board*

Use the NET*MUX4's single-ended RS-232 ports to link to controllers (with SNIB) via modems. Use the NET*MUX's multi-drop RS-485 connectors to daisy-chain up to 63 SNIBs (16 SNIBs maximum per NET*MUX4 port).

The recommended location is either above the ceiling or on the wall. The NET*MUX4 is normally placed near the PC or between the Host PC that controls it and the Controllers/ Modems the NET*MUX4 oversees.

The following table describes the maximum distances from each NET*MUX4 output to the last controller on a cable run:

Interface (baud)	Wiring Distance in feet (meters)
RS-232 (9600)	50 (15)
RS-485	4000 (1220)

*Table 2-26: NET*MUX4 Wiring Distances for 22 AWG Twisted, Shielded Pair*

The total distance from the NET*MUX4 to the last controller can be up to 4000 feet (1220 meters) for RS-485.

Figure 2-73 shows one possible configuration using the NET*MUX4 board.

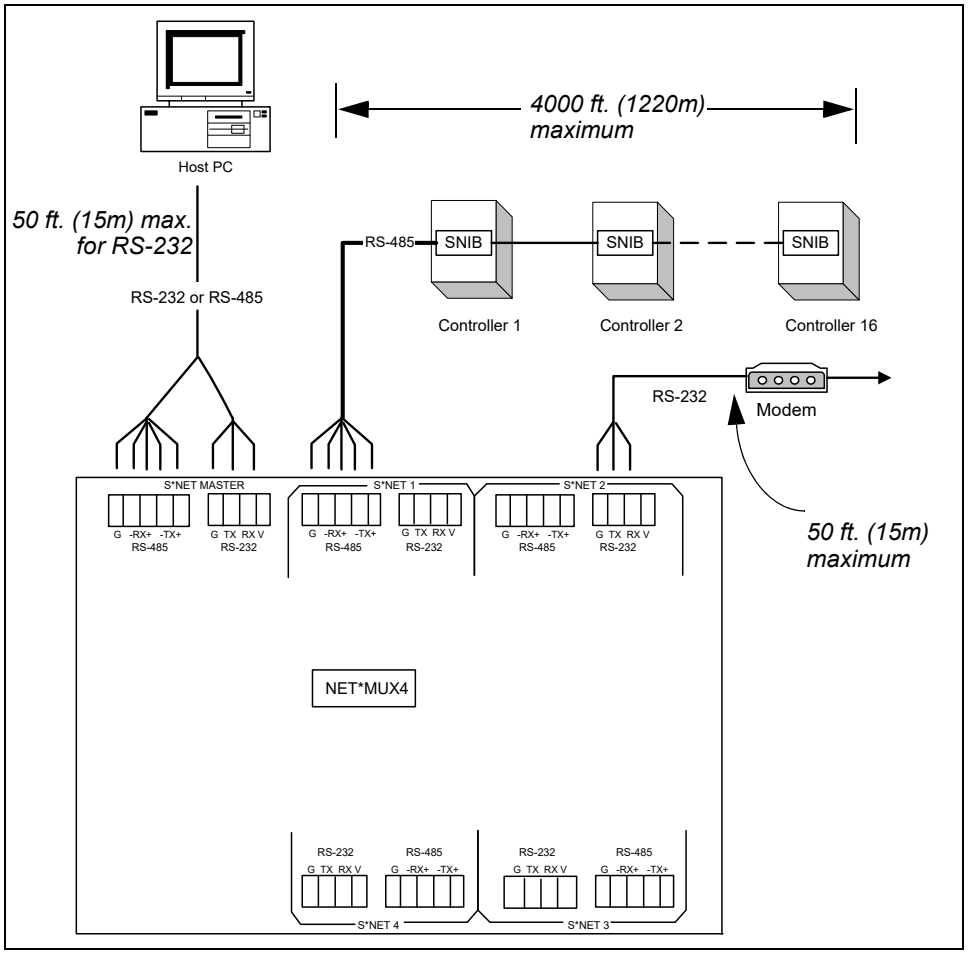


*Figure 2-73: NET*MUX4 Wiring*

The dimension and shipping weight for the NET*MUX4 is:

Dimension:	12”H x 12”W x 4”D (30.5cm x 30.5cm x 10cm)
Shipping Weight:	13.9 lbs (6.3 kg)

For detailed instructions on configuring and installing this communications device on the network, see “NET*MUX4 Network Multiplexor Installation” on page 7-331. For examples of how you can use the NET*MUX4 within a SCRAMBLE*NET network environment, refer to Chapter 6, “Application Examples”.

Adaptors and Connectors

There are a variety of cables and adaptors Hirsch supplies to link various parts of the SCRAMBLE*NET network. These are:

- ❑ NET*ADAPT Communications Adaptor (NA1) (External)
- ❑ MODEM*ADAPT Communications Adaptor (MA1/MA2)
- ❑ PC*CONNECT Network Connector (PC1)
- ❑ MODEM*CONNECT Network Connector (MC1/MC2)
- ❑ MODEM Cable (MC-PC)
- ❑ AT Adaptor Cable (AT-AC)
- ❑ NET*ADAPT-PC Communications Adaptor (NAPC) (Internal)
- ❑ Serial Printer Adaptor (SPA)

The following matrix provides help on how to select the cables/adaptors.

From: To:	Modem (RS-232)	SNIB (RS-232)	SNIB (RS-485)	NET*MUX4	Host PC	SCIB	XBox
Modem (RS-232)		MC1 MC2	MC1 MC2	MC1 MC2	MC-PC		RS-232 cable only
SNIB (RS-232)	MC1 MC2			RS-232 cable only	PC1		RS-232 cable only
SNIB (RS-485)	MC1 MC2			RS-485 cable only	NA1		RS-485 cable only
NET*MUX4	MC1 MC2	RS-232 cable only	RS-485 cable only	RS-232 RS-485	NA1		RS-485 RS-232
Host PC	MC-PC	PC1	NA1	NA1		NA1 PC1	NA1+PC3
Serial Printer						SPA	
XBox				RS-232 RS-485	NA1+PC3 DB9-DB9		PC3

Table 2-27: Adaptor and Connector Reference

When presented with a choice between RS-232 and RS-485, remember that RS-232 requires a 3-connector single shielded pair cable and RS-485 requires a 5-connector 2-single shielded pair cable. If you are planning to run more than 50 feet (15m) of cable between devices, always use RS-485.

NET*ADAPT Communications Adaptor (NA1)

The NET*ADAPT communications adaptor (NA1) is an external RS-232-to-RS-485 converter which enables the Host PC to connect to a networked DIGI*TRAC Controller and/or NET*MUX4 via multi-drop RS-485 communications.

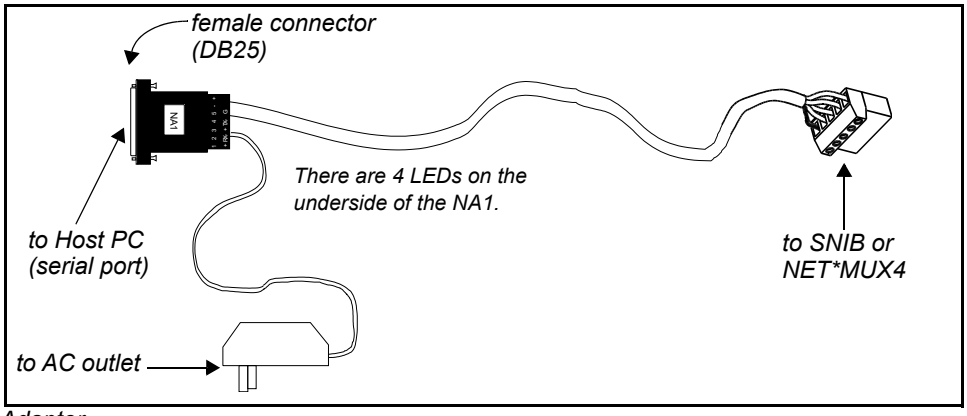


Figure 2-74: NA1 Adaptor

The NA1 connects to a:

- ❑ Host PC on one end (via direct connection to a serial COM port) and
- ❑ NET*MUX4 or SNIB-installed DIGI*TRAC Controller on the other end (via RS-485 cable)

The NA1 includes a 6 ft. (2m) cable. For more information about installing the NA1, see "NET*ADAPT Communications (NA1) Installation" on page 7-336.

MODEM*ADAPT Communications Adaptor (MA1/MA2)

Use the MODEM*ADAPT Communications Adaptor (MA1/MA2) for these purposes:

- ❑ MA1 is an RS-232-to-RS-485 converter which enables an RS-232 modem to connect to a SNIB or NET*MUX4. This enables up to 16 controllers on a single cable run at a remote site, over leased or dial-up phone lines. It has transmit and receive status LEDs for both the RS-232 and RS-485 ports to verify communications.
- ❑ MA2 is used to connect previous version SNIBs – version H or earlier that don't automatically convert RS-232 to RS-485 – to an RS-232 modem.

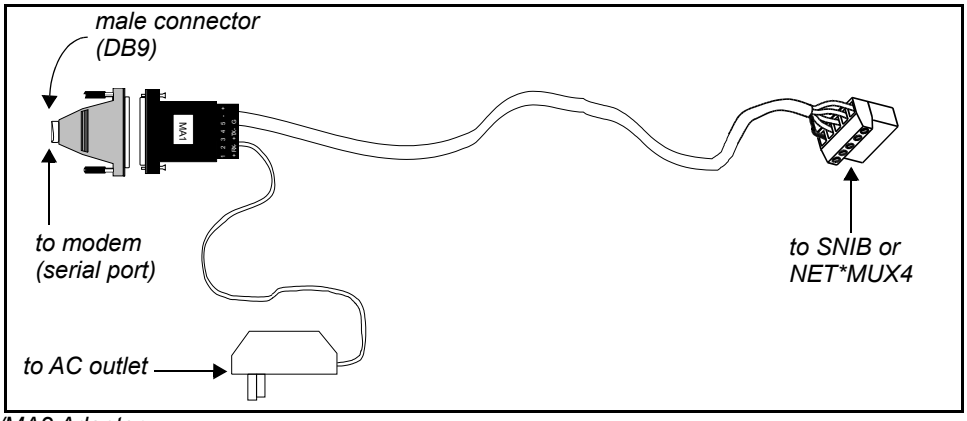


Figure 2-75: MA1/MA2 Adaptor

For information about configuring and installing the MA1/MA2, see “MODEM*ADAPT Communication Adaptor (MA1/MA2) Installation” on page 7-341.

PC*CONNECT Network Connector (PC1)

Use the PC1 network connector for connecting PCs to DIGI*TRAC terminal blocks via the RS-232 port.

One end of the PC1 is a standard DB25 female connector which can be easily hooked to a PC’s RS-232 serial COM port. The other end is a 4-pin terminal plug (3 terminals are used) for insertion into either a SNIB or NET*MUX4.

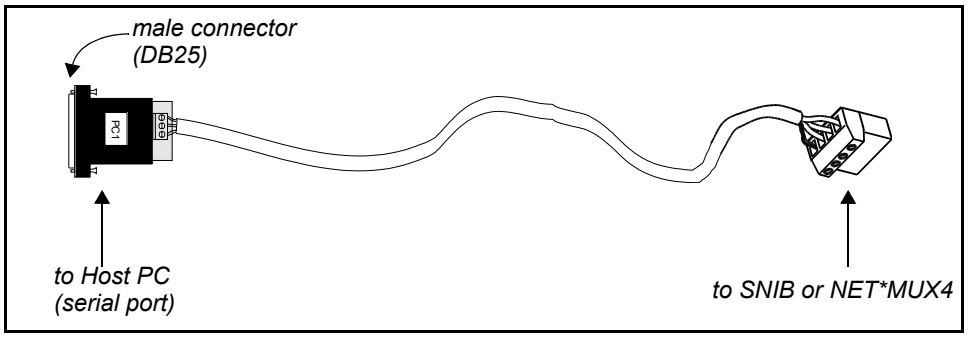


Figure 2-76: PC1 Connector

When connecting the PC1 to the NET*MUX4, first remove the PC1’s terminal block. The PC1 includes a 10 ft. (3m) cable.

For information about configuring and installing the PC1, see “PC*CONNECT Network Connector (PC1) Installation” on page 7-343.

MODEM*CONNECT Network Connector (MC1/MC2)

Use the MODEM*CONNECT Network Connector for connecting the modem’s RS-232 connector directly to a SNIB RS-232 terminal block on a controller.

The MC1 consists of a DB25 male connector on the modem end and a 4-pin terminal block on the SNIB end. The MC2 consists of a DB9 male connector on the modem end and a 4-pin terminal block on the SNIB end.

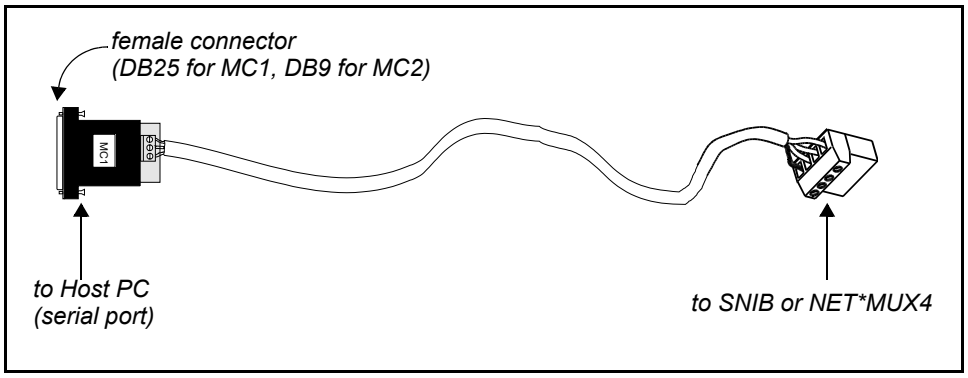


Figure 2-77: MC1/MC2 Connector

The MC1/MC2 includes a 10 ft. (3m) cable.

For information about configuring and installing the MC1/MC2, see "MODEM*CONNECT Network Connector (MC1/MC2) Installation" on page 7-340.

MODEM Cable (MC-PC)

Use the MC-PC or equivalent standard serial cable to connect a PC to a modem's RS-232 port. There is a DB25 female connector at both ends.

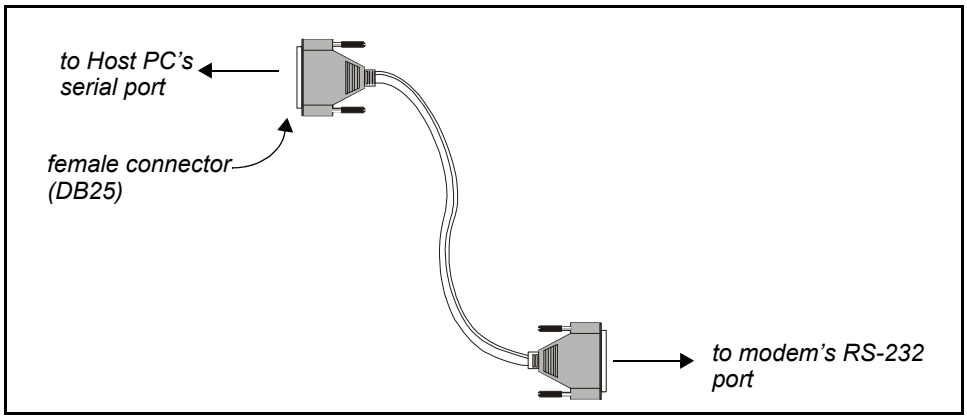


Figure 2-78: MC-PC Cable

The MC-PC includes a 3 ft. (1m) cable.

For information about configuring and installing the MC-PC, see "MODEM Cable (MC-PC) Installation" on page 7-343.

AT Adaptor Cable (AT-AC)

Use the AT-AC Adaptor Cable to convert a DB9 (male) serial port to a DB25 (male) serial port, such as adapting the NET*ADAPT to the NET*MUX4 (see Figure 7-96). The AT-AC has a DB9 (female) connector on one end and a DB25 (male) connector on the other end.

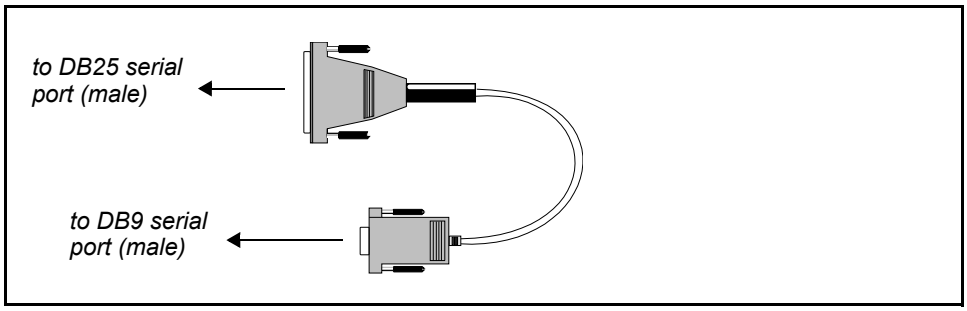


Figure 2-79: AT-AC Cable

The AT-AC includes a short 9 inch (23 cm) cable. For information about configuring and installing the AT-AC, see "AT Adaptor (AT-AC) Installation" on page 7-343.

NET*ADAPT-PC Communications Adaptor (NAPC)

The NET*ADAPT-PC Communications Adaptor (NAPC) is a full-size card that mounts in a PC and provides 2 serial ports from an IBM PC-compatible AT bus board. Both ports feature flexible addressing for any COM port address and interrupt combination.

For more information about configuring and installing the NAPC, see “NET*ADAPT-PC Communications Adaptor (NAPC) Installation” on page 7-339.

Serial Printer Adaptor (SPA)

The Serial Printer Adaptor (SPA) converts RS-232 to RS-485 for connections between the Serial Communications Interface Board (SCIB) in a DIGI*TRAC controller and a serial printer.

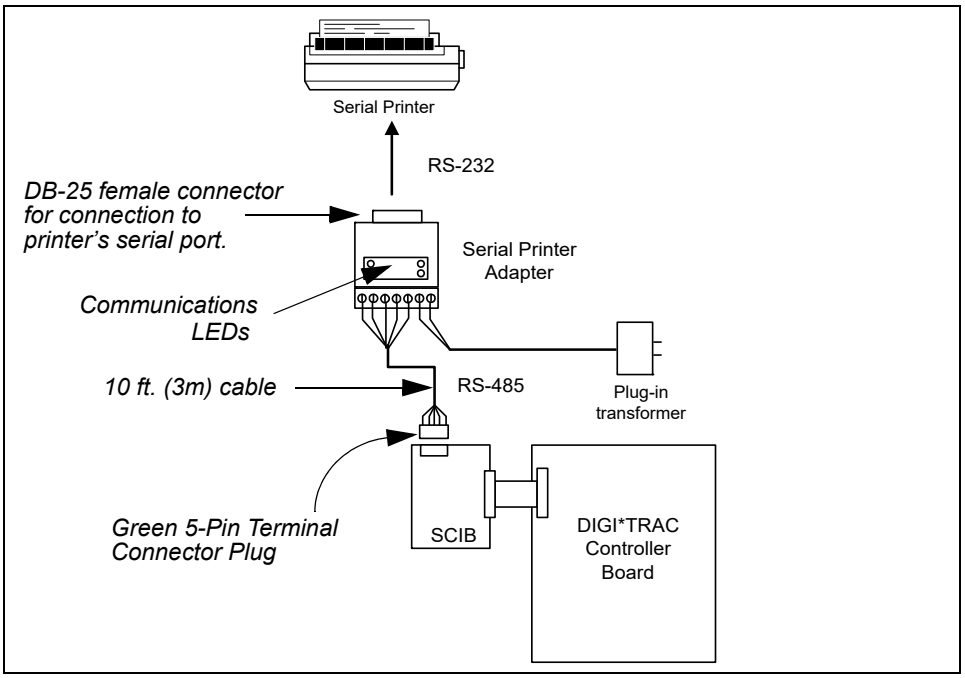


Figure 2-80: SPA Printer-to-SCIB Connection

For information about configuring and installing the SPA, see “Serial Printer Adaptor (SPA) Installation” on page 7-344.

Telecommunications: Modems/Transceivers

Hirsch supplies three types of modems/transceivers for three types of communication:

- ❑ Dial-Up Modems
- ❑ Leased Line Modems
- ❑ Fiber Optic Transceivers

Each of these devices uses a different type of line:

Device	Line Type
Dial-Up Modems	Dedicated phone line equal to your home phone line. No PBX lines.
Leased-Line Modems	Dedicated 2-wire full duplex or 3002 grade line.
Fiber Optic Transceivers	Fiber optic cable

Each device is discussed briefly below.

Dial-Up Modems (DM9600A-DL and EM9600-DL)

Dial-Up modems are available in two versions:

- ❑ DM9600A-DL DIGI*TRAC 9600 Baud Modem Assembly
- ❑ EM9600-DL External 9600 Baud Modem

The DM9600A-DL can be installed in a DIGI*TRAC controller enclosure for remote site management. When installed in this way, it can receive power (AC and standby) from the controller, and share the controller's protection from physical tampering.

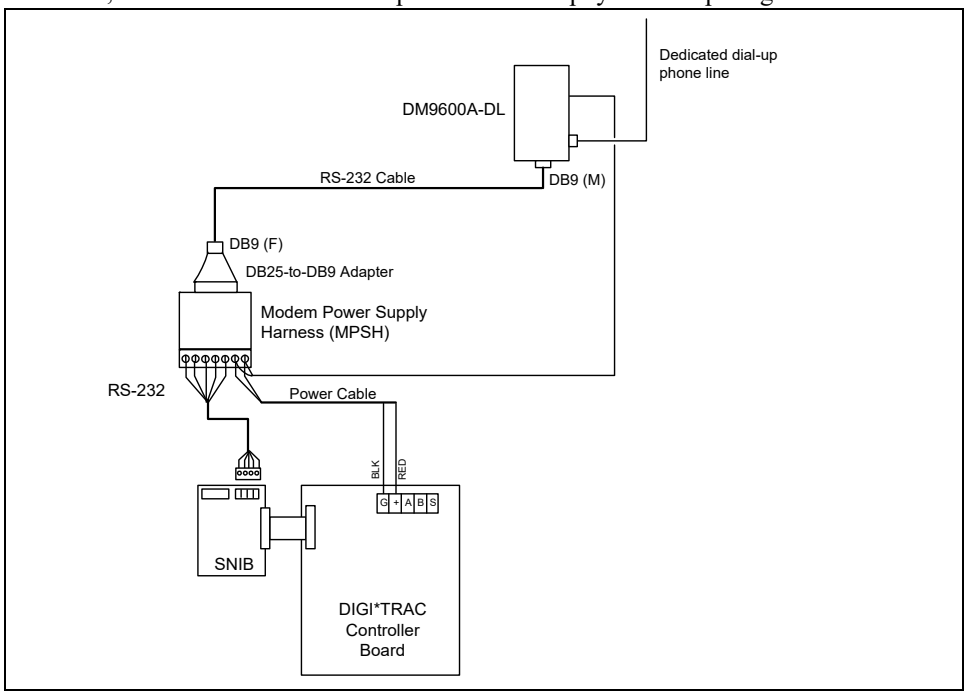


Figure 2-81: DM9600A-DL Connection to a Controller

The DM9600A-DL includes the cables, adaptor, and power supply harness as shown above.

The EM9600-DL is installed near a Host PC or NET*MUX4. It includes a power transformer. A cable, such as an MC-PC, is required for connection to a host PC.

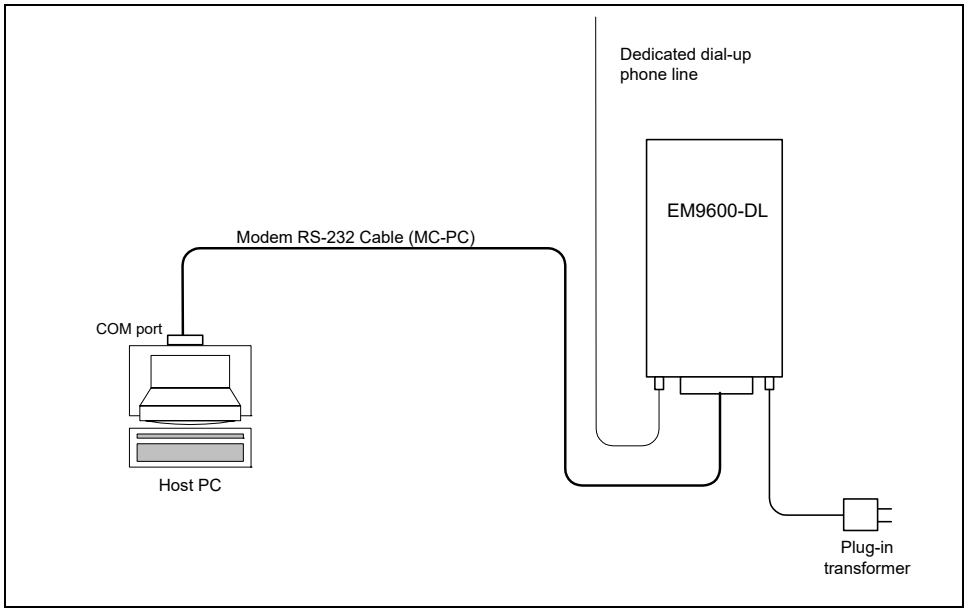


Figure 2-82: EM9600A-DL Dial-Up Modem Connections

The EM9600-DL can also be installed at a DIGI*TRAC controller in this manner:

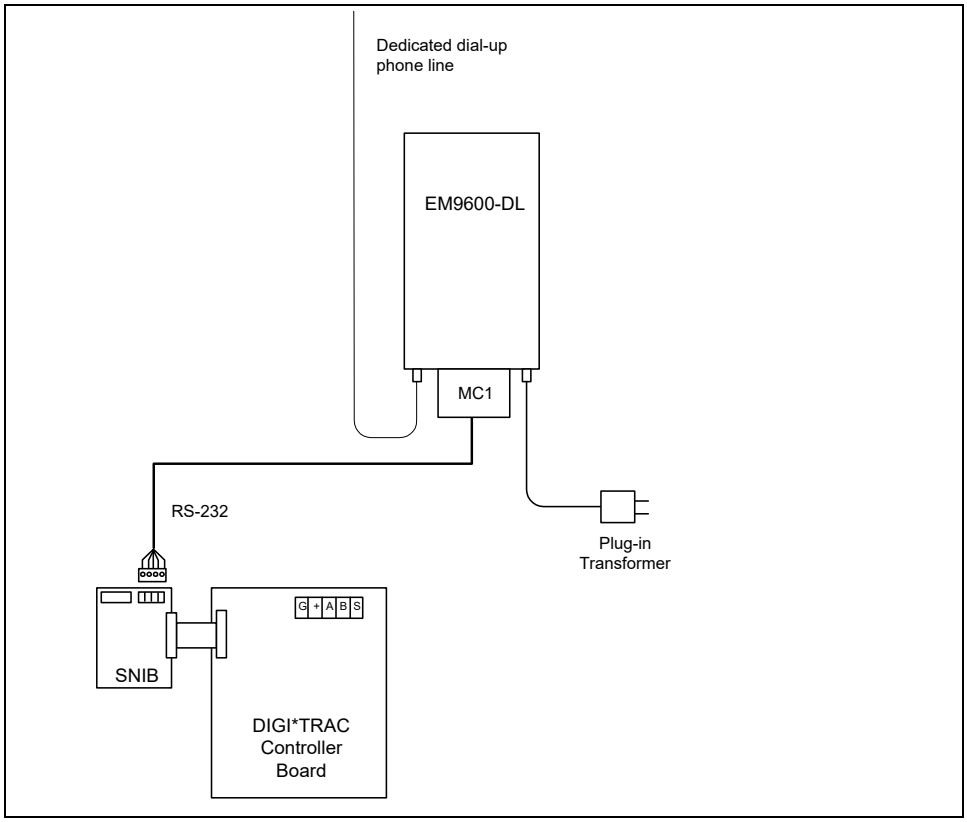


Figure 2-83: EM9600-DL Dial-Up Connections (Controller)

The dedicated phone line is connected to the modem via the ‘Line’ phone jack.

Note: Do not operate dial-up communications through a PBX.

Both dial-up modems operate at 9600 baud.

For more on setting up and installing the dial-up modem, see “Dial-Up Modem Installation” on page 7-345.

Leased-Line Modem

The EM9600-LL is installed near a Host PC or NET*MUX4 or controller. It includes a power transformer. A cable, such as an MC-PC, is required for connection to a host PC. The leased line is connected to the modem via the ‘Line’ phone jack.

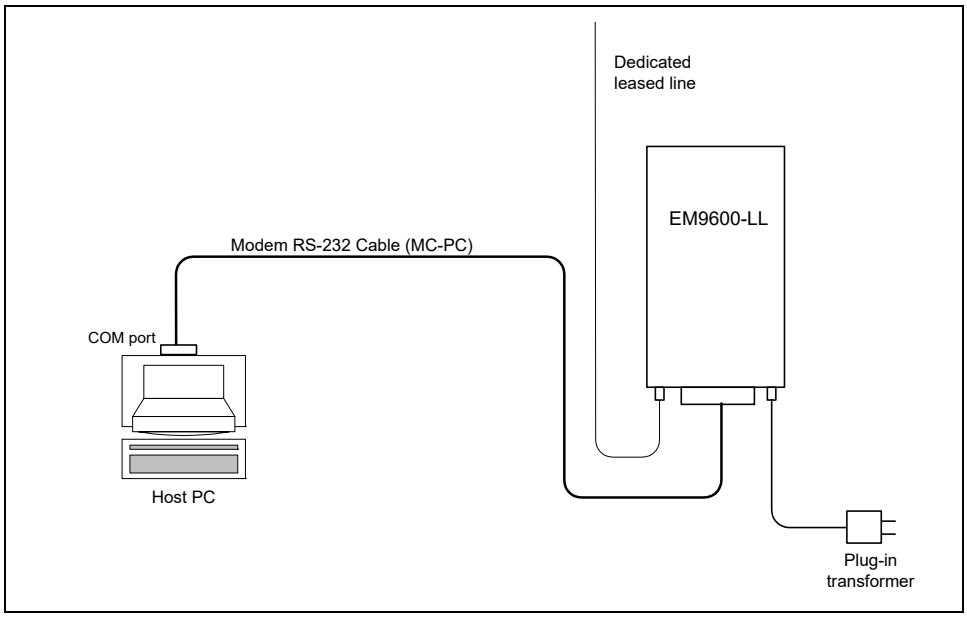


Figure 2-84: EM9600-LL Leased-Line Modem Connections (PC)

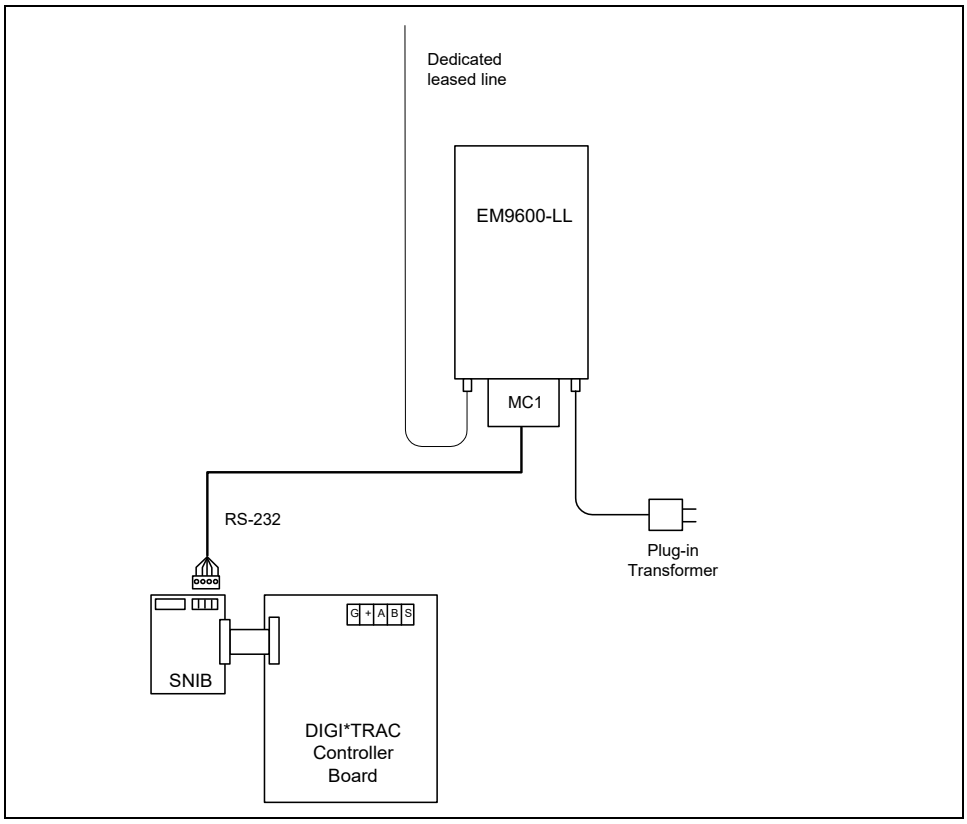


Figure 2-85: EM9600-LL Leased-Line Connections (Controller)

While running these modems, the Auto-Answer feature must be disabled at both the Host PC and remote modems for all brands and types of modems used. Auto-Answer is disabled at the factory for all Hirsch-supplied modems.

Note: PBX phone lines are not supported for leased-line connections.

For more on setting up and installing the leased-line modem, see “Leased-Line Modem Installation” on page 7-351.

Fiber Optic Transceivers

Hirsch currently supports FL Transceivers. All transceivers provide either a simplex (singlemode) or duplex (multimode) RS-422 data link by fiber optic transmission on one end and RS-232 or RS-485 terminal blocks on the other.

Fiber optic transceivers are used for various tasks including:

- ❑ Linking a ScramblePad and/or MATCH to a Controller over long distances
- ❑ Connecting SCRAMBLE*NET via a SNIB to a remote host PC over long distances
- ❑ Providing a highly secure transmission path, since communications are impossible to detect using electromagnetic sensing devices
- ❑ Immunity from electrical noise and transients

The FL transceiver does not support multidrop connections.

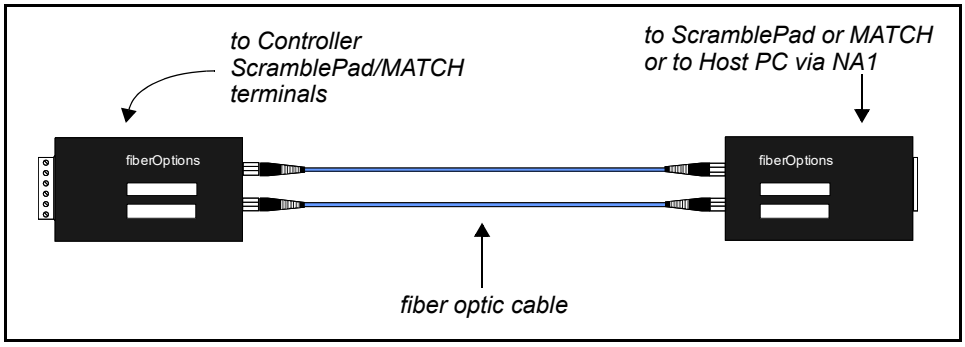


Figure 2-86: Fiber Optic Transceivers

There are 2 types of fiber optic strands in use for security data communications: multimode and singlemode fiber. They come in either 250µ or 500µ outside diameters. The multimode fiber has a core of either 62.5µ or 50.0µ. The singlemode fiber has a core of either 7µ or 9µ. Multimode fiber has a maximum distance of 5 miles; singlemode has a maximum distance of 100 miles. Multimode employs LED light while singlemode uses a laser.

Maximum lengths for each fiber size are shown here (where µ = micron):

Fiber Size	**Maximum Distance (ft./m)**
Multimode	
50.0 or 62.5µ	26,400 (8,047)
Singlemode	
7 or 9µ	528,000 (160,934)

Table 2-28: Fiber Optic Cable Lengths

Consult Hirsch for longer distance requirements.

Note: Do not place a fiber optic transceiver in the controller enclosure.

You can use fiber optic cable for both SCRAMBLE*NET and ScramblePad/MATCH communications circuits.

There are two versions of the transceiver:

- ❑ FLKM (ScramblePad/MATCH communications)
- ❑ FLN (Network communications)

To connect a remote ScramblePad/MATCH to a controller using a FL fiber optic link, connect one FLKM to the controller's SNIB. Connect the other FLKM to the remote ScramblePad/MATCH. The FLKM at the controller end does not require power; however, the FLKM at the ScramblePad/MATCH end does require a 28VDC power supply as shown in Figure 2-87.

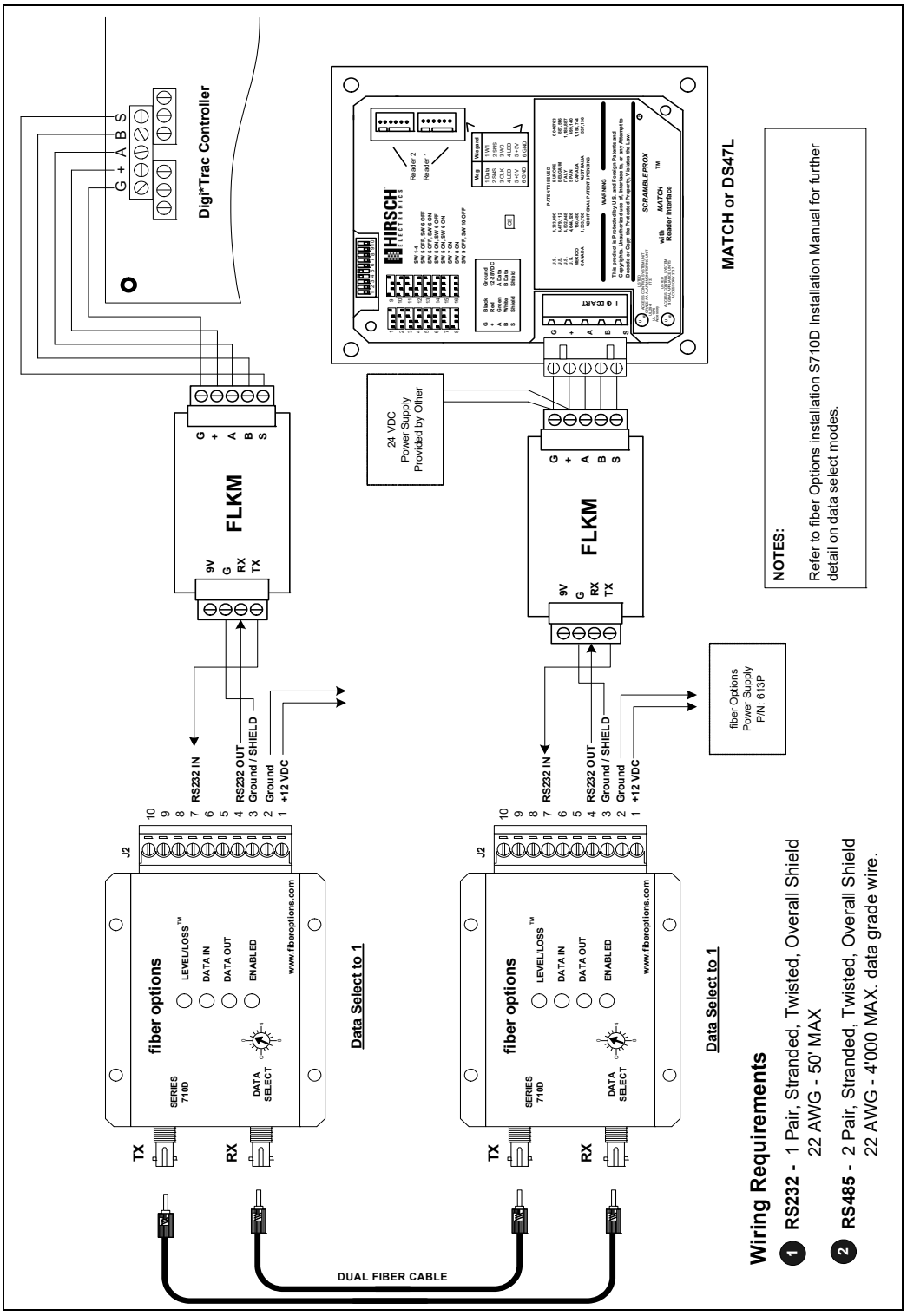


Figure 2-87: ScramblePad/MATCH to Controller Using FL Transceivers

To connect a remote host PC to a Controller, connect one FLN adaptor to the controller's SNIB and the other FLN to an NA1, which is connected to one of the Host PC's serial

ports. This arrangement is shown in Figure 2-88:

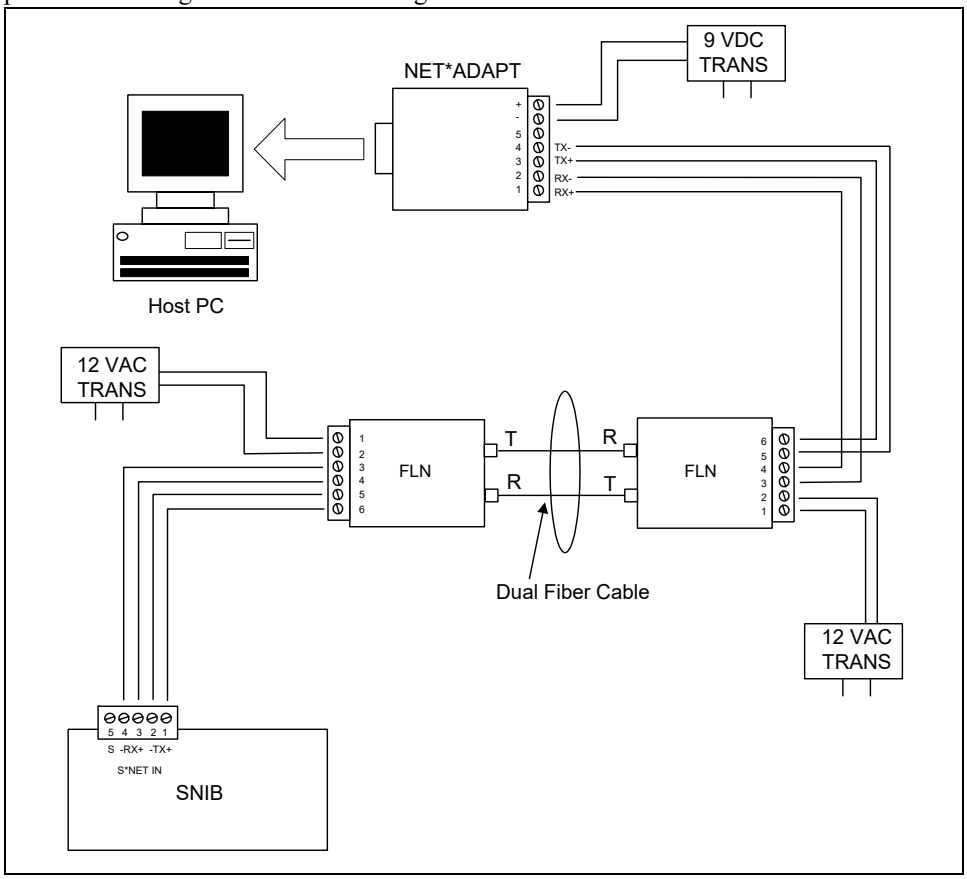


Figure 2-88: Host PC to Controller Using FL Transceivers

Yet another approach takes advantage of the XBox to communicate between the Host PC and a remote controller as shown in Figure 2-89:

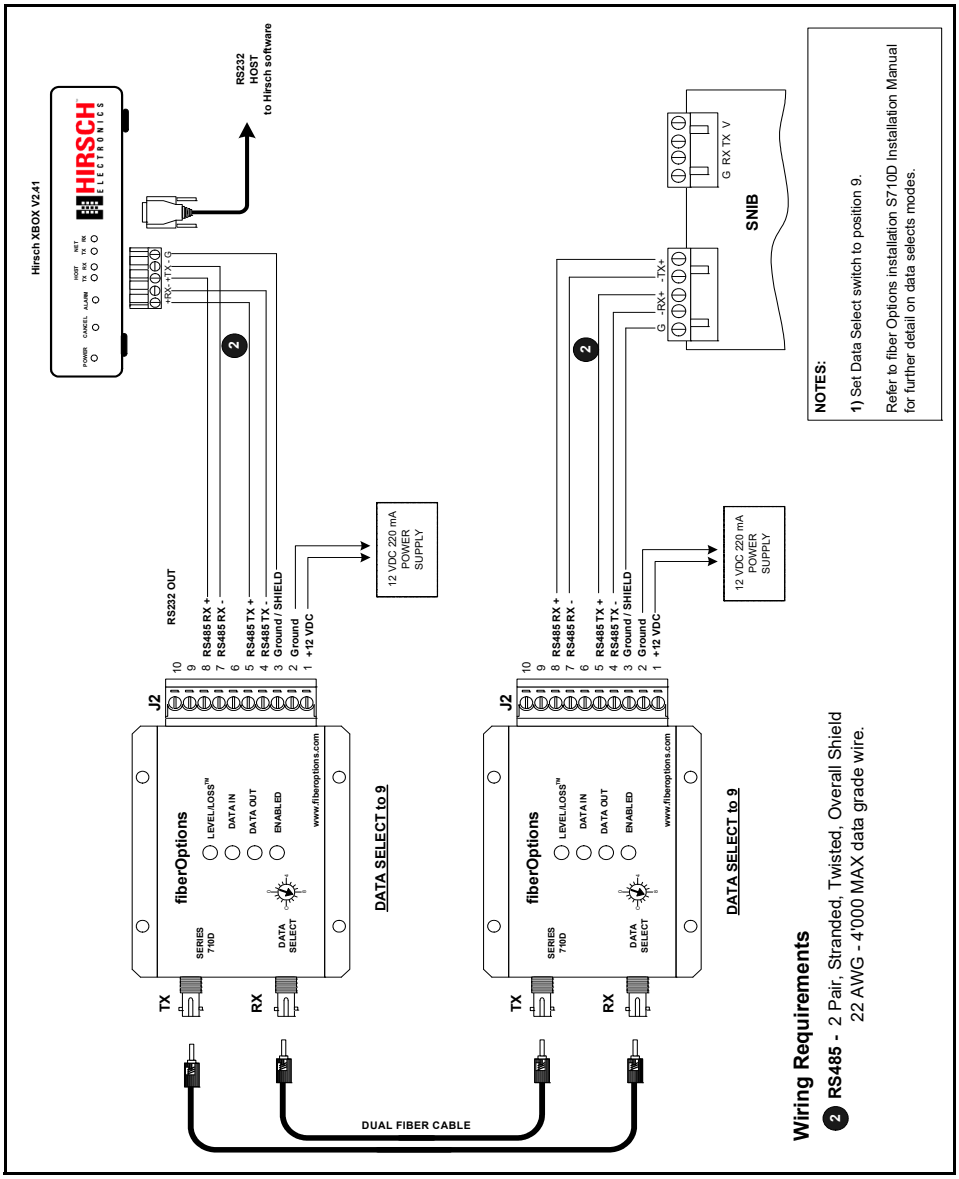


Figure 2-89: XBox to SNIB Communication using FLN

For more on the installation of FL transceivers, see “Fiber Optic Transceiver Installation” on page 7-355.

SCRAMBLE*NET Gateway (XBox)

The SCRAMBLE*NET Gateway (XBox) provides a high-speed gateway from a Host PC to a network of DIGI*TRAC controllers. The XBox can support up to 63 DIGI*TRAC Controllers through a single XBox. The XBox is shown in Figure 2-90:

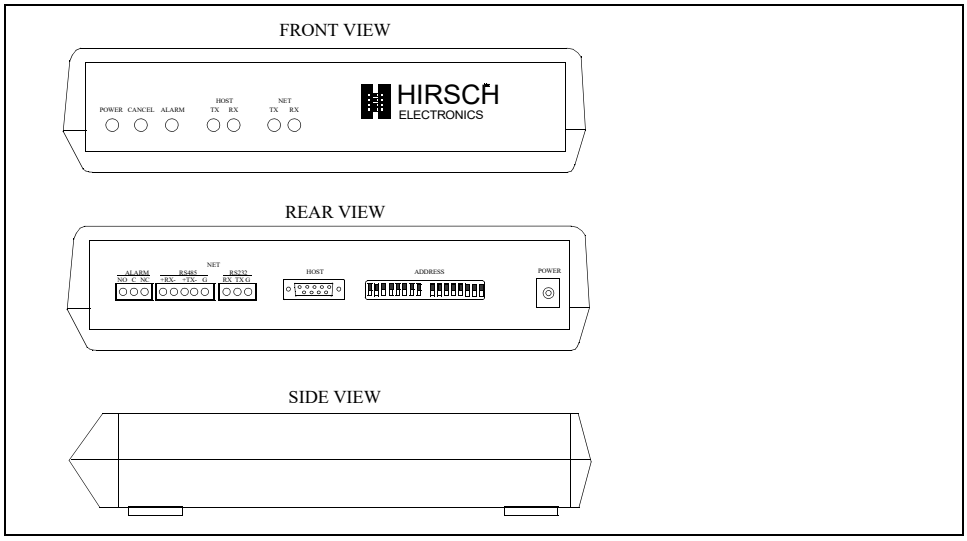


Figure 2-90: XBox Views

The XBox can connect to several outputs:

- ❑ Alarm
- ❑ S*NET Multi-Drop cable (RS-485)
- ❑ S*NET SNIB or Modem (RS-232)

On the other side, the XBox connects to the Host PC using either an RS-232 COM port or an RS-485 COM port. Hirsch can provide a RS-485 port for the Host PC through the installation of the NET*ADAPT for PC (NAPC) board. For more on the NAPC card, refer to page 2-109.

A new version of the XBox, the XBox-ME, comes in a metal enclosure and includes its own transformer. The XBox-ME is available for those installations requiring more security for their XBox sites.

Note: The SNIB2 incorporates the XBox and device server functions into one board. For more about this, refer to "Secure Network Interface Boards (SNIB, SNIB2, or SNIB3)" on page 2-96.

Dimensions: 1 inch (2.5 cm) high x 8 inches (20 cm) wide x 4 inches (10 cm) deep

Weight: 17 oz. (0.5 kg)

For more on configuring and installing the XBox, see "XBox Installation" on page 7-358.

XBox Connection Options

The XBox can be used for a variety of system configurations. The two most common connections are:

- ❑ Hookup for Multi-Dropped Controllers
- ❑ Hookup for Remote Dial-Up Controller

In its simplest configuration, the XBox is connected to a single controller like this:

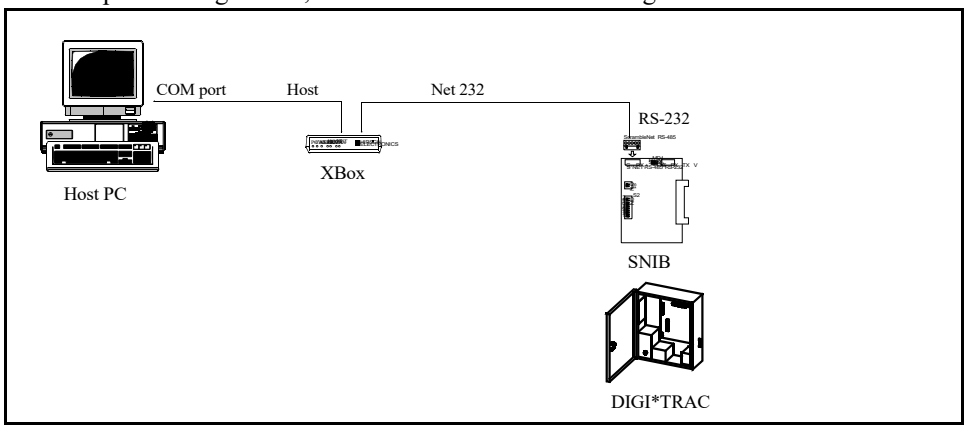


Figure 2-91: Basic XBox Connection to a Single Controller

The XBox can also be used to connect an array of SNIB-installed DIGI*TRAC controllers to a Host PC. This connection looks like this:

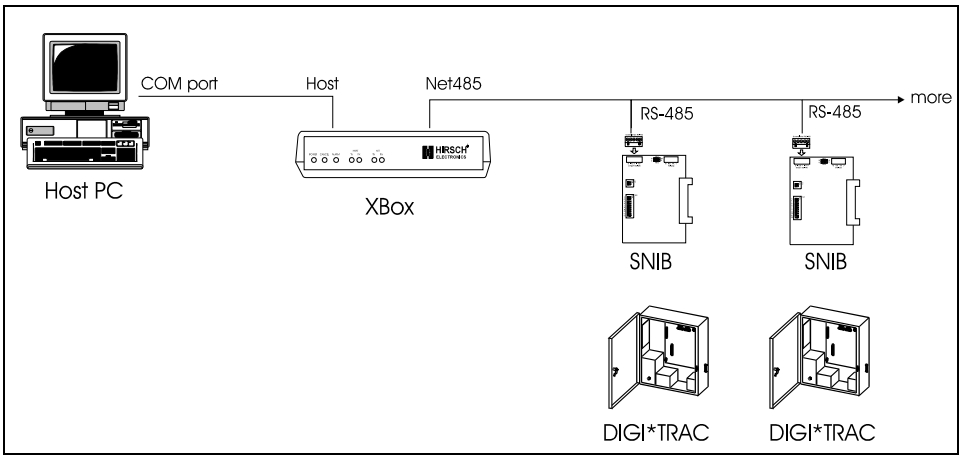


Figure 2-92: XBox Hookup for Multi-Dropped Controllers

For multi-drop connections, use the XBox's RS-485 connector.

The XBox can also be used to connect the Host PC to a remote SNIB-installed DIGI*TRAC Controller through modems (leased-line connections only).

This connection strategy looks like this:

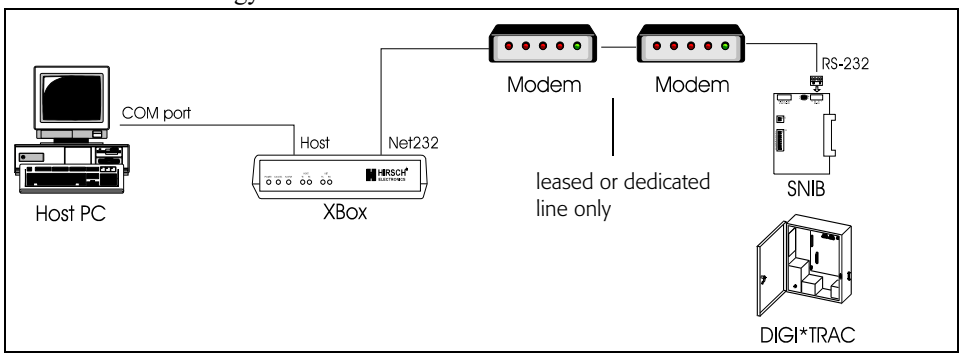


Figure 2-93: XBox Hookup for Remote Leased-Line Controller

Both of these arrangements can also include a NET*MUX4, enabling an even broader network dispersal as shown in Figure 2-94.

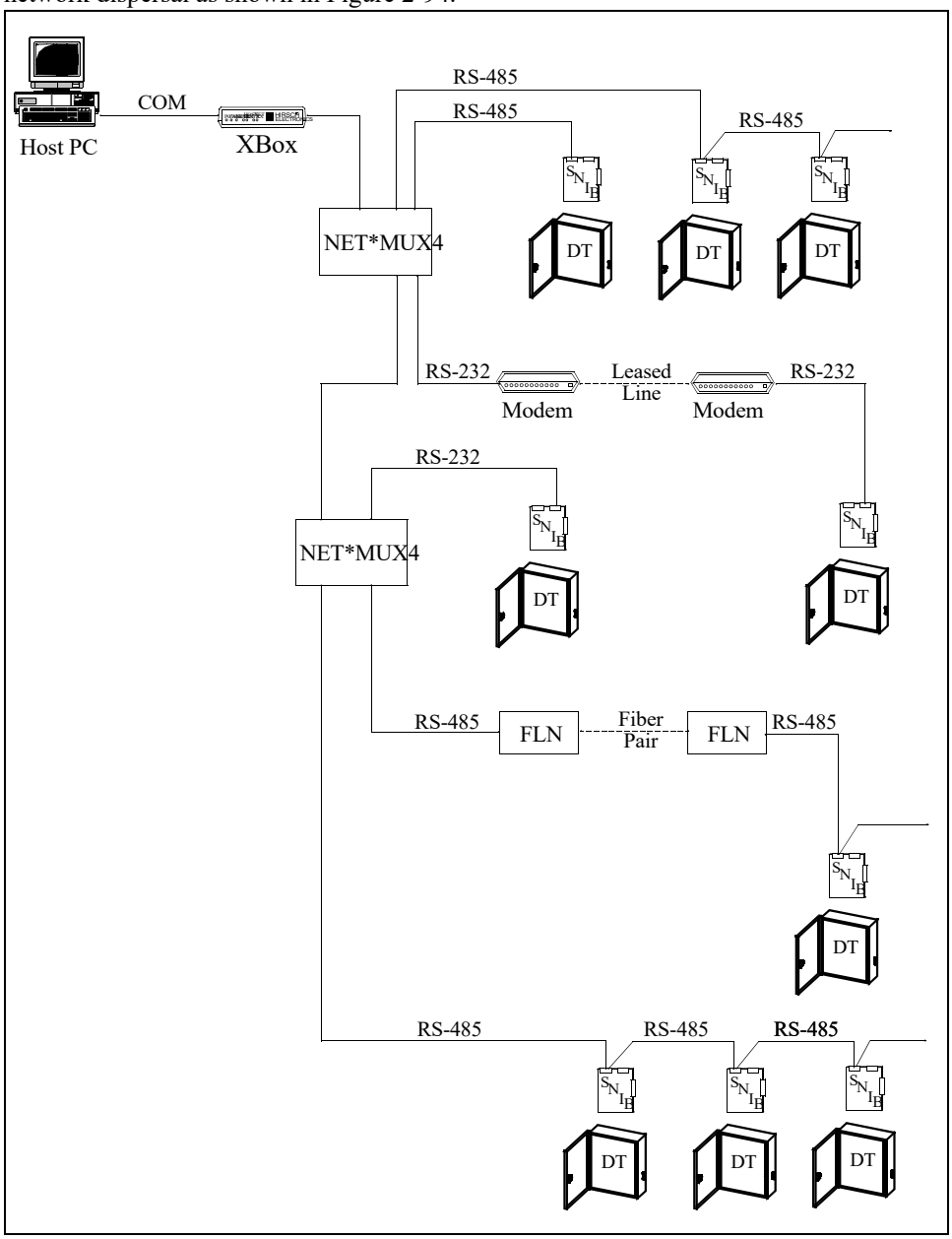


*Figure 2-94: Example of XBox Hook-Up with Cascaded NET*MUX4s*

Figure 2-94 shows how DIGI*TRAC components can be implemented to create large networks which incorporate private multidrop RS-485 and serial RS-232 cable as well as public phone and fiber optic lines. One XBox and two or more NET*MUX4s can be used to create a line of this size utilizing all these different line technologies.

To create even larger networks, multiple XBoxes can be connected, either to separate COM ports on the same Host PC or daisy-chained to the same COM port as in Figure 2-95.

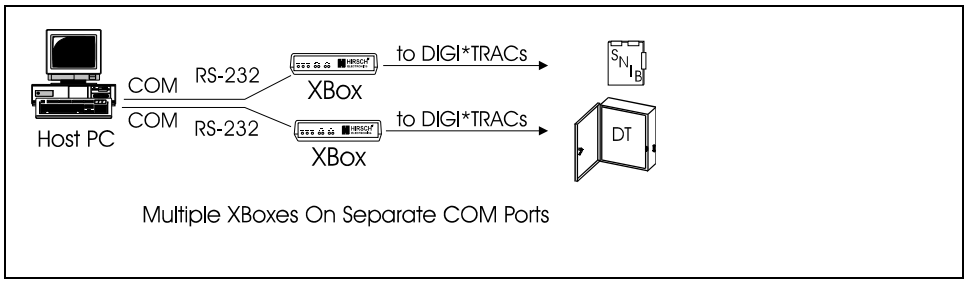


Figure 2-95: Multiple XBox Arrangements

The inclusion of Universal Serial Bus (USB) ports on most PCs has provided additional methods for connecting a host PC to an XBox. Since the XBox currently does not provide a USB connection, you must purchase a USB to DB-9 serial adapter from one of several manufacturers, such as Belkin. This enables you to connect the host PC to an XBox even if all your available COM ports are already used as shown in this example:

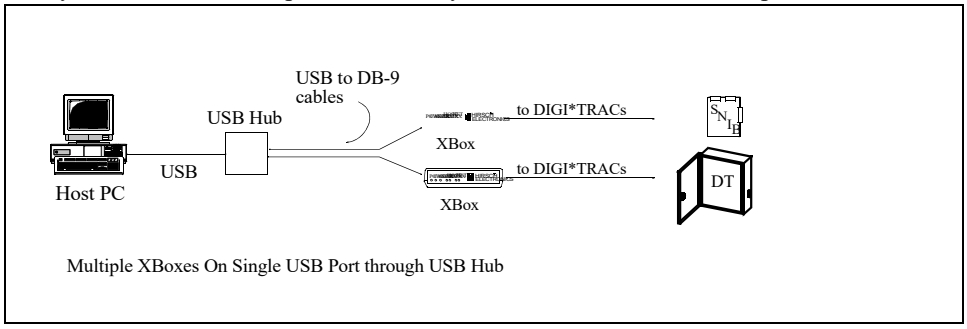


Figure 2-96: USB to XBox Examples

The Hirsch 4-port USB hub (Hirsch #USB-USB4) enables you to connect up to 4 USB devices to the same USB port on your host PC. By connecting a hub to a hub, even more devices can be connected.

Power input rating for the XBox is 12VDC, 300 mA. This is mandated by the XBox power supply included with the device.

For information about configuring and installing the XBox, see “XBox Installation” on page 7-358.

Network Communications: Device Servers

Modern security procedures no longer require dedicated lines and wiring. Hirsch supports the use of its products over both local area networks (LANs) and wide area networks (WANs) without diminishing security. Through this design, facilities in even widely separated locations can communicate with each other. For example, a single operator in Los Angeles might monitor and control security installations in New Mexico, New York, and London without compromising security in any location.

The normal method used for connecting elements of a Hirsch security system to either a LAN or WAN is through a device server or SNIB2. Device servers enable communications between serial connections, such as RS-232 and USB, and the Ethernet (TCP/IP). For this purpose, Hirsch currently supports several varieties of Lantronix and Digi device servers; the type you use in your installation depends on the type of Hirsch software you plan to use with the system:

Hirsch Application	Device Server Type
MOMENTUM	Lantronix MSS-1 or MSS-100
Velocity	Lantronix UDS-10 Digi One SP and Digi PortServer TS

Several examples of how these device servers can work on a system are shown below. The first example shows how you can utilize LAN/WAN networks to communicate amongst MOMENTUM clients and server while still maintaining hardwired connections to controllers. This arrangement does not use a device server.

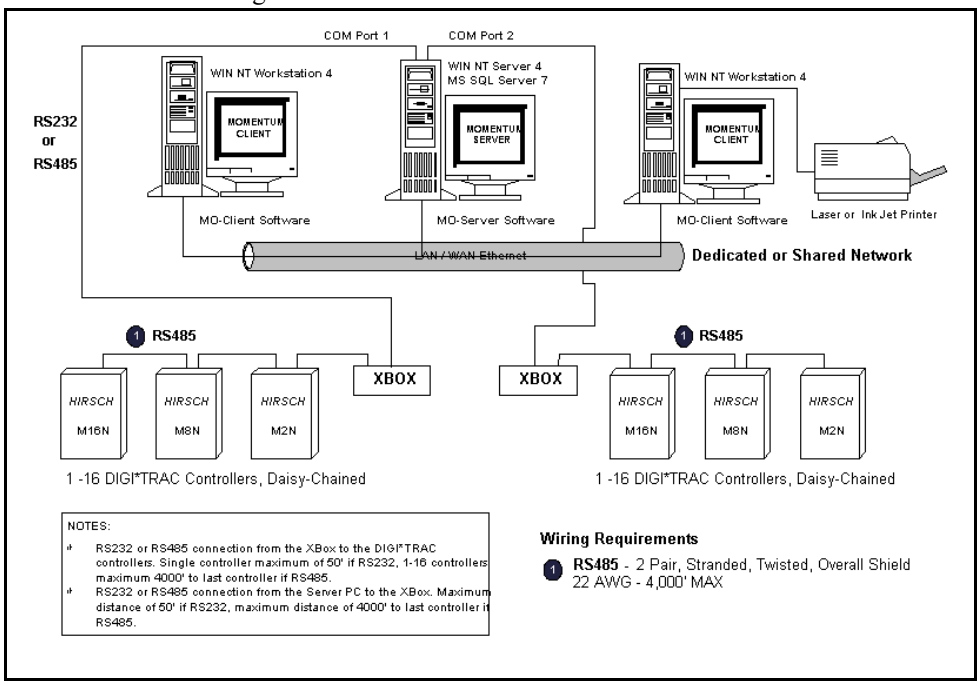


Figure 2-97: MOMENTUM Example: Server, Multiple Client, Hardwired Connections to Controllers

The second example utilizes device servers to incorporate XBoxes into the network.

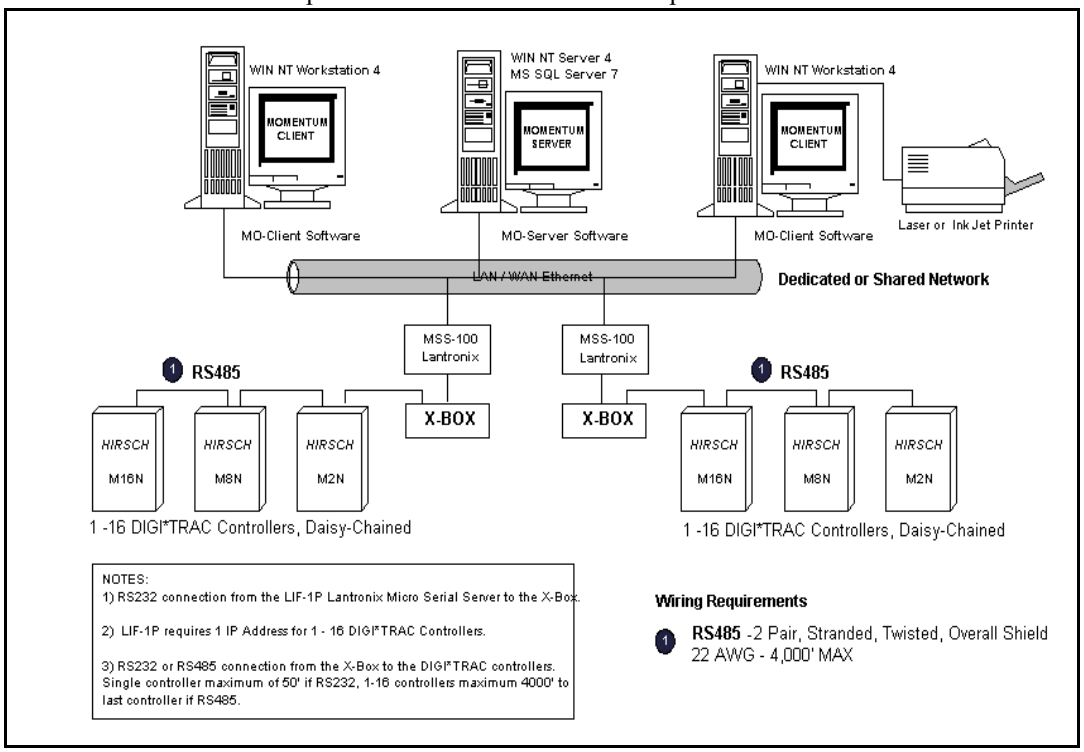


Figure 2-98: MOMENTUM Example: Server, Multiple Clients with LAN/WAN Connections

The third example shows how device servers can be used with Velocity installations.

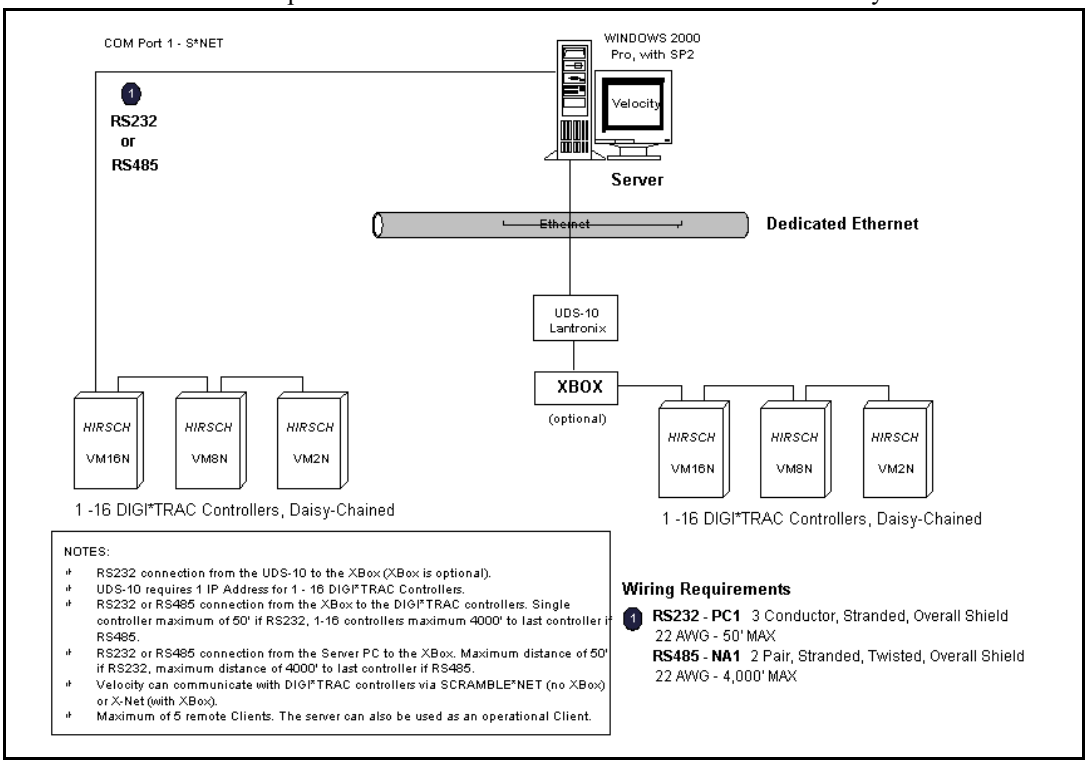


Figure 2-99: Velocity Example: Single User Dedicated Security Network

The fourth example shows how complex networks can be created using Velocity installations.

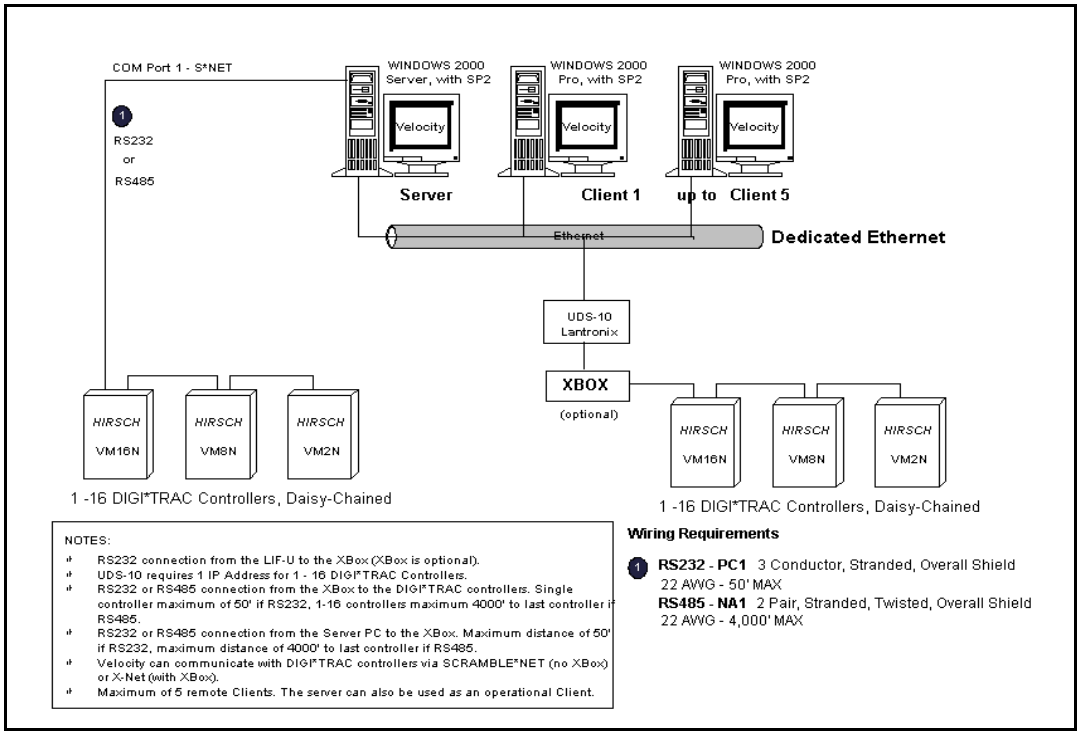


Figure 2-100: Velocity Example: Client/Server Dedicated Security Network

The fifth example shows how the Digi devices can simplify this configuration using Velocity:

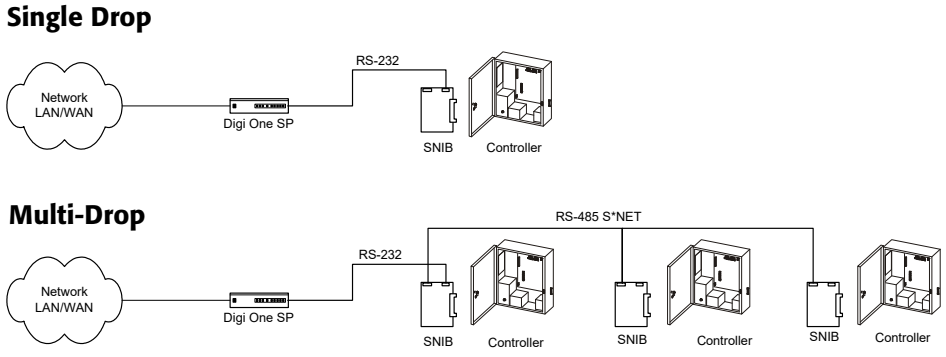


Figure 2-101: Velocity Example: Single& Multi-Drop Configurations Using Digi One SP

The sixth and final example, Figure 2-102, shows how the Digi PortServer can be used to achieve complex configurations for Velocity in both single and multi-drop.

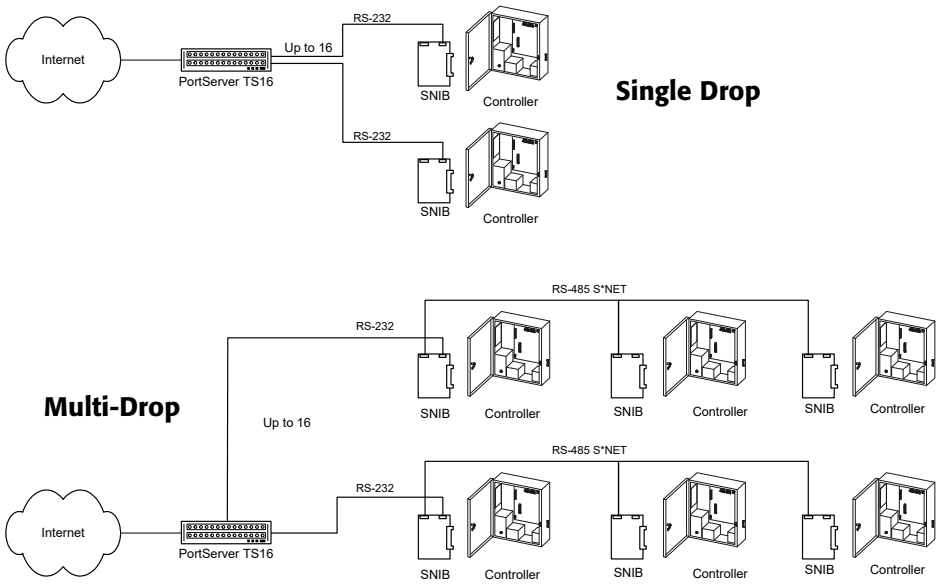


Figure 2-102: Velocity Example: Single & Multi-Drop Configurations Using Digi PortServer TS16

While device servers are an effective solution for many networked Hirsch systems, the new Hirsch SNIB2 can circumvent device servers and XBoxes entirely.

For more about the SNIB2, refer to "Secure Network Interface Boards (SNIB, SNIB2, or SNIB3)" on page 2-96.

For more information about installation, configuration, and use of these devices:

- ❏ For the MSS-1 and MSS-100, refer to Appendix A. "Lantronix MSS Installation," of the *MOMENTUM Users Guide* (Hirsch MAN003).
- ❏ For the UDS-10, refer to "Configuring UDS-10 Device Servers" in the *Velocity Quick Installation Guide* (Hirsch MAN004).
- ❏ For the Digi One SP, refer to "Digi One SP" in the *Velocity Quick Installation Guide* (Hirsch MAN004).
- ❏ For the Digi PortServer TS16, refer to "Digi PortServer TS 16" in the *Velocity Quick Installation Guide* (Hirsch MAN004).

Programming Basics

3

Overview

Initial programming (referred to as ‘setups’) is typically performed by the dealer or installer based on plans and specifications, or after consultation with the prospective client. Once the system is installed and operational, the client/owner usually performs additional programming to tailor the system to their unique requirements.

The setups determine how the system works. For instance:

- ❑ How many seconds is a door unlocked by a valid code?
- ❑ Does the front door automatically unlock at the start of the business day and relock at the close?
- ❑ Are all interior alarm sensors masked during certain times of the day or are they masked manually by code entry on an area-by-area basis?

Once setups are entered and the controller is configured for operation, users can be added to the database. This programming step typically answers: ‘Who goes Where and When.’

This chapter discusses the basics of programming the DIGI*TRAC system using easy-to-learn commands. This collection of commands is called the DIGI*TRAC Control Language (DCL).

These major topics are described here:

- ❑ Preparations for Programming
- ❑ Basic Programming Procedures
- ❑ How the firmware is Organized
- ❑ How to Program From the ScramblePad
- ❑ Command Flowchart
- ❑ Programming Application Guidelines

Preparations for Programming

Installing a DIGI*TRAC Access Control System enables you to control Who, When, Where and Why access will be granted and denied. To take full advantage of these capabilities requires well-organized and detailed information about

- ❑ How the system will operate
- ❑ What groups of users will be authorized access
- ❑ The times and days when access will be granted and denied
- ❑ Which access doors will be authorized for which groups of users

Where to Program

Programming a DIGI*TRAC controller is usually done in one of two ways:

1. **Controller Programming Via PC**
   The most common method for programming the DIGI*TRAC controller is from a PC with software such as Hirsch's SCRAMBLE*NET Access Manager (SAM). This enables the programmer or system manager to program any access point in a multi-controller system from one central location, whether connected by modem or hardwired.
2. **Controller Programming Via ScramblePad**
   Program from a ScramblePad installed near the controller or at a door. Programming from a ScramblePad enables you to manage all readers, inputs, and outputs connected to a single controller. This method is also a useful option if a host PC is unavailable.

Note: The ScramblePad you use for programming can either be dedicated to programming or the same one used for door access control.

This manual will focus on the use of a ScramblePad, in conjunction with a local printer, for programming.

Appendix A provides worksheets which aid you in programming for your specific system.

Basic Programming Procedures

Programming with the ScramblePad is simply a matter of pressing the START button, entering a series of parameters, separated by an asterisk (*), and concluding with the Pound key (#) which sends the entire string of numbers to the controller.

Figure 3-1 shows the face of a ScramblePad reader in its unscrambled state (the ScramblePad does not scramble while in Programming Mode):

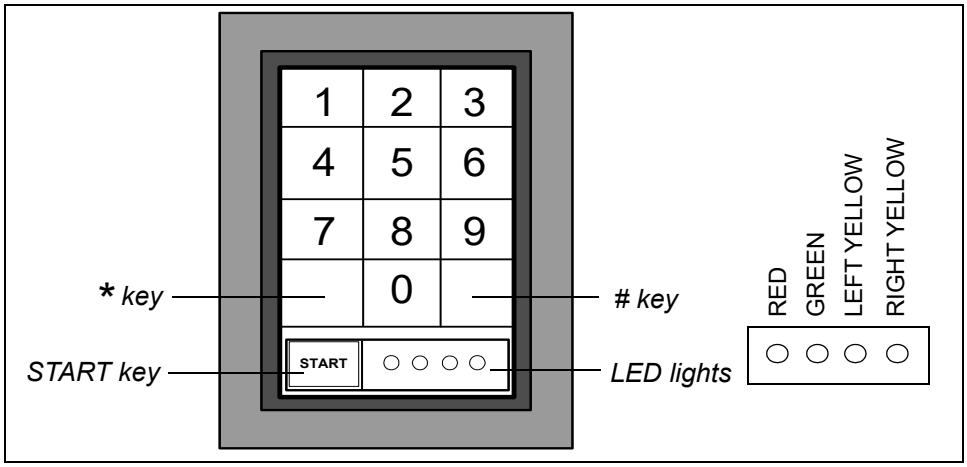


Figure 3-1: ScramblePad Setup

Note: The Asterisk and Pound keys are not labeled on the ScramblePad.

These keys are used in the following ways:

This Key:	Tells the Program That:
START	This is the beginning of the command sequence.
*	Another element of the command sequence follows, such as a variable or option. This is a *separator*.
#	This signals the *end* of the command sequence and *sends* it to the controller.

Programmers will see the results of their entries on the ScramblePad LEDs:

This LED state:	Tells You That:
Both Yellow LEDs Flashing	The ScramblePad is in Program Mode but the program entry code is still at the default (123) and should be changed.
Right Yellow LED Flashing	In Program Mode with entry code changed.
Red LED and Tone	Denied Command
Green LED	Granted Command

Table 3-1: ScramblePad LED Programming Responses

For basic instructions on how to enter commands, see “Programming From The ScramblePad” on page 3-45. For a complete explanation of commands and their syntax, refer to Chapter 4, “Command Reference”.

How the Firmware is Organized

Before explaining how to program, it is important to know how the firmware is organized. This will help in selecting the most appropriate command for the application.

The DIGI*TRAC Control Language (DCL) is organized around a number of concepts and affects several components. The basic structure of this program is explained in this section.

Note: It may be helpful to refer to the Glossary for terms used in this section.

Memory

The DCL program resides in firmware in the Command & Control Module (CCM) of the Controller. This module stores DCL in 'non-volatile' memory which doesn't need to be backed up by battery and cannot be changed by the user. Setups, User Database, and other user defined control sequences are in battery-backed RAM (Random Access Memory) and can be modified by the user.

DIGI*TRAC ships with many factory default settings which allow many functions to occur without additional programming; however, every installation will require some customization by entering commands. Entering commands is the process of programming a DIGI*TRAC controller from a ScramblePad keypad. Each command places values into the controller's RAM memory for the firmware to utilize as the on-board microprocessor executes its instructions.

All DIGI*TRAC controllers have the same CCM and therefore the same firmware. However, the hardware for each controller will support different quantities and types of inputs, outputs, and readers. For this reason, programming requires a knowledge of the hardware components selected for a particular installation as well as the universal firmware.

Hardware

DCL programming depends on the hardware configuration. The discrete addresses firmware uses to build tables of relationships between external components (such as a door contact) and internal components (such as time of day) are based on the following hardware configuration issues:

- ❑ The number and type of devices which are wired to which terminal blocks in the controller.
- ❑ The DIP switch settings made to the ScramblePad and MATCH.

Hardware configuration issues encountered while programming a Hirsch controller are included in the following sections.

Time

The controller uses an on-board hardware time clock for precise time keeping. DCL commands are used to set the time of day, the date (month, day, & year), and the day of week. As long as there is power (including battery backup), the hardware clock will keep accurate time and date.

Line Module Inputs

Line Module Inputs receive their address based on which terminal block the associated Line Module is wired to. For example, a door contact wired to a Line Module, which is in turn wired to Terminal Block 2 on a Model 8, will have an address of 2. Were the same door contact and Line Module wired to the third terminal block on the first AEB8 (Alarm Expansion Board) in the same Model 8, its address would be X3. If it were wired to the third terminal block on the second AEB8 in the Model 8, it would be assigned an address of X11.

*Note: DIGI*TRAC firmware supports 8 door line module inputs and 16 general purpose inputs, Expansion Line Module Inputs. Expansion Line Module Inputs use an X prefix to differentiate them from Door Inputs.*

RQE & Tamper Inputs

Request-to-Exit and Tamper inputs share the same address as the Line Module Input (see above). The Line Module is intelligent enough to send three separate signals to the controller indicating the type of alarm it senses: Line Module Input, RQE or Tamper. The firmware then uses the address—such as, 2 (on Door Terminal Block 2)—and the function—for example, RQE—to create a unique identifier for the input.

Relay Outputs

Relay Outputs receive their address based on which terminal block the associated lock, strike, control relay, or other controlled device is wired to. For example, a magnetic lock for door access control which is wired to Terminal Block 2 on a Model 8 will be assigned an address of 2. If a lighting contactor is wired to the third terminal block on the first REB8 (Relay Expansion Board) in the same Model 8, it would have an address of X3. If it were wired to the third terminal block on the second REB8 in the Model 8, it would have an address of X11.

*Note: DIGI*TRAC firmware supports 8 Door Relay Outputs and 64 general purpose, Expansion Relay Outputs. Expansion Relay Outputs use an X prefix to differentiate them from Door Relay Outputs. Outputs not physically used (wired) may be used as virtual points for programming.*

ScramblePads

ScramblePads receive their address based on their DIP Switch setting, not the terminal block to which they are wired. If a ScramblePad's DIP Switch is set to 2, the controller assumes it is associated with Door 2; if the switch is set for 7, it is associated with Door 7. There can be a maximum of 8 Doors.

For entry and exit applications, DIP Switch settings of 1 through 8 are assigned to entry devices and 9 through 16 are assigned to exit devices. To assign the correct exit device to the correct door, set the device's DIP Switch to 8 plus the door number. For example, the exit ScramblePad on Door 2 would have a DIP Switch address of 10, and the exit ScramblePad on Door 7 would have a DIP Switch address of 15.

Note: If a ScramblePad is used strictly for programming, it may have any unused DIP Switch address.

MATCH

MATCH, like the ScramblePad, receives its address assignment based on its DIP Switch setting, not the terminal block to which it is wired. A DIP Switch setting of 4 is associated with Door 4, and 8 is associated with Door 8, up to a maximum of 8 Doors. For entry/exit applications, the MATCH has a separate connector for an entry and exit reader. An additional DIP Switch on the MATCH configures the MATCH for one or two readers. A MATCH is included with the DS47L-series ScramblePad.

Dual Technology

When both a ScramblePad and a reader are used for entry and/or exit, the ScramblePad is wired to the MATCH. The same DIP Switch setting rules apply for dual technology as for single technology. The MATCH will combine the ScramblePads and readers into the basic unit of a DIGI*TRAC controller: the Door.

Firmware

Timers

Many of the DCL Commands utilize timers, such as to set the Door Timer, or the Door Open Too Long (DOTL) timer. Timers typically have parameters for the duration in seconds.

Time Zones

Time Zones may be visualized as a table with columns for the Time Zone number, Start Time, End Time, and Day of Week. The Week starts on Monday and ends on Sunday, but includes an eighth day which is used for holiday functions.

Figure 3-2 provides an example of a printout showing Standard Time Zones as they are returned by issuing CMD 88*3.

```
Standard Time Zone Setups and Status
  #       Start       End  MTWTFSSH 1234
  0: From 00:00  to  00:00 -------- ---- Inactive
  1: From 08:00  to  16:00 XXXXX--- ---- Active
  2: From 09:00  to  17:00 XXXXX--- XXXX Active
 65: From 00:00  to  24:00 XXXXXXXX XXXX Active
```

*Figure 3-2: CMD 88*3 Printout*

There are 65 Standard Time Zones, two of which are predefined: Time Zone 0, which represents ‘never’ and Time Zone 65 which specifies ‘always.’ In addition, there are Master Time Zones and Grand Master Time Zones, which support the grouping of Standard Time Zones for flexibility in programming.

Time-Based Functions

Time-based functions utilize a time zone to initiate a change of state or a control function. Examples of time-based functions include masking a line module input and door relay control for free access during normal working hours. DCL programming commands typically have parameters to designate the input or output, the time zone used, and the action required.

Access Zones

Access Zones link a time zone number to a door number. In this way, an access zone can be used to designate when and where a user can go. A single access zone may contain up to all 8 doors, each with a unique (or common) time zone number. Access zones may be visualized as a table with columns for access zone number and doors 1 – 8. Each access zone will have a time zone number under the door number to indicate the relationship. Figure 3-3 provides an example of a printout showing Access Zones as they are returned by issuing CMD 88*5.

```
Standard Access Zone Setups
   |  |  |        <-Time Zones->         |
AZS|TG|AL| R1| R2| R3| R4| R9|R10|R11|R12|
  0|--|--| - | - | - | - | - | - | - | - | - |
 65|--|--| 65| 65| 65| 65| 65| 65| 65| 65|
```

*Figure 3-3: CMD 88*5 Printout*

There are 65 Standard Access Zones two of which are predefined: Access Zone 0 which specifies ‘no doors/never’ and Access Zone 65 which indicates ‘all doors/always.’ In addition, there are Master Access Zones, which support grouping of Standard Access Zones for flexibility in programming.

Note: This printout shows that an Access Zone can also enable time-based Masking of Expansion Line Module Inputs as well as enable the Tagging or Alert functions.

Scramblepad/MATCH Functions

Anti-Passback control can be established for both ScramblePad and MATCH doors. Other functions specify whether the ScramblePad is silent; whether the display status is shown on the ScramblePad’s LEDs; whether a specific ScramblePad is used for programming; access, or both; whether the ScramblePad is used for control functions; and many more functions.

Duress

When ScramblePad or dual technology is used, the user can enter an extra ‘Duress’ digit which permits access while issuing a silent alarm. This is used for signalling security that the user is being forced to enter an area. To be used, this feature must be enabled prior to creating user codes using Commands 08 and 09.

Note: Only use this feature if someone will be monitoring the system.

Normally duress digits are entered immediately after the qualified user’s PIN code, like this:

```
184059 #
```

where 9 is the duress digit and 18405 is the user’s PIN number.

The following commands are important in using duress digits:

88*2#	This reports the status of Duress Alarm Mode and Code Generation.
35*UN#	This reports the Duress Digit of the User Number entered for UN.
08*1#	Turns on Duress Alarm Mode. The default is OFF.

09*1	Turns on Duress Code Generation. The default is OFF.
07*DD#	Changes the Duress Digit from the default of 9 to DD.
14*DD*UN#	Changes the Duress Digit to DD for the User Number UN.

Users

User Numbers are unique numbers used in lieu of names in the DIGI*TRAC controller for standalone applications. With memory expansion, up to 32,000 users can be assigned to the controller database. Users are assigned to Access Zones to determine who can go where and when. When a user is assigned to an Access Zone, they are also assigned their 3- to 8-digit Code (for ScramblePads) and/or their Card (for card readers).

When a User enters an authorized Code or presents an authorized Card, the Door will be momentarily unlocked and the Door Contact Alarm Masked, based on the defaults or user-defined parameters established in the setup programming.

Expansion Inputs/Outputs

Although Doors use Line Module Inputs and Relay Outputs, most general purpose alarm monitoring and control is done by Expansion Inputs and Outputs. As a general rule, firmware recognizes the points on the AEB8 and REB8 expansion boards as Expansion Inputs (XIs) and Expansion Relays (XRs). However, the points on the base Model 16 are actually Expansion Inputs and the points on the base Model SP are actually Expansion Relays to the firmware. It is important to enable these XIs and XRs and assign the points to Access Zones and Control Zones for general purpose monitoring and control. The procedure is similar to assigning doors but the addressing and printouts are different.

Control Zones

Control Zones link a Time Zone number to an Input/Relay number. In this way, a Control Zone can be used to designate when and which input can be masked, or relay controlled. A single Control Zone contains one Time Zone with up to 8 Door Inputs/Relays, up to 16 Expansion Inputs, and up to 64 Expansion Relays. Control Zones can be visualized as a table with columns for Control Zone #, Time Zone #, Door Input/Relays #, and Expansion Input/Relay #. Figure 3-4 provides an example of a printout showing Standard Control Zones as they are returned by issuing CMD 88*6.

Note: A Time Zone is only used to restrict the command when a Control Zone will be activated by a Card or Code. The Time Zone does not effect the triggering of a Control Zone by an input or an alarm.

```
Standard Control Zone Set Ups
 CZS| TZ | TAG|ALRT| ONBOARD  |
  0 |  0 | -- | -- |   None   |
  1 | 65 | -- | -- |   None   |


    | Expansion Relays or Inputs:
    |           1111111 11122222 22222333 33333334 44444444 45555555 55566666
 CZS| 12345678 90123456 78901234 56789012 34567890 12345678 90123456 78901234
  0 | -------- -------- -------- -------- -------- -------- -------- --------
  1 | XXXX---- -------- -------- -------- -------- -------- -------- --------
```

*Figure 3-4: CMD 88*6 Printout*

Line Module Inputs and Relay Outputs share a common address. Since Control Zones are operated based on entering Relay Control Codes or Alarm Control Codes at a ScramblePad, the Code function will actuate the set of Relays, or mask the set of Line Module Inputs as appropriate. Control Zones can also be triggered by cards at a reader or relays (for cascade control), a change in occupancy count, and so on.

There are 192 Standard Control Zones of which one is predefined: Control Zone 0 always indicates 'no relays & no inputs/never.' In addition, there are Master Control Zones which support special actions and groupings of Standard Control Zones.

Note: This printout shows that a Control Zone can also enable the Tagging or Alert functions.

User Access and Control Functions

A user can be assigned multiple codes and cards for use on a ScramblePad and reader. In addition to a code for access through a door, additional codes can control relays, mask line module inputs, and perform other access and control functions.

Note: When you use cards only, you must assign a new card for each new function defined.

An understanding of these functions is crucial when you begin to program the system. Functions include:

- ❑ Assigning unlock and relock privileges for users (CMD 15)
- ❑ Associating users with specific alarm and relay functions (CMDs 40–42/225/325)
- ❑ Setting time zone control of alarms and relays (CMDs 76/82)
- ❑ Associating input/output behavior with master control zone definitions (CMD 304)
- ❑ Defining function groups (CMDs 425/426)

For more about function groups, refer to "Function Groups" on page 3-28.

For practical purposes, control functions can be divided into two main categories:

- ❑ Relay or output functions
- ❑ Alarm or input functions

Each is explained on the following pages.

Relay/Output Functions

Relay or output functions involve escalating levels of priority. The lowest priority level is the access level, represented by the Momentary, Unlock, and Relock functions. These functions involve opening or closing a single door at the keypad/reader where the request is made. For this reason, this level of relay function can be defined based on an access zone (standard or master). The user can actuate a door relay timer, unlock or relock a door based on an access zone.

Higher levels of control—such as triggering, forcing, or locking relays—require you to define control zones rather than access zones since they can involve more than a single relay/output at the current keypad/door. These higher-level functions enable the user to control a large number of relays and other outputs from a local keypad or card reader.

The common output control functions are shown in Table 3-2 on page 3-12.

Pri	Function	Description	Comment
Lowest Level Access Codes, Single Relay Only			
LO	*Momentary*	Actuates the door timer for a period of time specified by the door timer.	*Momentary* and *Trigger* are the only two functions that are timed: going on then turning off according to a timer set to a predefined interval. All other functions are either On *or* Off. This is the lowest priority level of relay actuation. The door timer interval is defined using CMD 80. An access user is defined using Commands 10, 19–22, and so on.
	Unlock	Actuates the relay and leaves it on until it is relocked.	This affects only the door/relay at which it is issued and therefore requires an access zone to define it. This is the next lowest level of relay actuation; only momentary is lower. This function is defined using CMD 15.
	Relock	Relock a relay that has previously been unlocked.	This is the necessary twin to unlock. It must be used to negate the unlock function and return the door to its normal resting state. This affects only the door/relay at which it is issued and therefore requires an access zone to define it. This function is defined using CMD 15.
Mid-Level Control Codes, All Outputs within Standard Control Zone— All functions with higher priority than Relock can control outputs beyond a single door. Unlike Momentary, Unlock and Relock, the Trigger, Force, and Lock functions are specified by control zones, not access zones.			
MID	*Trigger*	Actuates the control timer for every output specified by the control zone. Once the timer times out, the relays/outputs are returned to their default resting states.	Trigger is a timed control function, like the Momentary access function: going on then turning off according to a control timer set to a predefined interval. All other functions are either On *or* Off. This function is defined using CMD 40. The control timer interval is defined using CMD 81. For an expansion relay timer, use CMD 181. A trigger can also be used to trigger multiple actions in a Master Control Zone.
	Force ON	Every relay/output in the control zone is actuated. The relay continues to be actuated until released.	This function can affect both onboard and expansion relays. This function is specified using CMD 40.
	Force ON Release	Returns all relays that were actuated by the Force ON condition to their default resting state.	This function can affect both onboard and expansion relays. This function is specified using CMD 40.

Table 3-2: Common Output Control Functions

Pri	Function	Description	Comment
	Force OFF	Disables all relays associated with this control zone.	This control is particularly useful for x-ray rooms or laboratories where no access is granted during an examination or experiment. This function is specified using CMD 40.
	Force OFF Release	Returns all relays that were forced off by the Force OFF control to their default resting state.	This function is specified using CMD 40.
Highest Level Control Codes, All Outputs within Standard Control Zone— The Lock functions—Lock Down, Lock Down Release, Lock Open, Lock Open Release—have the highest priority and will override both the lower-priority Trigger and Force control codes as well as the lowest-priority Momentary, Unlock, and Relock access codes.			
HI	*Lock Down*	Disables all relays/outputs associated with this control zone.	This is particularly useful for those facilities where absolutely no one is allowed within an area for a specified time. This function is specified using CMD 41.
	Lock Down Release	This undoes the Lock Down command and returns all relays/outputs associated with this control zone to the next highest condition currently in effect.	This function is specified using CMD 41.
	Lock Open	Actuates all relays associated with this control zone.	This is particularly useful for facilities where everyone is allowed to enter or exit an area for a specified time, such as during an emergency. This function is specified using CMD 41.
	Lock Open Release	This undoes the Lock Open condition and returns all relays/outputs associated with this control zone to the next highest condition currently in effect.	This function is specified using CMD 41.

Table 3-2: Common Output Control Functions (Continued)

‘Force’ and ‘Lock’ perform similar functions, but ‘Lock’ is a higher priority function than ‘Force’ and will override ‘Force’ commands. This means that you can construct sophisticated scenarios in which relays are locked open or down even while they are currently forced on or off. In this way, layers of authority can control relays, providing overrides and default conditions in the event of emergencies or failures. In this control stack, each time a high-priority function is withdrawn it can expose an underlying function still in effect.

For example, all relays in a control zone are forced on until the administrator enters a Lock Down, which immediately disables all the relays; once the administrator has left the area, the Lock Down is released and the relays are returned to a Force On condition. The guard can then open and go through the door. Once the Force On condition is released by a mid-level guard supervisor, a single door within the controlled area can be entered by a qualified guard, who could not have opened the door during the Lock Down.

The lock functions can also override time zones.

Time Zone Control of Relays

When time zones control relays, they are generally defined as being in one of three states as shown in Table 3-3:

Relay State	Description
Actuate relay	Relays are actuated during a time zone, going on at the start time of the zone and off at the end time of the zone. Defined by CMD 82*1*relay*TZ.
Disable relay	Relays are disabled during a time zone, becoming disabled at the start of the zone and ending the disable condition at the end of the time zone. During the time a relay is disabled, all access and mid-level control functions, including RQE, are disabled. Defined by CMD 82*2*relay*TZ.
Clear relay	Clears the current relay states for access and mid-level control functions at the end of a given time zone. The clear relay state does not affect relays controlled by a code of higher priority than a time zone, such as Lock Down and Lock Open. This automatically reverses a code- or card-activated relay from either access and mid-level control without manually resetting the relay. This feature is most generally used in combination with a manual Unlock by code or card to ensure an automatic Relock by time zone. Defined by CMD 82*3*relay*TZ.

Table 3-3: Time Zone Control of Relays

Control Function Priority

All commands have a priority defined in firmware. This priority schedule allows for manual and automatic override sequences while programming. Table 3-4 shows the priority schedule with the top item (Door Timer) having the lowest priority, and the bottom item (Lock Open) possessing the highest priority. Abbreviations used in CMD 88 printouts are also shown.

Priority		Abbrev.	Command
LO (AZ)	↓	DT	Door Timer – Momentary Access
		UL	Unlock
MID (CZ)		CT	Control Timer – Control Trigger Timer
		FN	Force On
		FF	Force Off
(TZ)		TA	Time Zone Actuated
		TD	Time Zone Disabled
(CZ)		ZA	Control Zone Actuated
		ZD	Control Zone Disabled
HI (CZ)		LD	Lock Down
		LO	Lock Open

Table 3-4: Command Function Priority

As indicated in Table 3-4, all functions are not equal priority within categories. For example, FF (Force Off) will override FN (Force On) or CT (Control Trigger Timer); LO (Lock Open) will override LD (Lock Down).

Alarm/Input Functions

Another classification of user control functions are the alarm functions. These are functions that apply to all line modules inputs.

Common line module input control functions include:

Function	Description	Comment
Momentary Single Mask	Momentarily disables the reporting of a single alarm condition from any of the line module inputs as defined by the card/code's control zone.	When this user function is used, it will mask the specified line module input for a single alarm actuation only. The function is defined by CMD 42.
Mask	Turns off reporting of all alarms from any of the line module inputs as defined by the code's control zone.	Line trouble reporting is not disabled during alarm masking. The function is defined by CMD 42.
Unmask	Restores alarm reporting of any input(s) as defined by the code's control zone.	Unmasking an alarm is the same as arming an alarm. The function is defined by CMD 42.
Cancel Entry Delay	Cancels the entry delay timer and prevents reporting of an alarm.	Use an Entry Delay Timer to control access to secure areas covered by the ScramblePad. This function is defined by CMD 42. The entry delay timer is specified by CMD 110.
Start Exit Timer	Starts the exit timer upon an exit request.	Enables user to exit a secure area without tripping an alarm. This function is defined by CMD 42. The exit timer is specified by CMD 110.
Mask Alarm & Cancel Entry Delay	Cancels an entry delay and masks all interior line module inputs for general building occupancy, or just mask specified inputs for occupancy of a specific area only, while other areas remain armed.	A convenient combined user function. This function is defined by CMD 42.
Start Exit Timer & Unmask	Starts exit timer and unmasks all interior line module inputs.	This function is used to re-secure either a whole building or only a specified area. This function is defined by CMD 42.
Pre-Arm Status	Tests all available inputs within the specified control zone and reports whether they are inactive (secure) or active (unsecured). This function only appears in CCM Version 7.x and later.	If all inputs are secure, the ScramblePad flashes its green LED once for an access grant and twice for a control. If there are unsecured inputs detected, the ScramblePad flashes its red LED and beeps—one beep for each active input. This function is defined by CMD 42.

Table 3-5: Common Line Input Control Functions

Function	Description	Comment
Conditional Unmask	Unmasks/arms all inputs in the specific control zone only if all inputs have been previously detected as secure. This function only appears in CCM Version 7.x and later.	This condition is defined using CMD 42.
Partial Unmask	Unmasks all inputs in the specified control zone previously detected as secure. All unsecured inputs are left unarmed. This function only appears in CCM Version 7.x and later.	When this condition is used, the ScramblePad flashes both the red and green LEDs, if some inputs are secure and other are not. Only the green LED flashes if all inputs are detected secure. This condition is defined using CMD 42.

Table 3-5: Common Line Input Control Functions (Continued)

Both Relay control and Line Module Input control functions are implemented by assigning a user number with control code and an associated control zone.

In addition to the standard input functions, there are several special functions. These include:

Special Function	Description	Comment
Alarm Cancel	Cancels all alarms within the specified control zone. This also enables the DIGI*TRAC Annunciator.	This condition is defined using CMD 44.
Watch Log	Logs code entry for tracking guards on their appointed rounds.	This doesn't grant access, only records the guard's progress. This condition is defined using CMD 44.
Time Log	Logs code entry for recording the arrival and departure times of time log code holders.	This records arrival and departure for time card purposes. This condition is defined using CMD 44.
Deadman Timer	Starts a deadman timer at code/card entry. If the timer expires before the employee's next code/card entry, an alarm is recorded.	This condition allows the system to track the safety and security of a user while a specific task is being performed. Deadman timers are common in many industrial applications such as railroads, refineries, and other dangerous or hazardous locations. This condition is defined using CMD 44. The deadman timer is set using CMD 358.

Table 3-6: Special Line Module Input Control Functions

Password Priority

There is yet one more area of prioritized control defined by software. Passwords can also have levels of authority within DIGI*TRAC. This means that each programmer can only access certain functions or tasks.

Passwords control ScramblePad access to programming mode. Passwords enable five levels of programming command restriction. Each level is only able to use certain programming commands according to the password level assigned to the operator's user number when added to the system. Any number of users can be assigned to any level. Each authorized operator is logged onto the system when programming mode is entered.

Note: Only one operator can be logged on at a time.

The five password levels are defined below:

Priority	Password Level	Restrictions
1	*System Password*	All Commands
2	*Executive Password*	All Commands Except Passwords
3	*Supervisor Password*	All Commands Except Setups
4	*Operator Password*	All Except Setups & Add or Print Users With Codes
5	*Service Password*	All Setups & Print Status, No User Commands

Master codes are defined using CMD 01. Password levels are assigned using CMD 02.

Alarm Control Blocks

Complex control sequences can be developed to follow the state of a line module input or relay output, or the condition of a line module input. Whether initiated by a change of state or condition, a control zone must be defined to establish the desired results. The appropriate command will define the desired action (for example, trigger or retrigger), the line module input (or relay output), and the control zone.

To make programming of complex sequences easy, the DCL includes *Alarm Control Blocks* (ACBs) also called *alarm action control blocks*. ACBs are used to produce results based on a detected condition, not just the state of line module inputs.

There are 383 ACBs predefined for each of the base and expansion inputs and outputs, as well as internal events such as low battery, and firmware-based alarms such as duress or passback violation. There are discrete ACBs for each of the line module inputs (Alarm, Door Open Too Long, and Tamper). Also, each ACB can be assigned to trigger a control zone or initiate a dial host command in a remote site management application.

Actions—such as triggering an alarm or dialing a host—are assigned to specific ACBs through CMD 261. A range of ACBs can be configured to perform one or more actions using CMD 461. Configure ACBs to trigger specific control zones using CMD 262.

To view all ACBs which have changed from the factory default, see CMD 460, starting on page 4-250.

Note: For the best understanding of how alarms and other events take action—such as which relays, if any, are triggered and when they are active in the system—print out a list of all ACBs using CMD 260. This provides you with a good idea of how the system operates. We recommend that you study this before you attempt to program any ACBs.

Print Functions

A printer should be used when programming from a ScramblePad. While many valuable reports can be produced, the firmware allows the printer to function as a teaching assistant or wizard. If you are unsure of the command or syntax, the printer will provide the information. If you make a mistake, the printer will tell you, and provide guidance on the correct entry as shown in this example:

```
Bad Format - Command or Value Too Long
>> Correct Command Syntax is:

Change Line Module for Alarm Input
      ST 270 * NN * I #
                1 - DTLM1 / MELM1
                2 - DTLM2 / MELM2
                3 - DTLM3 / MELM3
Please Re-Enter
```

Figure 3-5: Help Text Printout During Programming

Once a correct entry is made, the printer will confirm the entry with a printout of related and associated information. One of the most common commands for printouts produces a list of all Commands and their syntax. Another produces a list of all setups and status. The default setting for most user reports is to report everything. This is beneficial for initial setup and commissioning. However, it is good practice to turn off or disable reporting of items such as relay state changes. The user may also want to turn off Granted Transactions and RQE requests to focus reporting on alarms and exceptions.

Reporting can also take advantage of the User database and perform custom sorts and searches to print a list of users in an Access Zone or Control Zone, or a list of users with a special function such as Lock Down or Unmask privilege.

Programming Application Guidelines

This section provides you with additional information on application issues. Many of the terms used in DIGI*TRAC programming require additional explanation. Refer to the Glossary for a definition of terms. Also, read Chapters 1 and 2 for basic information about the DIGI*TRAC system.

What Is Access Control, Alarm Control, Relay Control?

A*ccess control* systems grant, record and report access to facilities, services, information, or other protected assets. In addition, they deny, detect, record and report unauthorized access to secured areas within a monitored facility or protected asset.

Alarm control systems are installed to detect the unauthorized entry into, or exit from, secure areas of a facility. They can detect and report the use of emergency fire exit doors or intrusion into a restricted office area. The system can control access to a warehouse, a lab, a cash room, anywhere that unauthorized access needs to be monitored and reported.

DIGI*TRAC offers access to alarmed areas by user, by time and by day, and on-site printed records of openings and closings. It even supervises alarm circuits 24 hours-a-day for trouble conditions or tampering attempts.

Relay control systems are used to control access to equipment, such as after-hours elevator access, heating and air conditioning usage, lighting, production or process control machinery, storage lockers or containers. Anything that can be controlled by a relay can be securely controlled by a DIGI*TRAC control system.

Access List

Make an Access List of Authorized Users. The list can come from the human resources department or from the supervisors of the controlled areas. The list needs to be organized in two ways: by Access Zone and by User Number. The Access Zone (User Group for SAM) is used to organize how, when and where access will be granted and denied. The user number is used to record who accessed an area.

Access Zones

DIGI*TRAC Systems control who goes where and when by organizing users into groups with the same level of access authority. Hirsch calls these groups Access Zones. In most organizations all users fall within uniform groups or job classifications such as administration, clerical, production, sales, or engineering.

Review a copy of the company Organization Chart to assist in group definitions. Assemble the Access List into groups of users that are authorized for access during the same hours of the same set of days for the same doors. Organizing users by Access Zone groups provides the system manager with several convenient and powerful methods of security management that will be discussed in further detail.

24-Hour 7-Day Access Control

In some cases access control systems are installed on doors that are always locked. Authorized users are permitted access to the locked area 24-hours-a-day, 7-days-a-week. There are no other restrictions applied. Either you have a code or card and are permitted access or you are not.

The installer/programmer of an area organized like this has two programming options to consider:

Common Access Zone

A common uniform Access Zone specifying 24-Hour Access to all doors can be defined with all authorized users assigned to that Zone. This may prove perfectly adequate for a very general access control operation. The advantage is simplicity, the disadvantage is a lower level of control.

For example, if the organization had a number of its employees strike and the management wanted to lock out their access during the labor dispute without disrupting the access authority of the other members of the Access Zone, they couldn't do so.

In another example, the organization may be adding a new computer room, storage area, or research lab, to which management wants to restrict access to some portion of the employees without changing access to the other areas. This could not be done with all users assigned to a single common Access Zone.

Either example would require significant reprogramming to break out the specified group of users into their own Access Zone. The small amount of extra work required to group authorized users into multiple independent Access Zones, even if they are all 24-hour zones, is often worth it in the long run.

Multiple Access Zones

Most systems require no more than 3 or 4 Access Zones to cover all groups of users. However, there are 128 Access Zones available in each system. Even when operating on a 24-hour basis it is wise for the installer/programmer to structure the system into multiple independent Access Zones. Having users organized by Zone allows rapid reorganization of access authority in response to an unexpected change in security operations. If for security reasons access needs to be limited for any user group by time-of-the-day / day-of-the-week, or restricted by door, then multiple independent Access Zones by user group are required.

Access Zone definitions consist of two items:

- ❑ Time Zones
- ❑ One or more authorized doors

The members of each Access Zone will be granted access at the selected doors during the specified Time Zones. Doors are specified by their number, 1 through 8, during Access Zone setup. By organizing a system into multiple Access Zones, a door can be rapidly added to or deleted from any specified group of users simply by redefining the group's Access Zone doors. It’s also simple to lock out an entire Access Zone by changing the Access Zones's Time Zone to 0 (zero), never. When access for the selected group is to be reauthorized, simply change the Time Zone.

Time Zones

Standard Time Zones are set up by the installer during the system programming procedure. Each Time Zone is defined by entering a Starting Time and an Ending Time for authorized access. This time period can be set to a full 24-hours or any limited set of hours. Each Time Zone also includes a set of 7 authorized days-of-the-week on which access will be granted during the specified hours-of-the-day. Time Zones can also be set up to automatically unlock and relock doors during hours of free or public access.

DIGI*TRAC systems also include the ability to define up to 30 scheduled holidays by date in advance. Time Zones can include holidays in the day selection. If holidays are included in the Time Zone of a user's Access Zone, access will be authorized when the system's calendar detects a scheduled holiday date. If holidays are not included in a Time Zone / Access Zone setup, that group of users will be denied access whenever the system detects a scheduled holiday for the entire day.

The programmer also has the option to group Time Zones. Up to 8 Standard Time Zones can be defined as a *Master Time Zone*. Additionally, up to 8 Standard or Master Time Zones can be defined as a *Grand Master Time Zone*.

Master Time Zones are used when:

- ❑ A Time Zone must extend past midnight
- ❑ Multiple start/end times occur on a single day
- ❑ Different start/end times occur on different days

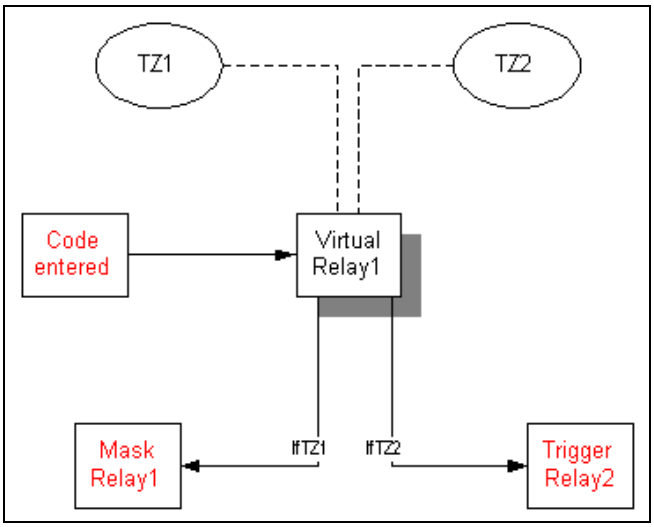
Virtual Relays

Virtual relays are definitions of expansion relays that have no physical presence. They are nonetheless extremely useful in constructing procedures which can be described by control zones.

Virtual relays are logical links between physical actions in which each virtual relay is a link in the chain of events leading to an output or alarm. While actual relays trigger circuits—like physical locks, annunciators, and CCTVs—virtual relays trigger only other virtual relays or actual relays: they aren't directly connected to a physical circuit.

A simple example would be an installation designed with a door, a ScramblePad, a button, a conveyor belt, and a lock. Normally, a code is entered at the ScramblePad and the door opens. However, when a code is entered at the beginning of another time zone, it turns on the conveyor belt instead.

One possible way of doing this is to set up a virtual relay which supplies the logic between the pushing of the button and the turning on of the conveyor belt in a Master Control Zone definition.



A more complex example might go like this: a customer wants the first person to enter a valid access code at the start of the day to unlock the front door. At lunch time, they want the door automatically relocked at the beginning of lunch time and unlocked again by the first valid code at the end of the lunch time. Then, at the end of the day, the security system should relock the front door. After hours, a valid code momentarily unlocks/relocks the door as usual. In addition, they want a relock code so if anyone leaves before the door automatically relocks, they can manually relock it.

After defining the required time zones, you would perform these tasks:

1. Define a SCZ to trigger the onboard relay (front door):

   START 45 * 1 * 65 * 1 #

   which means SCZ 1 always triggers Relay 1.

2. Define an MCZ which would unlock the front door:

   START 304 * 5 * 1 * 192 #

   where MCZ 192 unlocks SCZ 1.

3. Define a time zone for this MCZ:

   START 305 * 65 * 192 #

   in this case, TZ 65 (all the time) is associated with MCZ 192. In other words, unless masked, SCZ 1 always unlocks the door controlled by Relay 1.

4. Define a clear relay at the end of the day time zone:

   START 82 * 3 * 1 * 66 #

   which means Relay 1 is cleared at the end of MTZ 66 (defined as M-F 8-5).

5. Define a special SCZ that controls a virtual relay:

   START 45 * 2 * 65 * 0 #
   START 301 * 17 * 2 #

   This define SCZ 2 for TZ 65 (always) affecting Relay 0 (no physical relay), then adds a virtual expansion relay (VR 17) during SCZ 2.

6. Define the virtual relay to trigger the after-hours MCZ:

START 187 * 1 * 17 * 192 #

which means virtual relay VR 17 triggers MCZ 192.

7. Define the physical relay to trigger the special SCZ:

   START 87 * 1 * 1 * 2 #

   which means Relay 1 triggers SCZ 2.

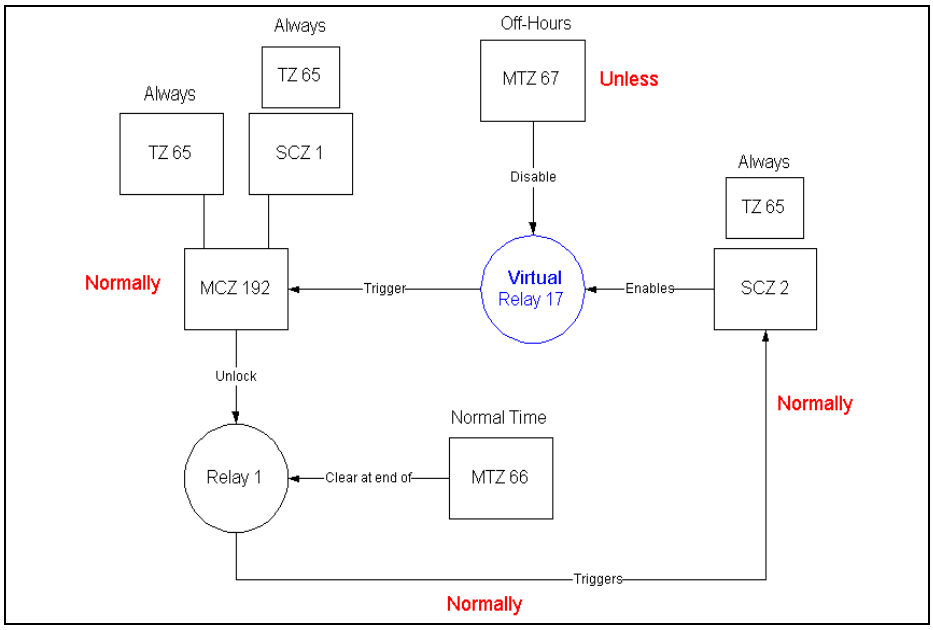
8. Define the time (after hours) during which the virtual relay is disabled:

   START 182 * 2 * 17 * 67

   which instructs the system to disable VR 17 during MTZ 67 (all those hours not defined by MTZ 66).

This means that during after hours mode, as defined by MTZ 67, VR 17 will be disabled, thus not allowing any code to trigger it which in turn does not allow the triggering of Relay 1 and the unlocking of the front door. However, during the day, defined by MTZ 66, the first access code entered after VR 17 is enabled triggers the MCZ to unlock the front door. Even if another code is entered after the front door is unlocked, it has no effect.

The following illustration shows this process:



As you can see, the virtual relay is used as a middle step in the logical sequence leading to the locking or unlocking of the front door.

User Numbers

Before CCM 7.0, user numbers were pre-allocated in each controller and assigned sequentially. This meant that systems with multiple controllers needed to assign different user (credential) numbers to the same person for each controller.

With CCM 7.0, a 9-digit User ID Number is used in place of the older user record number. User ID numbers are unsigned 32-bit long integers that go up to about 4,200,000,000 and easily support large systems with the ability to have a common number assigned to all users (credentials) within every controller.

While we define a user number as a possible 9-digit user ID number, it can actually exceed 999,999,999. In fact, the largest valid User ID Number can be 4,294,967,294.

SAM often assigns different user numbers to users in different controllers, while Velocity assigns a given user the same user ID number across controllers. Ironically, while SAM allows the operator to assign Time Zones and Access Zones by number to match across all controllers, Velocity picks its own numbers.

ID Formats (IDF)

Each of the preceding user ID categories requires a different ID type. Hirsch has created seven different ID formats (IDFs) each of which qualifies the user for a different access level and, depending on the door encountered (Card only, Code only, or Dual Technology), requires a different series of steps to enter or exit.

Each IDF is defined in Table 3-7, showing how each IDF would respond to a specific door configuration:

ID Format (IDF)	Dual Reader Normal Operation	Dual Reader Card + Code only	ScramblePad only	Card Reader only
IDF1: Keypad	Enter PIN	Enter PIN	Enter PIN	N/A
IDF2: Card	Present card*	Present card	N/A	Present card
IDF3: Dual	Present card, enter PIN	Present card, enter PIN*	N/A	N/A
IDF4: Card + Dual	Present card, enter PIN	Present card	N/A	Present card
IDF5: Keypad + Dual	Present card, enter PIN	Enter PIN	Enter PIN	N/A
IDF6: Keypad + Card	Present card or enter PIN	Present card or enter PIN	Enter PIN	Present card
IDF7: Keypad/Card/ Dual	Present card, enter PIN	Present card or code only	Enter PIN	Present card

Table 3-7: User ID Formats (IDFs)

* Function only available in CCM Version 6.6 and later. Earlier versions do not support this IDF feature.

In normal operation, if dual operation is available and the IDF specifies Dual as an option, then the card requires dual operation.

Each IDF can utilize a different number range and uses a different number of records as shown in Table 3-8:

IDF#	Numbers Allowed	Records Used
IDF1 – IDF7	Any	1 record

Table 3-8: IDF Number Range

In V7.0 and later, all ID formats use just one record.

At a dual-technology reader—one with a card reader and a keypad—both keypad-only and card-only users can be served in addition to Dual Code (Card + Code) users. Dual code users must use both the keypad and the card reader (in any order desired). For more about this, see “CMD 104: ENABLE CARD/CODE ONLY AT DUAL TECHNOLOGY READER DURING TIME ZONE” on page 4-127.

During times of high traffic volume, Hirsch has created a Card or Code Only Time Zone

(CCOTZ) feature through CMD 315. This means that at certain dual readers for specific times of the day, the controller will allow either Code Only or Card Only access to those users enrolled for that feature. To use this feature, a user must be enrolled as either Card Only or Code Only *and* Dual Access; then during a predefined time zone (CCOTZ) the qualified user can use just the one code or card to enter even though at other times it requires both card and code to enter. At the same time, even while in CCOTZ mode, users enrolled as Dual, Card Only, or Code Only, will still have access using their normal access methods. For more about this feature, see "CMD 315: ADD ACCESS USER WITH CODE & CARD & CARD+CODE (IDF 7)" on page 4-215.

User Management Commands

The DIGI*TRAC System provides extensive user management commands to enhance the control of secure areas. These include:

- ❑ Passback Control
- ❑ 2-Person Access Rule
- ❑ Occupancy Tracking and Reporting
- ❑ User Tagging
- ❑ Use-Count Control
- ❑ Absentee Rule Control
- ❑ Temporary Day Control

Each of these user management commands is defined below:

Passback Control	This requires users to pass through an entry reader, and, later, through an exit reader before their ID can be accepted at another designated entry reader. For more about this, refer to "Passback Zones (Physical Zones)" on page 3-26.
2-Person Access Rule	This rule provides a high level of security access control for specialized areas by requiring two authorized persons to be present to enter or exit the secure area. There are three variations of this rule available: • Two-Person "A/B" Rule. (A+B or B+A allowed; A+A or B+B disallowed.) If one person has "A" then they need to find someone with "B" to unlock the door. A user with neither the "A" nor "B" designation can go with anyone through a door with two-person rule. • Two-Person "Supervisor/Trainee" Rule. (S+S, S+T, or T+S allowed; T+T disallowed.) • Two-Person "Executive Override". This is another variation, which overrides the two-man rule. One access-grant unlocks the door For more about this, refer to CMDs 255-257 starting on page 4-181.
Escort/Visitor Access	Commands requiring enrolled visitors to be accompanied by one or more escorts. *Note: This can be thought of as an extension of the 2-person access rule.* For more about this, refer to "Escort/Visitor Access" on page 3-27.

Use-Count Control	This sets a maximum number of uses for which an authorized user can use their ID in order to enter a secure area or perform a control function. Up to a maximum of 31 uses can be allowed. Once the use-count expires the user is disabled or optionally deleted.
Occupancy Tracking and Reporting	This allows control over how many users occupy the secure area at any one time. The system counts the number entering and counts the number exiting. A running total is kept and whenever the total exceeds the maximum allowed or equals the minimum allowed, access is denied and an occupancy violation alarm is recorded. In addition, the occupancy count can be used to trigger a control zone for automatic masking and unmasking of the protected area and to change 2-Person Rule to 1-Person Rule once the area is occupied by the minimum required number of persons.
Tag Control/ Alert Control	The installer/programmer can *tag* a single user or a complete Access or Control Zone of users. When tagged, a tag alert report is printed on the system management printer whenever the tagged user or any member of the tagged Access or Control Zone enters the secure area. A single user or complete Access or Control Zone can be Alerted. Whenever the alerted user, or any member of the alerted Zone, enters the secure area or uses their Code at a ScramblePad Reader location, 4 beeps of the ScramblePad Reader's alarm tone are sounded to alert the user to the special alert condition.
Absentee Rule Control	This sets the maximum number of days a user may be absent and therefore not have used their ID to enter a secure area or perform a control function. Once the maximum number of absent days is reached the user is disabled or optionally deleted.
Temporary-Day Control	This sets which days of the current week and the next week the user can be authorized. Once the last day expires the user is disabled or optionally deleted.

Passback Zones (Physical Zones)

A new aspect of V.7.0 is the use of physical or passback zones. Physical zones are actually extensions of common passback and occupancy definitions, enabling the programmer to create an arbitrary topology around a reader or group of readers.

In V.6.6 and earlier, there were only three passback statuses that could be assigned using CMD 03:

- ❏ passback unrestricted (forgiven) – no passback restrictions placed on user in this area
- ❏ passback outside – ScramblePad/reader recognizes user are external to the assigned area
- ❏ passback inside – ScramblePad/reader recognizes user as inside the assigned area

Using V.7.0, a ScramblePad/reader can now be defined as an entry or exit point for up to 62 flavors of ‘inside.’ Each flavor defines a different physical zone that can exist within an area, floor, or building at the programmer’s discretion.

This makes possible new topologies for tracking occupancy and passback status, including the following two examples.

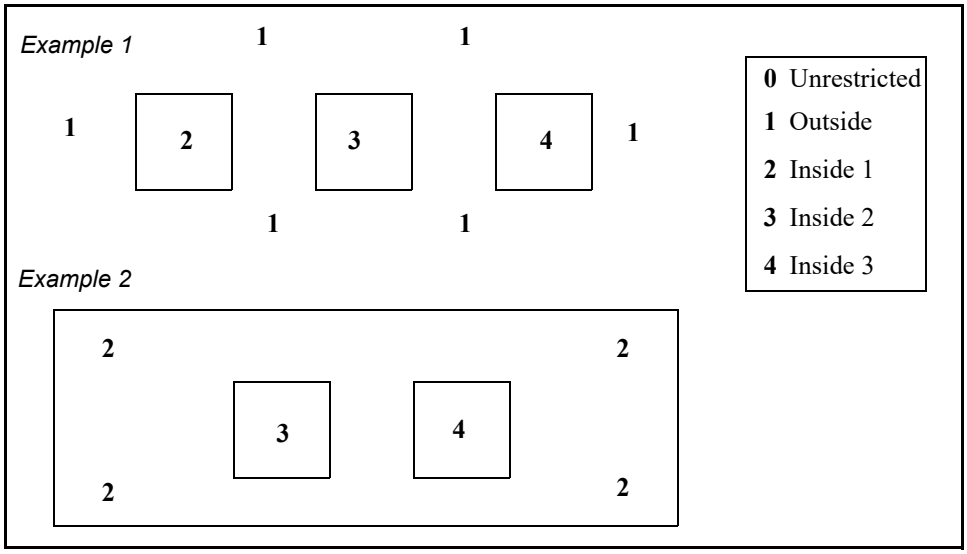


Figure 3-6: Passback Zone Examples

This means that readers or ScramblePads can be defined in this way:

Bits	Physical Zone
0	Unknown or unrestricted
1	Outside
2 - 63	Inside

Table 3-9: Passback Zone Bit Assignments

Physical Zones are defined using CMDs 246, 403, 421, and 435.

Escort/Visitor Access

Particularly in high-security installations, visitors cannot be allowed to enter restricted areas without escorts. Many government facilities, for example, allow officials to visit a high-security area, but only when accompanied by one or more escorts who can make sure that they don't wander away, see things they shouldn't, or get caught in dangerous situations. To accommodate such circumstances, DIGI*TRAC has created three rules enabling three types of escort/visitor access control:

- **Rule #1**—A qualified escort signifies the number of enrolled visitors he/she is accompanying by entering a number after his/her PIN code in this manner:

  `START 1234*6#`

  This example indicates that the qualified escort with a PIN of 1234 has indicated that he is escorting 6 visitors through a specified access zone. Once the number of visitors is specified, each visitor must enter their temporary card/code at the reader to gain admittance.

  This type of escort requires that the entrance to the access zone have both a code and card reader (dual technology) to allow the entry of a PIN and visitor parameter.

- **Rule #2**—A qualified escort swipes his/her card *after* an enrolled visitor swipes theirs. Each new visitor must be qualified by the escort's swipe before the access to the area is granted. This access point only requires a card reader.

❑ **Rule #3**—An escort swipes his/her card at an access point (Escort mode ON) then allows their visitors to swipe and enter at the access point. When all visitors have entered, an escort either swipes their card indicating that the entry of visitors is now complete (Escort mode OFF) or the mode is allowed to time out. This escort/visitor rule is handled by two escorts, one of whom can be positioned outside the door and the other is positioned inside the door. This access point only requires a card reader.

For more on setting up readers for visitor/escort access control, see CMD03 on page 4-33. For enrolling users as visitors and escorts, refer to CMD15 starting on page 4-48.

Function Groups

The *function group* is a new feature in V7.0. It combines the concept of the extension digit with the control function to create a new level of functionality for qualified users.

In earlier versions of DIGI*TRAC it was possible to perform a function by entering a specific code; for example, the first person to enter a building in the morning could punch in a series of codes that opened the front door, turned on the lights, started the air conditioner, and masked all alarms. A user could also initiate functions by entering one or more extension digits after his/her code in the same manner as they would enter duress digits. However, each new code extension enrolls a new user in the database – for example, PINs 1234, 12341, and 12342. From the controller's point of view, these are three different users and add three new entries to the code memory.

This is okay as long as the number of people who perform these functions is relatively small. But as the number of functions increases and the number of people who can perform them proliferates, download times increase, and the size of the code memory quickly reaches the maximum.

Function groups help alleviate this problem. Function groups decrease the size of the code memory by consolidating and centralizing control function procedures. Once defined, each function defined for a function group can be activated by any qualified user belonging to the relevant function group. For example, if User 0134 is added to Function Group 1 and Function Group 13 is defined in the following manner:

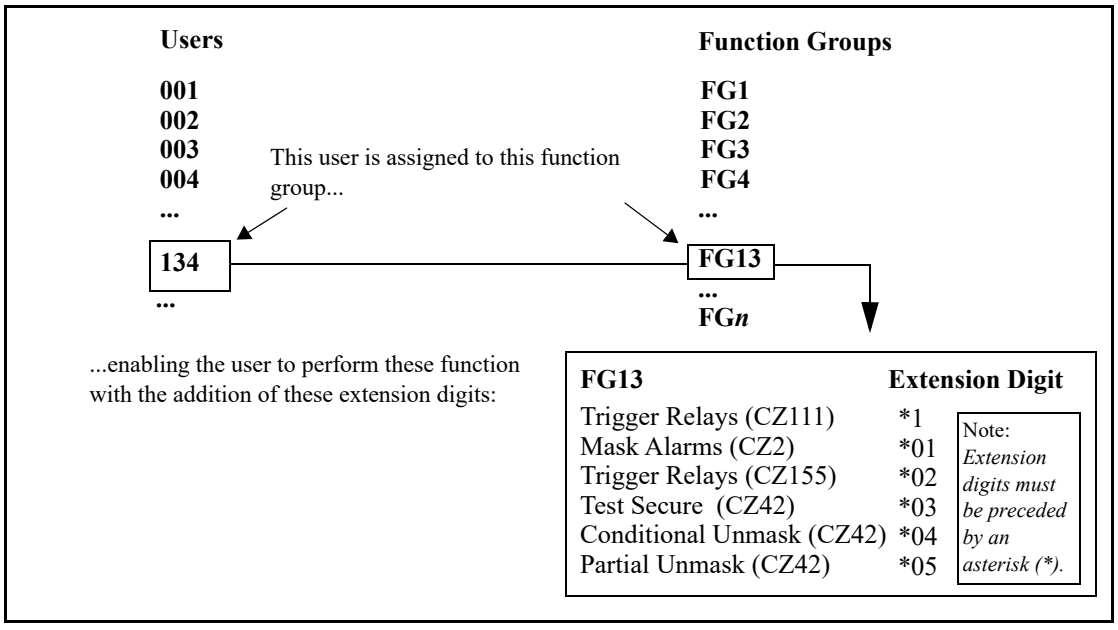


Figure 3-7: Function Group Example

then whenever User 134 adds an extension digit of '01' after her initial code (111 in the example) followed by an asterisk (for example: START 111*01#), it automatically masks the alarms defined for Control Zone 42 (that is, Alarms 1, 4, and 8).

To define a function group, assign users to that group, and provide them the extension digits they require to perform the assigned activities, you follow this procedure:

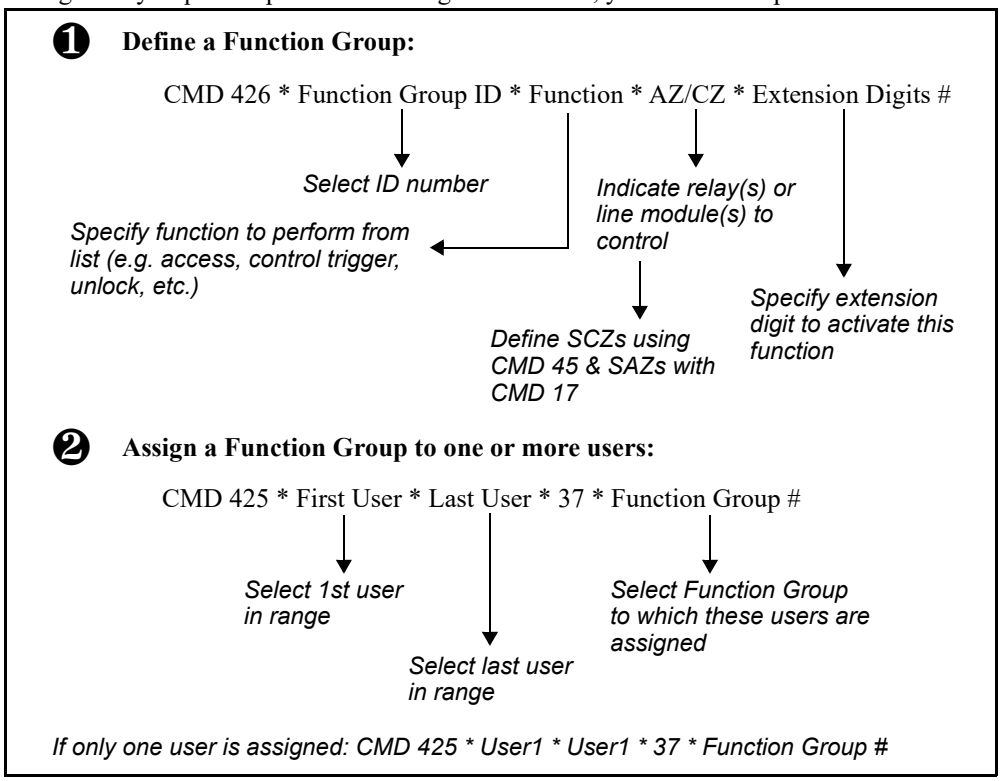


Figure 3-8: Function Group Procedure

In the example below, a series of commands leads to a definition of Function Group 13, specifies functions for that group, then assigns User 134 to the group.

`426*0#`	Clear all of the function group definitions. This is equivalent to resetting the function group memory and need not be done unless you must erase all current function groups.
`426*13*0*65#`	Set Function Group 13 to have a default function of Access.
	Set the following Function Extensions:
`426*13*1*111*1#`	1=Trigger Relays for CZ 111
`426*13*6*42*01#`	01=Mask Relays for CZ 42
`426*13*1*155*02#`	02=Trigger relays for CZ 155
`426*13*35*42*03#`	03=Test Secure for CZ 42
`426*13*36*42*04#`	04=Conditional Unmask for CZ 42
`426*13*43*42*05#`	05=Partial Unmask for CZ 42
	All of these CZs are defined using CMD 45 as shown in the following instructions.
`427*0#`	Use CMD 427 to print out your Function Group definitions, if required.

45*42*65*148# 45*111*65*12345678# 45*155*65*5678#	Set Standard Control Zone 42 to monitor Alarms 1, 4, and 8 for TZ65; set Standard Control Zones 111 and 155 to trigger relays (1-8 and 5-8 respectively) for TZ65.
16*134# 10*134*111*65# 425*1*134*134*37*13#	Delete old user 134 (if one exists). Create new user 134 with a PIN 111. Assign User 134 to Function Group 13.
99#	Exit Programming Mode.

This programming results in the following programmable controls at the keypad:

111	The base PIN will grant access.
111*01	Extension 01 will mask alarms.
111*1	Extension 1 will trigger relays.
111*02	Extension 02 will trigger a different set of relays.
111*03	Extension 03 will do a 'Test Secure' on the desired set of alarm inputs.
111*04	Extension 04 will do a 'Conditional Unmask' on the desired set of alarm inputs.
111*05	Extension 05 will do a 'Partial Unmask,' unmasking all, some, or none of the desired alarm inputs.

If you have enabled a user for a duress digit as well as qualified them for a function group, the duress digit comes directly after the user code and the function group extension digits come after the asterisk.

For example, if a user with the PIN '111' is defined for a duress digit of '9', the user would enter a duress code like this example:

```
1119
```

If the user wants to express a duress digit while also specifying function group controls, he/she would enter a code like one of these examples:

```
1119*01
1119*1
1119*02
```

Not only can you mix and match 1- and 2-digit code extensions, you can also use this feature on different lengths of codes.

For example, you might add a user with PIN 2941 and show that the user with 111 and the one with 2941 could both be enrolled with Function Group 13.

For more on each of these commands, refer to Chapter 4.

Threat Levels

Threat levels, also known as *security levels*, refer to crisis level situations where a higher threat level indicates heightened security.

Threat levels range from 0 to 99. Levels are defined by the operator or system administrator. Use 0 or 1 to indicate normal operation. If threat level is not used, the threat level stays at 0. If threat level support is used, start at 1 for situation normal and proceed upward from there.

All users can have security levels associated with them through CMD 421. A user with a security level of 99 will not be inconvenienced by any threat level situation. A user with a level of 10 can find himself locked out of the system when the threat level reaches 11 – 99.

Threat levels can be set controller-wide by a user code, by a host command, or by a master control zone. MCZs can only set values from 1 to 99. You can't use a MCZ to set a threat level at 0.

The threat level can also be designated reader by reader. For example, if dual technology readers are left in the CCOTZ mode during the day, they can be configured to revert automatically to dual codes when a particular threat level is reached.

Readers can be configured to deactivate automatically above a specific threat level so that it no longer accepts codes from anyone. The host can send a command to specific readers to set the threat level.

Commands that affect the setting of threat levels include CMDs 198, 247, 403, 421, and 446.

Access and Alarm Automation

Hirsch systems provide numerous methods to automate access control and alarm control functions. Each system can be set up to automatically unlock doors and relock doors on a timed schedule. Automatic locking enables free access during normal business hours and controlled access after business hours. Alarms on doors, emergency exit doors and interior spaces can be masked (disarmed) and unmasked (armed) on a timed schedule as well. Carefully plan automated controls to insure compliance with building occupancy, holiday and security schedules.

Card Enrollment

Another function you will use repeatedly is card enrollment. Enrollment is the process of registering cards into the controller memory for those installations which are using card reader technology. The methods and meanings for this process are explained below.

Card Enrollment Methods

Hirsch can provide pre-encoded mag stripe, proximity, or Wiegand cards for use on a multiple technology or card-only equipped system. Existing barcode cards may already be issued to the facility users in a retrofit installation. In either case, these cards have to be enrolled into the system before use. The MATCH requires card readers that produce an ABA/ISO Track 2 standard interface, or standard Wiegand 26- to 55-bit format. A MATCH reads the raw card data from the card and converts it into an eight-digit code. This technique eliminates the insecure, tedious, and error-prone manual data entry required to pre-load card data in most other card based systems.

When a card is used in combination with a keypad code, the MATCH sends all codes to the controller immediately. The firmware on the controller holds the card code if a key code is expected. If the card code is in the database, and the user has either IDF 4 or 7 (that is, card and dual options), the controller determines whether the requestor is allowed in right away. When the firmware holds a card code, the ScramblePad's first yellow LED will flash once.

On the DS47, there is an option to have the keypad "light up" when a card code is accepted and held. However, if you are trying to enroll prox cards at a DS47-SPX, you can't use the normal method of typing in a command; pass one or more prox cards across the reader. The SPX's lighted displays interfere with the prox card's field antenna and the SPX often cannot read the card. To overcome this problem, use this procedure:

1. Present the card FIRST while the DS47-SPX is OFF.
2. Enter one of the add user commands (CMD 310 - 315) such as:

```
310 * UN * AZ * #
```

It isn't necessary to wait to present the card until just before pressing #—the DS47 will hold card data in memory for 30 seconds after it is presented. (Don't forget the last asterisk before the pound sign.)

Local Card Enrollment

Card enrollment can be performed at a DIGI*TRAC MATCH Enrollment Station (DMES) on a locally-managed standalone system. This station consists of a ScramblePad and a MATCH-compliant card reader, each mounted in a stand positioned at the system printer. Alternately, cards can be enrolled at a dual technology reader installed at a door. Cards are enrolled by being read by the card reader, converted to a unique eight-digit code by the MATCH board algorithm, and stored in the controller's memory. On a single controller the enrollment process is simple and quick. If more than one locally managed standalone controller is used, the enrollment process must be repeated at each system.

Central Card Enrollment

Card enrollment can also be performed at a PC using host software such as SAM or Velocity on a network of controllers. In this case a SCRAMBLE*NET MATCH Enrollment Station (SMES) is installed at the SCRAMBLE*NET host PC and connected to a serial port on the PC.

Printing

Since all programming in a standalone controller is done from the ScramblePad, it is very valuable to have the results of any Programming Commands printed when they are entered. It's the best way to verify changes in System Setups. It's the *only* way to enable the controller to automatically generate Codes, because they are printed out as they are generated so they can be issued to authorized users.

DIGI*TRAC Systems also include a unique Operator Help capability. If an error is made when entering a Programming Command, the System will detect it and will print an error message – such as "value too big" – then will print the correct Command syntax (format). This kind of programming assistance is invaluable when entering infrequently used Commands or when entering Commands without a Programming Guide. In fact, if you know the Command number but not the correct format, try entering the Command followed by two asterisks and the # Key. For example:

```
START 10 ** #
```

The proper format for Command 10 is printed.

In addition, the complete set of Programming Commands can be printed by category, or in total, by using Command 00. Refer to Chapter 4, "Command Reference," for more information, or press:

```
START 00 * 0 #.
```

Using Printouts For Troubleshooting

If your controller is not operating normally, you can almost always find out what's wrong by printing out the System Setups and Status using Command 88. The most frequent problems result from programming or setup conflicts. It is possible to program events to occur that prevent other events from occurring, or prevent otherwise valid codes from working. All of these conditions can be examined in printouts. Just enter this command:

```
START 88 * 0 #
```

and see for yourself. This command is also helpful for reviewing the user list printout.

To print and review the characteristics of action control blocks (ACBs) which indicate how alarms take action, including which relays are triggered and when ACBs are active in the system, use this command:

```
START 460 * 0 #
```

For more information, see the "Factory Setup and Printout Guide" in Chapter 5 of this manual.

Using Printouts During Normal Operation

DIGI*TRAC controllers are factory-configured to print everything. This includes:

- ❑ Code transactions
- ❑ Alarms
- ❑ Relay state changes
- ❑ Daily midnight status reports
- ❑ Weekly System status reports

It is recommended that Relay State Changes be turned off immediately after commissioning since these can generate large amounts of unnecessary information which only confuse diagnosis of problems. Later, as required, this function may be re-enabled.

During initial system configuration and shakedown – usually the first 3 to 6 months of operation – the rest of the default data generated (code transactions, alarms, status reports) is useful for verifying controller operation since it is during this time that most of the problems occur and most of the questions can best be answered by referring to the printouts.

Once your facility is in full operation you can reduce the quantity of information printed by using Commands 05 and 06. Command 05 lets you turn off printing by category of events, such as relay state changes. Command 06 lets you turn off printing of granted, but not denied, code transactions and granted RQE events on a door by door basis.

When an alarm occurs, it is printed. It is also time-stamped by time, date, and location. Use Commands 106 and 107 to further reduce printed reports by disabling the printer during a specific Time Zone, or by disabling the daily midnight system status printout if desired.

Equipping a DIGI*TRAC controller with an optional Buffer Expansion Board (MEB/BE) increases the number of transactions and events that can be stored by the system. This enables the controller to retain transaction and event information even if a controller's attached printer runs out of paper over a long weekend. With sufficient memory, the buffered history log can record up to 130,000 events and 26,000 alarms in battery-protected internal memory. A controller without the MEB/BE can only store a standard buffer of 100 events and 100 alarms. Once the buffer fills it will automatically delete the oldest events and alarms as newer ones are recorded. If a printer is installed and operating, the buffer will always be empty.

See the "Printout Guide" in Chapter 5 for more examples of important printed reports.

Using Host-Based Commands

Host-based commands are generally invoked using a host computer connected to one or more controllers through one or more XBoxes. Because hosts are not limited to the 29-keystroke restriction mandated by the ScramblePad, the commands and their arguments can be far more complex. In fact, using host-based commands, programmers are only limited by the memory resident in XBox and panel buffers and/or the extended format of the messages in which the command parameters are embedded.

Programmers generally use these commands as calls through programmer-customized front-end applications. However, a programmer well-versed in DCL can also invoke these commands directly from a command line using a utility like SAM's Diagnostic Window or Hirsch's TestTool (available with MOMENTUM and Velocity). In addition, if the command is under 29 keystrokes, you can still enter a command from the ScramblePad.

For a description of all host-based commands currently defined for DCL, refer to "Host-Based Commands" starting on page 4-254.

Advanced Parameter Syntax

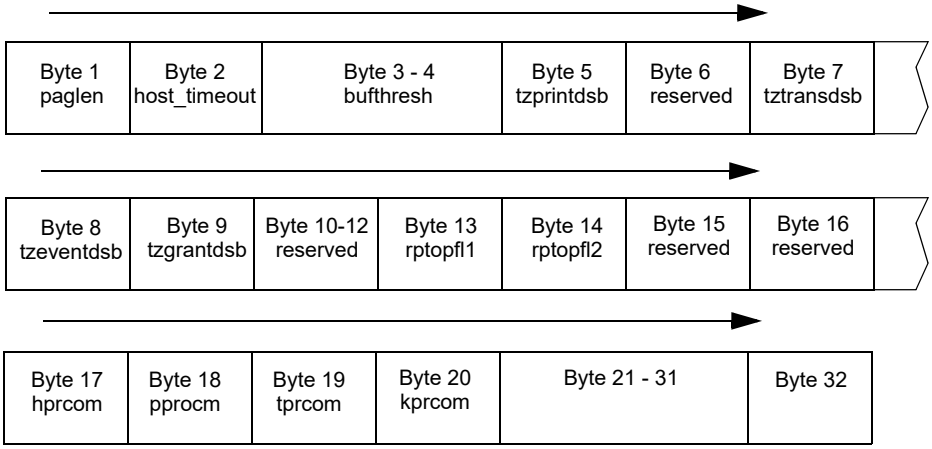
Note: This section is only relevant if you plan to use CMD 98 or CMD 198. Other host-based commands do not use this bitwise syntax. Use both commands with extreme care.

Most DCL commands use a relatively simple syntax with uncomplicated bit definitions. Many of these commands were restricted by the size and simplicity of messages used by the controller to define system properties. The XBox and V.7.0 CCM can use more complex messages. As a result, far fewer restrictions are placed on the length of the command line or the size of an argument or parameter field.

The freedom this provides for the programmer can be seen most clearly in the number of options available for any particular argument. For example, the host command 406 defines reporting options the host can define for one or more connected controllers through an XBox.

This command and its parameters are used to create a message that is sent to one or more

controllers via an XBox. In this case, the message is MSG 109 which looks like this:



Many of these byte fields only require you to select a single option, like *paglen* or *host_timeout*. If necessary, a single message can support a range of possible values from 0 up to 65,535; however, most ranges are smaller. For example, *host_timeout* can be decoded to any value between 10 and 255 seconds. This defines the number of seconds a host can wait before timing out. Similarly, *tzprintdsb* can be assigned any valid number for a time zone from 1 through 255. This designates a time zone during which the system printer is disabled.

Other bytes within a command or message support *multiple* options. These are designated by assigning each option a decimal value, then adding those decimal values together to render a unique number. Bits and the properties they represent are normally associated with decimal values in this way:

Bit	Decimal Value	Bit	Decimal Value	Bit	Decimal Value
0	1	**3**	8	**6**	64
1	2	**4**	16	**7**	128
2	4	**5**	32	**8**	256

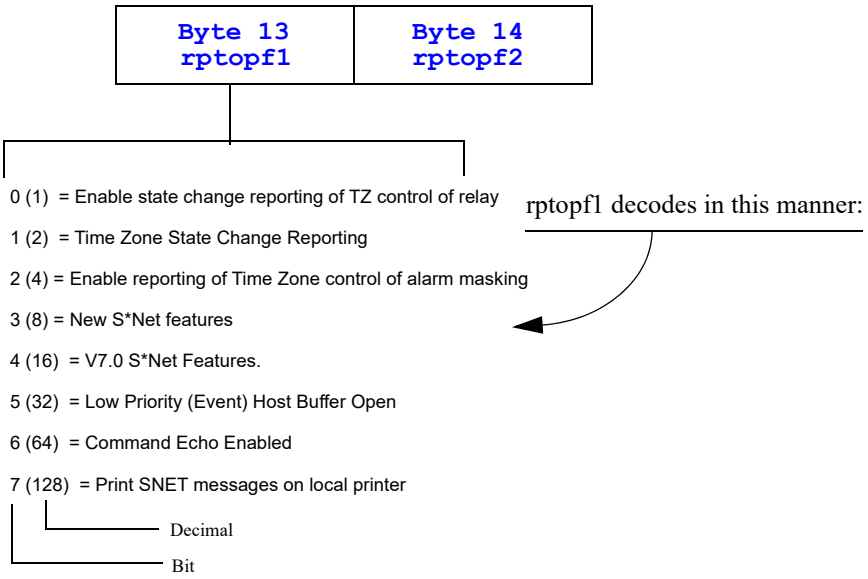
Table 3-10: Decimal to Bit Equivalencies

Using this technique, multiple bits can be assigned to an argument. For example, to include the options signified by Bits 0, 1, 2, and 7, you would add their decimal values to get a unique number, in this case:

```
1 + 2 + 4 + 128 = 135
```

This number can only define that combination of bit values.

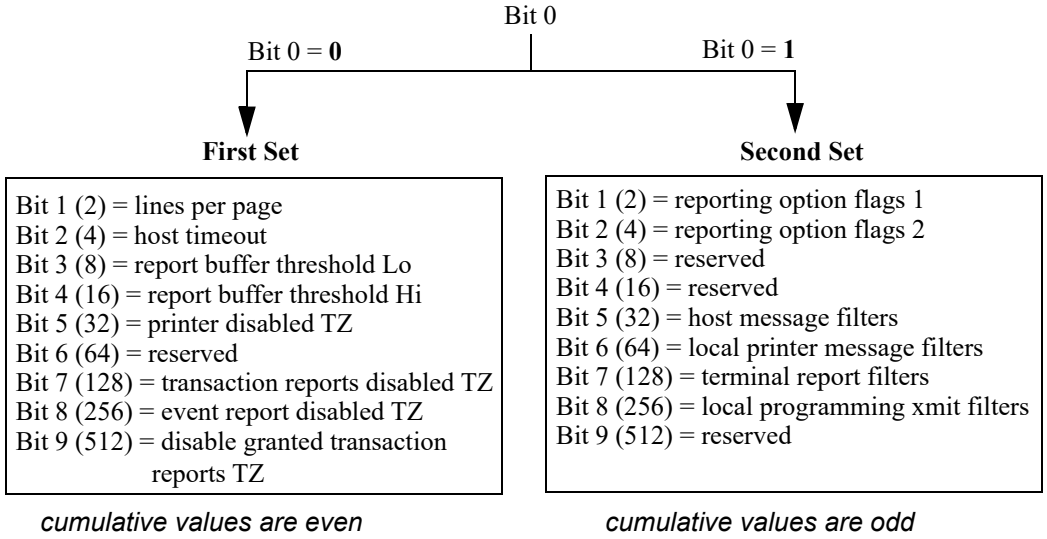
A real world example is provided by the previously mentioned MSG 109, in which several bytes, including rptopf1 and rptopf2, can support multiple choices as shown below:



As you can see, each selection is assigned a unique decimal value. To specify more than one of these options, simply add the bits together. For example, if Byte 13 is set to decimal 6, it means both Bit 1 (time zone reporting) and Bit 2 (reporting time zone control of alarm masking) parameters are specified.

Branching Options

You can also use this technique to choose between two sets of options. For example, this example command currently supports 18 options wherein Bits 1 through 9 are used twice, as shown below.



To determine which set of bits you are actually using, select a value for the first bit (Bit 0). If Bit 0 = 0 then the first set of options are selected and all cumulative values will be even, since decimal values for Bits 1 - 9 are all even. If Bit 0 = 1, then the second set of options are selected and the cumulative value of these will be odd (since even numbers + 1 = odd

numbers). An example of how this affects the argument is shown in the following table:

Decimal Value	First Set	Decimal Value	Second Set
2	Bit 1	3	Bit 1
4	Bit 2	5	Bit 2
6	Bits 1 & 2	7	Bits 1 & 2
8	Bit 3	9	Bit 3
10	Bits 3 & 1	11	Bits 3 & 1
12	Bits 3 & 2	13	Bits 3 & 2
14	Bits 1, 2, & 3	15	Bits 1, 2, & 3
and so on...			

An example of how this is used for the example command (CMD 406) is:

```
START 406 * 3 * 6 #
```

which means that Bit 1 from the second set of options—reporting option flags 1 (rptopf1)—is set to 6. As shown earlier, the value ‘6’ for rptopf1 decodes as Bit 1, time zone reporting, and Bit 2, reporting time zone control of alarm masking. If instead, the command is this:

```
START 406 * 2 * 16
```

it indicates that the Bit 1 from the first set of bit values are being used—specifying lines per page. This then means that the reporting page can contain 16 lines per page.

Command Flowchart

Programming consists of three categories: System Setups, Users, and Alarm & Control. Figure 3-9 provides a chart of System Setups.

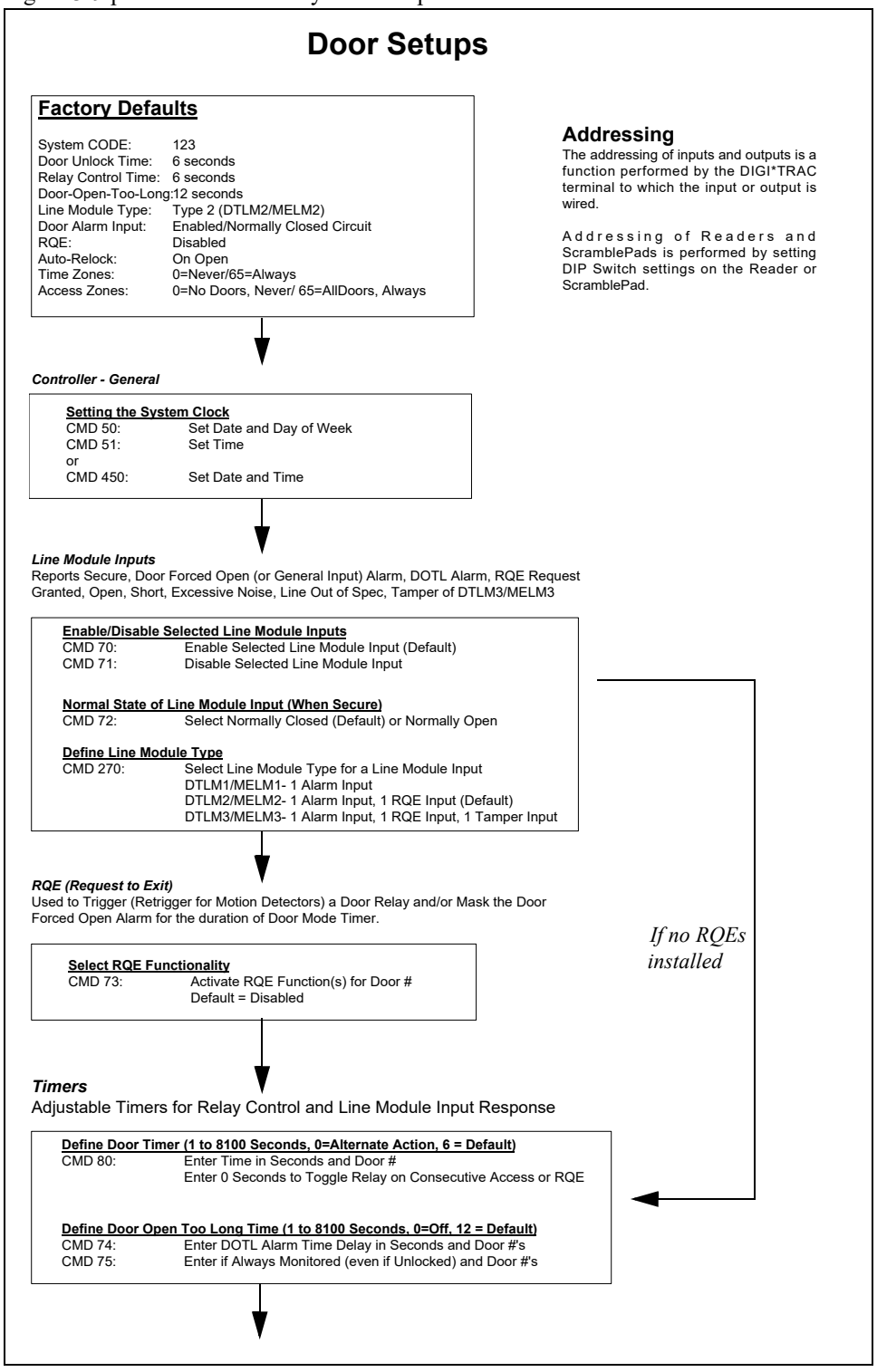


Figure 3-9: System Setups

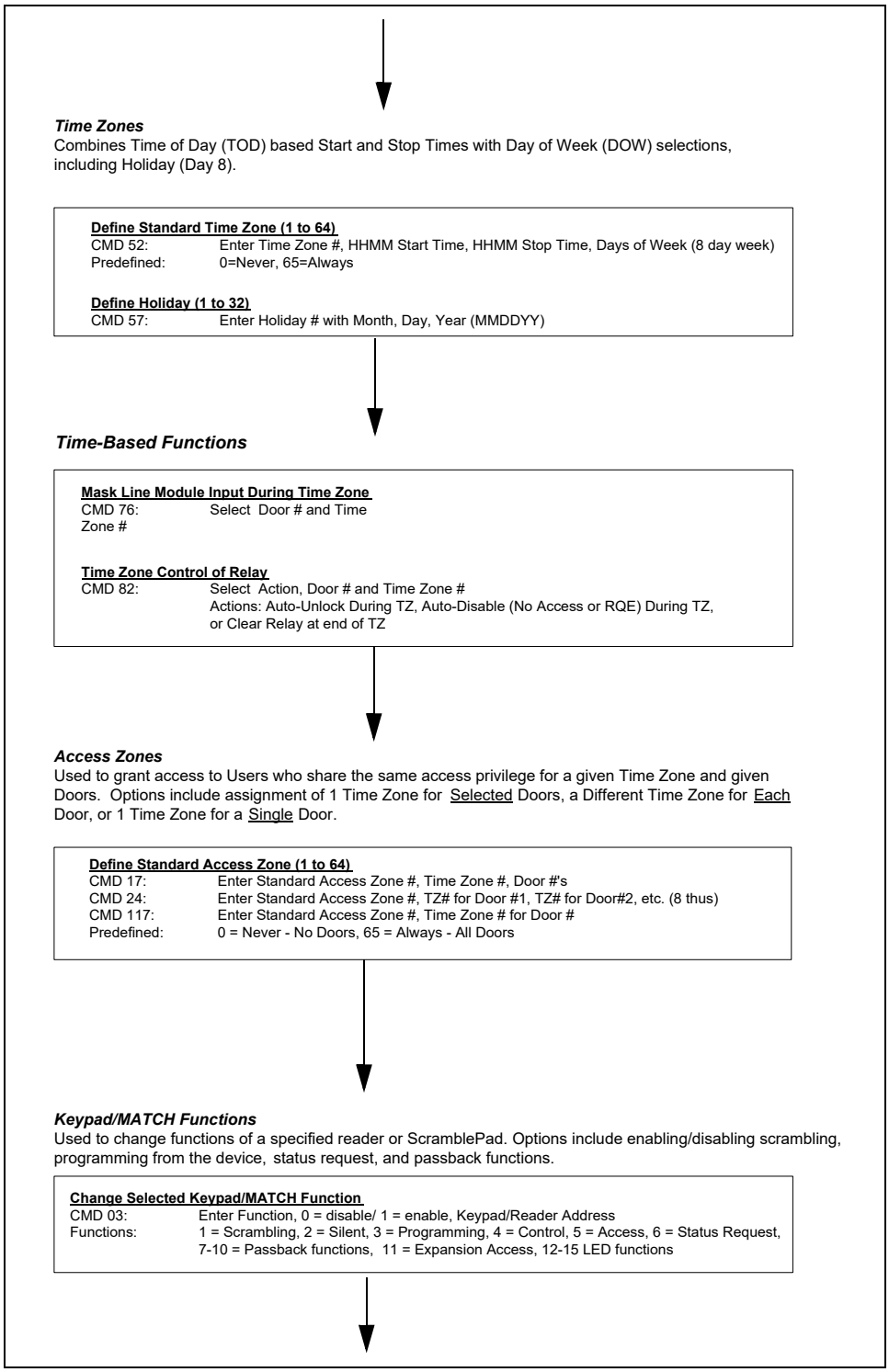


Figure 3-10: System Setups (continued)

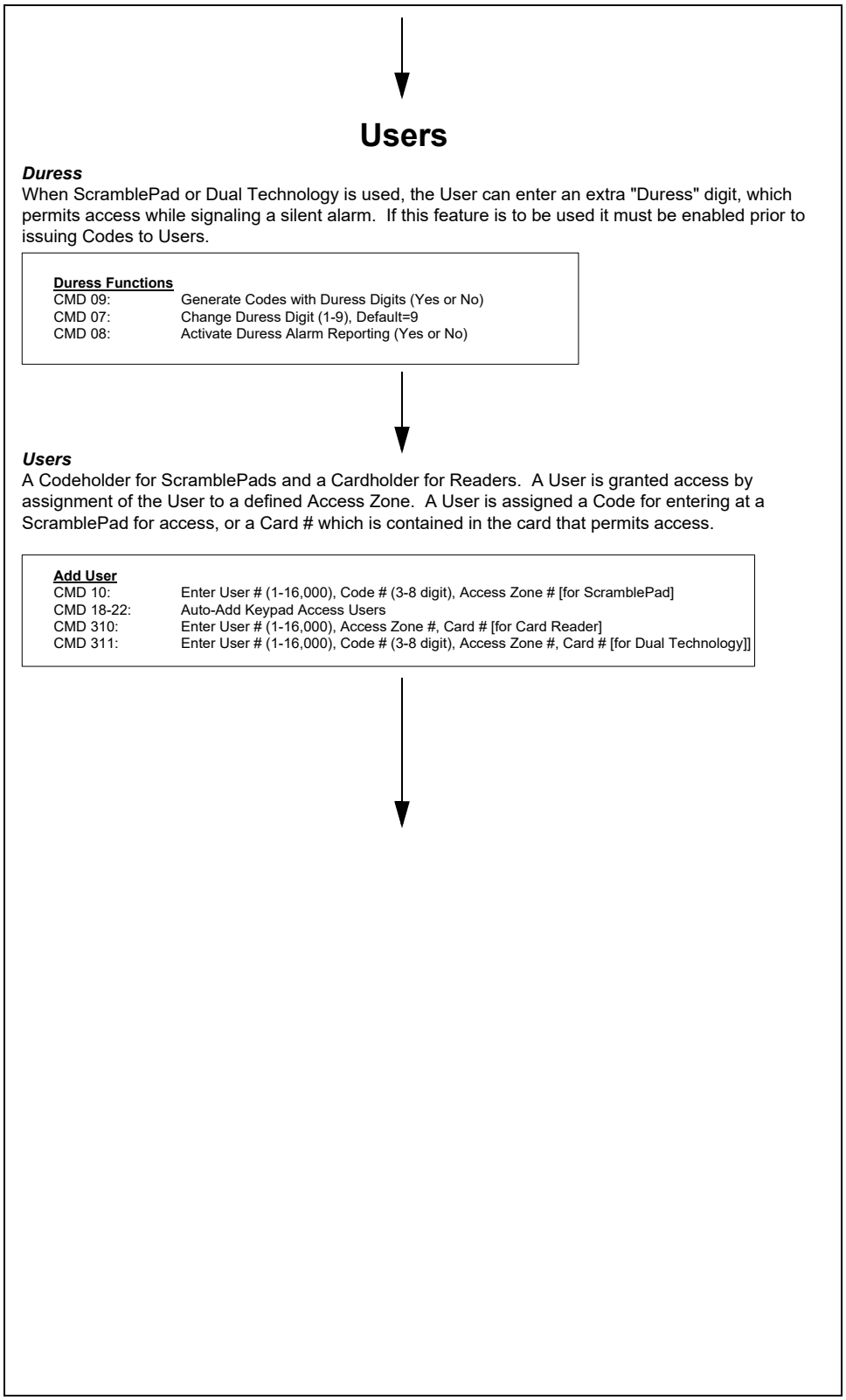


Figure 3-11: System Users

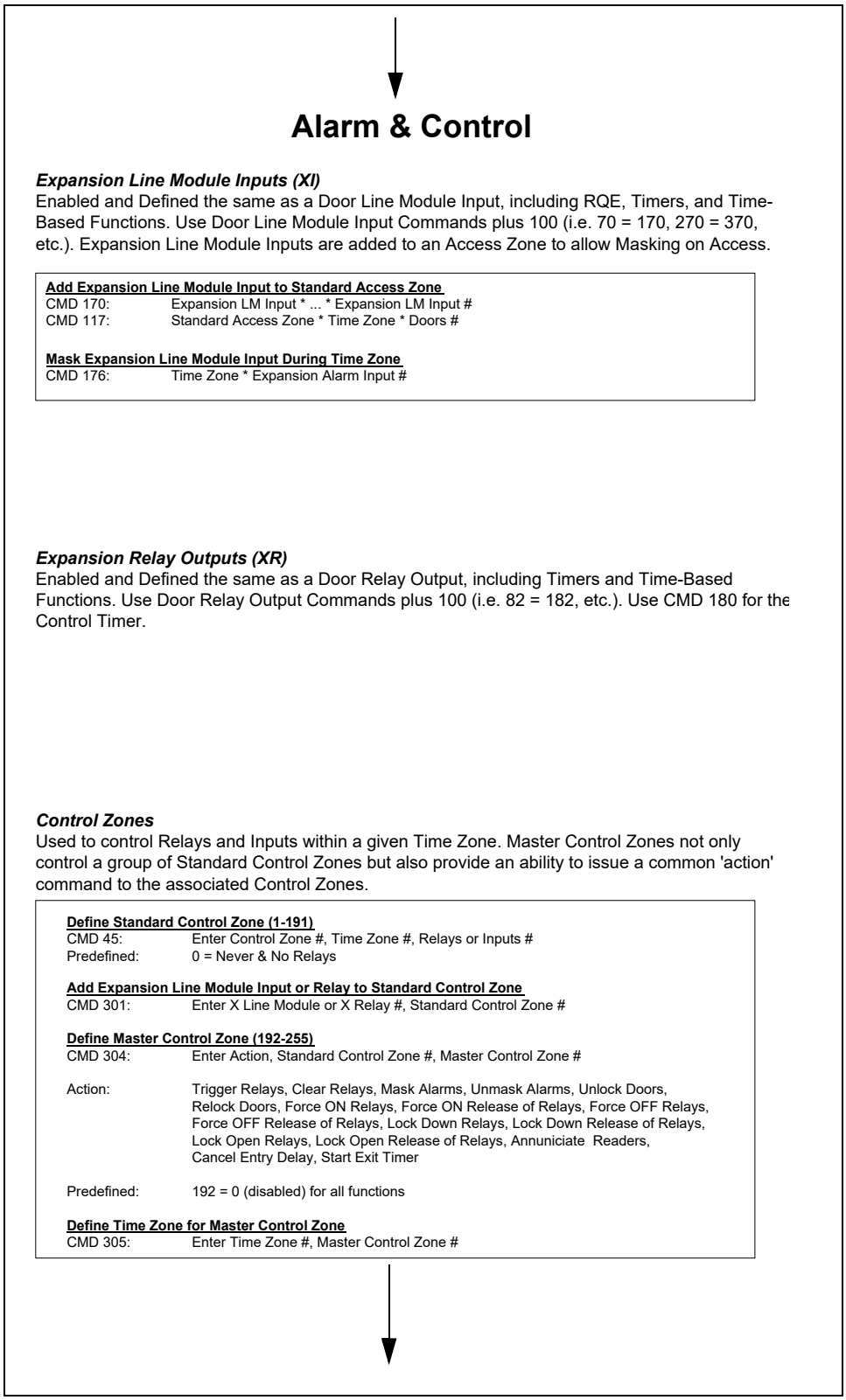


Figure 3-12: Alarm & Control

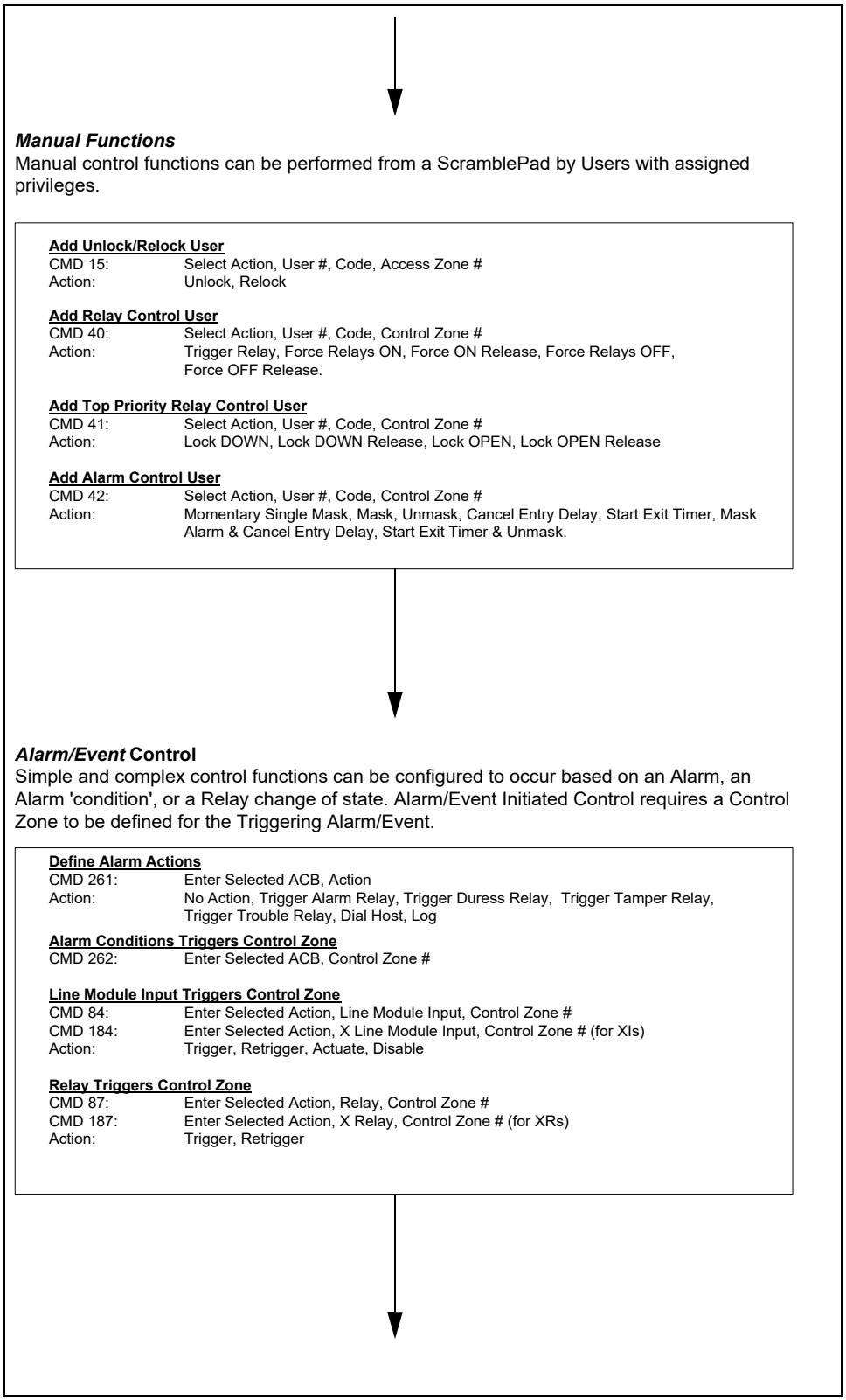


Figure 3-13: Alarm & Control (continued)

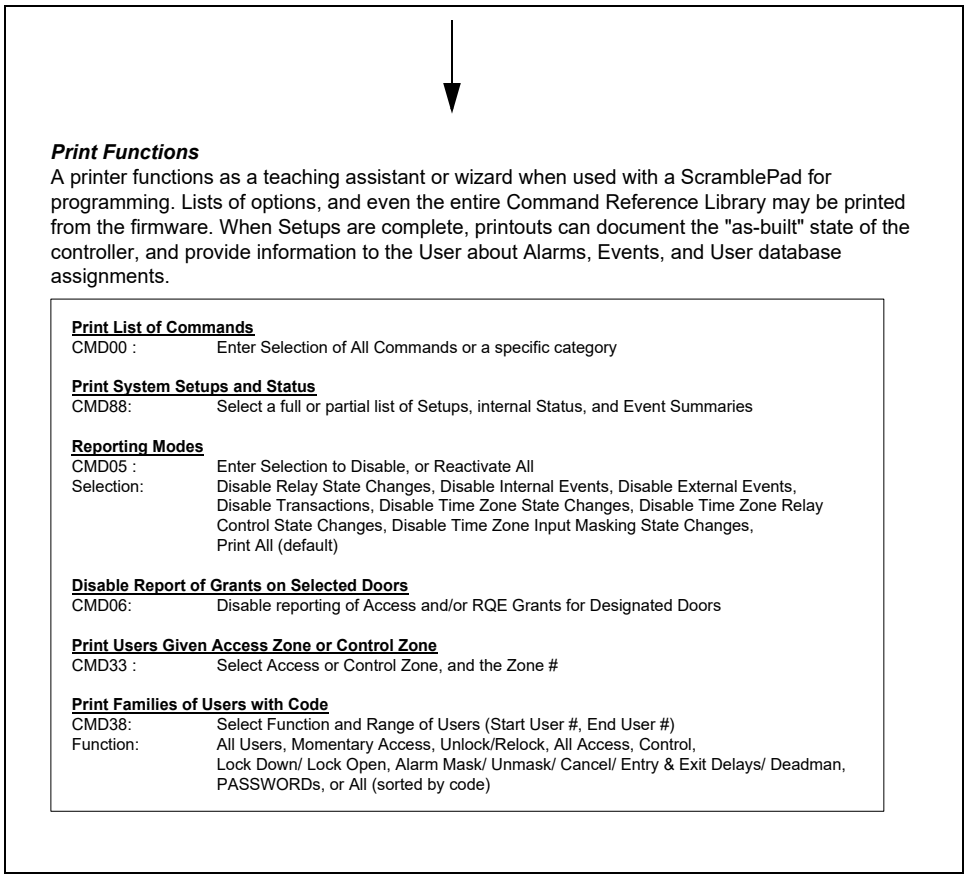


Figure 3-14: Alarm & Control (continued)

Appendix A provides worksheets which aid you in programming for your specific system.

Command Syntax

All Commands are entered via the ScramblePad, so they are numbers or digits. In addition, the START Key, the Asterisk (*) button, and the Pound (#) button are used.

Command line syntax consists of Command Numbers followed by Parameters. Some Commands contain multiple parameters each of which are separated by an asterisk (*). In many cases a parameter is a single entry from a list of possible entries.

Once the desired command is identified and parameters are selected, the entry process is initiated by pressing the START button, followed by the string of numbers for the Command and parameters, and ended by pressing the pound button (#).

The entry is stored in the ScramblePad until the pound (#) button is pressed, so the Pound (#) also functions as a 'send' button, transferring information to the DIGI*TRAC controller for action.

A typical command will have the following arrangement:

START→CMD number→*→1st parameter→*→2nd parameter→*
→last parameter→#

Where the arrow, →, indicates the next step.

For example, the command to set the Date and Day of Week (CMD 50) would be entered as this:

START→50→*→010101→*→4→#

As described in Chapter 4, the first parameter for CMD 50 (see page 4-82) defines the Date which is presented in the format MMDDYY. This means that '010101' equals January 1, 2001.

The second parameter defines the Day of Week which uses an 8-day week beginning on 1 = Monday and ending 7 = Sunday (an eighth day is provided to define a Holiday). So in this example, Day 4 equals Thursday.

Command lines can also support optional parameters – those parameters which are not required but can be supplied to augment a definition or specify additional conditions. In Chapter 4, "Command Reference," optional parameters are indicated by enclosing parameters in square brackets, [ ], such as in this example:

```
START 357 * Starting User Number * Ending User Number *
            Days This Week * [Days Next Week] #
```

In the preceding example, three parameters are required, but the fourth parameter, Days Next Week, is optional and can be added at the discretion of the user.

Programming From The ScramblePad

This section contains information on using the DIGI*TRAC Control Language (DCL) to program some of the more common aspects of the system using the ScramblePad keypad.

Note: If you are using a PC and host software such as SAM, DCL is transparent. SAM oversees the selection and proper formatting of commands and takes care of all error checking. This section and the following chapter (Chapter 4) are most useful for those users interested in acquiring proficiency with programming from the ScramblePad, or for using the diagnostic window in SAM.

How To Enter Programming Mode

To enter Programming Mode:

1. Press the **START** key.
2. Enter **123.**
3. Press the # key to send the system code to the controller.

   The # key is the lower right unmarked key, to the right of the zero key as shown in Figure 3-1, “ScramblePad Setup”, on page 3-5.

When in programming mode, the ScramblePad will not scramble its display for ease of command entry. While in programming mode, both yellow LEDs will be flashing if the program entry code is set to 123, or the right-most yellow LED will be flashing if the system code has been changed from 123 to a new system code.

The system is shipped from the factory with a programming code of 123. To protect the system from unauthorized programming, change this code to a new system code of your choice.

How To Enter A Programming Command

To enter a command:

1. Enter Programming Mode as described above.
2. Press the **START** key.
3. Enter the two- or three-digit command number.

   For a detailed explanation of each command number and its meaning, refer to Chapter 4, “Command Reference.”
4. Press the * key to enter additional command parameters and variables where required.

   The * key is the unmarked key to the left of the zero key, as shown in Figure 3-1, “ScramblePad Setup”, on page 3-5.

   The arrangement of command number and parameters is called *command syntax*, and is different for each command.

   For a complete list of all commands and the syntax they require, refer to Chapter 4, “Command Reference”.
5. Press the # key to send the Command to the Controller.

   The # key is the blank key to the right of the zero key as shown in Figure 3-1, “ScramblePad Setup”, on page 3-5.

If you have entered a valid command with no errors, the green LED on the ScramblePad flashes once.

If you have entered an invalid command, or committed a syntax or data entry error, the red LED flashes once and a tone sounds. The printer will also print an error message followed by the correct Command syntax for the selected Command.

The use of the printer to record programming commands is important. Always make sure the controller is connected to a printer (whether it is a local parallel printer or a remote serial printer) since this is one of the best ways of determining errors when they occur.

For more about this, see “Printing” on page 3-32.

How To Quit Programming Mode

To quit programming mode:

1. Press the **START** key.
2. Enter **99**.
3. Press the # key to send the command to the controller.

The controller will quit programming mode on its own after a designated number of minutes (eight minutes is the default) if no programming commands are entered on the keypad.

Note: You don’t have to exit Program Mode after each command. Enter all the commands you need, then exit when you’re finished.

Command Reference

4

Overview

This chapter details the Hirsch programming commands. It includes all the commands created or revised for version 6.6 as well as new version 7.x commands.

If you are new to programming, you should read Chapter 3 before continuing.

This chapter is divided into these parts:

- ❑ Command Index by Categories
- ❑ Command Index in Numeric Order with Password Level
- ❑ Command Changes and Behavior Differences (Version 6.6 versus Version 7.x)
- ❑ Command Reference

Command Index By Category

System Commands

CMD	Function	Page
00	Print Lists Of Commands	4-30
01	Change System Code	4-31
02	Add Passwords	4-32
96	Terminate Command In Progress	4-114
99	Quit Programming	4-125

Program User Commands

CMD	Function	Page
10	Add Access User (KEYPAD Only - IDF 1)	4-43
11	Redefine Access User	4-44
12	Change Any User Access or Control Zone	4-45
13	Change Any User CODE	4-46
15	Add Unlock/Relock User	4-48
16	Delete Any User	4-50
310	Add Access User (CARD Only - IDF 2)	4-210
311	Add Access User (DUAL Only - IDF 3)	4-211
316	Test CARD During Programming	4-216
325	Change Range of Users To New Function And Zone	4-220

Auto-Program User Commands

CMD	Function	Page
18	Change CODE Length For Auto-Generation	4-54
19	Auto Add Access User (Auto-Gen Code)	4-55
20	Auto Add Access User (Auto-Select User Number)	4-56
21	Auto Add Multiple Access Users (Auto-Gen Code & User Number)	4-57
22	Auto Add Multiple Access Users (Auto-Gen From Specified User Number)	4-58
23	Delete Range Of Users	4-59
220	Batch Add Access Users (Enroll CARD Only) (IDF 2)	4-169
223	Batch Enroll CARD To Existing Users (IDF 5,6,7)	4-170

CMD	Function	Page
224	Batch Change CARD For Existing Users (IDF 2,5,6,7)	4-171
225	Batch Restore Users	4-172

Program Multiple ID User Commands

CMD	Function	Page
312	Add Access User - CARD & DUAL (IDF 4)	4-212
313	Add Access User - KEYPAD & DUAL (IDF 5)	4-213
314	Add Access User - KEYPAD & CARD (IDF 6)	4-214
315	Add Access User - KEYPAD & CARD & DUAL (IDF 7)	4-215
320	Auto-Add Access Users - KEYPAD & DUAL (IDF 5)	4-217
321	Auto-Add Access Users - KEYPAD & CARD (IDF 6)	4-218
322	Auto-Add Access Users - KEYPAD & CARD & DUAL (IDF 7)	4-219

Program Control User Commands

CMD	Function	Page
40	Add Relay Control User	4-70
41	Add Top-Priority Relay Control User	4-71
42	Add Alarm Control User	4-72
43	Add Keypad Index Control User (IDF 1)	4-74
44	Add Special Control User	4-75

User Management Commands

CMD	Function	Page
46	Change Passback Mode	4-78
47	Forgive Passback For User	4-79
48	Forgive Passback/Occupancy Count For All Users	4-80
49	Tag Any User	4-81
146	Disable Passback/Occupancy Count During Time Zone	4-140
149	Alert Users	4-141
235	Change Occupancy Count Limits	4-174
236	Trigger Control Zone On Change In Occupancy Count	4-175
237	Change Occupancy Threshold For Auto-Disable Of 2-Person Access Rule	4-176
238	Single Zone Access	4-177
246	Define Passback Zone	4-178

CMD	Function	Page
255	Change 2-Person-Access-Rule	4-181
256	Change 2-Person-Access-Rule Mode For Relay	4-183
257	Disable 2-Person-Access-Rule During Time Zone	4-184
350	Auto-Delete On Expiration For Users	4-225
351	Use Count Mode For Users	4-226
352	Set Use Count For Users	4-227
353	Absentee Rule Mode For Users	4-228
354	Set Max Days Absent For Users	4-229
355	Forgive Absentee Users	4-230
356	Temporary-Day Mode For Users	4-231
357	Set Days For Temporary-Day Users	4-232
358	Set Deadman Timer	4-233
420	Enable/Disable Users Special Options	4-240
423	Print Users Extracurricular Data	4-244
425	Change Range of Users to New Function and Zone	4-245
426	Define Function Groups	4-246
427	List Function Groups	4-247

Print Users Without Code Commands

CMD	Function	Page
30	Print User Without CODE	4-61
31	Print Users Without CODE	4-62
32	Print First Available User Number	4-63
33	Print Users Given Access or Control Zone	4-64
34	Print Families Of Users Without CODE	4-65

Print Users With Code Commands

CMD	Function	Page
35	Print User With CODE	4-66
36	Print Users With CODE	4-67
37	Print User Given CODE	4-68

CMD	Function	Page
38	Print Families Of Users With CODE	4-69
330	Print Setups And Status By Printout Style For Families Of Users	4-222

Time Control Commands

CMD	Function	Page
50	Set Date & Day Of The Week	4-82
51	Set Time	4-83
52	Define Standard Time Zone	4-84
54	Define Master Time Zone	4-86
56	Clear Time Zone	4-87
57	Define Holiday	4-88
58	Clear Holiday	4-90
59	Clear All Holidays	4-91
154	Define Grand Master Time Zone	4-142
454	Define Master and Grand Master Time Zones	4-249

Access Zone Commands

CMD	Function	Page
17	Define Standard Access Zone - 1 Time Zone All Doors	4-51
24	Define Standard Access Zone - 1 Time Zone Per Door	4-60
117	Define Standard Access Zone - 1 Time Zone Specified Doors Only	4-137
204	Define Master Access Zone	4-167
217	Clear Access Zone	4-168
249	Tag Access Zone	4-180
349	Alert Access Zone	4-224
421	Set Users Special Options	4-241
422	Set Users Custom Access Zone	4-242

Control Zone Commands

CMD	Function	Page
45	Define Standard Control Zone	4-77
301	Add Expansion Alarm Or Relay To Standard Control Zone	4-201

CMD	Function	Page
302	Remove Expansion Alarm Or Relay From Standard Control Zone	4-202
303	Change Time Zone Of Standard Control Zone	4-203
304	Define Master Control Zone	4-204
305	Define Time Zone For Master Control Zone	4-206
306	Clear Master Control Zone	4-207
307	Define Linked Zones for Master Control Zone	4-208
345	Clear Standard Control Zone	4-223
449	Tag Control Zone	4-253
549	Alert Control Zone	4-253

Duress Alarm Commands

CMD	Function	Page
07	Change Duress Digit	4-40
08	Change Duress Alarm Mode	4-41
09	Generate CODEs With Duress Digits	4-42
13	Change Keypad User Code and Duress Digit	4-46
14	Add or Change Duress Digit for User or Range of Users	4-47

Alarm / RQE Commands

CMD	Function	Page
70	Enable Selected Line Module Inputs	4-92
71	Disable Selected Line Module Inputs	4-93
72	Change Selected Line Module Inputs	4-94
73	Change Selected RQEs	4-95
74	Change Door Open-Too-Long Interval	4-96
75	Door Open-Too-Long Active While Unlocked	4-97
76	Mask Line Module Input During Time Zone	4-98
77	Change CODE Tamper	4-99
78	Change Alarm Relay Mapping	4-100
79	Change Time For Alarm Relay	4-101
84	Line Module Input Triggers Control Zone	4-106
110	Change Entry/Exit Delay For Line Module Input	4-133
112	Disable Entry Delay For Line Module Input During Time Zone	4-135
259	Change Special Modes for Line Module Input	4-185

CMD	Function	Page
260	Print Alarm Action	4-186
261	Define Alarm Actions	4-187
262	Alarm Condition Triggers Control Zone	4-191
263	Reset Alarm Actions To Factory Settings	4-192
270	Change Line Module For Line Module Input	4-193
273	Disable RQE During Time Zone	4-194
373	Disable Expansion RQE During Time Zone	4-235
460	Print Action Control Blocks	4-250
461	Action Control Block Options	4-251

Expansion Line Module Input Commands

CMD	Function	Page
111	Change Entry/Exit Delay Time For Expansion Line Module Input	4-134
113	Disable Entry/Exit Delay Time For Expansion Line Module Input During Time Zone	4-136
170	Enable Expansion Line Module Input	4-143
171	Disable Expansion Line Module Input	4-145
172	Change Expansion Line Module Input	4-146
173	Change Expansion RQE	4-147
174	Change DOTL Timer Of Expansion Line Module Input	4-148
175	Expansion DOTL Always Active	4-149
176	Mask Expansion Line Module Input During Time Zone	4-150
180	Change Door Time For Expansion Line Module Input	4-151
184	Expansion Line Module Input Triggers Control Zone	4-155
186	Change Expansion Line Module Input Reporting Mode	4-157
370	Change Line Module For Expansion Line Module Input	4-234

Keypad/MATCH Commands

CMD	Function	Page
03	Change Selected Keypad / MATCH Functions	4-33
103	Change Selected MATCH Functions	4-126
104	Enable CARD-Only At Dual Technology Reader During Time Zone	4-127
247	Change Reader Threat Level Settings	4-179
405	Define Custom Card Reader Configuration	4-239

Relay Commands

CMD	Function	Page
79	Change Time For Alarm Relay	4-101
80	Change Door Time for Relay	4-102
81	Change Control Time Of Relay	4-103
82	Time Zone Control Of Relay	4-104
83	Clear Time Zone Control Of Relay	4-105
85	Change Line Module Input/Relay Contacts for Selected Relays	4-107
86	Change Relay & Line Module Input Operating/Reporting Mode	4-108
87	Relay Triggers Control Zone	4-109
274	Change Door-Open-Too-Long Warning	4-195
280	Change Access Delay Time For Door Relay	4-196
281	Change Control Delay Time For Control Relay	4-197
282	Define Special Needs Unlock Extensions	4-198
283	Change Timer for Relay in 1/4 Seconds	4-199
284	Change Extended Access Time for Relays	4-200
479	Change Time for Alarm Relays	4-252

Expansion Relay Commands

CMD	Function	Page
181	Change Control Time For Expansion Relay	4-152
182	Time Zone Control Of Expansion Relay	4-153
183	Clear Time Zone Control Of Expansion Relay	4-154
184	Expansion Line Module Input Triggers Control Zone	4-155
185	Change Line Module Input/Relay Contacts Of Expansion Relay	4-156
187	Expansion Relay Triggers Control Zone	4-158
374	Change Expansion Door Open Too Long Warning Time	4-236
381	Change Control Delay Timer Of Expansion Relay	4-237
383	Change Timer for Expansion Relay in 1/4 Seconds	4-238

Commands That Clear Settings Or Reset To Defaults

CMD	Function	Page
56	Clear Standard, Master Time Zones	4-87
59	Clear Holidays	4-91

98*18	Host Restore Setup - Clear all Time Zones, ACBs, Access Zones, Control Zones.	4-255
98*26	Reset Setups – Clear all Keypad Setups, Match Readers, Relays and Expansion Relays, Alarm Inputs and Expansion Inputs, Alarm Relay Times, and various miscellaneous setups.	4-255
217	Clear Standard or Master Access Zone(s)	4-168
306	Clear Master Control Zone(s)	4-207
345	Clear Standard Control Zone(s)	4-223

Reporting Commands

CMD	Function	Page
05	Reporting Modes	4-37
06	Disable Report Of Grants	4-39
105	Disable Device During Time Zone	4-128
106	Disable Reporting During Time Zone	4-129
107	Daily Report Mode	4-130
109	Invalid Code Reporting Mode	4-132
140	Set Report Buffer Alarm Threshold	4-138

Remote Site Management Commands

CMD	Function	Page
108	Time Zone Control Of Modem	4-131
193	Set Host Phone Number	4-163
194	Set Tone Or Pulse Dialing	4-164
195	Change Host Call Back	4-165

Print System Setups And Status Commands

CMD	Function	Page
88	Print System Setups and Status	4-110
188	Print Command Setups	4-159

Maintenance Commands

CMD	Function	Page
90	Maintenance	4-113
97	Change System Parameters	4-115
191	Change Page Length For Printer	4-161

CMD	Function	Page
192	Change Programming Time-out Interval	4-162
200	Change Printer Language	4-166

Host-Based Commands

CMD	Function	Page
98	Upload/Download Setup Commands	4-255
198	Host-Generated Commands	4-272
435	Define Occupancy Count Limits from Host	4-275
436	Define Occupancy Count Control Zones from Host	4-276
450	Set Date and Time From Host	4-277
457	Define Holidays From Host	4-279

Command Index In Numeric Order With Password Level

For a definition of password levels, refer to “CMD 02: ADD PROGRAMMING PASSWORD” on page 4-32.

CMD	Function	Level	Page
00	Print Lists Of Commands	12345	4-30
01	Change System Code	1	4-31
02	Add Passwords	1	4-32
03	Change Selected Keypads	125	4-33
05	Reporting Modes	125	4-37
06	Disable Report Of Grants	125	4-39
07	Change Duress Digit	1234	4-40
08	Change Duress Alarm Mode	125	4-41
09	Generate CODEs With Duress Digits	1234	4-42
10	Add Access User (Keypad Only – IDF 1)	123	4-43
11	Redefine Access User	123	4-44
12	Change Any User Access or Control Zone	123	4-45
13	Change Any User CODE	123	4-46
14	Add or Change Duress Digit for User or Range of Users	123	4-47
15	Add Unlock/Relock User	123	4-48
16	Delete Any User	1234	4-50
17	Define Standard Access Zone – 1 Time Zone All Doors	12345	4-51
18	Change CODE Length For Auto-Generation	1234	4-54
19	Auto Add Access User (Auto-Gen Code)	123	4-55
20	Auto Add Access User (Auto-Select User Number)	123	4-56
21	Auto Add Multiple Access Users (Auto-Gen Code & User Number)	123	4-57
22	Auto Add Multiple Access Users (Auto-Gen From Specified User Number)	123	4-58
23	Delete Range Of Users	1234	4-59
24	Define Standard Access Zone – 1 Time Zone Per Door	12345	4-60
30	Print User Without CODE	1234	4-61
31	Print Users Without CODE	1234	4-62
32	Print First Available User Number	1234	4-63
33	Print Users Given Access or Control Zone	1234	4-64

CMD	Function	Level	Page
34	Print Families Of Users Without CODE	1234	4-65
35	Print User With CODE	123	4-66
36	Print Users With CODE	123	4-67
37	Print User Given CODE	123	4-68
38	Print Families Of Users With CODE	123	4-69
40	Add Relay Control User	123	4-70
41	Add Top-Priority Relay Control User	123	4-71
42	Add Alarm Control User	123	4-72
43	Add Keypad Index Control User (IDF 1)	123	4-74
44	Add Special Control User	123	4-75
45	Define Standard Control Zone	12345	4-77
46	Change Passback Mode	125	4-78
47	Forgive Passback For User	1234	4-79
48	Forgive Passback/Occupancy Count For All Users	1234	4-80
49	Tag Any User	1234	4-81
50	Set Date & Day Of The Week	12345	4-82
51	Set Time	12345	4-83
52	Define Standard Time Zone	12345	4-84
54	Define Master Time Zone	12345	4-86
56	Clear Time Zone	12345	4-87
57	Define Holiday	12345	4-88
58	Clear Holiday	12345	4-90
59	Clear All Holidays	12345	4-91
70	Enable Selected Line Module Inputs	125	4-92
71	Disable Selected Line Module Inputs	125	4-93
72	Change Selected Line Module Inputs	125	4-94
73	Change Selected RQEs	125	4-95
74	Change Door Open-Too-Long Interval	125	4-96
75	Door Open-Too-Long Active While Unlocked	125	4-97
76	Mask Line Module Input During Time Zone	125	4-98
77	Change CODE Tamper	125	4-99
78	Change Alarm Relay Mapping	125	4-100

CMD	Function	Level	Page
79	Change Time For Alarm Relay	125	4-101
80	Change Door Time for Relay	125	4-102
81	Change Control Time Of Relay	125	4-103
82	Time Zone Control Of Relay	125	4-104
83	Clear Time Zone Control Of Relay	125	4-105
84	Line Module Input Triggers Control Zone	125	4-106
85	Change Line Module Input/Relay Contacts for Selected Relays	125	4-107
86	Change Relay & Line Module Input Operating & Reporting Mode	125	4-108
87	Relay Triggers Control Zone	125	4-109
88	Print System Setups and Status	12345	4-110
90	Maintenance	12345	4-113
96	Terminate Command In Progress	12345	4-114
97	Change System Parameters	12345	4-115
98	Upload/Download Setup Commands	12345	4-255
99	Quit Programming	12345	4-125
103	Change Selected MATCH Functions	125	4-126
104	Enable CARD-Only At Dual Technology Reader During Time Zone	125	4-127
105	Disable Device During Time Zone	125	4-128
106	Disable Reporting During Time Zone	125	4-129
107	Daily Report Mode	125	4-130
108	Time Zone Control Of Modem	125	4-131
109	Invalid Code Reporting Mode	125	4-132
110	Change Entry/Exit Delay For Line Module Input	125	4-133
111	Change Entry/Exit Delay Time For Expansion Line Module Input	125	4-134
112	Disable Entry Delay For Line Module Input During Time Zone	125	4-135
113	Disable Entry/Exit Delay Time For Expansion Line Module Input During Time Zone	125	4-136
117	Define Standard Access Zone – 1 Time Zone Specified Doors Only	1235	4-137
124	Define Standard Access Zone – 1 Time Zone Per Reader	1235	4-138
140	Set Report Buffer Alarm Threshold	12	4-139
146	Disable Passback/Occupancy Count During Time Zone	125	4-140

CMD	Function	Level	Page
149	Alert Users	1234	4-141
154	Define Grand Master Time Zone	12345	4-142
170	Enable Expansion Line Module Input	125	4-143
171	Disable Expansion Line Module Input	125	4-145
172	Change Expansion Line Module Input	125	4-146
173	Change Expansion RQE	125	4-147
174	Change DOTL Timer Of Expansion Line Module Input	125	4-148
175	Expansion DOTL Always Active	125	4-149
176	Mask Expansion Line Module Input During Time Zone	125	4-150
180	Change Door Mode For Expansion Line Module Input	125	4-151
181	Change Control Mode For Expansion Relay	125	4-152
182	Time Zone Control Of Expansion Relay	125	4-153
183	Clear Time Zone Control Of Expansion Relay	125	4-154
184	Expansion Line Module Input Triggers Control Zone	125	4-155
185	Change Line Module Input/Relay Contacts Of Expansion Relay	125	4-156
186	Change Expansion Line Module Input Reporting Mode	125	4-157
187	Expansion Relay Triggers Control Zone	125	4-158
188	Print Command Setups	12345	4-159
191	Change Page Length For Printer	12345	4-161
192	Change Programming Time-out Interval	12345	4-162
193	Set Host Phone Number	125	4-163
194	Set Tone Or Pulse Dialing	125	4-164
195	Change Host Call Back	125	4-165
198	Host-Generated Commands	12345	4-272
200	Change Printer Language	12345	4-166
204	Define Master Access Zone	125	4-167
217	Clear Access Zone	125	4-168
220	Batch Add Access Users (Enroll CARD Only) (IDF 2)	123	4-169
223	Batch Enroll CARD To Existing Users (IDF 5,6,7)	123	4-170
224	Batch Change CARD For Existing Users (IDF 2,5,6,7)	123	4-171
225	Batch Restore Users	123	4-172

CMD	Function	Level	Page
235	Change Occupancy Count Limits	123	4-174
236	Trigger Control Zone On Change In Occupancy Count	125	4-175
237	Change Occupancy Threshold For Auto-Disable Of 2-Person Access Rule	123	4-176
238	Single Zone Access	1234	4-177
246	Define Passback Zone (PZ Area)	1234	4-178
247	Change Reader Threat Level Settings	123	4-179
249	Tag Access Zone	1234	4-180
255	Change 2-Person-Access-Rule	125	4-181
256	Change 2-Person-Access-Rule Mode For Relay	125	4-183
257	Disable 2-Person-Access-Rule During Time Zone	125	4-184
259	Change Special Modes for Inputs	125	4-185
260	Print Alarm Action	125	4-186
261	Define Alarm Actions	125	4-187
262	Alarm Condition Triggers Control Zone	125	4-191
263	Reset Alarm Actions To Factory Settings	125	4-192
270	Change Line Module For Line Module Input	125	4-193
273	Disable RQE During Time Zone	125	4-194
274	Change Door-Open-Too-Long Warning	125	4-195
280	Change Access Delay Time For Door Relay	125	4-196
281	Change Control Delay Time For Control Relay	125	4-197
282	Define Special Needs Unlock Extensions	125	4-198
283	Change Timer for Relay in 1/4 Seconds	125	4-199
284	Change Extended Access Times for Relays	125	
301	Add Expansion Alarm Or Relay To Standard Control Zone	125	4-201
302	Remove Expansion Alarm Or Relay From Standard Control Zone	125	4-202
303	Change Time Zone Of Standard Control Zone	125	4-203
304	Define Master Control Zone	125	4-204
305	Define Time Zone For Master Control Zone	125	4-206
306	Clear Master Control Zone	125	4-207
307	Define Linked Zones for Master Control Zone	125	4-208
310	Add Access User (CARD Only – IDF 2)	123	4-210
311	Add Access User (DUAL Only – IDF 3)	123	4-211
312	Add Access User - CARD & DUAL (IDF 4)	123	4-212

CMD	Function	Level	Page
313	Add Access User - KEYPAD & DUAL (IDF 5)	123	4-213
314	Add Access User - KEYPAD & CARD (IDF 6)	123	4-214
315	Add Access User - KEYPAD & CARD & DUAL (IDF 7)	123	4-215
316	Test Card During Programming	123	4-216
320	Auto-Add Access Users - KEYPAD & DUAL (IDF 5)	123	4-217
321	Auto-Add Access Users – KEYPAD & CARD (IDF 6)	123	4-218
322	Auto-Add Access Users – KEYPAD & CARD & DUAL (IDF 7)	123	4-219
325	Change User To New Function And Zone	123	4-220
330	Print Setups And Status By Printout Style For Families Of Users	12	4-222
345	Clear Standard Control Zone	125	4-223
349	Alert Access Zone	1234	4-224
350	Auto-Delete On Expiration For Users	1234	4-225
351	Use Count Mode For Users	1234	4-226
352	Set Use Count For Users	1234	4-227
353	Absentee Rule Mode For Users	1234	4-228
354	Set Max Days Absent For Users	1234	4-229
355	Forgive Absentee Users	1234	4-230
356	Temporary-Day Mode For Users	1234	4-231
357	Set Days For Temporary-Day Users	1234	4-232
358	Set Deadman Timer	123	4-233
370	Change Line Module For Expansion Line Module Input	125	4-234
373	Disable Expansion RQE During Time Zone	125	4-235
374	Change Expansion Door-Open-Too-Long Warning Time	125	4-236
381	Change Control Delay Timer Of Expansion Relay	125	4-237
383	Change Timer for Expansion Relay in 1/4 Seconds	125	4-238
405	Define Custom Card Reader Configuration	12345	4-239
420	Enable/Disable Users Special Options	12345	4-240
421	Set Users Special Options	12345	4-241
422	Set Users Custom Access Zone	12345	4-242
423	Print Users Extracurricular Data	12345	4-244

CMD	Function	Level	Page
425	Change Range of Users to New Function and Zone	12345	4-245
426	Define Function Groups	12345	4-246
427	List Function Groups	12345	4-247
435	Define Occupancy Count Limits from Host	12345	4-275
436	Define Occupancy Count Control Zones from Host	12345	4-276
449	Tag Control Zone	125	4-253
450	Set Date and Time From Host	12345	4-277
454	Define Master and Standard Time Zone (66-149)	12345	4-249
457	Define Holidays from Host	12345	4-279
460	Print Action Control Blocks	12345	4-250
461	Action Control Block Options	12345	4-251
479	Change Time for Alarm Relays	12345	4-252
549	Alert Control Zone	1234	4-253

Command Changes and Behavior Differences

Many commands used in CCM 6.6 have been updated with new options for CCM 7.0. Other commands are completely new to CCM 7.0. Still other commands behave differently depending on which version of the CCM you are using.

These changes and behavior differences can be relevant to Hirsch software, since some applications employ CCM 6.6 while others employ CCM 7.0. These are:

Hirsch Software	CCM Used
S*NAP	6.6 or earlier
SAM	6.6 or earlier
MOMENTUM	6.6 or earlier
Velocity	7.0 or later

Differences and changes are even more relevant to keypad programmers, since programming a controller with a CCM 6.6 is different than programming with CCM 7.0 and later.

The differences are outlined in the following subsections.

New 7.0 Commands

These commands have been added to CCM 7.0 and do not work with CCM 6.6.

CMD	Description	Page
246	Define Passback Zone	4-178
247	Change Reader Threat Level Settings	4-179
273	Disable RQE for Time Zone	4-194
274	Change Door Open Too Long Warning Time	4-195
284	Change Extended Access for Relays	4-200
373	Disable Expansion RQE for Time Zone	4-235
374	Change DOTL Warning Time Of Expansion Alarm Input	4-236
405	Change Custom Card Reader Configuration	4-239
420	Enable/Disable Users Special Options	4-240
421	Set Users Special Options	4-241
422	Set Users Extracurricular Data	4-242
423	Print Users Extracurricular Data	4-244
424	Print Users with Access at Door/Reader/Input	4-244
425	Change User to New Function And Zone	4-245
454	Define Master or Grand Master Time Zone 66-149	4-249
479	Change Time for Alarm Relays	4-252

In addition to the preceding commands, there are more than a dozen host-generated com-

mands. Several of these host commands are listed at the end of this section (including CMDs 98 and 198). Other host commands are not documented here since they are meant for Hirsch programming and troubleshooting, not for keypad programming.

For more about selected host commands, go to “Host-Based Commands” on page 4-254.

New Options for Existing Commands

The new CCM 7.0 command set has also added new options to older CCM 6.x commands. These are:

CMD	Description	Comment	Page
05	Reporting Modes	Enable/disable option removed	4-37
06	Disable Report of Grants	RQE and Access doors selectable	4-39
18	Change CODE Length For Auto-Generation	Card Length option added	4-54
37	Print User Given CODE	Card options IDF 2-7	4-68
52	Define Standard Time Zone	Holiday table option added	4-84
57	Define Holiday	superseded by host command	4-88
58	Clear Holiday	superseded by host command	4-90
59	Clear All Holidays	Year clear option added	4-91
88	Print System Setups and Status	New options added	4-110
97	Change System Parameters	SCIB extension options added	4-115
108	Time Zone Control Of Modem	Time zone options added	4-131
170	Enable Expansion Alarm Input(s)	Expansion input options added	4-143
171	Disable Expansion Alarm Input(s)	Expansion input options added	4-145
261	Define Action Control Block(s)	New ACBs added	4-187
270	Change Supervised Line Module For Alarm Input	Two or more line modules can be defined in same line	4-193
325	Change User To New Function And Zone	Seven new options (29 - 41) added	4-220
330	Print Setups And Status By Printout Style For Families Of Users	One option and two styles added	4-222
352	Set Use Count or Temp Days For Users	Extends uses range from 31 to 255	4-227
353	Absentee Rule Mode For Users	Extends absences range from 63 to 255	4-228

CMD	Description	Comment	Page
354	Set Max Days Absent For Users	Extends absence range from 63 to 255	4-229
357	Set Days For Temporary-Day Users	Replaces this command with a day count option	4-232

Changes in Behavior

There are certain ways in which controllers respond to Version 6.x commands that differentiate them from Version 7 commands. These changes in behavior are reflected in the Hirsch software that support these CCM versions. A description of these differences as well as other apparent limitations follows.

All Software

One of the major differences between CCM 7.0 and CCM 6.6 is the way it handles IDFs. As shown in Table 2-10, CCM 6.6 stores different IDFs in different ways: the controller can store twice as many IDF 1, 2, and 3 as it can IDF 4, 5, 6; IDF 7 takes up even more space (four IDF 1, 2 or 3s can be stored for every one IDF 7).

CCM 7 makes no distinctions between IDFs. To the newer version, just as many IDF7s can be stored as IDF1s. And because of its more efficient code, Version 7 can pack more IDFs than Version 6.6 into the available memory space. This has an effect on all commands in which IDFs figure, such as batch user access definition (CMDs 210 – 224) and access user definitions (CMDs 310 – 322). While IDFs are still a prevailing principle in code and card creation, they no longer impose on memory in Version 7 as they did in earlier versions.

Velocity

CCM 7.0 commands are compatible with this program. Velocity has been designed for use with the new CCM version and accepts the full list of the new commands. In particular, Velocity utilizes the new host-based commands, such as 98 and 198, to send packets of instructions to the relevant controller's CCM. Host-based commands cannot be interpreted by pre-7.0 CCMs.

Other behaviors include:

- ❑ Three new alarm types are supported: pre-arm status, conditional unmask, and partial unmask. All three alarms check the status of all alarm points specified in their governing SCZ even if those inputs are disabled. For this reason, don't include disabled alarm points in your SCZ.
- ❑ At the current time, user numbers 65536 – 65539 don't work properly in most commands. Avoid these numbers.
- ❑ Passback settings for CMD 432 should maintain: when set from the Host and echoed back to the controller, they should stay set.
- ❑ Disabled inputs generate input state change messages.
- ❑ 'Overnight time zones' do not work as one might expect. For example, if you set an STZ of 22:00-06:00 Monday, the CCM interprets this as midnight to 6 AM on Monday, then 10 PM to midnight of the same day. To set a STZ from 10 PM on Monday to 6 AM on Tuesday, you would have to define two separate time zones, 22:00-24:00 Monday and 00:00-06:00 Tuesday.

MOMENTUM

At the current time, MOMENTUM only uses Version 6.6 CCMs. This precludes the use of all host-based commands that were part of the Version 7 updates. If a MOMENTUM operator tries to send a raw Version 7 command to an attached MOMENTUM controller (using the Loop Monitor or Hirsch Test Tool), the controller will reject the command. Even if the controller contains an updated Version 7 CCM, MOMENTUM has no way of using or tracking such a command.

Other influences of Version 7 on behavior:

- ❑ On IDF 2-7 users, cards won't work and access is denied. Code record downloads write the wrong card value to the database. Instead of appending zeros to the MATCH code, the CCM appends Fs and stores the wrong 16-digit code. To avoid this, use Version 6.6.
- ❑ CMD 06*2 won't work since it requires a new RQE ACB that MOMENTUM doesn't support.
- ❑ The program records message termination errors from message 102. To avoid this, use Version 6.6.

SAM

SAM works seamlessly with controllers containing CCM Version 6.6 and earlier firmware. It can also communicate with CCM Version 7.x firmware (7.2.07 and earlier); however there are limitations: SAM cannot utilize any of the host-based commands that were part of the Version 7 updates. If a SAM operator tries to send a raw Version 7 command to an attached controller (using the Diagnostic Window), the controller will reject the command.

Note: SAM cannot communicate with controllers using CCM Version 7.3.x or later.

Other common behaviors are:

- ❑ In Version 7, 'Overnight time zones' do not work as one might expect. For example, if you set an STZ of 22:00-06:00 Monday, the CCM interprets this as midnight to 6 AM on Monday, then 10 PM to midnight of the same day. To set a STZ from 10 PM on Monday to 6 AM on Tuesday, you would have to define two separate time zones, 22:00-24:00 Monday and 00:00-06:00 Tuesday.
- ❑ Trailing zeroes can be added to or deleted from the end of IDF 3 (dual technology) PINs.
- ❑ MATCH Reader 8 does not respond to setups through SAM. This is a bug with SAM, not the firmware.
- ❑ Memory expansion boards are not recognized in the System Configuration screen's 'User Database Capacity' field. The maximum default number of code records reported is 1000; however, if you perform a **Load From System** then press **F8 Update**, the maximum number of records for a CCM 7 controller is 4095.
- ❑ Code records are downloaded correctly but IDF 2 – 7 users are not displayed correctly in the Diagnostic window when CMD 36 is used.
- ❑ CMD 06*2 won't work since it requires a new RQE ACB that SAM doesn't support.
- ❑ Setting up an access zone with expansion access points will fail when it downloads to the controller. SAM will fail if you try to specify expansion access points that exceed the number of installed expansion alarm inputs.

- ❑ The expansion access portion of the Standard Access Zone does not apply. Any attempt at a expansion access-configured keypad/reader results in the access zone using the time zone for the door that would correspond to the reader number (that is, Readers 9 – 16 would refer to the time zones for Doors 1 – 8.
- ❑ Version 6.x compatibility for Version 7 holiday tables does not extend to manual holidays. A manual holiday is treated as if it were an unnumbered, regularly scheduled holiday. To revoke a manual holiday, delete the holiday using CMD 457*0*YYYY*MMDD#.
- ❑ In the Diagnostics window, an 88*29 command shows all virtual relays designated as *2u* rather than the number they represent.

S*NAP

S*NAP only uses Version 6.6 or earlier CCMs. If a S*NAP operator tries to send a raw Version 7 command to an attached S*NAP controller, the controller will reject the command.

Other behaviors include:

- ❑ The Network Manager only shows V5 and V6 controllers, not Version 7. The V6 and V7 motherboards are identical from S*NAP's point-of-view. A Version 7 CCM reports to SNAP as a Version 6 board.
- ❑ CMD 06*2 won't work since it requires a new RQE ACB that S*NAP doesn't support.

Command Reference

The following section provides detailed information on all the commands used in the DIGI*TRAC Control Language (DCL).

The topics covered for each command are:

- ❏ Syntax
- ❏ Variables (where appropriate)
- ❏ Description
- ❏ Examples
- ❏ Defaults
- ❏ Related Commands

In the following section, the square bracket [ ] is used to indicate that the variable or parameter is optional and need not be included unless necessary.

The icon in the Related Commands subsection of each command indicates the command used to print out the current settings for the specific command.

CMD 00: PRINT LISTS OF COMMANDS

Syntax: `START 00 * NN #`

Variables: NN

0	All Commands
1	System Commands
2	Program User Commands
3	Auto-Program User Commands
4	Program Multiple ID User Commands
5	Program Control User Commands
6	User Management Commands
7	Print Users Without Codes Commands
8	Printer Users With Code Commands
9	Time Control Commands
10	Access Zone Commands
11	Control Zone Commands
12	Duress Commands
13	Alarm/RQE Commands
14	Expansion Alarm Commands
15	Keypad/MATCH Commands
16	Relay Commands
17	Expansion Relay Commands
18	Report Commands
19	Remote Site Management Commands
20	Print System Setups and Status
21	Maintenance Commands
22	Glossary

Description:

A printout of each or all of the Command Categories may be generated from the controller's permanent memory. Automatic Context Sensitive Help prints the correct syntax for any individual Command whenever a programming error is made.

Examples:

```
START 00 * 2 #
```

Prints Program User Commands

```
START 00 * 11 #
```

Prints Control Zone Commands

Default:

None

Related CMDs:

CMD 88 – Print System Setups and Status
CMD 01 - Change System Code

CMD 01: CHANGE SYSTEM CODE

Syntax: `START 01 * SYSTEM CODE #`

Description:

The system code controls Scramblepad access to programming mode.

The system code may be set to any available 3-8 digit code and is permanently assigned to User 0. It is factory set to 123 on system start up. It is important to protect the security of your system by changing the system code to a code of your choice at system start up. The longer the code the greater the security. A 7- or 8-digit code is recommended.

There is a system code reset button on the controller board which, when depressed for 5 seconds, will return the system to a system code of 123. This is the only method available to return to a system code of 123 as command 01 will not allow programming a Code to 123.

If the system code is not changed from 123 to a new code, you will receive the following warning on the system printer once every four hours:

```
Warning! System CODE is 123!
```

In addition, if the system code is still set to 123 when Programming Mode is active at a ScramblePad, both yellow LEDs blink in unison. Once the code is changed, only the second yellow LED blinks whenever you enter Programming Mode.

Note: A special control command is available for networked controllers from the SAM software that disables the system code reset button. DO NOT hold the controller's reset button down more than 5 seconds if it does not work. Holding the button down for 30 seconds will cold start the controller and erase all programmed information from memory.

Further restriction of programming may be implemented through the command 02, add password.

*Note: This command is unavailable from S*NAP software.*

Example:

```
START 01 * 66402139 #
```

Changes SYSTEM CODE To 66402139

Default:

123

Related CMDs:

CMD 35, 36, 38*8, 330 – Print User, Users, or Family of Users with Codes
CMD 99 – Quit Programming

Adding and Changing Codes

CMD 02 – Add Programming Pass/word
CMD 13*0 – Change User Codes
CMD 90*2#/97*6 – Enable/Disable Master Code Reset

Keypad Setups

CMD 03*3 – Change Reader Function (Programming)
CMD 403 – Change Selected Keypad / MATCH Functions From Host

CMD 02: ADD PROGRAMMING PASSWORD

Syntax: `START 02 * PASSWORD Level * User Number * Code #`

Variables: PASSWORD Level

1 - System Code PASSWORD
2 - Executive PASSWORD
3 - Supervisor PASSWORD
4 - Operator PASSWORD
5 - Service PASSWORD

Description:

Passwords control ScramblePad access to programming mode. Passwords enable five levels of programming command restriction. Each level is only able to use certain programming commands according to the password level assigned to the operator's user number when added to the system. Any number of users may be assigned to any level. Each authorized operator is logged onto the system when programming mode is entered. Only one operator may be logged on at a time. For each command's allowed password levels, refer to "Command Index In Numeric Order With Password Level" on page 4-17. The five password levels are defined below:

Password Level	Restrictions
1. System Password	All Commands
2. Executive Password	All Commands Except Passwords
3. Supervisor Password	All Commands Except Setups
4. Operator Password	All Except Setups & Add or Print Users With Codes
5. Service Password	All Setups & Print Status, No User Commands

Table 4-1: Password Levels

Note: Passwords are assigned to Access Zone 65. This allows Programming Command entry 24 hours a day, any day. CMD 12 may be used to restrict the use of any Password to the times and days of any specified Access Zone.

Examples:

```
START 02 * 1 * 1 * 17964484 #
```

Add SYSTEM CODE Password As User 1 With Code 17964484

```
START 02 * 4 * 2 * 49173068 #
```

Add Operator Password As User 2 With Code 49173068

```
START 02 * 5 * 3 * 88629174 #
```

Add Service Password As User 3 With Code 88629174

Default:

123 System code for User Zero (0).

Related CMDs:

CMD 35, 36, 38*8, 330 – Print User, Users, or Family of Users with Codes
CMD 99 – Quit Programming

Changing and Deleting Codes

CMD 01, 13*0 – Change System (User 0) Code
CMD 13, 325 – Change Any Keypad User Code; Change User's Function
CMD 16, 23 – Delete Any User, Range of Users

Keypad Setups

CMD 03*3 – Change Reader Function (Programming)
CMD 403 - Change Selected Keypad / MATCH Functions From Host

CMD 03: CHANGE SELECTED KEYPAD/MATCH FUNCTIONS

Syntax: `START 03 * NN * 1/0 * Address 1-8 [* Address 1-8] #`

Variables: **NN**

1	Scramble
2	Silent
3	Programming
4	Control
5	Access
6	Status Request
7	Passback Entry
8	Passback Exit
9	Passback Internal
10	Passback Unrestricted – External
11	Expansion Alarm Access
12	Red LED ON
13	Green LED ON
14	Yellow LED 1 ON
15	AC Fail = Yellow LED 1 Blink
16	Set Green LED while relay is active
17	Set Green LED during door delay
18	Use keypad numeric LEDs as annunciator
19	Allow User Count Display
20	Code Tamper Disables User
21	Silent Code Tamper
22	Deny Codes Under Duress
23	Flash Yellow LED 1 during control delay
24	Latching Code Tamper Rule
25	Sequential Code Tamper Rule
26	Sequential Code Tamper Rule #2
27	ScramblePad DS47 is 980313 or similar: "digits in the wrong order"
28	Timed Passback Rule
29	Visitor/Escort Rules – Visitors Must Be Accompanied by Escort
30	Visitor/Escort Rule #2 – Visitor can go first, wait for visitor
31	Visitor/Escort Rule #3 – Escort code toggles Vis/Esc mode
32	Use Keypad Numeric LEDs to display Visitor Count

1/0

1	ON
0	OFF

Description:

To change the function of any ScramblePad/MATCH Reader:

1. Select the function number, such as 1 for display Scramble.
2. Select 1 to turn the function ON or 0 to turn it OFF
3. Select the ScramblePad/MATCH Reader Addresses to be changed.

ScramblePad/MATCH Readers are selected by entering 1 through 8 in the first set for Addresses 1 through 8, and by selecting 1 through 8 in the second set for Addresses 9 through 16.

If no Addresses from either set of 8 are being changed, enter a 0 (zero).

For example, pressing:

```
START 03 * 1 * 0 * 1 * 0 #
```

changes scramble feature to OFF (normal pattern) for ScramblePad 1.

Each ScramblePad keypad can be set to scramble a normal digit pattern. ScramblePad keypads will not scramble in Programming Mode.

Each ScramblePad Keypad may operate in silent mode. ScramblePads/MATCH Readers may be set to not accept various types of Codes such as Programming (ScramblePad only), Control, or Access Types. ScramblePad Keypads may be set to not accept a status display request. The Status Display Request allows a User to request the Status of any Relay or Line Module Input from any ScramblePad Keypad.

Note: Functions 1, 2, 3, 6, 12, 13, 14, and 15 apply to ScramblePad Keypads only.

To operate the status request, press:

```
START * #
```

This results in a display of the status of the Relay and Alarm input associated with the ScramblePad Keypad address from which the request was entered.

For example, requesting the status at ScramblePad 1 displays the status of Relay 1 and Alarm 1.

To request the status of any other point, press:

```
START * Point_ID_Number #
```

For example, pressing

```
START * 8 #
```

from ScramblePad 1 displays the status of Relay 8 and Alarm 8 at ScramblePad Keypad 1. If you press

```
START * 01 #
```

from ScramblePad 1 it displays the status of Expansion Relay 1 and Expansion Alarm 1, if either or both are installed.

The status request LEDs can indicate these conditions:

LEDs	Status Request
No LEDs	Input masked & enabled.
Yellow 2	Input masked & enabled. Door open.
Yellow 2 + Tone	Input masked & enabled. Line fault.
Yellow 1	Input disabled.
Green	Input masked & enabled. Relay energized.
Green + Yellow 2	Input masked & enabled. Door open. Relay energized.
Green + Yellow 2 + Tone	Input masked & enabled. Line fault. Relay energized.
Green + Yellow 1	Input disabled. Relay energized.
Red	Input enabled. Unmasked or door grant in progress.

LEDs	Status Request
Red + Yellow 2	Input enabled. Unmasked or door grant in progress. Door open.
Red + Yellow 2 + Tone	Input enabled. Unmasked or door grant in progress. Line fault or Door forced/open.
Red + Green	Input enabled. Unmasked or door grant in progress. Relay energized.
Red + Green + Yellow 2	Input enabled. Unmasked or door grant in progress. Door open. Relay energized.
Red + Green + Yellow 2 + Tone	Input enabled. Unmasked or door grant in progress. Line fault or Door forced, Door open. Relay energized.

LEDs can also be configured to indicate delay conditions. For example, 03*17*1 sets the keypad/MATCH to flash its green LED while the door delay period is counting down. The door delay is set by CMD 280. Similarly, 03*23*1 sets the first yellow LED to flash while the timer is counting down the control delay time. The control delay time is set by CMD 281.

For Passback and Occupancy Violation to work, ScramblePad/MATCH Reader addresses must be defined as Entry, Exit, Internal or Unrestricted (No Passback Status).

An internal ScramblePad/MATCH Reader will only grant access if the user has been detected as inside the secure perimeter after coming through an entry ScramblePad/MATCH Reader. Once the controller detects the same user has exited through an exit ScramblePad/MATCH Reader, any attempt to use that user's code or card at an internal door will be denied and reported as a passback violation.

To link a ScramblePad/MATCH Reader to an expansion line module input for access-by-alarm control, select number 11.

ScramblePad can be set to always keep the Red, Green and Yellow LED 1 status indicators on.

AC Fail can be set to blink Yellow LED 1, if required.

CMD 03*27 provides for limited compatibility with certain older DS47 revisions.

Examples:

```
START 03 * 3 * 0 * 1234578 * #
```

Change Programming Capability OFF to ScramblePad keypads 1 2 3 4 5 7 & 8.

```
START 03 * 7 * 1 * 34 * #
```

Change Passback Entry Address ON to Keypads/MATCH Readers 3 & 4.

```
START 03 * 8 * 1 * * 34 #
```

Change Passback Exit Address ON to Keypads/MATCH Readers 11 & 12.

```
START 03 * 23 * 1
```

Enable the First Yellow LED to flash during a specified control delay period.

Default:

NN	Function	Initial State
1	Scramble	ON
2	Silent	OFF
3	Programming	ON
4	Control	ON

NN	Function	Initial State
5	Access	ON
6	Status Request	ON
7	Passback Entry	OFF
8	Passback Exit	OFF
9	Passback Internal	OFF
10	Passback Unrestricted	ON
11	Expansion Access	OFF
12	Red LED ON	OFF
13	Green LED ON	OFF
14	Yellow LED 1 ON	OFF
15	AC Fail = Yellow LED 1 Blink	OFF
16	Set Green While Relay Active	OFF
17	Set Green Flash During Door Delay	OFF
18	Use Keypad Numeric LEDs as annuniciator	OFF
19	Allow User Count Display	OFF
20	Code Tamper Disables User	OFF
21	Silent Code Tamper	OFF
22	Deny Codes Under Duress	OFF
23	Set First Yellow Flash During Control Delay	OFF

Related CMDs:

General

CMD 88*11 – Print Keypad/Match Setups and Status

CMD 188*3 – Print Setup Changes for Keypad/MATCH

CMD 17 – Define Standard Access Zone

*03*3 –Programming Functions*

CMD 01, 02 – Add or Change Programming Codes

*03*4 – Control Functions*

CMD 45 – Define Standard Control Zone

*03*7, 03*8, 03*9, 03*10 –Passback Functions*

CMD 46 – Change Passback Mode

CMD 146 – Disable Passback and Occupancy Control During Time Zone

CMD 05: REPORTING MODES

Syntax: `START 05 * NN # (V7 version)`
`START 05 * NN [* 1/0] # (V6.6 version)`

Variables: NN

1	Disable Relay State Changes
2	Disable Internal Events
3	Disable External Events
4	Disable Transactions
5	Disable Time Zone State Changes
6	Disable Time Zone Relay Control State Changes
7	Disable Time Zone Input Masking State Changes
8	Print All
9	Input State Change
10	MOMENTUM SCRAMBLE*NET Protocol
11	VELOCITY SCRAMBLE*NET Protocol

1/0 (V6.6 only)

1	Enable mode listed above	(05*8*0# now disables all)
0	Disable mode listed above	(05*8*1# now enables all)

Description:

Disable Relay State Changes	turns off the reporting of relay state changes and will conserve printer paper and buffered event storage. Effective with V6.6, a cold-started controller will have relay state changes enabled as the factory default. You can use 05*1*1# to enable it, and 05*8# or 05*8*1# will still turn on every mode. CMD 05*1*1# will enable relay state changes and will also send the current relay states to the host if the host has logged on with CMD 198*6. CMD 05*9*1# will enable input state changes for all enabled inputs, and will also send the current input states to the host.
Disable Internal Events	turns off the reporting of automatic time generated events, when Time Zones Start and End, and Relay State Changes.
Disable External Events	turns off the reporting of Alarm, AC, Box and Address Tamper alarm restorals, On-lines and Installation Errors, UPS restoral, Alarm Secure, line trouble clear, Passback Violations and printer on-line.
Disable Transactions	turns off the reporting of all Code generated transactions, but not alarms.
Disable Time Zone State Changes	turns off the reporting of Time Zone activation and deactivation.
Disable Time Zone Relay State Changes	turns off the reporting of Time Zone-driven relays and their change of state.
Disable Time Zone Input Masking Changes	turns off the reporting of Time Zone-driven input masking changes.
Print All	reenables reporting of all changes and transactions. Also re-enables printing of access and RQE Grants for CMD 06.

Input State Change	enables reporting of input state changes. This affects all alarm inputs and expansion inputs at once. The default is disabled. See also CMD 98*33.
MOM S*NET Protocol	enables reporting of the MOMENTUM S*NET protocol. The default is disabled.
Velocity S*NET Protocol	enables reporting of the Velocity S*NET protocol. The default is disabled. The normal method for enabling V7.0 protocol is logging on with CMD 198*6.

Command 05 disables the reporting of any selected items to the local printer, to the remote serial printer and to the Host PC if the controller is networked.

Use the optional argument (1/0) to enable or disable the specified reporting mode. If this argument is not used, disabled (0) is assumed except for 05 * 8.

Note: Most users disable Relay State Changes.

Examples:

```
START 05 * 1 #
```

Disables Reporting Of Relay State Changes

```
START 05 * 2 #
```

Disables Reporting Of Internal Events

```
START 05 * 3 * 1 #
```

Enables Reporting Of External Events

```
START 05 * 8 * 0 #
```

Disables reporting of all Changes

Default:

05*1*1 - Enable Relay State Changes [Vn. 6.6]
05*2*1 - Enable Internal Events
05*3*1 - Enable External Events
05*4*1 - Enable Transactions
05*5*1 - Enable Time Zone State Changes
05*6*1 - Enable Time Zone Relay Control State Changes
05*7*1 - Enable Time Zone Input Masking State Changes
05*9*0 - Disable Input State Change Reporting
05*10*0 - No MOMENTUM-compatible SCRAMBLE*NET Protocol
05*11*0 - No V7.0-compatible SCRAMBLE*NET Protocol

Related CMDs:

CMD 88*23 – Print Reporting Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Reporting and Printing Setups

CMD 06 – Disable printing of grants on selected doors
CMD 105, 106 – Disable Device or Disable Reports During Time Zone
CMD 107, 90*2#/97*1 – Daily Report Printing On/Off
CMD 109 – Invalid Code/ID Reporting Mode

CMD 06: DISABLE REPORT OF GRANTS ON SELECTED DOORS

Syntax: `START 06 * N * DOORS #` (Version 6.6 and earlier)

`START 06 * 1 * DOORS(Access) * DOORS(RQE) #` (Version 7)

Variables: N

1 Access
2 RQE

Description:

CMD 06 disables the reporting of granted access by door. The reporting of granted RQEs may also be selectively disabled by door.

Note: This command enables/disables reporting for all of the doors at once.

To re-enable reporting of grants, set the doors to 0 (none) for either or both functions or enter CMD 05 * 8 #.

*Note: Command 06 disables the reporting of grants to the local printer, the remote printer and to the SCRAMBLE*NET Manager PC if the System is networked.*

To disable grant reporting on doors 5-8 and enable grant reporting on doors 1-4, use 06*NN*5678#.

In Version 7.0, both grant-disable masks can be set with one command. In Version 7.0, the Access Grant reporting masks have also been moved to the readers/keypads – see CMD 403. The RQE reporting mask option sets the "log" time zone to 0 or 65 in the corresponding ACBs 65 through 72, see CMD 461. Using these commands will let you enable/disable a specific door or reader's grant reporting without affecting the other doors/readers.

Examples:

```
START 06 * 1 * 1 #
```

Disable Reporting Of Granted Access On Door 1

```
START 06 * 2 * 1234 #
```

Disable Reporting Of RQE Grants On Doors 1 To 4

```
START 06 * 1 * 1234 * 5678 #
```

Disable Reporting of Granted Access on Doors 1-4, and RQE Grants on Doors 5-8. [Vn. 7.0]

Related CMDs:

CMD 88*23 – Print Reporting Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Reporting and Printing Setups

CMD 05 – Reporting Modes
CMD 105, 106 – Disable Device or Disable Reports During Time Zone
CMD 109 – Invalid Code/ID Reporting Mode. Command 06 disables the reporting of Grants to the local printer, the remote printer and to the Host PC, if the controller is networked.

CMD 07: CHANGE DURESS DIGIT

Syntax: `START 07 * Duress Digit #`

Description:

A Duress Alarm is generated whenever an authorized Code is used along with its duress digit if the Duress Alarm Mode is set to on. The default duress digit is set to 9; however, any digit, 1-9, can be added to any or all of the user codes in the system when they are either manually or automatically generated for the first time, if CMD 09 is set to ON (the default setting is OFF).

Determine whether the duress feature will be needed so that all Codes have duress digits when they are initially added to the System.

Different duress digits may be assigned to individual Users or groups of Users by changing the duress digit before adding a new User or generating a group of Users.

To add or change duress digits to existing Codes, see CMD 14.

Example:

```
START 07 * 3 #
```

Change Duress Digit to 3

Default:

9

Related CMDs:

CMD 88*2 – Print System Information

CMD 188*4 – Print Setup Changes for Reporting and Duress

CMD 08 – Change Duress Alarm Mode
CMD 09 – Generate Codes With Duress Digit
CMD 14 – Add or Change Duress Digit for User or Range of Users

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 313, 314, 315, 320-322 – Add Users
CMD 18 – Change Keypad Code Length for Auto-Generation

CMD 08: CHANGE DURESS ALARM MODE

Syntax: `START 08 * N #`

Variables: N

0 OFF (disable)
1 ON (enable)

Description:

The feature is turned OFF on system start-up so that no reporting occurs. This means that even though duress digits have been assigned, they do not work unless the Duress Alarm Mode is enabled.

A Duress Alarm is reported as a User Under Duress on the printer and trips the Duress Alarm Relay.

Example:

```
START 08 * 1 #
```

Change Duress Mode to ON

Default:

OFF

Related CMDs:

CMD 88*2 – Print System Information

CMD 188*4 – Print Setup Changes for Reporting and Duress

Duress Setups

CMD 07 – Change Duress Digit
CMD 09 – Generate Codes With Duress Digit
CMD 14 – Add or Change Duress Digit for User or Range of Users

Alarm Setups

CMD 261 – Define Alarm Actions

CMD 09: GENERATE ALL CODES WITH DURESS DIGIT

Syntax: `START 09 * N #`

Variables: N

0 NO (disable)
1 YES (enable)

Description:

Generate Codes with duress digits must be set to ON for Users to have duress capability. Any digit, 1-9, may be added to any or all of the User Codes in the System when they are either manually or automatically generated for the first time. It is important to decide if the Duress feature will ever be desired so that all Codes have duress digits initially assigned.

To add or change duress digits to existing Codes, see CMD 14.

Example:

```
START 09 * 1 #
```

Generate All Codes With Duress Digit

Default:

NO

Related CMDs:

CMD 88*2 – Print System Information

CMD 188*4 – Print Setup Changes for Reporting and Duress

Duress Setups

CMD 07 – Change Duress Digit
CMD 08 – Change Duress Alarm Mode
CMD 14 – Add or Change Duress Digit for User or Range of Users

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 313, 314, 315, 320-322 – Add Users

CMD 10: ADD KEYPAD ACCESS USER (IDF 1)

Syntax: `START 10 * User Number * Code * Access Zone#`

Description:

An Access Code momentarily unlocks a door. The door unlock time is set with CMD 80 and can be set from 1 second up to 8,100 seconds (2 hours and 15 minutes). If the door time is set to 0 (zero), Access Codes will cause the relay to toggle on and off on successive code entries.

Each User is assigned a user number from 1 - 999 (1-4000 or 1-16,000 with an optional MEB/CE Code Expansion Board Installed) for reference during programming. When the System printer prints each code transaction it prints the time, date, User Number, Reader and door numbers and the result of the code entry, granted or denied.

Each Access User is assigned a unique 3- to 15-digit code or is issued a card. The Access Code is the combination of numbers the user actually enters on the ScramblePad keypad to unlock the door. The card is used in a MATCH Card Reader to unlock a door. Several related codes or cards may be assigned to the same person to perform other command and control functions.

Note: If Duress Codes are used, Command 09, Generate Codes with Duress Digit, must be enabled before any Codes are added to the controller's memory.

Each Access User must be assigned to an Access Zone. Access Zones determine the access authority of a group of Users. An Access Zone is defined with a Time Zone and a set of valid doors. (See CMDs 17, 24 and 117.)

Access Zone 65 authorizes access "Always to All Doors."

Access Zone 0 (Zero) restricts access, "locks out," all Users in that Zone, to "Never, No Doors."

Examples:

```
START 10 * 124 * 14291 * 65 #
```

Add User 124 with Code 14291 To Access Zone 65

Default:

None

Related CMDs:

CMD 32 – Print First Available User Number

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 15, 19-22, 40-42, 44, 310-315, 320-322 – Add Users

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

CMD 16, 23 – Delete Any User, Range of Users

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

CMD 14 – Add or Change Duress Digit For User or Range Of Users

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)

CMD 204 – Define Master Access Zone (66-127)

CMD 11: REDEFINE KEYPAD ACCESS USER (IDF 1 & 6)

Syntax: `START 11 * User Number * Code * Access Zone #`

Description:

Redefine enables the Programmer to change any or all of an existing Access User's parameters.

Each field must have data entered when this Command is used. In order to lock out an individual User without changing any other information associated with that User, use this Command and set the Access Zone to 0 (Zero) or use Command 12.

Examples:

```
START 11 * 124 * 14291 * 0 #
```

Redefine User 124 To Access Zone 0 - No Access

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10 – Add Keypad Access User (IDF 1)

CMD 314 – Add Access User with Code & Card (IDF 6)

Changing and Deleting Users

CMD 12, 13, 325 – Change User(s) Codes, Zones, and/or Functions

CMD 16, 23 – Delete Any User, Range of Users

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)

CMD 204 – Define Master Access Zone (66-127)

CMD 12: CHANGE ANY USER ACCESS OR CONTROL ZONE (All IDFs)

Syntax: `START 12 * User Number * Zone (AZ or CZ) #`

Description:

Change Any User Access Zone or Control Zone allows an Operator to change a User's Access or Control Authority.

This Command is especially useful for disabling or locking out any User by changing their Access Zone to 0 (Zero). This Command is also frequently used to change new and unissued Users, kept in the controller's memory, to a specified Access Zone upon issuance to a new employee. In systems with Dual Technology Readers and Multiple ID Users, Command 12 is used to disable the Keypad Code ID Only from working at the Dual Technology Door.

Examples:

```
START 12 * 45 * 0 #
```

Change User 45 To Access Zone 0 (No Access)

```
START 12 * 663 * 1 #
```

Change User 663 To Access Zone 1

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 313-315, 320-322 – Add Users

Changing and Deleting Users

CMD 11, 13, 325 – Change User(s) Codes, Zones, and/or Functions

CMD 16, 23 – Delete Any User, Range of Users

CMD 13: CHANGE KEYPAD USER CODE (IDF 1 & 6)

Syntax: `START 13 * User Number * Code [* Duress] #`

Description:

Change any User Code allows an Operator to change a User's Keypad Code whenever required.

If duress is enabled, use this feature to change a user's keycode and duress digit. If you specify a duress digit of 0, it will disable the duress option for that user.

Note: If the system's duress options were changed since this user was added, you'll need to specify the desired duress digit; otherwise it will change it for you.

If a user has been defined

- ❏ without Duress, then later Duress is enabled and a duress digit is set
- ❏ with one duress digit and the system duress digit is later changed

then changing that user's keypad code will also automatically update their duress digit to the current setting.

Examples:

```
START 13 * 6 * 298165 #
```

Change Code for User 6 to 298165

```
START 13 * 200 * 201 * 1 #
```

Change Code for User 200 to 201 and specify 1 as the extra duress digit for that user

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 313-315, 320-322 – Add Users

Changing and Deleting Users

CMD 11, 12, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

CMD 14 – Add or Change Duress Digit for User or Range of Users

CMD 14: ADD OR CHANGE DURESS DIGIT FOR USER OR RANGE OF USERS (IDF 1 & 6)

Syntax: `START 14 * Duress Digit * User #`

`START 14 * Duress Digit * First User * Last User #`

Description:

This command enables the operator to add or change the duress digit, or remove it (if you specify 0), for the designated user or users. If changing a user's duress digit would create a code conflict, the user's keycode and duress digit are left unchanged and a report is generated describing the conflict.

This command only affects those IDF 1 & 6 users affected by CMD 13.

Examples:

```
START 14 * 1 * 298165 #
```

Add or Change the Duress Digit for User 298165 to 1.

```
START 14 * 2 * 201 * 205 #
```

Add or Change the Duress Digit for users 201 through 205 to 2.

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 313-315, 320-322 – Add Users

CMD 13 – Change Keypad User Code (IDF 1 & 6)

Changing and Deleting Users

CMD 11, 12, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

CMD 15: ADD KEYPAD UNLOCK / RELOCK USER (IDF 1)

Syntax: `START 15 * N * User Number * Code * Access Zone #`

Variables: N

1 Unlock
2 Relock
3 Extended Access
4 Visitor Access
5 Escort Access

Description:

An Unlock Code unlocks a door until manually relocked by a Relock Code or automatically relocked at the end of a specified Time Zone (Command 82). Unlock and Relock User Codes require separate User numbers and Codes from each other.

Consider assigning a Relock Code to Access Zone 65 to prevent time restrictions on relocking. In some cases a “common” Relock Code is posted at the door so that any User finding a Door unlocked can immediately relock it.

Extended Access is similar to ordinary access (see CMD 10), with an added feature: if PIN*NNN# is used for access instead of just PIN#, the relay fires for NNN extra minutes, or the door can be held open NNN extra minutes, or a combination of both. The maximum value of NNN is set per door, to a value of 0-1440.

Extended Access and Relay Priorities: In Hirsch's Relay Priority scheme, Extended Access falls between Access and Unlock. The "Clear Relay" function will clear an Extended Access (see CMD 082 for Clear Relay At End Of Time Zone; CMD 304 for Master Control Zone option 2, Clear Relays). If Extended Access is in progress, a regular "Access" will have no visible effect, because the relay is already energized. "Relock" has no effect on the Extended Access.

Extended Access and Auto-Relock: "Auto-Relock On Open" and "Auto-Relock Off" will have no effect on Extended Access; in this instance, Extended Access behaves more like Unlock, i.e. you can open and shut the door as many times as you like. "Auto-Relock On Close" will clear Extended Access; in this instance, Extended Access behaves more like Access.

Visitor Access assigns a person visitor status, indicating the access zone and code the visitor can use. This enables a visitor to enter a restricted area when accompanied by an enrolled escort. The Visitor must be enrolled using this command for a specific access zone. Under the default Visitor/Escort Rule #1, an escort must enter his access code first, then specify the number of visitors that are accompanying him/her before the Visitor can enter the assigned code. Only the number of visitors specified by the escort at the keypad/reader are allowed access.

Escort Access assigns a user escort status, meaning that the escort can enter a restricted area with a specified number of visitors. The escort must enter the PIN specified here followed by the number of visitors he/she is escorting, in this form:

```
START [Escort Code] * [number of visitors] #
```

For example, START 1234 * 4 # indicates that the escort has four visitors to enter. Only the number of visitors specified can enter the area, beyond which access is denied.

Examples:

```
START 15 * 1 * 400 * 82341 * 4 #
```

Add Unlock User 400 With Code 82341 With Access Zone 4

```
START 15 * 2 * 401 * 82342 * 65 #
```

Add Relock User 401 With Code 82342 With Access Zone 65

```
START 15 * 4 * 331 * 331 * 2 #
START 15 * 4 * 332 * 332 * 2 #
START 15 * 4 * 333 * 333 * 2 #
```

Adds three Visitors, identified as Users 331 through 333, that can enter Access Zone 2 using PINs 331 – 333

```
START 15 * 5 * 221 * 221 * 1 #
START 15 * 5 * 222 * 222 * 1 #
```

Adds two Escorts, identified as Users 221 and 222, that can enter Access Zone 1 using PINs 221 – 222

Default:

None

Related CMDs:

- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 88*17 – Print Detailed Relay Status Only

Adding Users

CMD 10, 19-22, 40-42, 44, 310-315, 320-322 – Add Users

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

Controlling Relays

CMD 82 – Time Zone Control of Relay

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)

CMD 204 – Define Master Access Zone (66-127)

Defining Readers

CMD03 – Change Selected Keypad/MATCH Functions

CMD 16: DELETE ANY USER (All IDFs)

Syntax: `START 16 * User Number #`

Description:

Delete any User erases the User record from the database and makes both the User Number and Code available for reuse.

To track the use of a Code of a former employee do not Delete it with this Command. Use Command 12 to change its Access Zone to 0. This will produce a printed record of any access attempts by the disabled User's Code.

Example:

```
START 16 * 124 #
```

Delete User 124 From System Memory

Default:

None

Related CMDs:

 CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 310-315, 320-322 – Add Users

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

CMD 23 – Delete Range of Users

CMD 17: DEFINE STANDARD ACCESS ZONE (1-64)

Syntax: `START 17 * Standard Access Zone * Time Zone * Doors [* Doors] #`

Variables: **Doors**
Doors/Readers. Associates specified Doors (and corresponding Readers) where, for example, 125 means Doors 1, 2, and 5 which assumes the association of corresponding readers 1, 2, 5, 9, 10, and 13.

Description:

Access Zones are one of the most important features defined in a DIGI*TRAC controller. Access Zones serve as a method to organize users controlled by your controller into groups who share the same access authority. Furthermore, Access Zones enable the rapid change of access authority for entire groups of users with a single programming command.

Access Zones answer these three questions: Who, When, Where.

Who	Every Access User is assigned to an Access Zone. All Users within that Zone have the same access authority.
When	Each Access Zone is assigned one Time Zone. A Time Zone controls the starting time, ending time and days of the week, including Holidays, on which access will be granted to members of the specified Access Zone.
Where	Each Access Zone is assigned a set of Doors. This determines through which Doors members of the specified Access Zone can gain access.

CMD 17 defines Standard Access Zones *for one time zone and all doors*. Define Standard Access Zone requires the selection of a time zone and a set of doors assigned to one of 64 available access zones. Access Zone 0 is preassigned as “Never - No Doors” and Access Zone 65 is preassigned as “Always - All Doors”.

Note: AZ 0 and AZ 65 cannot be changed or deleted.

Special Applications:

Expansion Alarm Inputs can be assigned to a Standard Access Zone. This enables these Alarm Inputs to be accessed, or masked, by the same Access Code issued to a User to access a door. It also enables assignment of Individual ScramblePad Keypads to Alarm Inputs for discreet alarm zone masking by alarm zone control. Alarm Control Codes, under Command 42, enable any alarm input to be masked from any ScramblePad Keypad.

Command 201 will be phased out in Version 7.0.

Note: Standard Access Zones 1-64 are undefined in a new System. (In other words, "Never - No Doors" until they've been defined otherwise.)

These Zones may be defined for use in establishing the "Who, When and Where" controls for proper access management.

Note: CMD 17 automatically assigns the same time zone to each door of a standard access zone. CMD 24 requires the programmer to specify a time zone for each door of an access zone when door-by-door time zone control is required. CMD 117 allows a time zone to be set for a specified door without affecting the time zone of any other door.

Note: Master Access Zones are available consisting of up to 8 Standard Access Zones combined and assigned to a group of users. This enables enhanced access control capabilities over large multi-building sites or in special secure environments with special access programs and areas such as cleared conference rooms.

In Version 6.6.0, Access Zones are arranged individually by reader, using the second ‘Doors’ variable to specify a different set of doors corresponding to Readers 9-16. CMD 124 has been added to facilitate this.

Example:

```
START 17 * 1 * 1 * 125 #
```

Define Standard Access Zone 1 as Time Zone 1 and Doors 1, 2, and 5 (including Readers 1, 2, 5, 9, 10, and 13.

```
START 17 * 2 * 3 * 45 * 6
```

Define Standard Access Zone 2 as Time Zone 3 for Readers 4, 5, and 14.

```
START 17 * 7 * 8 * 0 * 78
```

Define Standard Access Zone 7 as Time Zone 8 for Readers 15 and 16 only.

Default:

There are two pre-defined Access Zones in the system:

Access Zone 0 (zero)	**"Never - No Doors"** This Zone may be used to maintain unissued IDs in the System for immediate assignment whenever required. With an Access Zone of 0, they are not able to be used. Whenever an ID is to be issued, all that is necessary is to use CMD 12 to change this User from AZ 0 to a defined Access Zones with the required access authority. Access Zone 0 may also be used to "lockout" a User.
Access Zone 65	**"Always - All Doors" and "All Readers"** This Zone is useful to rapidly assign to any Access User who has the authority to enter any area, any time of any day. The only disadvantage of using Access Zone 65 is that its times, days and doors are not changeable.

Related CMDs:

CMD 88*5 – Print Standard Access Zone Setups

CMD 188*5 – Print Setup Changes for Standard Access Zones

Access Zone Setups

CMD 24 – Define Standard Access Zone (1-64), 1 Time Zone Per Door
CMD 117 – Define Standard Access Zone (1-64), 1 Time Zone, Specified Doors
CMD 124 – Define Standard Access Zone, Readers 1-8 or 9-16 only
CMD 204 – Define Master Access Zone (66-127)
CMD 249, 349 – Tag/Alert Access Zone

Time Zone Setups

CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones

Add/Change/Print Users

CMD 33 - Print Users Given Access Zone
CMD 10 - Add Access User
CMD 11 - Redefine Access User
CMD 12 - Change Any User Access Or Control Zone
CMD 15 - Add Unlock/Relock User
CMD 19 - Auto-Add Access User
CMD 20 - Auto-Add Access User
CMD 21 - Auto-Add Multiple Access Users
CMD 22 - Auto-Add Multiple Access Users

CMDs 18-22: AUTO-ADD KEYPAD ACCESS USER(s) (IDF 1)

DIGI*TRAC has the capability to automatically add a single access user and code or to add multiple access users and codes.

This feature is most often used on system start up when there are no users or codes in the controller memory. The controller has a true random number generator which will create a unique keypad code for an unused user number or range of numbers. It may also be used as a convenient and secure way to add a single new user to the system whenever required.

CMD 18 is used to establish the code length for any auto-generated codes (CMDs 19, 21, 22). The longer the code the greater the security. Seven-digit codes are the factory default setting and are recommended and are easily memorized because of their similarity to phone numbers.

Whenever an Operator Auto-Adds codes, DIGI*TRAC will print them as they are added. This list must be audited before the codes are issued for use. Some codes that are randomly generated may not be acceptable for use, such as 1234567 or 1111111. These are valid randomly generated codes but are insecure. They can be edited with CMD 13 or deleted and re-auto-generated. It is also possible for independent Controllers to auto-generate identical codes. The shorter the code the greater the chance of having duplicate codes. Longer codes are recommended.

CMD 18: CHANGE KEYPAD CODE LENGTH FOR AUTO-GENERATION

Syntax:

```
START 18 * Length # (Version 6.6 and earlier)
START 18 * Length * [Card Length] #  (Version 7)
```

Variables:

Length

Allowed length for the auto-generation of keypad (PIN) codes.

Card Length

This option is available in Version 7.0 as a convenient method of formatting user code record printouts, using CMD 36 etc. Acceptable values are 8, 10, 12, 14, 16.

Description:

Keypad codes can be auto-generated in any uniform length from 3-15 digits long and will be printed with Codes showing.

Note: Secure these printouts.

The length may be changed for each auto-generation of keypad codes.

The code length defined by this command will be used as the default length when the program attempts to deduce an IDF 4 user's original keycode (where IDF 4 = card code & dual code). The code length default value is factory set to 7 digits and the card length is 8 digits.

Note: This command is used with all auto-generate commands including CMDs 19, 21, and 22.

The 'Card Length' option is available as a convenience for formatting user code record printouts. (CMD 36, etc.) Valid values are 8, 10, 12, 14, 16.

Example:

```
START 18 * 8 #
```

Auto-Generate Codes 8 Digits Long

```
START 18 * 12 * 10
```

Set the PIN length to 12 digits and the card length to 10 digits

Default:

Code Length = 7 digits

Card Length = 8 digits

Related CMDs:

- CMD 88*2 – Print System Information
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 188*4 – Print Setup Changes for Reporting and Duress

Adding Users

CMD 19 – Auto-Add Access User, Random Code
CMD 21 – Auto-Add Multiple Access Users, Random Codes, Next Available User Numbers
CMD 22 – Auto-Add Multiple Access Users, Random Codes, Specified User Numbers

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

CMD 19: ADD ACCESS USER - KEYPAD CODE ID ONLY (Define User Number and Auto-Gen Code)

Syntax: `START 19 * User Number * Access Zone #`

Description:

The Programmer may add a specific User and have the Controller auto-generate a unique Keypad Code for that User.

Example:

```
START 19 * 291 * 3 #
```

Add User 291 To Access Zone 3 and Auto-Generate Code

Default:

None

Related CMDs:

- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 20-22, 40-42, 44, 310-315, 320-322 – Add Users
CMD 18 – Change Keypad Code Length for Auto-Generation
CMD 20 – Auto-Add Access Code, Next Available User Number
CMD 21-22 – Auto-Add Keypad Access Users (IDF 1)
CMD 21 – Auto-Add Multiple Access Users, Random Codes, Next Available User Numbers
CMD 22 – Auto-Add Multiple Access Users, Random Codes, Specified User Numbers

Changing Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 20: ADD ACCESS USER - KEYPAD CODE ID ONLY (Auto-User Number, Specify Code)

Syntax: `START 20 * Code * Access Zone #`

Description:

The controller will select the next available User Number for a Programmer specified Code.

The Programmer may check to see if a selected Code is available or has already been issued with Command 37.

Example:

```
START 20 * 55712 * 1 #
```

Add User With Code 55712 To AZ 1 And Auto-Add User Number

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

CMD 37 – Print User given Code

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 310-315, 320-322 – Add Users
CMD 18-22 – Auto-Add Keypad Access Users (IDF 1)
CMD 19 – Auto-Add Access User, Random Code
CMD 21 – Auto-Add Multiple Access Users, Random Codes, Next Available User Numbers

Changing Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 21: ADD ACCESS USERS - KEYPAD CODE ID ONLY (Auto-Add Users & Codes)

Syntax: `START 21 * Number of Users * Access Zone #`

Description:

Multiple users may be added by specifying how many Users are desired.

The controller will skip over any existing Users as it auto-adds new users.

Example:

```
START 21 * 100 * 1 #
```

Add 100 Users To AZ 1 And Auto-Add User Number

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 310-315, 320-322 – Add Users
CMD 18 – Change Keypad Code Length for Auto-Generation
CMD 19 – Auto-Add Access User, Random Code
CMD 20 – Auto-Add Access Code, Next Available User Number
CMD 22 – Auto-Add Multiple Access Users, Random Codes, Specified User Numbers

Changing Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 22: ADD ACCESS USERS - KEYPAD CODE ID ONLY (Auto-Add Users & Codes From Specified User Number)

Syntax: `START 22 * Starting User Number * Number of Users * Access Zone #`

Description:

Multiple users may be added by specifying the starting user number and the number of users.

The controller will skip over any existing users as it auto-adds new users.

Example:

```
START 22 * 500 * 25 * 1 #
```

Add 25 Users To AZ 1 Auto-Add User Numbers & Codes Starting At User Number 500

Default:

None

Related CMDs:

 CMD 32 – Print First Available User Number

 CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-21, 40-42, 44, 310-315, 320-322 – Add Users
CMD 18 – Change Keypad Code Length for Auto-Generation
CMD 19 – Auto-Add Access User, Random Code
CMD 20 – Auto-Add Access Code, Next Available User Number
CMD 21 – Auto-Add Multiple Access Users, Random Codes, Next Available User Numbers

Changing Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

Duress Setups

CMD 07, 09 – Change Duress Digit, Generate Codes with Duress Digit

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 23: DELETE RANGE OF USERS (All IDFs)

Syntax: `START 23 * Starting User Number * Ending User Number #`

Description:

Multiple users may be deleted by specifying the range of user numbers to be deleted.

All users within the specified range will be deleted from the controller memory making these user records available for reuse.

Example:

```
START 23 * 25 * 50 #
```

Delete User 25 Through User 50

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16 – Delete Any User.

CMD 24: DEFINE STANDARD ACCESS ZONE 1-64 (One Time Zone Per Door/Reader)

Syntax:

```
START 24 * Access Zone * Time Zone For Door 1 *
                         Time Zone For Door 2 *
                         Time Zone For Door 3 *
                         Time Zone For Door 4 *
                         Time Zone For Door 5 *
                         Time Zone For Door 6 *
                         Time Zone For Door 7 *
                         Time Zone For Door 8 #
```

Description:

Use this command to define a Standard Access Zone in which only one time zone is assigned per door. This enables access by time zone on a door-by-door basis. Each door in a Standard Access Zone can be restricted by any of the available time zones. For example, entering Time Zone 0 for a door restricts all access at that door.

*Note: In this command it is not necessary to define the Reader/Door number. DIGI*TRAC knows that the first delimiter after the Access Zone number is Reader/Door 1, the next delimiter is Reader/Door 2, and so on.*

This command enables you to define time zones for Doors 1-8. In other words, the same TZs are assigned to both sides of the door: this means both readers 9-16 and readers 1-8 are defined.

Each door must have a time zone value assigned. When a door is not authorized in an access zone, enter Time Zone 0 in that door field. Command 117 allows one or more time zones to be changed for a specified door without affecting the time zone setting of any other door(s).

Refer to Command 17 for a convenient method to add Standard Access Zones with 1 Time Zone For All Doors.

CMD 24 defines readers 1-8 and readers 9-16 enabling you to use the same set of eight time zones, if only eight are specified.

Note: For the M2 Controller, only 4 door times will be accepted.

Example:

```
START 24*10*65*0*1*5*0*0*0*0#
```

Define Standard Access Zone 10 To Time Zone 65 On Door 1, TZ 0 On Door 2 5 6 7 & 8, TZ 1 On Door 3, TZ 5 On Door 4. As you can see from this example, DIGI*TRAC assumes that the first delimiter after the Access Zone number is Reader/Door 1, the next delimiter is Reader/Door 2, and so on.

Default:

AZ0 = Never – No Doors

AZ65 = Always – All Doors

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*5 – Print Standard Access Zone Setups
- CMD 188*5 – Print Setup Changes for Standard Access Zones

Access Zone Setups

CMD 17 – Define Standard Access Zone (1-64), 1 Time Zone, Selected Doors
CMD 117 – Define Standard Access Zone (1-64), 1 Time Zone, Specified Doors
CMD 124 - Define Standard Access Zone, 1 Time Zone Per Reader
CMD 204 – Define Master Access Zone (66-127)

Time Zone Setups

CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones

Holiday Setups

CMD 57 – Define Holiday

CMD 30: PRINT USER WITHOUT CODE

Syntax: `START 30 * User Number #`

Description:

Use this command to print a single user record stored in a DIGI*TRAC controller's user database by entering the user number.

Example:

```
START 30 * 12 #
```

Print User Record 12 Without the Code Showing

Default:

None

Related CMDs:

- CMD 31, 33, 34 – Print Users, Users by Zone, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 – Print User given Code

CMD 31: PRINT USERS WITHOUT CODE

Syntax: `START 31 * Starting User Number * Ending User Number #`

Description:

Use this command to print a list of registered users by entering the starting user number and the ending user number.

Example:

```
START 31 * 10 * 15 #
```

Print User Records 10 Through 15 Without Codes Showing

Default:

None

Related CMDs:

- CMD 30, 33, 34 – Print User, Users by Zone, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 – Print User given Code

CMD 32: PRINT FIRST AVAILABLE USER - FROM SPECIFIED USER NUMBER

Syntax: `START 32 * Starting User Number #`

Description:

Print the first available user above the specified user number. This helps the operator locate the next available user number above the user number specified.

Example:

```
START 32 * 500 #
```

Print First Available User Number 500 or Above

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 – Print User given Code

Adding Users

CMD 10, 15, 19-22, 40-42, 44, 310-315, 320-322 – Add Users

CMD 33: PRINT USERS GIVEN ACCESS ZONE OR CONTROL ZONE

Syntax: `START 33 * N * Zone Number #`

Variables: N

1 Access Zone (0 - 127)
2 Control Zone (0 - 255)

Description:

Print users given access zone or control zone allows the listing of all users assigned to the specified Zone.

If Access Zone is selected (N = 1), the Zone Number can be in the range 0 - 127. As you can see, users of master access zones can be printed as well as users of standard access zones.

When a control zone is selected (N = 2), the Zone Number can be in the range 0 - 255. This means the operator can print users associated with master control zones (192 - 255) as well as standard control zones.

*Note: When using S*NAP, the codes will show when this command is executed if the setup for S*NAP has codes set to 'Reveal.'*

Example:

```
START 33 * 1 * 65 #
```

Print all users in Access Zone 65

```
START 33 * 2 * 35 #
```

Print all users in Control Zone 35

```
START 33 * 2 * 216 #
```

Print all users in Master Control Zone 216

Default:

None

Related CMDs:

- CMD 30, 31, 34 – Print User, Users, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 – Print User given Code

Changing and Deleting Users
CMD 16, 23 – Delete Any User, Range of Users
Access Zone Setups
CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)
Control Zone Setups
CMD 45, 304 – Define Standard, Master Control Zone

CMD 34: PRINT FAMILIES OF USERS WITHOUT CODE

Syntax: `START 34 * NN * Starting User Number * Ending User Number #`

Variables: NN

1	All Users
2	Momentary Access
3	Unlock / Relock
4	All Access
5	Control
6	Lock Down / Lock Open
7	Alarm Mask / Unmask / Cancel / Entry & Exit Delays / Deadman
8	Passwords
9	Users Inside
10	Tagged Users
11	Alerted Users

Description:

Families of users may be printed by selecting the desired group from the list. Only users of that type will be printed in the report.

User Family Number 9, Users Inside, will print a list of those users currently within the passback perimeter. This requires that the controller be using the passback feature with ScramblePad/MATCH Readers defined as entry and exit using Command 03 or 403. If passback is not enabled, the controller will list users as UNK, Unknown, passback status.

Examples:

```
START 34 * 2 * 0 * 999 #
```

Print All Momentary Access Users

```
START 34 * 9 * 0 * 999 #
```

Print All Users Currently Inside Passback Perimeter

Default:

None

Related CMDs:

- CMD 30, 31, 33 – Print User, Users, or Users by Zone, Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 – Print User given Code

Changing and Deleting Users

CMD 16, 23 – Delete Any User, Range of Users

CMD 35: PRINT USER WITH CODE

Syntax: `START 35 * User Number #`

Description:

Use this command to print a user record *with the code showing* from the DIGI*TRAC controller's user database by entering the User Number.

*Note: For Codes to be displayed, the Setup for S*NAP must have Codes set to 'Reveal.'*

Note: Secure these printouts since they show the user's entry/exit code.

Example:

```
START 35 * 468 #
```

Print User Record 468 With Code Showing

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 36, 38, 330 – Print Users, or Family of Users with Codes
- CMD 37 – Print User given Code

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

CMD 36: PRINT USERS WITH CODE

Syntax: `START 36 * Starting User Number * Ending User Number #`

Description:

Use this command to print a sequence of users. This sequence is defined by entering the starting user number and the ending user number. Each user is printed *with their code showing*.

*Note: For Codes to be displayed, the Setup for S*NAP must have Codes set to 'Reveal.'*

Secure printouts created with CMD 36 since they show the user's entry/exit code.

Note: In SAM, IDF 2 – 7 users are not displayed correctly in the Diagnostic window when CMD 36 is used.

Example:

```
START 36 * 200 * 225 #
```

Print User Records 200 Through 225 With Codes Showing

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 38, 330 – Print User or Family of Users with Codes
- CMD 37 – Print User given Code

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

CMD 37: PRINT USER GIVEN CODE

Syntax: `START 37 * Code #` (Only works for IDFs 1, 5, 6, 7)
`START 37 * Code * Card #` (Only works for IDFs 3–7, Version 6.6 and earlier)
`START 37 * 0 * Card/Code #` (Only works for IDFs 2–7, Version 7)

Description:

Use this command to determine the user number for users who only knows their keypad codes, not their user numbers.

In V6.6 or later, this command can also be used to look up dual users by specifying both card and code. This only works for IDFs 3 - 7.

In V7.0 or later, if a Code or Card of '0' (one digit) is specified, the controller will look for a following argument indicating the card-only or code-only user number. This feature is only available for IDFs 2 - 7.

*Note: For codes to be displayed, the setup for S*NAP must have codes set to 'Reveal.'*

Example:

```
START 37 * 27256 #
```

Print User Record For Code 27256

```
START 37 * 0 * 0567 #
```

Print User Record For Card 0567

```
START 37 * 27256 * 0567#
```

Print User Record For Dual User who possesses both code 27256 and card 0567

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

CMD 38: PRINT FAMILIES OF USERS WITH CODE

Syntax: `START 38 * N * Starting User Number * Ending User Number #`

Variables: N (family)

1 All Users
2 Momentary Access
3 Unlock / Relock
4 All Access
5 Control
6 Lock Down / Lock Open
7 Alarm Mask / Unmask / Cancel / Entry & Exit Delays / Deadman
8 Passwords
9 All Users, Sorted By Code (before V7.0)

Description:

Families of users can be printed by selecting the desired group from the list. Only users of the specified type will be printed in the report *with codes showing* in the report's Code field.

For versions prior to 7.0, N = 9 (All, Sorted By Code) will list all users by codes regardless of the range specified. For Version 7.0 and later, the switch N = 9 is no longer supported.

Note: Secure these printouts since they show the user's entry/exit code.

For Codes to be displayed, the setup for S*NAP must have codes set to "Reveal."

Examples:

```
START 38 * 5 * 0 * 999 #
```

Print All Control Users With Codes Showing

```
START 38 * 8 * 0 * 999 #
```

Print All Password Operators With Codes Showing

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 35, 36, 330 – Print User or Users with Codes
- CMD 37 – Print User given Code

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

CMD 40: ADD KEYPAD RELAY CONTROL USER (IDF 1)

Syntax: `START 40 * N * User Number * Code * Control Zone #`

Variables: N

1 Control Trigger
2 Force ON
3 Force ON Release
4 Force OFF
5 Force OFF Release

Description:

Control codes can operate any combination of relays simultaneously from any ScramblePad/MATCH reader as defined by a control zone. They can override all types of access codes and override each lower priority level control code. Relays can be set to trigger their control time momentarily from 1-8100 seconds, or toggled ON and OFF on consecutive trigger code entries (see CMD 81). To add a card relay control user use CMD 325 to convert a keypad relay control user to a card relay control user.

Relays can be Forced ON by a code and remain on until released by a corresponding Force ON release code. Relays can be Forced OFF (disabled) by a code and remain disabled until released by a corresponding Force OFF Release code.

Note: Force OFF disables the Request To Exit function.

Consider assigning all release type control codes to a control zone with a time zone of 65, "Always". This will prevent any unintentional time restrictions from keeping an authorized user from releasing a control condition that requires releasing.

Examples:

```
START 40 * 2 * 650 * 73451 * 1 #
```

Add Force ON Code 73451 To User 650 And Control Zone 1

```
START 40 * 3 * 651 * 73452 * 2 #
```

Add Force ON Release Code 73452 To User 651 And Control Zone 2

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 88*17 – Print Detailed Relay Status Only
- CMD 88*19 – Print Detailed Expansion Relay Status Only

Adding Users

CMD 10, 15, 19-22, 41, 42, 44, 310-315, 320-322 – Add Users
CMD 41 – Add Keypad Top-Priority Relay Control User (IDF 1)

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

Relay Setups

CMD 81 – Change Control Time of Relay
CMD 82 – Time Zone Control of Relay
CMD 85 – Change Operation for Selected Relays
CMD 86 – Change Relay & Alarm Operating & Reporting Modes
CMD 87 – Relay Triggers Control Zone
CMD 281 – Change Control Delay for Relay

CMD 41: ADD KEYPAD TOP-PRIORITY RELAY CONTROL USER (IDF 1)

Syntax: `START 41 * N * User Number * Code * Standard Control Zone #`

Variables: N

1 Lock DOWN
2 Lock DOWN Release
3 Lock OPEN
4 Lock OPEN Release

Description:

Lock DOWN codes disable any relays in its control zone and prevent any lower priority codes from working or time zone initiated events from occurring. It will maintain the Lock Down condition until cleared by a Lock DOWN Release Code.

Note: Lock DOWN disables the Request To Exit function.

Lock OPEN Codes actuate any or all relays and maintain them actuated until released by a Lock OPEN Release Code.

Consider assigning all release type control codes to a control zone with a time zone of 65, "Always". This will prevent any unintentional time restrictions from keeping an authorized User from releasing a control condition that requires releasing.

Use CMD 325 to convert a card access code to a card top-priority relay control user.

Examples:

```
START 41 * 1 * 652 * 73453 * 1 #
```

Add Lock DOWN Code 73453 To User 652 And Control Zone 1

```
START 41 * 2 * 653 * 73454 * 2 #
```

Add Lock DOWN Release Code 73454 To User 653 And Control Zone 2

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 88*17 – Print Detailed Relay Status Only
- CMD 88*19 – Print Detailed Expansion Relay Status Only

Adding Users
CMD 10, 15, 19-22, 40-42, 44, 310-315, 320-322 – Add Users
CMD 40 – Add Keypad Control User (IDF 1)

Changing and Deleting Users
CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

Control Zone Setups
CMD 45, 304 – Define Standard, Master Control Zone

Relay Setups
CMD 81 – Change Control Time of Relay
CMD 82 – Time Zone Control of Relay
CMD 85 – Change Operation for Selected Relays
CMD 86 – Change Relay & Alarm Operating & Reporting Modes
CMD 87 – Relay Triggers Control Zone
CMD 281 – Change Control Delay for Relay

CMD 42: ADD KEYPAD ALARM CONTROL USER (IDF 1)

Syntax: `START 42 * NN * User Number * Code * Control Zone #`

Variables: NN

1 Momentary Single Mask
2 Mask
3 Unmask
4 Cancel Entry Delay
5 Start Exit Timer
6 Mask Alarm and Cancel Entry Delay
7 Start Exit Timer and Unmask
8 Pre-Arm Status
9 Conditional Unmask
10 Partial Unmask

Description:

A *Momentary Single Mask* code momentarily disables the reporting of a single alarm condition from any of the line module inputs as defined by the code's control zone. This means that when this user function is used, it will mask the specified line module input for a single alarm actuation only. If the masking timer is still active when the specified line module input is tripped for a second or more times, it will report as a new alarm on that input. When a momentary single mask is used on a door associated input and the auto-relock function of the door is off, the mask will last as long as the door unlock time, no matter how many times the door is opened and closed during the masked time. If the auto-relock function is on, the door can only be opened and closed once or a new alarm will occur.

An alarm *Mask* code turns off the reporting of all alarms from any of the line module inputs as defined by the code's control zone. Neither type of mask code prevents line trouble alarm reporting, such as shorts or open line conditions.

An alarm *Unmask* code restores the alarm reporting of any input(s) as defined by the code's control zone. Consider assigning unmask codes to a control zone with a time zone of 65 to prevent time restrictions on the unmasking of masked line module inputs. To add a card alarm control user use Command 325 to convert a keypad alarm control user to a card alarm control user.

A *Cancel Entry Timer* code is used to cancel the entry delay timer and prevent the reporting of an alarm. An Entry Delay Timer can be used to control access to secure areas where the ScramblePad is located within the area.

A *Start Exit Timer* enables exiting the same secure area without tripping an alarm.

Mask Alarm and Cancel Entry Timer is a convenient combined user function that can cancel an entry delay and mask all interior line module inputs for general building occupancy, or just mask specified Inputs for occupancy of a specific area only, while other areas remain armed.

Likewise, *Start Exit Timer and Unmask* combines the start exit timer function with the unmask function and is often used to re-secure an entire building or only a specified area.

Pre-Arm Status—also known as ‘Test If Secure’ or ‘Check Secure’—tests all available inputs within the specified control zone and reports whether they are inactive (secure) or active (unsecured). If all inputs are secure, the ScramblePad flashes its green LED once for an access grant and twice for a control. If there are unsecured inputs detected, ScramblePad flashes its red LED and beeps—one beep for each active input.

Conditional Unmask—also known as ‘Unmask If Secure’—unmasks/arms all inputs in the specific control zone, but only if all inputs have been previously detected as secure.

Partial Unmask—also known as 'Force Arm' or 'Arm Around'—unmasks all inputs in the specified control zone previously detected as secure. All unsecured inputs are left unarmed. When this condition is used, the ScramblePad flashes both the red and green LEDs, if some inputs are secure and other are not. Only the green LED flashes if all inputs are detected secure. For example, if the boss leaves the safe in his office open, you can arm what is 'armable' around it, knowing that the door to his office (containing the open safe) will be armed.

Note: The three new alarm types—pre-arm status, conditional unmask, and partial unmask—check the status of all alarm points specified in their governing SCZ even if those inputs are disabled. For this reason, don't include disabled alarm points in your SCZ.

Example:

```
START 42 * 1 * 301 * 3011 * 4 #
```

Add Momentary Alarm Mask Code 3011 To User 301 And Control Zone 4

Default:

None

Related CMDs:

CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 15, 19-22, 40, 41, 44, 310-315, 320-322 – Add Users
CMD 44 – Add Keypad Special Control User

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

Alarm Inputs

CMD 110 Change Entry/Exit Delay for Alarm Input

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

Relay Setups

CMD 40 – Add Relay Control User
CMD 41 – Add Top-Priority Relay Control User
CMD 81 – Change Control Time of Relay
CMD 82 – Time Zone Control of Relay
CMD 85 – Change Operation for Selected Relays
CMD 86 – Change Relay & Alarm Operating & Reporting Modes
CMD 87 – Relay Triggers Control Zone
CMD 281 – Change Control Delay for Relay

CMD 43: ADD KEYPAD INDEX CONTROL USER (IDF 1)

Syntax: `START 43 * N * User Number * Code #`

Variables: N

1 Manual Holiday, Schedule 1
2 Manual Holiday, Schedule 2
3 Manual Holiday, Schedule 3
4 Manual Holiday, Schedule 4
5 Manual Non-Holiday, Schedule 1
6 Manual Non-Holiday, Schedule 2
7 Manual Non-Holiday, Schedule 3
8 Manual Non-Holiday, Schedule 4
9 Forgive All Users
10 Clear Code Tamper
11 Display This Side Users Count
12 Display Other Side Users Count

Description:

The first four variables (1 - 4) control the assignment of previously-defined holiday schedules to specific user numbers (credentials) using specific codes. Variables 5 - 8 essentially repeal assignment of holiday schedules to a user number using a specific code.Forgive all users provides a quick way to nullify any grant denials issued for a door and enables people to leave the area controlled by the door no matter what their grant status is. This is particularly useful for emergency procedures. Clear Code Tamper enables a user number with the proper code to clear code tamper alarms at a specific location. For example, if an specified operator or guard needs to reset a keypad, this can be accomplished using the assigned code. Display This Side/ Other Side Users Count enables a qualified user with the proper code to see how many people are within a particular area or outside of that area.

Examples:

```
START 43 * 1 * 45 * 777 #
```

Add Schedule 1 holidays to User 45 using Code 777

```
START 43 * 9 * 505 * 2323 #
```

Forgive all users at the reader actuated by user 505 using Code 2323

```
START 43 * 1 * 45 * 777 #
```

Add Alarm Cancel Code 777 To User 45

```
START 43 * 4 * 505 * 23231 #
START 43 * 4 * 506 * 23232 #
```

Add both Start (User 505) and Stop (User 506) Deadman Timer Codes

Related CMDs:

CMD 38 – Print Families of Users with Codes

CMD 88 – Print System Setups

CMD 12 – Change Any User Access or Control Zone
CMD 40 – Add Relay Control User
CMD 41 – Add Top Priority Relay Control User
CMD 42 – Add Alarm Control User
CMD 45 – Define Standard Control Zone
CMD 81 – Change Control Time of Relay
CMD 301 – Add Expansion Point to Standard Control Zone
CMD 358 – Set Deadman Timer

CMD 44: ADD KEYPAD SPECIAL CONTROL USER (IDF 1)

Syntax: `START 44 * NN * User Number * Code #`

Variables: NN

1 Alarm Cancel
2 Watch Log
3 Time Log
4 Deadman Timer

Description:

An Alarm Cancel Code clears the controller's dedicated alarm relay outputs and causes the standard or optional expanded alarm buffer to print its contents. The standard alarm buffer holds approximately 1,500 of the most recent alarms. The optional expanded alarm buffer board holds an additional 2,000 of the most recent alarms. This code duplicates the effect of pressing the alarm cancel button on the controller board.

The Alarm Cancel function has a second function: activating the DIGI*TRAC Annunciator (DTA). When programmed, it enables an operator to activate the DTA by entering the correct user number and code.

A Watch Log Code entry is a logging code for tracking guards on their appointed rounds. A Time Log Code entry is a logging code for recording the arrival and departure times of time log code holders.

To add a card special control user use CMD 325 to convert a keypad special control user to a card special control user.

A Deadman Timer Code is a special control code used to track the safety and security of a user while a specific task is being performed. The use of “deadman timers” is common in many industrial applications such as railroads, refineries and other dangerous or hazardous locations.

Before the task is begun, the user enters a deadman timer code on a specified keypad which *starts* the deadman timer count down sequence. Once the task is completed, the user enters a different deadman timer code on a specified keypad to *stop* the count down. If the user is interrupted, delayed, or otherwise prevented from entering the stop code, the deadman timer will run out and cause a deadman expiration alarm to be reported on the system printer and on the alarm relay.

Deadman users must have at least two codes: one to start the timer and one to stop the timer. The timer for each code is set with CMD 358 for 0–65,000 seconds. The start time is set to the required number of seconds to complete the assigned task. The stop timer is set to 0 (zero) seconds to clear and cancel the deadman timer count down sequence.

Deadman Timer Setups can be printed by entering CMD 88 * 2 #. If deadman codes are used for a guard tour sequence a different Start Timer may be assigned to a code associated with a keypad. This allows the guard to enter a unique code per keypad in the tour thus varying the time allowed to travel between Keypads. For instance, a Code of 789-1 could be entered at keypad 1 and 789-2 at keypad 2. Each code could be assigned a different time based on the average travel time from keypad 1 to 2 and 2 to 3, etc.

Each Deadman user is assigned to a standard control zone. The standard control zone is used to define which keypads are authorized for the entry of the Deadman Codes. Since Deadman Codes do not affect line module inputs or relay outputs, no onboard alarms or relays are defined. Instead, authorized keypad locations are specified by using expansion points 1-16 in the control zone definition. See CMD 301. Use CMD 12 to assign a deadman user to the required standard control zone.

Example:

```
START 44 * 1 * 45 * 777 #
```

Add Alarm Cancel Code 777 To User 45. User 45 can activate an attached Annunciator by entering the code 777.

```
START 44 * 4 * 505 * 23231 #
START 44 * 4 * 506 * 23232 #
```

Add both Start (User 505) and Stop (User 506) Deadman Timer Codes

Default:

None

Related CMDs:

 CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes

 CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

 CMD 88*7 – Print Relay Setups and Status

Adding Users

CMD 10, 15, 19-22, 40-42, 310-315, 320-322 – Add Users

CMD 42 – Add Keypad Alarm Control User

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

CMD 16, 23 – Delete Any User, Range of Users

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

Relay Setups

CMD 81 – Change Control Time of Relay

*Deadman Timer (44*4)*

CMD 358 – Set Deadman Timer

CMD 45: DEFINE STANDARD CONTROL ZONE

Syntax: `START 45 * Standard Control Zone * Time Zone * Relays or Inputs #`

Description:

A Control Zone manages the use of relay control codes and alarm control codes. A control zone consists of a time zone and any combination of available relays for output control, or inputs for alarm control.

There are 192 standard control zones available (0 -191). Control Zone 0 is predefined as "Never & No Relays - No Inputs" This allows control codes to be maintained in memory with a CZ of 0. Note that CZ 0 cannot be changed. To enable any control code user simply use CMD 12 to change the user's control zone to an appropriate control zone.

See CMD 301 for information on expansion inputs/relays. See CMD 304 for information on master control zones.

A defined control zone may be shared by relay control codes and by alarm control codes. Whichever code type is assigned to that zone, when entered, will affect the appropriate function. Relay control codes actuate a set of relays and alarm control codes mask/unmask a set of alarm points.

The way in which the relay and/or input in this SCZ is used is determined by the Master Control Zone.

Note: A Time Zone is only used to restrict the command when a Control Zone will be activated by a Card or Code. The Tiime Zone does not effect the triggering of a Control Zone by an input or an alarm.

Example:

```
START 45 * 1 * 65 * 12345678 #
```

Define Standard Control Zone 1 With TZ 65 And All Doors/Inputs

Default:

CZ0 = Never, No Relays, and No Inputs

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*6 – Print Standard Control Zone Setups
- CMD 88*16 – Print Master Control Zone Setups
- CMD 188*7 – Print Setup Changes for Standard Control Zones

Adding Users
CMD 40 – Add Keypad Relay Control User
Time Zone and Holiday Setups
CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones
CMD 57-59 – Define, Clear Holidays
Relay Setups
CMD 81 – Change Control Time of Relay
Control Zone Setups
CMD 301 – Add Expansion Line Module Input or Relay to Standard Control Zone
CMD 303 – Change Time Zone of Standard Control Zone
CMD 304 – Define Master Control Zone
CMD 345 – Clear Standard Control Zone

CMD 46: CHANGE PASSBACK MODE

Syntax: `START 46 * N #`

Variables: N

1 OFF
2 Report / Alarm / Deny Access
3 Report / Alarm / Forgive
4 Report / Deny Access
5 Report / Forgive
6 Occupancy Violation Report ON
7 Occupancy Violation Report OFF

Description:

The Passback Mode is off when the controller starts up. When the mode is set to on, passback violations will always be reported. They may also be set to trigger the alarm relay, deny access or grant access by automatically forgiving the violation.

In order to track the entry and exit of Users into and out of a secure perimeter, an entry and exit ScramblePad/MATCH reader must be installed on the controlled area and must be set with CMD 03 as entry and exit ScramblePad/MATCH readers. In addition, passback can control access to an internal area when properly set up. Access to internal areas will only be granted to a User once they have entered the secure area through an entry ScramblePad/MATCH reader.

Occupancy Violation counts the number of users entering a secure area through an entry ScramblePad/MATCH reader and keeps a running total. As users exit from the secure area through an exit ScramblePad/MATCH reader, they are subtracted from the running total. Whenever the number of users inside reaches the minimum or maximum levels set with CMD 235, an occupancy violation alarm report is sent to the system printer. In addition, the controller reports the user number of the user who violated the occupancy rule. As long as the violation continues the alarm message will automatically repeat at 2 minute intervals. In order for occupancy tracking to operate properly one of the available passback modes must first be enabled. Other automated functions based on the occupancy count are available by using CMDs 235, 236 and 237.

Example:

```
START 46 * 2 #
```

Change Passback Mode to Report On Printer / Trip Alarm Relay / And Deny Access

Default:

Passback Mode OFF, Occupancy Violation Reporting OFF

Related CMDs:

- CMD 34*9 – Print Users Inside
- CMD 88*2 – Print System Information
- CMD 188*9 – Print Setup Changes for Passback & User Management

Passback Functions

- CMD 03*7, 03*8, 03*9, 03*10 – Change Reader Functions (Passback)
- CMD 47 – Forgive Access User
- CMD 48 – Forgive Passback & Occupancy Count for All Users
- CMD 146 – Disable Passback and Occupancy Control During Time Zone
- CMD 235 – Change Occupancy Count Limits
- CMD 236 – Trigger Control Zone on Change in Occupancy Count

Relay Setups

- CMD 79 – Change Time For Alarm Relay

CMD 47: FORGIVE ACCESS USER

Syntax: `START 47 * User Number #`

Description:

In the event of a passback violation and denied access, an operator may use a forgive an access user command, thus allowing the user's code to grant access and the controller to resume passback tracking.

Example:

```
START 47 * 56 #
```

Forgives user 56 one passback violation and grants access to reestablish user passback status as in or out.

Default:

None

Related CMDs:

CMD 34*9 – Print Users Inside

Passback Functions

CMD 46 – Change Passback Mode

CMD 48 – Forgive Passback & Occupancy Count for All Users

CMD 48: FORGIVE PASSBACK & OCCUPANCY COUNT FOR ALL USERS

Syntax: `START 48 #`

Description:

Use this command to reset the status of all users having access to a passback/occupancy controlled area. Once this command is used, the controller automatically picks up the in or out location of every user the next time the user's code is used at a ScramblePad/MATCH reader. In addition, a forgive command resets the occupancy count of the passback/occupancy controlled area to zero.

Example:

```
START 48 #
```

Forgives all users one passback violation and grants access to reestablish all users passback status. Useful after building or area evacuation. Also sets number of users inside to 0 (zero), so the interior area should be unoccupied when this command is issued to insure an accurate inside user count.

Default:

None

Related CMDs:

CMD 34*9 – Print Users Inside

Passback Functions

CMD 46 – Change Passback Mode
CMD 47 – Forgive Access User

CMD 49: TAG ANY USER OR RANGE OF USERS

Syntax: `START 49 * N * Starting User Number * Ending User Number #`

Variables: N

0 Tag User NO (disable)
1 Tag User YES (enable)
2 Tag User NO (disable) (V6.5 and earlier)

Description:

Tagging a user causes the system to print a tag alert message and activate the trouble alarm relay whenever any tagged user's code is used at a ScramblePad/MATCH reader.

Example:

```
START 49 * 1 * 751 * 751 #
```

Tags user 751 to cause a tag alert alarm message on system printer and to trigger trouble relay.

Default:

None

Related CMDs:

- CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes
- CMD 35, 36, 38, 330*10 – Print User, Users, or Family of Users with Codes
- CMD 260 – Print Alarm Action(s)

Tag and Alert Setups

CMD 149 – Alert User or Range of Users
CMD 249, 349 – Tag/Alert Access Zone
CMD 449, 549 – Tag/Alert Control Zone

Relay Setups

CMD 79 – Change Time For Alarm Relay

CMD 50: SET DATE & DAY OF THE WEEK

Syntax: `START 50 * MMDDYY * Day of Week #`

Variables: MMDDYY/Day of Week

Date:	
January	01
February	02
March	03
April	04
May	05
June	06
July	07
August	08
September	09
October	10
November	11
December	12
Day:	
Monday	1
Tuesday	2
Wednesday	3
Thursday	4
Friday	5
Saturday	6
Sunday	7

Description:

Set date & day of the week. Setting the date and day of the week sets the controller clock-calendar for accurate access restriction, automatic event scheduling and transaction reporting on the system printer or on the SCRAMBLE*NET. The accuracy of all time controlled functions depends on this setting. Set date as Month Day Year: **MMDDYY**. Set day of the week number for the current day. This Command sets the time in each controller, not in the PC. DIGI*TRAC controllers assume the year is in the range 1990-2089.

Example:

```
START 50 * 010101 * 3 #
```

Set the Date to Wednesday, January 1, 2001, Wednesday

Default:

For CCM 7.0 and later, after a cold start, the controller clock defaults to midnight (0000), January 1, 2000. For CCM 6.6 and earlier, the clock defaults to midnight, January 1 of the year in which the CCM was programmed.

Related CMDs:

 CMD 88*1 – Print Date, Time, Version Number

 CMD 188*1 – Print Setup Changes for Date, Time, Version Number

Date, Time, and Holidays

CMD 51 – Set Time

CMD 57-59 – Define, Clear Holidays

Time Zone Setups

CMD 52, 54, 454 – Define/Clear Standard Time Zone

CMD 51: SET TIME

Syntax: `START 51 * Hour Minute (HHMM) #`

Variables: Hour / Minute

0000 = Midnight	1200 = Noon
0100 = 1 AM	1300 = 1 PM
0200 = 2 AM	1400 = 2 PM
0300 = 3 AM	1500 = 3 PM
0400 = 4 AM	1600 = 4 PM
0500 = 5 AM	1700 = 5 PM
0600 = 6 AM	1800 = 6 PM
0700 = 7 AM	1900 = 7 PM
0800 = 8 AM	2000 = 8 PM
0900 = 9 AM	2100 = 9 PM
1000 = 10 AM	2200 = 10 PM
1100 = 11 AM	2300 = 11 PM

Description:

Setting the correct time is critical for accurate access restriction, automatic event scheduling and transaction reporting on the system printer or SCRAMBLE*NET. Also see CMD 50. Set time in 24-hour time.

Example:

```
START 51 * 0915 #
```

Set the time to 9:15AM

Default:

After cold start, the controller clock defaults to midnight (0000) January 1, 2000 for CCM V7.0 and later. For CCM 6.6 and earlier, the controller defaults to midnight, January 1 of the year in which the CCM was programmed.

Related CMDs:

CMD 88*1 – Print Date, Time, Version Number

CMD 188*1 – Print Setup Changes for Date, Time, Version Number

Date, Time, and Holidays

CMD 50 – Set Date & Day of the Week

CMD 57-59 – Define, Clear Holidays

Time Zone Setups

CMD 52 – Define Standard Time Zone 1-64

CMD 52: DEFINE STANDARD TIME ZONE 1-64

Syntax:

```
START 52 * Standard Time Zone * HHMM * HHMM * Days #
(Version 6.6 or earlier)
START 52 * Standard Time Zone * HHMM * HHMM * Days * [1234] #
(Version 7)
```

Variables:

HHMM
Start Time and Stop Time in Hours and Minutes

Days
Days of the week you want to *include* in the time zone, where:

1 = Monday	5 = Friday
2 = Tuesday	6 = Saturday
3 = Wednesday	7 = Sunday
4 = Thursday	8 = Overrides Holiday Schedules

If a holiday is specified, you can use the next optional variable, [1234], to specify which one of four holiday options is designated.

[1234]

If you specify Day 8 in the Days option, it overrides the holiday schedule. There are two ways to override a holiday schedule: selecting Day 8 when placing the days in the standard time zone (CMD 52) or selecting a 0 when defining a holiday schedule (CMD 57). This variable is only available for V7.0 and later.

Description:

Time zones are used to restrict the use of codes by time and by day when used to define an access zone. They are also used to control automatic events such as alarm masking and relay actuation for automatic unlocking and relocking of a door or set of doors when used to define a control zone.

Standard time zones are set up to have a start time, a stop time and a set of valid days, which may include any day programmed in the controller as a Holiday, Day 8.

Master time zones are defined with CMD 54. Master time zones can include up to 8 standard time zones. Master time zones allow “Super Users” with complex access authority and allow complex timing sequences for managing relays and alarms.

Grand master time zones allow up to 8 standard or master times zones to be combined for even more sophisticated time management functions.

See CMD 154. Time Zones 0, Never, and 65, Always, are available for use and cannot be changed.

Appendix A provides Worksheets to help you plan your controller setups, including time zone controls.

Example:

```
START 52 * 1 * 0730 * 1800 * 12345 #
```

Define standard time zone 1 as 7:30AM to 6:00PM Monday-Friday

```
START 52 * 2 * 0000 * 2400 * 8 * 2 #
```

TZ 2 is active during Holiday Schedule 2

Default:

TZ 0 = 00:00 to 00:00 No Days (Never)
TZ 65 = 00:00 to 24:00 All Days (Always)

Related CMDs:

CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
CMD 188*10 – Print Setup Changes for Time Zones

Access Zone Setups
CMD 17, 24, 117 – Define Standard Access Zone (1-64)
Control Zone Setups
CMD 45 – Define Standard Control Zone
CMD 303 – Change Time Zone of Standard Control Zone
CMD 305 – Define Time Zone for Master Control Zone
Date, Time, and Holidays
CMD 50, 51 – Set Date and Day of the Week, Set Time
CMD 57-59 – Define, Clear Holidays
Time Zone Setups
CMD 54 – Define Master Time Zone 66-129
CMD 56 – Clear Time Zone
CMD 154 – Define Grand Master Time Zone 130-149
CMD 454 – Define Master or Grand Master Time Zone
Alarm Setups
CMD 76 – Mask Alarm Input During Time Zone
Relay Setups
CMD 82 – Time Zone Control of Relay

CMD 54: DEFINE MASTER TIME ZONE 66 - 129

Syntax: `START 54 * Standard Time Zone * Master Time Zone * Column 1-8 #`

Time Zones restrict the use of codes to particular time periods for access zones or the automatic scheduling of an event when used to define a control zone. Most time zones include only one set of start times and end times and set of valid days. When more complex time controls are required, any combination of up to 8 standard time zones may be assigned to master time zones.

The most common use of master time zones is to define a time schedule such as Monday to Friday 8AM to 5PM and Saturday 8AM to noon. This requires two standard time zones to be defined. One to cover Monday to Friday and one to cover Saturday only. The two standard time zones are then added to one master time zone to achieve the required time control.

Another common use of master time zones is defining times that span or crossover midnight—for example, the weekday night shift (6 PM to 6 AM, Monday-Friday). This time period can be defined by a master time zone that includes the STZs 1800-2400 M-F and 0000-0600 T-S. Notice that Monday is not included in the second STZ but Saturday is, because weekday nightshifts usually end on Saturday at 6 AM and begin on Monday at 6 PM. Weekend nightshifts begin on Saturday at 6 PM and end Monday at 6 AM.

A master time zone is active when any of its standard time zones is active. A master time zone can be used in any command that calls for a time zone.

Appendix A provides worksheets to help you plan your controller setups including time zone controls.

Examples:

```
START 54 * 1 * 68 * 3 #
```

Add Standard Time Zone 1 To Master Time Zone 68 In Column 3

```
START 54 * 2 * 68 * 4 #
```

Add Standard Time Zone 2 To Master Time Zone 68 In Column 4

Default:

None

Related CMDs:

CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones

CMD 188*10 – Print Setup Changes for Time Zones

Access Zone Setups
- CMD 17, 24, 117 – Define Standard Access Zone (1-64)

Control Zone Setups
- CMD 45 – Define Standard Control Zone
- CMD 303 – Change Time Zone of Standard Control Zone
- CMD 305 – Define Time Zone for Master Control Zone

Date, Time, and Holidays
- CMD 50, 51 – Set Date and Day of the Week, Set Time
- CMD 57-59 – Define, Clear Holidays

Time Zone Setups
- CMD 52 – Define Standard Time Zone 1-64
- CMD 56 – Clear Time Zone
- CMD 154 – Define Grand Master Time Zone (130-149)
- CMD 454 – Define Master or Grand Master Time Zone

Alarm Setups
- CMD 76 – Mask Line Module Input During Time Zone

Relay Setups
- CMD 82 – Time Zone Control of Relay

CMD 56: CLEAR TIME ZONE

Syntax:
```
START 56 * Any Time Zone #
START 56 * First Time Zone * Last Time Zone #
```

Description:

Any Time Zone may be completely cleared with this Command except TZ0 and TZ65.

As an option, you can specify a range of time zones to clear.

Example:

```
START 56 * 44 #
```

Clears Standard Time Zone 44 To No Time - No Days

Default:

None

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 188*10 – Print Setup Changes for Time Zones

Time Zone Setups

CMD 52, 54, 454 – Define Standard, Master Time Zones
CMD 154 – Define Grand Master Time Zone (130-149)

CMD 57: DEFINE HOLIDAY

Syntax: `START 57 * Holiday * MMDDYY #`

Description:

*Note: In Version 7.0, this command is obsolete but is retained for backwards compatibility. Use CMD 457*1 to add holidays to the current year and next year's "Holiday Table 1."*

Any calendar date may be programmed to be a scheduled holiday. When the controller detects a holiday, it refers to its time zones to determine if any normally scheduled event, such as automatic unlocking, is to occur on a holiday or is to be skipped. Whenever a code is entered at a ScramblePad/MATCH reader it is also checked to see if it is authorized during a scheduled holiday or not.

The controller has two holiday controls available:

- ❑ A list of up to 30 scheduled holidays by date.
- ❑ A holiday day field which may be selected as valid when defining a time zone.

These two controls work in unison to perform special controls during scheduled Holidays.

If no holidays are defined, then normal access will be granted and automatic events will occur on each valid day of their respective time zones, even if on one of those days, the building is closed for normal business. If however, the controller's calendar detects a day as a scheduled holiday, then general access will be denied and automatic events will be skipped.

During closed business days it may be necessary for selected groups of users to gain authorized access to the area being controlled. This is accomplished by making the eighth day valid when defining the time zone that controls the group's access authority. Likewise, any special automatic events, such as outdoor security lighting controllers, may be switched on even during a scheduled holiday by making day 8 a valid day in their controlling time zones.

*Note: In Version 7.0 and later this command is obsolete for instructions sent from a host. Use CMD 457*1 to add holidays to current and next year's "Holiday Table 1." For instructions programmed from a ScramblePad, continue to use this command.*

Holidays 31 & 32 are special. On the date specified for Holiday 31 the controller time will "Spring Forward 1 Hour" at 02:00 and on Holiday date 32 the controller time will "Fall Back 1 Hour" at 02:00 to allow for automatic compensation for daylight savings time, if required.

Note: On Holiday 32, after the time falls back from 02:00AM to 01:00AM, there will be one hour of overlap in the recorded or printed history log for that date. There will be two one hour periods from 01:00 to 02:00 hours for that date.

For S*NAP users, Holidays 31 and 32 only affect the time setting of the controllers and not the PC. If the S*NAP Host PC has the Master Clock Setup enabled, it will reverse the automatic time change in the controllers affected by Holidays 31 and 32. Therefore to use both automatic daylight savings time and master clock you must remember to disable the S*NAP Host master clock setup before the date of each Holiday and re-enable it the day after the holiday has occurred.

V7.0 enables you to add a holiday wherever there's an open space in the holiday table by specifying a holiday number of 0. V7.0 also has unlimited holiday capacity for the current calendar year and for the next year following, including 30 additional slots to "pre-load" holidays for successive years, if needed. The theoretical maximum number of holidays at any one time, therefore, is 760 – 761 if there's a leap year involved.

V7.0 assumes years are in the range 1990-2089. To override this, use MMDDYYYY instead of MMDDYY. For example, 25 August 2063 could be specified as 082563 or as 08252063. (This is for historical reasons. If you cold-start an old controller and then immediately upgrade the firmware, it's better to be five or ten years off rather than ninety-five.)

Examples:

```
START 57 * 1 * 010101 #
```

Define January 1, 2001 As Holiday 1

```
START 57 * 2 * 010201 #
```

Define January 2, 2001 As Holiday 2

```
START 57 * 3 * 070401 #
```

Define July 4, 2001 As Holiday 3

Default:

None

Related CMDs:

CMD 88*13 – Print Holiday Setups

CMD 188*2 – Print Setup Changes for Holidays

Date, Time, and Holidays

CMD 50, 51 – Set Date & Day of the Week, Set Time
CMD 52 – Define Standard Time Zone
CMD 58, 59 – Clear Holiday, Clear All Holidays
CMD 90*4 – Manual Holiday
CMD 457 – Define Holidays from a Host

Time Zone Setups

CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones

CMD 58: CLEAR HOLIDAY

Syntax: `START 58 * Holiday #`

Description:

Use this command to remove a holiday from the holiday schedule so the controller will not go into holiday operation. As each holiday expires at midnight, it is automatically removed from the schedule.

*Note: In Version 7.0 and later this command is obsolete if issued from a host. Use the host CMD 457*0 to clear holidays from the current and next year's list of holidays. If you are programming from a ScramblePad, continue to use this command.*

Example:

```
START 58 * 12 #
```

Clear Holiday 12 To No Date

Default:

None

Related CMDs:

CMD 88*13 – Print Holiday Setups

CMD 188*2 – Print Setup Changes for Holidays

Holidays

CMD 57 – Define Holiday
CMD 59 – Clear All Holidays
CMD 90*4 – Manual Holiday
CMD 457 – Define Holiday(s) From Host

Time Zone Setups

CMD 56 – Clear Time Zone

CMD 59: CLEAR ALL HOLIDAYS

Syntax:
```
START 59 #   (Version 6.6 or earlier)
START 59 * YYYY#   (Version 7)
```

Variables: YYYY

Year you want cleared including all four possible holidays.

Description:

Use this command to manually clear all holidays at once.

Version 7.0 enables you to clear an entire year's worth of holidays. All four holiday tables will be cleared.

Example:

```
START 59 #
```

This will clear all Holidays from the controller

Default:

None

Related CMDs:

CMD 88*13 – Print Holiday Setups

CMD 188*2 – Print Setup Changes for Holidays

CMD 57, 58 – Define, Clear Holiday

CMD 90*4 – Manual Holiday

CMD 457 – Define Holiday(s) from Host

Time Zone Setups

CMD 56 – Clear Time Zone

CMD 70: ENABLE SELECTED LINE MODULE INPUTS

Syntax: `START 70 * Inputs #`

Description:

A DTLM/MELM is required.

Note: This command is not available on M16 and MSP controllers.

Line Module Inputs must be enabled to sense and report the status of the required line modules (DTLM/MELM) and the devices they monitor. All Line Module Inputs are Factory set to be enabled on controller start-up.

When a Line Module Input is set to operate and report as a Door it will report the following conditions:

- ❑ Secure
- ❑ Door Forced Open
- ❑ DOTL Alarm (Door Held Open Too Long)
- ❑ RQE Request Granted
- ❑ Open
- ❑ Short
- ❑ Excessive Noise
- ❑ Line Out Of Spec
- ❑ Tamper (DTLM3/MELM3 Only)

When the line module input is set to operate and report as an alarm it will report Door Forced condition as an Alarm Open and a Door Open Too Long alarm will report as an Alarm Active Too Long. All other reporting remains the same.

When a Request To Exit (RQE) push-button or sensor is activated, it will mask the line module input for the door time. When a line module input is masked by a time zone or by an alarm masking code, or is masked when a relay is actuated by an access code, unlock code, time zone or control code, only the door forced or line module input report is masked. All other reporting remains active.

Example:

```
START 70 * 1234 #
```

Enable Line Module Inputs 1 2 3 & 4 To Report Alarms

Default:

Enabled

Related CMDs:

- CMD 88*8 – Print Alarm Setups and Status
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Adding Users

CMD 42 – Add Keypad Alarm Control User

Alarm Setups

CMD 71, 72 – Disable, Change Selected Line Module Inputs
CMD 73 – Change Selected RQEs (Request to Exit)
CMD 74 – Change Door-Open-Too-Long Interval
CMD 75 – Door-Open-Too-Long Active While Door Unlocked (Yes/No)
CMD 76 – Mask Line Module Input During Time Zone
CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 270 – Change Line Module Type for Line Module Input

CMD 71: DISABLE SELECTED LINE MODULE INPUT

Syntax: `START 71 * Inputs #`

Description:

A DTLM/MELM is required.

Any set of line module inputs may be disabled to prevent them from operating, or to prevent the reporting of a defective sensor, sensor cable or DTLM/MELM, until service is available. Disable all unused Inputs.

Note: When an Input is disabled, all reporting is off and the associated RQE will not work.

Example:

```
START 71 * 4 #
```

Disable All Alarm Reporting From Input 4

Default:

Enabled

Related CMDs:

- CMD 88*8 – Print Alarm Setups and Status
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 70, 72 – Enable, Change Selected Line Module Inputs
CMD 76 – Mask Line Module Input During Time Zone
CMD 171 – Disable Expansion Line Module Input

CMD 72: CHANGE SELECTED LINE MODULE INPUTS

Syntax: `START 72 * N * Inputs #`

Variables: N

1 Normally Open (When Secure)
2 Normally Closed (When Secure)

Description:

A DTLM/MELM is required.

Alarm sensor inputs are usually normally closed switches when secure and open on alarm. They may be set to Normally Open for sensors whose contacts are normally open when secure, if required.

Example:

```
START 72 * 1 * 1267 #
```

Change Line Module Inputs 1 2 6 & 7 To Normally Open When Secure

Default:

Normally Closed

Related CMDs:

CMD 88*8 – Print Alarm Setups and Status

CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 70, 71 – Enable, Disable Selected Line Module Input
CMD 73 – Change Selected RQEs (Request to Exit)
CMD 172 – Change Expansion Line Module Input
CMD 270 – Change Line Module Type for Line Module Input

CMD 73: CHANGE SELECTED RQEs (Request To Exit)

Syntax: `START 73 * N * Inputs #`

Variables: N

1 RQE Triggers Relay And Masks Alarm
2 RQE Masks Alarm Only
3 RQE Retriggers Relay And/Or Mask While Activated
4 RQE Triggers Relay And/Or Mask Once When Activated
5 RQE OFF
6 RQE Triggers Relay and Masks Alarm Once When Activated (same as #1 + #4)
7 RQE Masks Alarm Only Once When Activated (same as #2 + #4)
8 RQE Triggers Relay and Masks Alarm While Activated (same as #1 + #3)
9 RQE Masks Alarm Only While Activated (same as #2 + #4)

Description:

A DTLM/MELM is required (series 2 or 3).

Each RQE Input is Factory set to OFF.

The RQE input may be set to trigger the relay, for use with magnetic locks, if required. The RQE will trigger the relay once unless it is set to retrigger the relay for as long as it is activated, such as when using a motion sensor for automatic RQE activation. While the relay is triggered, the associated line module input will be masked. If Auto-Relock is off, CMD 85, the RQE will mask the input for the entire Door Mode time. The door may be opened and closed any number of times during this time without causing a Forced Door alarm. To allow only a single use of the door, Auto-Relock must be enabled.

For RQE devices to work properly (normally open on secure), the input must be enabled (factory default is enabled) by CMD 70 if it has been disabled with CMD 71. For functions 3 and 4 to operate properly, function 1 must first be selected.

If the RQE is disabled, either by default or by 73*5, using 73*3 or 73*4 will automatically do the equivalent of 73*1.

Examples:

```
START 73 * 1 * 1 #
```

Change RQE On Door 1 To Trigger Relay

```
START 73 * 3 * 1 #
```

Change RQE On Door 1 To Retrigger While Actuated By A Motion Detector For Automatic Exit Control

Default:

RQE OFF

Related CMDs:

CMD 88*10 – Print Door Setups and Status

CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 74 – Change Door-Open-Too-Long Interval
CMD 75 – Door-Open-Too-Long Active While Door Unlocked (Yes/No)
CMD 76 – Mask Line Module Input During Time Zone
CMD 173 – Change Expansion RQE (Request To Exit)
CMD 270 – Change Line Module Type for Line Module Input

Relay Setups

CMD 80 – Change Door Time of Relay

CMD 74: CHANGE DOOR-OPEN-TOO-LONG INTERVAL

Syntax: `START 74 * DOTL Timer * Inputs #`

Description:

Use this command to define the DOTL interval for an input. A DTLM/MELM is required for this command.

The unauthorized opening of a door is reported as a forced entry. The door is also monitored if held open-too-long beyond an adjustable time delay of 0-8100 (0=Off) seconds. Both door alarm conditions print and trigger the alarm relay.

The DOTL Timer starts when its associated relay deactivates.

Example:

```
START 74 * 15 * 12 #
```

Define DOTL Alarm Delay To 15 Seconds For Doors 1 & 2

Default:

12 seconds

Related CMDs:

CMD 88*10 – Print Door Setups and Status

CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 73 – Change Selected RQEs (Request to Exit)
CMD 75 – Door-Open-Too-Long Active While Door Unlocked (Yes/No)
CMD 76 – Mask Line Module Input During Time Zone
CMD 174 – Change Expansion Door Open Too Long Time
CMD 270 – Change Line Module Type for Line Module Input

Relay Setups

CMD 80 – Change Door Time of Relay
CMD 282 – Define Special Needs Unlock Extension Time

CMD 75: DOOR-OPEN-TOO-LONG WHILE DOOR UNLOCKED

Syntax: `START 75 * N * Input #`

Variables: N

0 NO
1 YES

Description:

Use this command to define a DOTL condition even if the door is unlocked legally. A DTLM/MELM is required.

The door-held-open condition normally does not report on a door unlocked by time zone or unlock code. It may be made to report on an unlocked door by making DOTL active when unlocked.

If the input associated with the door is masked by code or masked by a time zone, then a DOTL alarm will not report even if the DOTL is active while the door is unlocked. When you set the auto-relock of a door to OFF using CMD 85, the DOTL timer does not start until the door mode timer goes to zero.

If Auto-Relock On Open is enabled (also using CMD 85), the DOTL timer starts as soon as the door is opened.

Example:

```
START 75 * 1 * 1 #
```

Sets door-open-too-long alarm reporting always on even when a door is legally unlocked by an unlock code or by a time zone. Protects fire doors from being propped open when unlocked.

Default:

No (NN = 0 or 2)

Related CMDs:

CMD 88*10 – Print Door Setups and Status

CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 73 – Change Selected RQEs (Request to Exit)
CMD 74 – Change Door-Open-Too-Long Interval
CMD 76 – Mask Line Module Input During Time Zone
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked
CMD 270 – Change Line Module Type for Line Module Input

Relay Setups

CMD 80 – Change Door Time of Relay

CMD 76: MASK LINE MODULE INPUT DURING TIME ZONE

Syntax: `START 76 * Line Module Input * Time Zone #`

Description:

Use this command to mask an alarm input (line module input) during a specified time zone. A DTLM/MELM is required for this command.

Line module inputs may be automatically masked during specific times of the day to disable alarm reporting. Line trouble reporting is not disabled during alarm masking.

Automatic masking is removed by setting the masking time zone of an input to time zone 0 (zero), never.

Example:

```
START 76 * 1 * 1 #
```

Masks Line Module Input Reporting On Door 1 During Time Zone 1

Default:

Time Zone 0

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*8 – Print Alarm Setups and Status
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones
CMD 270 – Change Line Module Type for Line Module Input

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 176 – Mask Expansion Line Module Input during Time Zone

Relay Setups

CMD 82 – Time Zone Control of Relay

CMD 77: CHANGE CODE/ID TAMPER

Syntax: `START 77 * N * Time #`

Variables: N

0 Minutes to lock out the reader
1 Time penalty in seconds for each invalid code (default)
2 Alarm threshold in seconds to exceed for tamper alarm

Time
1 - 100 minutes/seconds depending on N selection

Description:

The controller detects invalid code entries at ScramblePads or card readers. An invalid code is one that does not exist in the controller's memory or is being used at the wrong door or at the wrong time. Code tampering is reported on the printer and trips the tamper alarm relay if 3 invalid codes are entered on a ScramblePad or at a card reader within 1 minute.

In V7.0 and later, the controller can be set to specify the amount of time in minutes that a reader is locked out after a code tamper alarm has been invoked. No entry at this keypad/reader will be recognized for the specified time period. If additional incorrect entries are attempted, this extends the lock-out interval. When this switch is selected (N = 0), the time argument is calculated in minutes rather than seconds. The default value is 1 minute.

The controller may be adjusted to alarm on a single invalid code, or more than three, through adjusting the invalid Code Tamper Alarm Penalty timer, factory set at 20 seconds, or the Alarm Threshold timer, set at 50 seconds. On start-up, the controller alarms once three invalid codes are entered within approximately a minute. Setting the penalty timer more than the threshold or the threshold less than the penalty will cause the alarm to trip on a single invalid code entry.

To disable Code Tamper alarms, set the penalty timer to 1 and the threshold to 100.

Once a Code Tamper alarm occurs, the controller reports the ScramblePad/MATCH Reader involved, locks out the ScramblePad keypad and any attached MATCH Reader from further code entry attempts and sounds its tone steadily while flashing its red status LED for about a minute. Any additional invalid code entries at that ScramblePad or card reader will immediately regenerate a code tamper alarm condition. Tamper mode remains in effect for the duration of the penalty time designated by the Time variable.

Example:

```
START 77 * 0 * 2 #
```

Sets reader lock-out time to 2 minutes

```
START 77 * 1 * 45 #
```

Changes Code Tamper Time Penalty To 45 Seconds To Trip Code Tamper Alarm On One Invalid Code Entry At Any ScramblePad/MATCH Reader.

Default:

Code Tamper Time Penalty = 20

Code Tamper Alarm Threshold = 50

Related CMDs:

- CMD 88*2 – Print System Information
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 79 – Change Time For Alarm Relay

CMD 78: CHANGE ALARM RELAY MAPPING

Syntax: `START 78 * RY1 [* RY2 * RY3 * RY4] #`

Variables:
RY1 General Alarms
RY2 Duress Alarms
RY3 Tamper Alarms
RY4 Trouble Alarms

Description:

DIGI*TRAC M2, M8, M16, and MSP/M64 controllers have one to four dedicated alarm relays; however, the M1N controller does not have dedicated alarm relays. This command enables a control relay to trigger when one of the dedicated alarm relays would normally fire.

If only one base relay number is specified, it applies to all four alarm relays. Default setting for the Model 1N is "78 * 4 #" – any alarm relay will trigger control relay 4.

The numbers to which you can set RY1 – RY4 are in the range of 0 – 72:

0	the Alarm Relay does not trigger any other relays
1 – 8	the Alarm Relay triggers a Base Relay (1-8)
9 – 72	the Alarm Relay triggers an Expansion or Virtual Relay (1-64)

This command is active in V6.6 or later.

Example:

```
START 78 * 1 #
```

Changes all four Alarm Relays to trigger Relay 1.

```
START 78 * 2 * 3 * 2 * 1 #
```

Changes Alarm Relays to trigger Relay 2 for General, Relay 3 for Duress, Relay 2 for Tamper, and Relay 1 for Trouble.

Default:

78 * 4 # for M1N

Related CMDs:

CMD 88*2 - Print System Information

CMD 188*14 - Print Setup Changes for Relays

Alarm Setups

CMD 08 - Change Duress Alarm Mode
CMD 77 - Change Code/ID Tamper
CMD 261 - Define Action Control Block

CMD 79: CHANGE TIME FOR ALARM RELAY

Syntax: `START 79 * Time * NN #`

Variables: NN (Dedicated Alarm Relay)

1 General Alarms
2 Duress Alarms
3 Tamper Alarms
4 Trouble Alarms

Description:

DIGI*TRAC controllers have four dedicated alarm relay types. The Timer can be set for each relay, from 0 (zero), do not actuate on alarm, to 8100 seconds.

Controllers with a single alarm relay use the same four separate alarm timers to trip the relay. Each timer is set individually. If any of the 4 alarm timers is active the relay will actuate. If one or more of the four conditions is not meant to trip the relay, set its timer to 0 (Zero).

This setup is used for special interface capability to digital communicators that transmit any of the four system alarm conditions:

- ❑ General Alarms on Relay 1
- ❑ Duress Alarms on Relay 2
- ❑ Tamper Alarms on Relay 3
- ❑ Trouble Alarms on Relay 4

to a monitored central station alarm company or to trip local annunciation systems at a central guard station.

The *General Alarm Relay* is tripped by Door Forced or Held Opens, Input Tamper, Input Shorted, Noisy, Open, and Out-of-Spec, Occupancy and Passback Violations, and Dead-man Timer Expired.

The *Duress Alarm Relay* is tripped by a user entering their code with a duress digit at a keypad.

The *Tamper Alarm Relay* is triggered by Box Tamper, ScramblePad/MATCH Reader Physical Tamper and Code Tampering.

The *Trouble Alarm Relay* is tripped by Power Failures, Battery Problems, Network Inactive, Keypad, MATCH, Printer and Modem Off-Lines, Report Buffer Threshold Exceeded, and Tag Alerts.

Example:

```
START 79 * 10 * 1 #
```

Changes Alarm Relay 1 Actuation Time On Alarm To 10 Seconds

Default:

General Alarms = 60
Duress Alarms = 60
Tamper Alarms = 60
Trouble Alarms = 60

Related CMDs:

- CMD 88*2 – Print System Information
- CMD 188*14 – Print Setup Changes for Relays

CMD 08 – Change Duress Alarm Mode
CMD 77 – Change Code/ID Tamper
CMD 261 – Define Alarm Actions

CMD 80: CHANGE DOOR TIME OF RELAY(S)

Syntax: `START 80 * Seconds * Relay 1 * [Relays 2 - 8] #`

Description:

Each of a controller's base relays can be set up with simultaneous, yet different timers: Door Timer and Control Timer.

The *Door Timer* can be momentary with an adjustable time of 1-8100 seconds. It can also toggle its relay ON and OFF on consecutive Access Code or RQE entries if the time is set to 0 (zero) seconds. A Relay's Door Timer is used by both access codes and the RQE input.

The Door Timer only applies to the controller's door relays. On the M1N, this means that only Relay 1 has a Door Timer.

Door Mode Time applies to the alarm as well. If your relay/alarms are not set up to operate as Doors, this Door Mode Time only applies to the alarm input, not to the relay.

In Version 6.5 and earlier, you can only specify one relay per command. In Version 6.6 and later, you can specify up to 8 relays with the same command, where each relay is separated by asterisks. The second through eighth relay arguments are optional.

For information on the Control Timer, see CMD 81.

Note: This command is not available on either M16 or MSP controllers.

Example:

```
START 80 * 6 * 3 #
```

Change Door Unlock Timer To 6 Seconds For Door 3

```
START 80 * 6 * 3 * 5 * 6 #
```

Change Door Unlock Timer To 6 Seconds For Doors 3, 5, and 6

Default:

6 seconds

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 88*10 – Print Door Setups and Status
- CMD 188*14 – Print Setup Changes for Relays

Adding Users
CMD 10, 19-22, 220, 311-315, 320-322 – Add Access Users

Alarm Setups
CMD 73 – Change Selected RQEs (Request to Exit)
CMD 74 – Change Door-Open-Too-Long Interval
CMD 75 – Door-Open-Too-Long Active While Door Unlocked (Yes/No)

Relay Setups
CMD 81 – Change Control Time of Relay
CMD 85 – Change Operation for Selected Relays
CMD 280 – Change Door Delay for Relay
CMD 282 – Define Special Needs Unlock Extension Time

CMD 81: CHANGE CONTROL TIME OF RELAY

Syntax: `START 81 * Seconds * Relay 1 * [Relays 2 - 8] #`

Description:

Each of a controller's base relays can be set up with simultaneous yet different, timers: Control Timer and Door Timer.

The *Control Timer* can be momentary with an adjustable time of 1-8100 seconds. It can also toggle a relay ON and OFF on consecutive Control Trigger Code entries if its time is set to 0 (zero) seconds. A Relay's Control Time is used by Control Trigger Codes as well as by a line module input or relay to trigger a Control Zone.

In Version 6.5 and earlier, you can only specify one relay per command. In Version 6.6 and later, you can specify up to 8 relays with the same command, where each relay is separated by asterisks. The second through eighth relay arguments are optional.

For more information on the Door Timer see CMD 80.

Note: This command is not available on M16 or MSP controllers.

Examples:

```
START 81 * 60 * 5 #
```

Change Control Time To 60 Seconds For Relay 5

```
START 81 * 0 * 7 #
```

Change Control Time To Latch ON/Latch OFF For Relay 7

```
START 81 * 0 * 5 * 6 * 7 #
```

Change Control Time To Latch ON/Latch OFF For Relays 5, 6, and 7

Default:

6 seconds

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 188*14 – Print Setup Changes for Relays

Adding Control Users

CMD 15 – Add Keypad Unlock/Relock User (IDF 1)
CMD 40 – Add Keypad Relay Control User
CMD 41 – Add Keypad Top-Priority Relay Control User (IDF 1)

Relay Setups

CMD 80 – Change Door Time of Relay
CMD 82 – Time Zone Control of Relay
CMD 86 – Change Relay & Alarm Operating & Reporting Modes
CMD 85 – Change Operation for Selected Relays
CMD 87 – Relay Triggers Control Zone
CMD 181 – Change Control Time for Expansion Relay
CMD 281 – Change Control Delay for Relay

CMD 82: TIME ZONE CONTROL OF RELAY

Syntax: `START 82 * N * Relay * Time Zone #`

Variables: N

1 Actuate Relay During Time Zone
2 Disable Relay During Time Zone
3 Clear Relay At End Of Time Zone

Description:

Relays may be actuated (door unlocked) during a time zone, going on at the start time of the zone and off at the end time of the zone.

Relays may be disabled during a time zone, becoming disabled at the start of the zone and reenabled at the end of the zone.

Note: During the time a relay is disabled, all access functions, including RQE, are disabled.

The current state of any relay may be auto-cleared at the end of a time zone to insure the automatic reversal of a code activated relay without the need for a manual resetting of the relay. This feature is most often used in combination with a manual Unlock by Code to ensure an automatic Relock by Time Zone.

This feature will not affect relays controlled by a code of higher priority than a time zone, such as Lock Down and Lock Open.

*Note: Use CMD 88 * 7 to print the current status of all controller relays. This is the best method to determine why a relay may not be performing the way it is expected to on a Code entry or other event. See Chapter 5 for more information.*

Examples:

```
START 82 * 1 * 1 * 1 #
```

Auto-Unlock Door 1 During Time Zone 1

```
START 82 * 2 * 1 * 5 #
```

Auto-Disable Relay 1 (No Access) During Time Zone 5

```
START 82 * 3 * 6 * 1 #
```

Automatically Lock Door 6 At The End Of Time Zone 1

Default:

Time Zone = 0 (Never)

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*7 – Print Relay Setups and Status
- CMD 88*10 – Print Door Setups and Status
- CMD 188*14 – Print Setup Changes for Relays

Adding Control Users

CMD 15 – Add Keypad Unlock/Relock User (IDF 1)
CMD 40 – Add Keypad Relay Control User
CMD 41 – Add Keypad Top-Priority Relay Control User (IDF 1)

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones

Alarm Setups

CMD 76 – Mask Line Module Input During Time Zone

Relay Setups

CMD 83 – Clear Time Zone Control of Relay
CMD 85 – Change Operation for Selected Relays
CMD 182 – Time Zone Control of Expansion Relay

CMD 83: CLEAR TIME ZONE CONTROL OF RELAY

Syntax: `START 83 * Relay #`

Description:

Time Zone control of any relay may be cleared (reset to none) with this command.

*Note: Use CMD 88 * 7 to print the current status of all controller relays. This is the best method to determine why a relay may not be performing the way it is expected to on a code entry or other event. See Chapter 5 for more information.*

Example:

```
START 83 * 1 #
```

Clear Time Zone Control Of Door 1 To None

Default:

None

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 88*10 – Print Door Setups and Status
- CMD 188*14 – Print Setup Changes for Relays

Relay Setups

CMD 82 – Time Zone Control of Relay
CMD 83 – Clear Time Zone Control of Relay
CMD 183 – Clear Time Zone Control of Expansion Relay

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones

CMD 84: LINE MODULE INPUT TRIGGERS CONTROL ZONE

Syntax: `START 84 * NN * Line Module Input * Control Zone #`

Variables: NN

1 Trigger
2 Retrigger
3 Actuate
4 Disable

Description:

Any line module input can trigger any control zone. To cancel an alarm trigger of a control zone set the specified input to trigger control zone 0 (none).

To *trigger* a control zone means to start the zone's relay control timers at the moment the alarm occurs. The relay timers will start and time out even if the alarm stays active.

To *retrigger* means that the relay timers are not started until the alarm event restores.

To *actuate* a control zone means to actuate its relays for as long as the alarm is active and release them the moment the alarm restores. The Relay Timers are ignored when "Actuate" is used.

To *disable* means the relays are disabled while the alarm is active. Once it restores the disabled state is cleared.

If the relays have control delays programmed, they will be recognized by the trigger and retrigger controls but not by the actuate and disable controls.

This feature allows special control capabilities such as turning on perimeter lights when a line module input is triggered, or for annunciation of a specific line module input, or control of HVAC and lighting systems. When using a master control zone in this command, master control zones can only be triggered, not retriggered, actuated or disabled.

See CMD 260, 261 and 262 to have alarm conditions trigger control zones.

Example:

```
START 84 * 1 * 4 * 8 #
```

Line Module Input 4 Triggers Control Zone 8

Default:

None

Related CMDs:

- CMD 88*8 – Print Alarm Setups and Status
- CMD 88*16 – Print Master Control Zone Setups
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Control Zone Setups

CMD 45 – Define Standard Control Zone
CMD 184 – Expansion Line Module Input Triggers Control Zone

Relay Setups

CMD 81 – Change Control Time of Relay

CMD 85: CHANGE LINE MODULE INPUT/RELAY CONTACTS FOR SELECTED RELAYS

Syntax: `START 85 * NN * Relays #`

Variables: NN

1 Relay Rests ON
2 Relay Rests OFF
3 Auto-Relock On Door Close
4 Auto-Relock On Door Open
5 Auto-Relock OFF

Description:

Using this command, you can invert the operation and outputs of each relay.

On controller start-up, relays are set to Rest OFF in the de-energized state and the outputs are as marked on the circuit board. However, using this command, each relay can be changed to Rest ON in the energized state effectively inverting the meaning of the outputs: the normally open contact becomes the normally closed contact.

For example, when controlling elevators always change the relays to Rests ON. This is to ensure that if the control system power fails, the relay coil will be de-energized, thus allowing the elevator to be used.

Auto-Relock occurs 1/2 second after the door opens if the door is equipped with a door switch reporting to a DTLM or MELM. Auto-Relock may be set to activate on door closure for use with special lock and door control systems or turned off for use with mag locks with internal door status sensors.

Examples:

```
START 85 * 1 * 45678 #
```

Change Relays 4 5 6 7 & 8 To Fail Safe For Elevator Control

```
START 85 * 5 * 1 #
```

Change Auto-Relock OFF For Mag Lock With Sensor For Door 1

```
START 85 * 3 * 2 #
```

Change Auto-Relock To Relock Lock 1/2 Second After Door 2 Is Closed To Allow For Door To Settle Before Relocking

Default:

Relay Rests OFF

Auto-Relock on Door Opening

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 88*8 – Print Alarm Setups and Status
- CMD 88*10 – Print Door Setups and Status
- CMD 88*17 – Print Detailed Relay Status Only
- CMD 188*14 – Print Setup Changes for Relays

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 73 – Change Selected RQEs (Request to Exit)

Relay Setups

CMD 81 – Change Control Time of Relay
CMD 185 – Change Function of Expansion Relay

CMD 86: CHANGE RELAY & ALARM OPERATING & REPORTING MODES

Syntax: `START 86 * NN * Relay/Line Module Input #`

Variables: NN

1 Relay operates as a control relay / Alarm reports as an alarm
2 Relay operates as a door / Alarm reports as a forced door

Description:

Changing the operation of a door redefines line module input reporting and access code operation. Line module inputs on non-doors will print out as an alarm, not as Door Forced Open, whenever they are tripped.

Access codes or IDs entered at ScramblePad/MATCH readers of 'non-doors' will not actuate a relay when entered. A valid access code/ID will only mask the alarm associated with the ScramblePad/MATCH reader from which it is entered. This gives individual alarm zone control by code and by ScramblePad/MATCH reader. This is not possible with alarm control codes which can mask any input from any ScramblePad/MATCH Reader. This capability gives passback control to alarm management on non-doors.

Any relay/line module input can be changed to report as an alarm and not a door. Relay/Line Module Input 1 can be a door and Relay/Line Module Input 2 can be an alarm-only input.

Example:

```
START 86 * 1 * 4 #
```

Defines Relay 4 As A Non-Door Relay & Alarm Reports As An Alarm.

Default:

Relays operate as door/alarm reports at forced door.

Related CMDs:

CMD 88*7 – Print Relay Setups and Status

CMD 188*14 – Print Setup Changes for Relays

Adding Users
CMD 10, 19-22, 311-315, 320-322 – Add Access Users
CMD 15, 40-42, 44 – Add Control Users

Alarm Setups
CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 186 – Change Expansion Line Module Input Reporting Mode

Relay Setups
CMD 79 – Change Time For Alarm Relay
CMD 80 – Change Door Time of Relay

CMD 87: RELAY TRIGGERS CONTROL ZONE

Syntax: `START 87 * NN * Relay * Control Zone #`

Variables: NN

1 Trigger
2 Retrigger

Description:

Use this command to enable a specified relay to trigger or retrigger another relay or set of relays through a control zone. This is used for such tasks as shunting a door alarm switch monitored by another controller.

When using a master control zone in this command, master control zones may only be triggered, not retriggered, actuated, or disabled.

Example:

```
START 87 * 1 * 4 * 8 #
```

Relay 4 Triggers Control Zone 8

Default:

None

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 88*16 – Print Master Control Zone Setups
- CMD 188*14 – Print Setup Changes for Relays

Control Zone Setups
CMD 45 – Define Standard Control Zone
Relay Setups
CMD 81 – Change Control Time of Relay
Alarm Setups
CMD 84 – Line Module Input Triggers Control Zone
CMD 187 – Expansion Relay Triggers Control Zone

CMD 88: PRINT SYSTEM SETUPS AND STATUS

Syntax:
```
START 88 * NN # (Version 6.6 or earlier)
START 88 * NN [* First * Last] # (Version 7)
```

Variables: NN

0	Complete System Setups and Status
1	Date, Time, Version Number
2	System Information
3	*Standard Time Zones*
4	*Master Time Zones*
5	*Standard Access Zones*
6	*Standard Control Zones*
7	*Relays*
8	*Alarm / RQE Inputs*
9	*Alarm Special Setups and Status*
10	*Doors*
11	*Keypads / MATCH*
12	*MATCH*
13	Holidays
14	*Grand Master Time Zones*
15	*Master Access Zones*
16	*Master Control Zones*
17	*Detailed Relay Status Only*
18	*Expansion Relays*
19	*Detailed Expansion Relay Status Only*
20	*Expansion Alarm / RQE Inputs*
21	*Expansion Alarm Special Setups and Status*
22	Expansion Line Module Input Door Setups
23	Reporting Setups
24	Remote Site Management Setups
25	System Power Status (of AC power, standby battery, and memory battery)
26	Transactions Since Midnight
27	Occupancy, *Passback, Two-Person Rule* Controls
28	*Virtual Relays*
29	*Detailed Virtual Relay Status*
30	HEC Factory Diagnostics
31	Special Needs Unlock Extension Times
32	*Special Keypad / MATCH Setups*
33	*Special MATCH card mapping*

First / Last

All NN subcommands that support this option are marked in *italics* above.

Description:

- Printing a full or partial system status report lists setups, internal status, and event summaries. This report is auto-generated on every Sunday at midnight. An abbreviated version is automatically printed each day at midnight unless disabled by command.

- ❑ Printing the date, time and version prints the current date, time and the controller's CCM Version Number. It also reports the number of users inside and the total number of users in the controller's database.
- ❑ Printing controller information prints all of the controller's setup parameters.
- ❑ Printing the standard time zones prints a list of standard time zones with their starting time, ending time and days, and their current active or inactive state. Printing the master time zones prints a list of any of the master time zones which have been assigned standard time zones and their current active or inactive state.
- ❑ Printing the access zones or control zones prints their time zone and door/relay setups.
- ❑ Printing the relays & doors prints the relay setup tables and the relay status display. The detailed report shows the exact current status of each relay for troubleshooting assistance.
- ❑ Printing the line module inputs prints the line module input setup tables and their current state.
- ❑ Printing the keypads/MATCH prints the keypads/MATCH reader setup tables.
- ❑ Printing the holidays prints the Holiday list.
- ❑ Printing the HEC Factory Diagnostics prints a list of numerical tables useful to Hirsch factory engineers in diagnosing the internal performance of the controller and its attached system.

Note: No sensitive information is contained in these printouts.

- ❑ Several extensions have been added to V6.6 enabling the user to specify only a range of components from that device group. These optional arguments apply to the following command arguments:
  - 88 * 5 * First * Last # – Prints a range of Standard Access Zones
  - 88 * 6 * First * Last # – Print a range of Standard Control Zones
  - 88 * 15 * First * Last # – Print a range of Master Access Zones
  - 88 * 16 * First * Last # – Print a range of Master Control Zones
  - 88 * 18 * First * Last # – Print a range of Expansion Relays
  - 88 * 19 * First * Last # – Print a range of Detailed Expansion Relay Status.
  - 88 * 28 * First * Last # – Print a range of Virtual Relays
  - 88 * 29 * First * Last # – Print a range of Detailed Virtual Relay Status

  For a complete list of values generated when you use one or more of these command variations, refer to Chapter 5.
- ❑ In V6.6, the 88*0 printout prints the various sections in a different order than V6.5. An 88*0 printout is composed of most of the individual printouts put together, 88*1 and up. Since V6.6, they print out in numeric order (that is, Grand Master Time Zones, 88*14, prints out *after* Holidays, 88*13, instead of after the Master Time Zones, 88*4).
- ❑ If you have a specific need for the V6.5 format, use 88*0*1 to print the sections in the old arrangement.
- ❑ In V6.6, options 5, 6, 15, 16, 18, 19, 28, and 29 may take up to two additional arguments. If present, only the indicated item or items will be printed.
- ❑ There's a variant option, 88*0*2#, which prints options 1, 2, 3, 4, 14, 5, 15, 6, 16, 7, 8, 11, 13, 18, 28, 20, 23, 24, 27, 31, 33.

- ❑ In SAM's Diagnostics window, an 88*29 command shows all virtual relays designated as *2u* rather than the number they represent.

*Note: In V7, 88*11 and 88*12 send the same message which does not include the MATCH LED1/LED2 settings.*

Examples:

```
START 88 * 1 #
```

Prints Time, Date, Controller CCM Version, Number Of Users Inside & Total Users

```
START 88 * 16 * 193 #
```

In V6.6 and later, prints Master Control Zone #193.

```
START 88 * 28 * 20 * 30 #
```

In V6.6 and later, prints Virtual Relays 20 through 30.

Defaults:

None

Related CMDs:

- CMD 36 – Print Users with Codes
- CMD 188 – Print List of All Changes since cold start
- CMD 260 – Print Alarm Action(s)

See Chapter 5 for more on Commands 88 and 188.

CMD 90: MAINTENANCE

Syntax: `START 90 * NN #`

Variables: NN

1 Controller Reset and Memory Check
2 Controller Maintenance (enable CMD 97)
4 Manual Holiday

Description:

Perform a CMD 90 * 2 before issuing a CMD 97. For more about CMD 97, refer to page 4-115.

CMD 90 * 4, Manual Holiday, places the controller in a holiday schedule for the balance of the current day. This is useful for a half-day holiday shutdown schedule such as on Christmas Eve day when many businesses close at noon. It is also useful during emergency situations—such as snow, major power outage, floods, hurricanes, earthquakes, or other unforeseen events—when employees need to be sent home suddenly during normal working hours.

Examples:

```
START 90 * 2 #
START 97 * 9 * 0 * 0 * 0 * 0 #
```

Enable CMD 97 then enable midnight reports

Default:

None

Related CMDs:

*Hidden Commands (90*2)*
CMD 97*1 – Change SCIB Setups
CMD 97*2 – Set Default Encryption Key
CMD 97*4 – Set Host Password
CMD 97*5 – Change Buffer Control
CMD 97*6 – Change System Code Reset
CMD 97*7 – Enable/Disable Command Echo
CMD 97*8 – Set Host Timeout
CMD 97*9 – Set No Midnight Report
*Manual Holiday (90*4)*
CMD 57-59 – Define, Clear Holidays

CMD 96: TERMINATE COMMAND IN PROGRESS

Syntax: `START 96 #`

Description:

This command is used to terminate the programming command currently in progress. This command is used to terminate batch-add commands or a long report or printout if required.

*Note: This command cannot be executed from S*NAP software.*

Examples:

```
START 96 #
```

Terminates Current Command in Process

Default:

None

Related CMDs:

All

CMD 97: CHANGE SYSTEM PARAMETERS

Syntax:

```
START 90 * 2 #
START 97 * NN * P1 * P2 * P3 * P4 #
```

Variables: NN

1 - Set Up Serial Printer
2 - Set Default Encryption Key
4 - Set Host Password
5 - Change Buffer Control
6 - Enable/Disable System Code Reset
7 - Enable/Disable Command Echo
8 - Set Host Timeout
9 - Set No Midnight Report
10 - Set SCIB extension options (Version 6.6 and later)

Description:

This command provides a way to change several important controller features. Each of these variables requires a slightly different syntax and is explained in more detail on the following pages.

Version 7.0 includes several new sets of system parameters, including dynamic allocation of memory expansion boards, code record databases, event buffers, network buffers, and printer buffers.

*Note: CMD 97 must always be immediately preceded by CMD 90 * 2.*

Related CMDs:

CMD 97*1 – Set Up Serial Printer
CMD 97*2 – Set Default Encryption Key
CMD 97*4 – Set Host Password
CMD 97*5 – Change Buffer Control
CMD 97*6 – Enable/Disable System Code Reset
CMD 97*7 – Enable/Disable Command Echo
CMD 97*8 – Set Host Timeout
CMD 97*9 – Set No Midnight Report
CMD 97*10 – Set SCIB extension options

CMD 97 * 1: CHANGE SCIB SETUPS

Syntax:
```
START 90 * 2 #
START 97 * 1 * Baud Rate * Parity * Data Bits * Stop Bit #
```

Variables: Baud Rate/Parity/Data Bits/Stop Bits

Baud Rates	0	300 Baud
	1	600 Baud
	2	1200 Baud
	3	2400 Baud
	4	4800 Baud
	5	9600 Baud
Parity	0	No Parity
	1	Odd Parity
	2	Even Parity
Data Bits	7	7 Data Bits
	8	8 Data Bits
Stop Bits	1	1 Stop Bit
	2	2 Stop Bits

Description:

This Command is used to change the SCIB settings to match the serial printer's or terminal's capabilities. Make sure the serial printer's dip switches if available, match the selected settings.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 1 * 3 * 1 * 8 * 1 #
```

Sets the SCIB For 2400 Baud, Odd Parity, 8 Data Bits, 1 Stop Bit

Default:

None

Related CMDs:

CMD 88*2 – Print System Information
CMD 90 – Maintenance Command

CMD 97*2: SET DEFAULT ENCRYPTION KEY

Syntax:
```
START 90 * 2 #
START 97 * 2 * P1 * P2 * P3 * P4 #
```

Variables:
P1 – Bits 0-15
P2 – Bits 16-31
P3 – Bits 32-47
P4 – Bits 48-63

Description:

Sets default HES encryption key.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 2 * 123 * 123 * 123 * 123 #
```

Defines the default encryption key

Related CMDs:

CMD 97*4 – Set Host Password

CMD 97*4: SET HOST PASSWORD

Syntax:
```
START 90 * 2 #
START 97 * 4 * P1 * P2 * P3 * P4 #
```

Variables:
P1 – Bits 0-15
P2 – Bits 16-31
P3 – Bits 32-47
P4 – Bits 48-63

Description:

Sets host communications password.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 4 * 123 * 123 * 123 * 123 #
```

Defines host password

Related CMDs:

CMD 97*2 – Set Default Encryption Key

CMD 97 * 5: CHANGE BUFFER CONTROL

Syntax:

```
START 90 * 2 #
START 97 * 5 * N * 0 * 0 * 0 #
```

Variables: N

0 Close Buffer
1 Open Buffer, No Printout of Status

Description:

This command is used to change the state of the communications and printer buffers.

When set to Close Buffer, the buffer will not send its contents to a local printer (if one is installed), or to the S*NAP PC when it first connects to the system.

When set to Open Buffer, the contents of the buffer are sent in real time to the local printer.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 5 * 0 * 0 * 0 * 0 #
```

Closes the buffer

Default:

None

Related CMDs:

CMD 88*2 – Print System Information
CMD 90 – Maintenance Command

CMD 97 * 6: CHANGE SYSTEM CODE RESET

Syntax:

```
START 90 * 2 #
START 97 * 6 * N * 0 * 0 * 0 #
```

Variables: N

0 Disable
1 Enable, No Printout of Status

Description:

This command is used to disable the controller's reset button. Normally when the reset switch is pressed for 5 seconds the current system code is deleted and returned to the factory default of 123. When this command is used to disable this function, it is not possible to reset the system code without a cold start.

! CAUTION **Pressing the System Code Reset switch for 30 seconds causes a cold start which erases all codes and setups in memory and resets the system code to 123. This command does not disable the cold start capability of the System Code Reset switch.**

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 6 * 1 * 0 * 0 * 0 #
```

System Code Reset to 123 is Enabled

```
START 90 * 2 #
START 97 * 6 * 0 * 0 * 0 * 0 #
```

System Code Reset to 123 is Disabled

Default:

None

Related CMDs:

CMD 88*2 – Print System Information
CMD 90 – Maintenance Command

CMD 97*7: ENABLE/DISABLE COMMAND ECHO

Syntax:

```
START 90 * 2 #
START 97 * 7 * N * 0 * 0 * 0 #
```

Variables: N

0 Disable
1 Enable

Description:

Use this command to enable or disable a command echo. This can be useful when establishing communications with certain types of terminals or panels.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 7 * 0 * 0 * 0 * 0 #
```

The command echo is disabled.

Related CMDs:

CMD 88 – Print System Setups and Status

CMD 97 * 8: SET HOST TIMEOUT

Syntax:

```
START 90 * 2 #
START 97 * 8 * 10-255 * 0 * 0 * 0 #
```

Description:

Use this command to reset the host timeout from a value between 10 and 255 seconds. This means that if the attached host PC does not receive any input from the controller within the specified interval, the PC will issue an alarm.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 8 * 100 * 0 * 0 * 0 #
```

Resets the host timeout to 100 seconds.

Default:

10 seconds

Related CMDs:

CMD 88*2 – Print System Information
CMD 90 – Maintenance Command

CMD 97 * 9: SET NO MIDNIGHT REPORT

Syntax:

```
START 90 * 2 #
START 97 * 9 * N * 0 * 0 * 0 #
```

Variables: N

0 Midnight Reports
1 No Midnight Reports

Description:

This command is used to disable or re-enable the default midnight report. Normally the controller will send a complete report to the system printer every day at midnight. However, there may be occasions – like extended holidays or building shutdowns – when generating such a report is unnecessary or inconvenient.

This does not disable an attached PC from receiving a report from the controller.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Before using this command, you must disable the standard CMD 107.

Examples:

```
START 90 * 2 #
START 97 * 9 * 1 * 0 * 0 * 0 #
```

Disables midnight report generation.

Default:

In V6.6, all midnight reports are disabled by default. In Version 6.6 and later, enabled is the default.

Related CMDs:

CMD 88*2 – Print System Information
CMD 90 – Maintenance Command

CMD 97*10: SET SCIB EXTENSION OPTIONS

Syntax:

```
START 90 * 2 #
START 97 * 10 * 0 * Reader * AZ * 0 #
```

Variables:

Reader
1-16 to identify annunciator-equipped DS47 ScramblePad associated with this SCIB.

AZ
Access Zone for self-enrolled users.

Description:

Use this command to set SCIB extension options. Additional hardware may be required.

*Note: The command START 90 * 2 # must be issued each time just before using CMD 97.*

Examples:

```
START 90 * 2 #
START 97 * 10 * 0 * 1 * 65 * 0 #
START 98 * 31 * 1 * 0 * 0 * 0#
```

Self-enrolled users are enrolled with Access Zone 65. Auto-generated CODEs will appear on DS47 reader #1, hardware permitting.

Default:

SCIB extensions disabled.

Related CMDs:

CMD 88 – Print System Setups and Status

CMD 99: QUIT PROGRAMMING

Syntax: `START 99 #`

Description:

To quit the current programming session enter CMD 99. The controller will automatically quit programming mode after 8 minutes without programming activity on the programming Scramblepad keypad.

Change the programming mode timeout using CMD 192.

When in programming mode at a ScramblePad keypad, the ScramblePad will not scramble its display. It will display normal telephone keypad positions for ease of data entry during programming. Once the session is over and CMD 99 is entered, the ScramblePad keypad will return to Scramble Secure mode, unless the scramble feature has previously been turned off.

*Note: This Command is not available from S*NAP Software.*

Example:

```
START 99 #
```

Quits Programming Mode.

Default:

None

Related CMDs:

CMD 192 – Change Programming Mode Timeout Interval

CMD 103: CHANGE SELECTED MATCH FUNCTIONS

Syntax: `START 103 * N * 1/0 * Address 1-8 [* Address 9-16] #`

Variables: **N**

1 Channel 1 Card Reader LED Reversed
2 Channel 2 Card Reader LED Reversed
3 Physical Tamper
4 Card Reader LED follows Local Relay
5 Card Reader ScramblePad Sharing
6 DTA Externally Powered, allow keypress to activate LCD Unit Backlight
7 DTA Backlight ON continually
8 DTA Display Threat Level

1/0

1 ON
0 OFF

Address 1 - 8
012345678

Address 9 - 16 (optional)
012345678

Description:

This command controls several functions of the MATCH Reader Interface Board (MRIB) or the card readers attached to the MRIB. The factory setup for the reader status LED is to be normally off and to momentarily turn on when a card is read. This command allows the status LED functions to be reversed.

The MRIB can detect when the bezel of its mounting base is removed and can report the bezel OFF as a physical tamper alarm on the system printer, on the tamper alarm relay, and on the host PC, if installed. The factory setup for physical tamper is OFF. This command enables tamper reporting to be changed to ON.

When you enable Card Reader ScramblePad Sharing, it allows a ScramblePad or reader to use both reader types in the same dual technology setup. Ordinarily, a ScramblePad is only allowed to recognize one reader type at a time; however, some companies must provide access for employees who possess either a mag stripe card or a prox card in addition to a code. This feature enables employees to enter their code then swipe either their prox or mag stripe card to gain access.

There are several new options added for the DTA (DIGI*TRAC Annunciator). These enable backlighting and display threat levels.

Example:

```
START 103 * 1 * 1 * 1 * 0 #
```

Changes Card Reader Address 1 LED on Channel 1 to ON

Default:

Channel 1 & 2 reader LED not reversed

Physical Tamper disabled

Related CMDs:

CMD 88*12 – Print Match Setups and Status

CMD 188*3 – Print Setup Changes for Keypad/MATCH
CMD 03 – Change Selected Keypad/Match Functions
CMD 104 – Enable CARD/CODE-Only At Dual Technology
CMD 403 – Change Selected Keypad / MATCH Functions From Host [V 7.0 and later]

CMD 104: ENABLE CARD/CODE ONLY AT DUAL TECHNOLOGY READER DURING TIME ZONE

Syntax: `START 104 * NN * Address * Time Zone #`

Variables: NN

1 Reader On Channel 1
2 Reader On Channel 2

Description:

This command enables the use of a card only at a dual technology reader during the specified time zone. This is often used at a card-only entry during normal working hours and at a dual (card + code) entry after hours. This command enables use of Card Only on either the entry or exit (Channel 1 or Channel 2) readers, or both.

To disable the use of card-only mode and return the reader to dual at all times, reenter the command with time zone 0.

For a list of available ID formats and their behavior, refer to Table 3-7 on page 3-24.

Example:

```
START 104 * 1 * 1 * 1 #
```

Enable Card Only at the Entry Reader of Channel 1 During Time Zone 1

```
START 104 * 1 * 1 * 0 #
```

Enable Dual Always and Disable Card Only at any time on the entry reader of Channel 1

Default:

None. No Dual readers will read Card Only.

Related CMDs:

CMD 88*12 – Print Match Setups and Status

CMD 188*3 – Print Setup Changes for Keypad/MATCH

CMD 03 – Change Selected Keypad/Match Functions

Time Zone Setups

CMD 52, 54, 154 – Define Standard, Master, Grand Master Time Zones

Adding Users

CMD 312, 313, 315 – Add Users, IDF 4, 5, 7.

CMD 105: DISABLE DEVICE DURING TIME ZONE

Syntax: `START 105 * Device * Time Zone #`

Variables:

Device

1 Printer
2 SNIB

Description:

This command allows the printer and/or SNIB to be disabled during the specified time zone. This reduces the quantity of printouts which occur during high activity periods, or during any time period that printed records are not required.

Disabling the printer prevents all transactions from being logged to the printer and to the controller's internal memory buffer.

The SNIB can be disabled during specified times to disable network communications to and from the specified controller. If the network is active when the SNIB is disabled, communications will remain active until the S*NET host PC logs off the network. Logging back on will not be allowed until the SNIB is enabled at the end of the specified Time Zone.

To re-enable any device, re-enter the command and specify Time Zone 0 for that device.

Example:

```
START 105 * 1 * 1 #
```

Disable Printer During Time Zone 1

```
START 105 * 1 * 0 #
```

Reenable Printer to Always Print

Default:

Printer Always Prints

SNIB Always Communicates

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*23 – Print Reporting Setups
- CMD 188*4 – Print Setup Changes for Reporting and Duress

Reporting and Printing Setup

CMD 05 – Reporting Modes
CMD 06 – Disable printing of grants on selected doors
CMD 106 – Disable Reporting During Time Zone
CMD 107, 90*2#/97*1 – Daily Report Printing On/Off
CMD 109 – Invalid Code/ID Reporting Mode

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones
CMD 108 – Time Zone Control of Modem

CMD 106: DISABLE REPORTING DURING TIME ZONE

Syntax: `START 106 * Report Type * Time Zone #`

Variables: Report Type

1 Transaction Reporting
2 Event Reporting
3 Grant Reporting

Description:

This command disables all code & RQE transaction reports, granted and denied, from reaching the system printer, or the host PC, if the controller is networked. All events, internal and external, can also be disabled during the specified time zone. Grant only transactions can be disabled during the specified time zone. Any denied transactions continue to be reported.

Note: Disabling these reports prevents them from being logged to the printer, buffer, and Host PC.

Example:

```
START 106 * 2 * 1 #
```

Disable printed events during Time Zone 1

Default:

None are disabled. All report.

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*23 – Print Reporting Setups
- CMD 188*4 – Print Setup Changes for Reporting and Duress

Reporting and Printing Setups

CMD 05 – Reporting Modes
CMD 06 – Disable printing of grants on selected doors
CMD 105 – Disable Device During Time Zone
CMD 107, 90 * 2 # / 97 * 1 # – Daily Report Printing On/Off
CMD 109 – Invalid Code/ID Reporting Mode

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones

CMD 107: DAILY REPORT PRINTING

Syntax: `START 107 * NN #`

Variables:

NN

0 - OFF
1 - ON

Description:

This Command disables the automatic Daily Report of System Status that occurs every night at midnight. It also disables the Sunday Midnight System Status and configuration Report.

In V6.6 and later, the daily maintenance report no longer reports the system setups and status. Get these using CMD 88*0.

*Note: This Command does not disable the daily midnight report from going to the S*NAP PC.*

Example:

```
START 107 * 1 #
```

Enable The Daily Midnight Report

Default:

Daily Report Printing OFF

Related CMDs:

CMD 88*23 – Print Reporting Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Reporting and Printing Setups

CMD 05 – Reporting Modes
CMD 90*2# / 97*1 – Disable Daily Report
CMD 106 – Disable Reporting During Time Zone

CMD 108: TIME ZONE CONTROL OF MODEM

Syntax: `START 108 * NN * Time Zone #` (Version 6.6 and earlier)
`START 108 * 1 * TZ1 * TZ2 * TZ3 * TZ4 #` (Version 7)

The first command syntax applies to all versions. The second command syntax is only applicable to V7.0 and later.

Variables: NN

1 Trigger Dialing Host
2 Postpone Dialing Host
3 Cancel Dialing Host
4 Disable Answering Host

Description:

This command is part of the Remote Site Management feature set. It enables time zone control of the modem at a remote site. The modem can be set to dial the host PC at the main site at the *start time* of a specified time zone. This selection can be used to automatically upload a remote site's buffered events and alarms on a daily or weekly scheduled basis. It can also be used to provide a level of "supervision," or automatic check-in, 'I'm OK' message, between any remote site and the main site. The second selection can be used to delay any alarms or events from dialing the host until the *end time* of the selected time zone. The third selection will cancel any attempt to dial the host during the specified time zone and the fourth selection disables the controller from answering the host during the specified time zone.

In Version 6.6 the dialing modem stops attempting to contact the remote site after trying 255 times in succession. (A typical attempt takes 30-40 seconds; 255 tries takes 1 to 3 hours.) The modem will resume trying the next time something triggers its modem dialer logic, or the next day, whichever comes first; however, after 255 attempts it will stop again.

In V7.0 and later, you can specify up to four time zones as triggers for dialing the host.

Examples:

```
START 108 * 1 * 5 #
```

Dial Host At Start Time Of Time Zone 5

```
START 108 * 4 * 1 #
```

Disable Answering Host During Time Zone 1

```
START 108 * 1 * 2 * 4 * 5 #
```

Dial Host At Start Time Of Time Zone 2, Time Zone 4, and Time Zone 5

Default:

None. No Time Zone control of modem.

Related CMDs:

- CMD 88*23 – Print Reporting Setups
- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*24 – Print Remote Site Management Setups
- CMD 188*4 – Print Setup Changes for Reporting and Duress

Modem Setups

CMD 193 – Set Host Phone Number(s)
CMD 194 – Select Tone or Pulse Dialing
CMD 195 – Change Host Call-Back

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones
CMD 105* 2 – Disable SNIB During Time Zone

CMD 109: INVALID CODE REPORTING MODE

Syntax: `START 109 * NN #`

Variables: NN

0 OFF
1 ON
2 OFF

Description:

This command is used to track & record the occurrences of invalid code usage at each ScramblePad or card reader on the controller. An invalid code is one that *does not exist* in the controller's database or memory. In some installations, system managers are concerned over attempts to guess valid codes or the unauthorized use of an unreported lost, stolen, or unidentified card by either authorized users or unauthorized users. This feature can track these attempts by recording each use of an invalid code, which may be immediately followed by the use of a valid code. When this feature is enabled the actual invalid code entered will be printed out.

The ability to record invalid codes can illustrate if an orderly sequence or a random sequence of codes is being used in an attempt to discover a valid code. Likewise, it may disclose infrequent honest errors by authorized users during the code entry process such as digit transpositions or incorrect digit sequences.

When invalid codes are turned ON, it will display both invalid ScramblePad and MATCH codes.

Note: Invalid Code Reporting can be used to determine a card's 8-digit MATCH code at a dual technology reader. Simply present the unenrolled card, then enter 000# at the ScramblePad. When the combination of card + 000 is denied by the controller, the card's MATCH code is sent to the host.

In Version 6.6, at a dual technology reader with “Invalid Code Reporting” enabled, an invalid card and code combination will result in the controller sending the card code to the host. Version 6.6, when presented with an unenrolled card, will wait for a code and then looks up the resulting dual code in the database, even when in “Card/Code Only Mode” (CMD 109). This means that invalid code reporting doesn't take effect until after the dual code is rejected. “Invalid Code Reporting” can still be used to determine a card's 8-digit MATCH code at a dual technology reader. Simply present the unenrolled card, then enter 000# at the ScramblePad. When the combination of card + 000 is denied by the controller, the card's MATCH code is then sent to the host.

Examples:

```
START 109 * 1 #
```

Changes Invalid Code Reporting To ON

Default:

Invalid Code Reporting OFF

Related CMDs:

CMD 88*23 – Print Reporting Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Reporting and Printing Setups

CMD 05 – Reporting Modes
CMD 06 – Disable printing of grants on selected doors
CMD 105, 106 – Disable Device or Disable Reports During Time Zone
CMD 107, 90*2/97*1 – Daily Report Printing On/Off

CMD 110: CHANGE ENTRY / EXIT DELAY FOR LINE MODULE INPUT

Syntax: `START 110 * N * Delay Time (0-255 secs) * Line Module Input #`

Variables:

N

1 Entry Delay
2 Exit Delay

Description:

Entry and exit alarm delays are required when security system designs call for the alarm control ScramblePad/MATCH Reader to be placed inside the secure area. The entry/exit delay range is 0 - 255 seconds.

When an entry delay is used, an authorized person enters the secured area which causes an alarm condition on the line module input monitoring the entrance door or area. The alarm is not reported if the authorized individual proceeds to the interior ScramblePad/MATCH reader and enters a cancel entry delay code. If the cancel entry delay code is not entered in time, the alarm will be reported. An entry delay warning report is sent to the system printer whenever an input with an entry delay time goes into alarm. An audible entry or exit delay tone can be sounded on the ScramblePad if required by using a master control zone.

This command enables the setting of the entry delay timer. To re-secure the same facility, an exit timer code is required to enable the authorized user to leave the facility without causing an alarm. An Exit Delay Warning report is sent to the system printer whenever an exit delay code is used.

To disable the use of an Entry or Exit Delay Timer set the delay time to 0 (zero).

Example:

```
START 110 * 1 * 45 * 1 #
```

Change the Entry Delay Timer To 45 Seconds on Line Module Input 1

Default:

Entry delay = 0 seconds (delay disabled)

Exit delay = 0 seconds (delay disabled)

Related CMDs:

- CMD 88*8 – Print Alarm Setups and Status
- CMD 88*9 – Print Alarm Special Setups and Status
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Adding Users
CMD 42 – Add Keypad Alarm Control User
Control Zone Setups
CMD 45 – Define Standard Control Zone
CMD 304 – Define Master Control Zone
Alarm Setups
CMD 111 – Change Entry/Exit Delays For Expansion Line Module Input
CMD 112 – Disable Entry Delay for Line Module Input during Time Zone
CMD 113 – Disable Entry Delay for Expansion Line Module Input during Time Zone

CMD 111: CHANGE ENTRY/EXIT DELAY FOR EXPANSION LINE MODULE INPUT

Syntax: `START 111 * N * Delay Time (0-255 secs) * Expansion Line Module Input #`

Variables:

N

1 Entry Delay
2 Exit Delay

Description:

Entry and exit alarm delays are required when security system designs call for the alarm control ScramblePad/MATCH reader to be placed inside the secure area. The entry/exit delay range is 0 - 255 seconds.

When an entry delay is used an authorized person enters the secured area which causes an alarm condition on the line module input monitoring the entrance door or area. The alarm is not reported if the authorized individual proceeds to the interior ScramblePad/MATCH reader and enters an cancel entry delay code. If the cancel entry delay code is not entered in time, the alarm will be reported. An entry delay warning report is sent to the system printer whenever an input with an entry delay time goes into alarm. An audible entry or exit delay tone can be sounded on the ScramblePad if required by using a master control zone.

This command enables the setting of the entry delay timer. To re-secure the same facility an exit timer code is required to enable the authorized user to leave the facility without causing an alarm. An exit delay warning report is sent to the system printer whenever an exit delay code is used.

To disable the use of an entry or exit delay timer, set the delay time to 0 (zero).

Example:

```
START 111 * 1 * 45 * 8 #
```

Change the Entry Delay Timer To 45 Seconds on Expansion Line Module Input 8

Default:

Entry Delay = 0 seconds (delay disabled)

Exit Delay = 0 seconds (delay disabled)

Related CMDs:

- CMD 88*9 – Print Alarm Special Setups and Status
- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Adding Users
CMD 42 – Add Keypad Alarm Control User

Control Zone Setups
CMD 45 – Define Standard Control Zone
CMD 301 – Add Expansion Line Module Input or Relay to Standard Control Zone

Alarm Setups
CMD 110 – Change Entry/Exit Delays For Line Module Input
CMD 112 – Disable Entry Delay for Line Module Input during Time Zone
CMD 113 – Disable Entry Delay for Expansion Line Module Input during Time Zone

CMD 112: DISABLE ENTRY DELAY FOR LINE MODULE INPUT DURING TIME ZONE

Syntax: `START 112 * Time Zone * Line Module Input #`

Description:

Entry delays may be disabled during specified times of selected days by time zone on an input-by-input basis. This allows a secure facility to operate with tighter security, requiring access codes, or lock and key entry, plus cancel entry delay codes, during night time hours and normal access security, requiring only access codes, during day time hours.

Example:

```
START 112 * 1 * 1 #
```

Disable Entry Delay during Time Zone 1 For Line Module Input 1

Default:

Entry delays are not disabled by Time Zone

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*8 – Print Alarm Setups and Status
- CMD 88*9 – Print Alarm Special Setups and Status
- CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

CMD 110 – Change Entry/Exit Delays For Line Module Input
CMD 113 – Disable Entry Delay for Expansion Line Module Input during Time Zone

Time Zone Setups
CMD 52, 54, 56, 454 – Define/Clear Standard, Master Time Zones

CMD 113: DISABLE ENTRY DELAY FOR EXPANSION LINE MODULE INPUT DURING TIME ZONE

Syntax: `START 113 * Time Zone * Expansion Line Module Input #`

Description:

Entry delays may be disabled during specified times of selected days by time zone on an input-by-input basis. This allows a secure facility to operate with tighter security, requiring access codes, or lock and key entry, plus cancel entry delay codes, during night time hours and normal access security, requiring only access codes, during day time hours.

Example:

```
START 113 * 1 * 8 #
```

Disable Entry Delay during Time Zone 1 For Expansion Line Module Input 8

Default:

Entry delays are not disabled by Time Zone

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 111 – Change Entry/Exit Delays For Expansion Line Module Input
CMD 112 – Disable Entry Delay for Line Module Input during Time Zone

Time Zone Setups

CMD 52, 54, 56, 454 – Define/Clear Standard, Master Time Zones

CMD 117: DEFINE STANDARD ACCESS ZONE (1-64) – 1 TIME ZONE, SPECIFIED DOORS ONLY

Syntax: `START 117 * Standard Access Zone * Time Zone * Doors #`
`(Other versions)`
`START 117 * Standard Access Zone * Time Zone * Doors * Doors #`
`(Version 6.7 only)`

Variables:

Doors
Doors/Readers. Associates specified Doors (and corresponding entry/exit Readers) where 125 means Doors 1, 2, and 5 which assumes the association of corresponding readers 1, 2, 5, 9, 10, and 13.

In Version 6.7, Access Zones may be arranged individually by reader, using the second Doors option to specify a different set corresponding to readers 9-16.

Description:

This command is used to define a Standard Access Zone by specifying one time zone for a specified group of doors. This allows a time zone to be set or changed for one or more doors of an access zone without affecting the other doors of the same zone.

Unlike this command, CMD 24 requires a time zone to be specified *for each and every door* of the specified access zone. Also, CMD 24 does not allow partial changes to the time zone specification of an Access Zone. CMD 117 allows the time zone of a single door to be changed without specifying a time zone for any other door. CMD 17 forces the time zone to be the same for all doors of the specified Access Zone. CMD 117 does not force the Time Zone for all doors, but allows individual settings one door at a time.

Example:

```
START 117 * 4 * 1 * 2 #
```

Sets Time Zone For Door 2 (Readers 2 and 10) only to Time Zone 1 in Access Zone 4

```
START 117 * 5 * 2 * 24 * 12 #
```

Sets Time Zone For Readers 2, 4, 9, 10 only to Time Zone 2 in Access Zone 5

Default:

None

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*5 – Print Standard Access Zone Setups
- CMD 188*5 – Print Setup Changes for Standard Access Zones

Access Zone Setups

CMD 17 – Define Standard Access Zone (1-64), 1 Time Zone, Selected Doors
CMD 24 – Define Standard Access Zone (1-64), 1 Time Zone Per Door
CMD 124 – Define Standard Access Zone, 1 Time Zone Per Reader
CMD 204 – Define Master Access Zone (66-127)
CMD 249, 349 – Tag/Alert Access Zone

Time Zone Setups

CMD 52, 54, 56, 454 – Define/Clear Standard, Master Time Zones

CMD 124: DEFINE STANDARD ACCESS ZONE, 1 TIME ZONE PER READER

Syntax:

```
START 124 * Access Zone * NN * TZ For Reader 1/9 *
                                    TZ For Reader 2/10 *
                                TZ For Reader 3/11 *
                                TZ For Reader 4/12 *
                                TZ For Reader 5/13 *
                                TZ For Reader 6/14 *
                                TZ For Reader 7/15 *
                                TZ For Reader 8/16 #
```

Variables: NN

1 Readers 1-8
2 Readers 9-16

Description:

This command enables you to define standard access zones, using one time zone per reader. Each reader must be assigned a time zone.

Using one time zone per reader expands the capability of access zones by restricting access by time zone on a reader by reader basis. Each reader in a standard access zone can be restricted by any of the available time zones. Entering Time Zone 0 for a reader restricts all access at that reader.

CMD 24 defines Readers 1-8 and Readers 9-16 to use the same set of eight time zones. CMD 124 enables you to set Readers 1-8 separately from Readers 9-16. Possible applications include entry/exit readers where the exit readers must be configured to allow exit at any time.

Each reader must have a time zone value entered during programming. When a reader is not authorized in an access zone, enter Time Zone 0 in that reader field.

CMD 117 allows one or more time zones to be changed for a specified reader without affecting the time zone setting of any other reader(s).

Refer to CMD 17 for a convenient method to add standard access zones with one time zone for all doors.

Example:

```
START 124 * 10 * 1 * 40 * 0 * 1 * 5 * 0 * 0 * 0 * 0 #
START 124 * 10 * 2 * 65 * 65 * 65 * 65 * 65 * 65 * 65 * 65 #
```

Assign Standard Access Zone 10 To Time Zone 40 on Reader 1, TZ 0 on Reader 2 5 6 7 & 8, TZ 1 on Reader 3, TZ 5 on Reader 4, and TZ 65 on Readers 9-16.

Related CMDs:

- CMD 88*3, 88*4, 88*14 - Print Standard, Master, Grand Master Time Zones
- CMD 88*5 - Print Standard Access Zone Setups
- CMD 188*5 - Print Setup Changes for Standard Access Zones

Access Zone Setups

CMD 17 – Define Standard Access Zone (1-64), 1 Time Zone, Selected Doors
CMD 24 – Define Standard Access Zone (1-64), 1 Time Zone Per Door
CMD 117 - Define Standard Access Zone (1-64), 1 Time Zone Per Door, Specified Doors
CMD 204 – Define Master Access Zone (66-127)
CMD 249, 349 – Tag/Alert Access Zone

Time Zone Setups

CMD 52, 54, 56, 154, 454 – Define/Clear Standard, Master Time Zones

Holiday Setups

CMD 57 – Define Holiday

CMD 140: SET REPORT BUFFER ALARM THRESHOLD

Syntax: `START 140 * Report Buffer Alarm Threshold #`

Description:

This Command is part of the Remote Site Management feature set. It establishes the quantity of alarm events in either the standard on-board alarm buffer or the optional expanded alarm buffer that will cause the controller at the remote site to dial the Host PC.

The standard on-board buffer can hold up to 100 alarm events so its threshold setting can be from 1 event to 100 events. The expanded buffer can hold up to 22,300 events so its setting can be from 1 event to 22,300 events.

Examples:

```
START 140 * 50 #
```

Dial Host When 50 Alarm Events Are In the Standard Buffer

```
START 140 * 1000 #
```

Dial Host When 1,000 Alarm Events Are In the Expanded Buffer

Default:

Report Buffer Threshold = None

Related CMDs:

- CMD 88*23 – Print Reporting Setups
- CMD 188*4 – Print Setup Changes for Reporting and Duress

Alarm Setups

CMD 261 – Define Alarm Actions
CMD 146 – Disable Passback and Occupancy Control During Time Zone

CMD 146: DISABLE PASSBACK AND OCCUPANCY CONTROL DURING TIME ZONE

Syntax: `START 146 * Time Zone #`

Description:

This command enables passback controls to be disabled during a specified time zone. This is often used to disable passback controls during shift changes, lunch periods, or other times of high traffic to reduce the number of inadvertent passback violations. The controller automatically issues a forgive all users just prior to re-enabling passback. This command also disables occupancy counting and controls during the specified time zone.

This means that if the controller has been programmed to respond in an automatic mode to occupancy counts, such as mask or unmask an area, or go from 2-person access rule to 1-person access rule, then these features will not be operational during the specified time zone. The controller automatically issues a forgive all users just prior to re-enabling occupancy controls which means it sets the inside user count for the controlled area to zero.

Example:

```
START 146 * 1 #
```

Disable Passback And Occupancy Controls During Time Zone 1

Default:

Passback Disabled During Time Zone 0 (Never)

Related CMDs:

- CMD 88*2 – Print System Information
- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*11 – Print Keypad/Match Setups and Status
- CMD 188*9 – Print Setup Changes for Passback & User Management

Passback Functions

CMD 03*7, 03*8, 03*9, 03*10 – Change Reader Functions (Passback)
CMD 46 – Change Passback Mode

Time Zone Setups

CMD 52, 54, 56 – Define/Clear Standard, Master Time Zones

CMD 149: ALERT USER OR RANGE OF USERS

Syntax: `START 149 * NN * Starting User Number * Ending User Number #`

Variables: NN

0 Alert NO
1 Alert YES

Description:

Alert a user is utilized to notify a user that a special condition exists such as: a message is waiting, a new code is to be issued, a briefing is scheduled, a meeting is required, etc.

The alert is sounded as 4 short beeps of the ScramblePad Keypad's alarm annunciator when the user enters their valid code at any ScramblePad Keypad in the system. Alert does not work on a MATCH reader unless it is at a dual technology reader which includes a ScramblePad. The alert for the specified user is active until it has been turned off.

The alert message does not trigger any relays.

Example:

```
START 149 * 1 * 100 * 100 #
```

Alerts User 100

Default:

No users are alerted

Related CMDs:

CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes

CMD 35, 36, 38, 330*11 – Print User, Users, or Family of Users with Codes

Tag and Alert Setups

CMD 49 – Tag any User or Range of Users
CMD 249, 349 – Tag/Alert Access Zone
CMD 449, 549 – Tag/Alert Control Zone

CMD 154: DEFINE GRAND MASTER TIME ZONE (130-149)

Syntax: `START 154 * STZ/MTZ * Grand Master Time Zone * Column #`

Description:

A Grand Master Time Zone (GTZ) is used for special time management control applications when multiple time zones are required to manage access, alarms or relays with frequent and complex time changes. A grand master time zone consists of up to 8 standard (STZ) or master time zones (MTZ).

The printed Grand Master Time Zone Report appears as follows:

	Time Zones - Column								
GTZ	1	2	3	4	5	6	7	8	
130	0	0	0	0	0	0	66	0	Inactive
131	67	0	68	94	0	0	0	0	Active

Notice that GTZ 130 has 7 time zones set to 0 (zero), never, and 1 set to MTZ 66, and its current status is inactive.

GTZ 131 has several time zones programmed in columns 1, 3 and 4. One of these time zones contains a time zone which has a start time and end time that includes the current time so that zone is active.

Example:

```
START 154 * 66 * 130 * 7 #
```

Add Master Time Zone 66 To Column 7 of Grand Master Time Zone 130

Default:

None

Related CMDs:

CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones

CMD 188*10 – Print Setup Changes for Time Zones

Time Zone Setups

CMD 52, 54, 56, 454 – Define/Clear Standard, Master Time Zones

CMD 170: ENABLE EXPANSION LINE MODULE INPUT

Syntax: `START 170 * Expansion Input #` (Version 6.6 or earlier)
`START 170 * Expansion Input [* Exp. Input...* Exp. Input] #` (Version 7)

Description:

Expansion line module inputs are factory set to be enabled to sense the alarm devices attached to the required DTLM or MELM on start-up. Unused inputs should be disabled with Command 171.

When an expansion line module input is set to report as an alarm, as it is on factory setup, it will report the following conditions:

- ❑ Secure
- ❑ Alarm
- ❑ Mask Request Granted
- ❑ Open
- ❑ Short
- ❑ Excessive Noise
- ❑ Line Out Of Spec
- ❑ Tamper (DTLM3/MELM3 Only)

When the line module input is set to report as a door with CMD 186, the alarm will report as a Door Forced Open and as Door Open Too Long. All other reporting remains the same.

When a Request To Exit (RQE) push button or sensor is activated it will mask the line module input for the door mode time. When a line module input is masked by a time zone or by an alarm masking code, or is masked when a relay is actuated by an access code, unlock code, time zone or control code, only the door forced or line module input report is masked. All other reporting remains active.

Note: When an Input is disabled, all reporting is off and the associated RQE will not work.

Using V7.0, you can enable or disable up to 8 expansion inputs all at once as shown in the extended arguments. V7.0 also supports a new alarm expansion board type, AEB, that enables you to install up to four input expansion boards—and up to 32 expansion inputs—into one controller.

Example:

```
START 170 * 1 #
```

Enable Expansion Line Module Input 1 To Report Alarms

```
START 170 * 2 * 3 * 4 * 15 * 16 #
```

For V7.0, this enables Expansion Alarm Input 2, 3, 4, 15, and 16 to Report Alarms.

Default:

Enabled

Related CMDs:

- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 171 – Disable Expansion Line Module Input
CMD 172 – Change Expansion Line Module Input

CMD 173 – Change Expansion RQE (Request To Exit)
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked
CMD 176 – Mask Expansion Line Module Input during Time Zone
CMD 180 – Change Door Time for Expansion Line Module Input

CMD 171: DISABLE EXPANSION LINE MODULE INPUT

Syntax: `START 171 * Expansion Input #` (Version 6.6 or earlier)
`START 171 * Expansion Input [* Exp. Input... * Exp. Input] #` (Version 7)

Description:

Expansion line module inputs are factory set to be enabled to sense the alarm devices attached to the required DTLM or MELM on start up. Unused Inputs should be disabled with this command.

With V7.0, you can enable or disable up to 8 expansion inputs at once using the extended arguments.

When disabled, all reporting is off.

Note: When an Input is disabled, all reporting is off and the associated RQE will not work.

Example:

`START 171 * 1 #`

Disable All Alarm Reporting From Expansion Line Module Input 1

START 171 * 2 * 3 * 4 * 15 * 16 #

For Version 7.0 and above, disables all alarm reporting from Expansion Alarm Input 2, 3, 4, 15, and 16.

Default:

Enabled

Related CMDs:

- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 170 – Enable Expansion Line Module Input

CMD 172: CHANGE EXPANSION LINE MODULE INPUT

Syntax: `START 172 * NN * Expansion Input #`

Variables: NN

1 Normally Open (When Secure)
2 Normally Closed (When Secure)

Description:

Alarm sensor inputs are usually Normally Closed switches when secure and open on alarm. They may be set to Normally Open for sensors whose contacts are normally open when secure.

Example:

```
START 172 * 1 * 1 #
```

Change Expansion Line Module Input 1 To Normally Open When Secure

Default:

Normally Closed

Related CMDs:

CMD 88*20 – Print Expansion Alarm/RQE Setups and Status

CMD 88*21 – Print Expansion Alarm Special Setups and Status

CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 173 – Change Expansion RQE (Request To Exit)
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked
CMD 176 – Mask Expansion Line Module Input during Time Zone

CMD 173: CHANGE EXPANSION RQE

Syntax: `START 173 * N * Expansion Input #`

Variables: N

1 RQE Re-Triggers Mask While Activated
2 RQE Triggers Mask Once When Activated
3 RQE OFF

Description:

Each RQE input is factory set to OFF.

The RQE will trigger the masking of the input once unless it is set to continuously trigger for as long as it is activated.

Note: An expansion RQE cannot trigger an expansion relay.

Expansion line module inputs set to operate/report as a door can be used to monitor auxiliary doors such as emergency fire exits. These doors may be authorized employee exits but not entrances. The RQE input would be used to mask the door forced alarm upon authorized exit. Door Open Too Long alarm reporting also operates on expansion line module inputs reporting as doors.

Expansion line module inputs are set to report as zone alarms from the factory. In this case the RQE reports as Mask Request Granted. This enables local masking from high security key switches or other normally open switch devices.

Note: A DTLM2/3 or MELM2/3 is required.

Examples:

```
START 173 * 1 * 1 #
```

Change RQE on the expansion input 1 to re-trigger masking

Default:

RQE OFF

Related CMDs:

- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 88*22 – Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 172 – Change Expansion Line Module Input
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked
CMD 176 – Mask Expansion Line Module Input during Time Zone

CMD 174: CHANGE EXPANSION DOOR OPEN TOO LONG TIME

Syntax: `START 174 * DOTL Time * Expansion Input #`

Description:

Any expansion line module input may be set up to report as a door. The unauthorized opening of a door is reported as a Door Forced Open. The door is also monitored for being held Open-Too-Long beyond an adjustable time delay of 0-8100 (0=Off) seconds. Both door alarm conditions report on the printer and trigger the alarm relay.

The Door-Open-Too-Long timer starts at the end of the door mode timer. For example, if the door unlock timer is set to 6 seconds and the door is held open, the DOTL timer starts after the 6 second door unlock time expires. If the DOTL Timer is set to 10 seconds the alarm will sound after 16 seconds total time has expired.

Note: A DTLM/MELM is required.

Example:

```
START 174 * 15 * 1 #
```

Define Door-Open-Too-Long Alarm Delay To 15 Seconds For Expansion Input 1

Default:

12 seconds

Related CMDs:

- CMD 88*10 – Print Door Setups and Status
- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 88*22 – Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 172 – Change Expansion Line Module Input
CMD 173 – Change Expansion RQE (Request To Exit)
CMD 175 – Expansion DOTL Active While Input Unlocked
CMD 176 – Mask Expansion Line Module Input during Time Zone
CMD 282 – Define Special Needs Unlock Extension Time

CMD 175: EXPANSION DOTL ACTIVE WHILE INPUT UNLOCKED

Syntax: `START 175 * N * Expansion Input #`

Variables: N

0 NO
1 YES
2 NO (for V6.5 and earlier)

Description:

Any expansion line module input can be set up to report as a door. The door held open alarm will not report on an expansion input masked by time zone or code. It may be made to report on a masked input by making DOTL active when the input unlocked by an unlock code, momentary mask code, or RQE retriggers.

If the input associated with the door is masked by a code or time zone, then a DOTL alarm will not report even if the DOTL is active while the door is unlocked.

Note: A DTLM/MELM is required.

Example:

```
START 175 * 1 * 1 #
```

Sets DOTL Alarm Reporting Always On Even When Expansion Input 1 Is Legally Unlocked By an Unlock Code Or By A Momentary Mask Code. Protects Fire Doors From Being Propped Open When “Unlocked”.

Default:

NO

Related CMDs:

- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 88*22 – Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 172 – Change Expansion Line Module Input
CMD 173 – Change Expansion RQE (Request To Exit)
CMD 174 – Change Expansion Door Open Too Long Time
CMD 176 – Mask Expansion Line Module Input during Time Zone

CMD 176: MASK EXPANSION LINE MODULE INPUT DURING TIME ZONE

Syntax: `START 176 * Time Zone * Expansion Line Module Input #`

Description:

Expansion line module inputs may be automatically masked during specific times of the day to disable alarm reporting. Line trouble reporting is not disabled during alarm masking. Masking is removed by setting an input's masking time zone to 0 (zero).

Note: A DTLM/MELM is required.

Example:

```
START 176 * 1 * 1 #
```

Masks Alarm Reporting On Expansion Line Module Input 1 During Time Zone 1

Default:

Time Zone 0 (No Automatic Masking)

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Time Zone Setups

CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 172 – Change Expansion Line Module Input
CMD 173 – Change Expansion RQE (Request To Exit)
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked

CMD 180: CHANGE DOOR TIME FOR EXPANSION LINE MODULE INPUT

Syntax: `START 180 * Door Timer * Expansion Line Module Input #`

Description:

The expansion line module inputs masking time is set up with the door timer.

Any expansion line module input may be set to operate and report as a door or as an alarm. Each input may be assigned to an access zone or to a control zone, or to both, depending on how the input is to be controlled.

When assigned to an access zone for one-ScramblePad/MATCH Reader-to-one-input type control, the access code used to mask an input uses the door timer as the masking timer. When assigned to a control zone for any-ScramblePad/MATCH Reader-to-any-input type control, the control code used to mask the input also uses the door timer as the masking timer.

The door time is momentary with an adjustable time of 0-8100 seconds (0=Toggle). An expansion line module input's door timer is used by access codes and the RQE input.

For more information on expansion input control time, see CMD 181.

Example:

```
START 180 * 10 * 1 #
```

Change Door Time To 10 Seconds For Expansion Line Module Input 1

Default:

6 seconds

Related CMDs:

- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 88*22 – Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Adding Users
CMD 10, 19-22, 310-315, 320-322 – Add Access Users
CMD 15, 40, 41, 44 – Add Control Users

Alarm Setups
CMD 170, 171 – Enable, Disable Expansion Line Module Input

Relay Setups
CMD 181 – Change Control Time for Expansion Relay

CMD 181: CHANGE CONTROL TIME FOR EXPANSION RELAY

Syntax: `START 181 * Control Time * Expansion Relay #`

Description:

The control time determines how long an expansion relay will be actuated by a control code or by an alarm or relay triggered control zone. The control time may be momentary with an adjustable time of 1-8100 seconds. It can toggle ON and OFF on consecutive trigger code entries if the timer is set to 0 (zero) seconds.

A relay's control time is used by control codes as well as by a line module input or relay to trigger a control zone.

For more information on the door timer for expansion inputs, see Command 180.

Example:

```
START 181 * 10 * 1 #
```

Change Control Time To 10 Seconds For Expansion Relay 1

Default:

6 seconds

Related CMDs:

- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 88*28 – Print Virtual Relay Setups and Status
- CMD 188*15 – Print Setup Changes for Expansion Relays

Adding Users

CMD 10, 19-22, 310-315, 320-322 – Add Access Users
CMD 15, 40, 41, 44 – Add Control Users

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 180 – Change Door Time for Expansion Line Module Input

Relay Setups

CMD 181 – Change Control Time of Relay

CMD 182: TIME ZONE CONTROL OF EXPANSION RELAY

Syntax: `START 182 * N * Expansion Relay * Time Zone #`

Variables: N

1 Actuate Relay During Time Zone
2 Disable Relay During Time Zone
3 Clear Relay At End Of Time Zone

Description:

Expansion relays may be actuated during a time zone, going on at the start time of the zone and off at the end time of the zone.

Expansion relays may be disabled during a time zone, becoming disabled at the start of the zone and reenabled at the end of the zone.

The current state of any relay may be auto-cleared at the end of a time zone to insure the automatic reset of a lower priority code activated event without the need for a manual resetting of the event.

Examples:

```
START 182 * 1 * 1 * 1 #
```

Auto-Actuate Expansion Relay 1 During Time Zone 1

```
START 182 * 2 * 1 * 5 #
```

Auto-Disable Expansion Relay 1 During Time Zone 5

```
START 182 * 3 * 6 * 1 #
```

Auto-Clear Expansion Relay 6 At The End Of Time Zone 1

Default:

Actuate Relay during Time Zone 0 (Never)

Disable Relay during Time Zone 0 (Never)

Clear Relay at the end of Time Zone 0 (Never)

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 88*19 – Print Detailed Expansion Relay Status Only
- CMD 88*28 – Print Virtual Relay Setups and Status
- CMD 188*15 – Print Setup Changes for Expansion Relays

Adding Control Users

CMD 15 – Add Keypad Unlock/Relock User (IDF 1)
CMD 40 – Add Keypad Relay Control User
CMD 41 – Add Keypad Top-Priority Relay Control User (IDF 1)

Time Zone Setups

CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones

Alarm Setups

CMD 180 – Change Door Time for Expansion Line Module Input
CMD 183 – Clear Time Zone Control of Expansion Relay

CMD 183: CLEAR TIME ZONE CONTROL OF EXPANSION RELAY

Syntax: `START 183 * Expansion Relay #`

Description:

Time zone control of any expansion relay can be cleared and reset to none.

Use CMD 88 * 18 to print the current status of expansion relays. This is the best method to determine why a relay is performing in a certain way on a code entry or other event. See Chapter 5 for more information on this 88 command.

Example:

```
START 183 * 1 #
```

Clear Time Zone Control Of Expansion Relay 1 To None

Default:

None

Related CMDs:

- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 188*15 – Print Setup Changes for Expansion Relays

Time Zone Setups
CMD 52, 54, 56, 154, 454 – Define/Clear Standard, Master, Grand Master Time Zones

Alarm Setups
CMD 180 – Change Door Time for Expansion Line Module Input

Relay Setups
CMD 182 – Time Zone Control of Expansion Relay

CMD 184: EXPANSION LINE MODULE INPUT TRIGGERS CONTROL ZONE

Syntax: `START 184 * N * Expansion Line Module Input * Control Zone #`

Variables: N

1 Triggers
2 Re-Triggers
3 Actuate
4 Disable

Description:

Any expansion line module input can trigger any control zone. To cancel an alarm trigger of a control zone set the specified input to trigger control zone 0 (none). To trigger a control zone means to start the zone's relay control timers at the moment the alarm occurs. The relay timers will start and time out even if the alarm stays active. To retrigger means that the relay timers are not started until the alarm event restores. To actuate a control zone means to actuate its relays for as long as the alarm is active and release them the moment the alarm restores.

The relay timers are ignored when 'actuate' is used. To disable means the relays are disabled while the alarm is active. Once it restores the disabled state is cleared. If the relays have control delays programmed, they will be recognized by the trigger and retrigger controls but not by the actuate and disable controls.

This feature allows special control capabilities such as turning on perimeter lights when an alarm is triggered, or for annunciation of a specific line module input, or control of HVAC and lighting systems. When using a master control zone in this command, master control zones can only be *triggered*, not retriggered, actuated, or disabled.

Example:

```
START 184 * 1 * 1 * 1 #
```

Line Module Input 1 Triggers Control Zone 1

Default:

None

Related CMDs:

- CMD 88*6 – Print Standard Control Zone Setups
- CMD 88*16 – Print Master Control Zone Setups
- CMD 88*17 – Print Detailed Relay Status Only
- CMD 88*19 – Print Detailed Expansion Relay Status Only
- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Relay Setups
CMD 81 – Change Control Time of Relay
Alarm Setups
CMD 84 – Line Module Input Triggers Control Zone

CMD 185: CHANGE FUNCTION OF EXPANSION RELAY

Syntax: `START 185 * N * Expansion Relay #`

Variables: N

0 Relay Rests OFF
1 Relay Rests ON
2 Relay Rests OFF (for V6.5 and earlier)

Description:

The operation and outputs of each relay may be inverted. On system start up they rest in the de-energized, or OFF state and the outputs are as marked on the circuit board. Each relay may be changed to rest in the energized or ON state which inverts the meaning of the outputs: the normally opened contact becomes the normally closed contact.

For example, when controlling elevators, always change the relays to resting ON. This ensures that if the control system power fails, the relay coil will be de-energized, falling to the OFF condition, thereby allowing the elevator to be used.

Examples:

```
START 185 * 1 * 1 #
```

Change Expansion Relay 1 To Rest ON For Elevator Control

Default:

Relay Rests OFF

Related CMDs:

- CMD 88*17 – Print Detailed Relay Status Only
- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 88*19 – Print Detailed Expansion Relay Status Only
- CMD 88*28 – Print Virtual Relay Setups and Status
- CMD 188*15 – Print Setup Changes for Expansion Relays

Relay Setups

CMD 81 – Change Control Time of Relay
CMD 85 – Change Operation for Selected Relays

CMD 186: CHANGE EXPANSION LINE MODULE INPUT REPORTING MODE

Syntax: `START 186 * N * Expansion Line Module Input #`

Variables: N

1 Report As A Door
2 Report As An Alarm

Description:

Any expansion line module input may be set up to report as a door or as an alarm zone. Each input may be assigned to an access zone, control zone, or both, depending on how the input is to be controlled.

When set to report as a door, the input will report Door Forced Open and Door Open Too Long alarms. This can provide monitoring and reporting of secure emergency exit doors. If these doors are to be used for authorized exit, they should be equipped with RQE push button or motion sensors to mask the Door Forced Alarm condition. If they are held open too long, a DOTL alarm will occur.

Each of these doors can be equipped with a ScramblePad and controlled with an access code. This enables *access by alarm* on these doors. Opening them without a code will cause a Door Forced Alarm. They can also be controlled from a central ScramblePad after an intercom request from the door location. An access request to a central office would enable an operator to enter a code to momentarily mask the specific door authorized for use.

When set up as an alarm zone, the input will report alarm and alarm active too long conditions. The alarm report occurs when the input is first tripped. An AATL alarm functions like a DOTL alarm on a door. If a code has been entered to mask a line module input momentarily but the sensor stays tripped after the momentary mask time expires, an AATL will be reported.

Example:

```
START 186 * 1 * 1 #
```

Expansion Line Module Input 1 Reports As A Door

Default:

Report as an Alarm

Related CMDs:

- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 88*22 – Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked

CMD 187: EXPANSION RELAY TRIGGERS CONTROL ZONE

Syntax: `START 187 * N * Expansion Relay * Control Zone #`

Variables: N

1 Triggers
2 Retriggers

Description:

Any expansion relay can trigger any control zone. To cancel a relay trigger of a control zone set the specified input to trigger Control Zone 0 (none). To trigger a control zone means to start the zone's relay control timers at the moment the expansion relay changes state. The relay timers will start and time out even if the relay stays actuated. To retrigger means that the relay timers are not started until the relay reverts back to its resting state.

This feature allows special control capabilities such as shunting other alarm panels when a relay is triggered, or for annunciation of a specific relay output, or control HVAC and lighting systems. When using a master control zone in this command note that master control zones can only be *triggered*, not retriggered, actuated, or disabled.

Example:

```
START 187 * 1 * 2 * 6 #
```

Expansion Relay 2 Triggers Control Zone 6

Default:

None

Related CMDs:

- CMD 88*16 – Print Master Control Zone Setups
- CMD 88*17 – Print Detailed Relay Status Only
- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 88*19 – Print Detailed Expansion Relay Status Only
- CMD 88*28 – Print Virtual Relay Setups and Status
- CMD 188*15 – Print Setup Changes for Expansion Relays

Control Zone Setups

CMD 45 – Define Standard Control Zone
CMD 84 –Line Module Input Triggers Control Zone
CMD 184 – Expansion Line Module Input Triggers Control Zone

Relay Setups

CMD 181 – Change Control Time for Expansion Relay

CMD 188: PRINT COMMAND SETUPS

Syntax: `START 188 * NN * [NN...] #`

Variables: NN

0	System Setups Command Report	
1	Clock Setups	CMD 50 - 51
2	Holiday Table Setups	CMD 57 - 59
3	Keypad Setups	CMD 3, 103 - 104
4	Reporting Mode Setups	CMD 05-09, 18, 105-109, 140, 191-195
5	Standard Access Zone Setups	CMD 17, 24, 117, 201, 203, 217, 249, 349
6	Master Access Zone Setups	CMD 204, 217, 249, 349
7	Standard Control Zone Setups	CMD 45, 301-303, 345
8	Master Control Zone Setups	CMD 304-307
9	Passback & User Management Setups	CMD 46, 146, 235-238, 255-257
10	Standard Time Zone Setups	CMD 52, 54, 56, 154
11	Alarm Action Control Blocks Setups	CMD 261
12	Alarm & Sense Input Setups	CMD 70-77, 84, 110, 112, 270
13	Expansion Line Module Input Setups	CMD 111, 113, 170-176, 180, 184, 186
14	Relay Setups	CMD 79-83, 85-87, 280-281
15	Expansion Relay Setups	CMD 181-183, 185, 187

Any setup changed using one of the commands cited above will be reported by CMD 188.

Description:

Use this command to print a full or partial report list of changes made to setups since cold start. For a complete list of all setup values, refer to CMD 88.

Printing the date, time and version prints the current date, time and the controller's CCM Version Number.

Printing the standard time zones prints a list of all standard time zones defined with their starting time, ending time and days, and their current active or inactive state. Printing the master time zones prints a list of any of the master time zones which have been assigned standard time zones and their current active or inactive state. Printing the access zones or control zones prints their time zone and door/relay setups.

Printing the relays prints the relay setup tables and the relay status display. The detailed report shows the exact current status of each relay changed since cold start.

Printing the alarm and sense inputs prints a list of alarm and sense inputs modified from default and their current state. Printing the keypads/MATCH values prints the keypads/MATCH reader setup tables. Printing the holidays prints the holiday list.

For Version 6.6 and later, this command allows printout of up to ten arguments.

For a complete list of values generated when you use one or more of these command variations, refer to "Print Setup Guide" starting on page 5-35.

Note: No sensitive information is contained in these printouts.

Examples:

```
START 188 * 0 #
```

Print a list of all system components modified since cold start

```
START 188 * 2 #
```

Prints the CMD 57's used to set up all holiday tables.

```
START 188 * 10 * 14 #
```

Prints list of all Time Zones and Relays changed since cold start

Defaults:

None

Related CMDs:

- CMD 36 – Print Users with Codes
- CMD 88 – Print List of All Current Values
- CMD 260 – Print Alarm Action(s)

See Chapter 5 for more on Commands 88 and 188.

CMD 191: CHANGE PAGE LENGTH FOR PRINTER

Syntax: `START 191 * LINES #`

Description:

All DIGI*TRAC controllers include the capability to print in different languages. To accommodate these languages, different countries will use different paper lengths for their standard computer paper. For instance, the standard European paper size is A4. In addition, some companies use larger or smaller paper formats, like legal size or A4, in their system printers, allowing the controller to print more lines or fewer lines of text on a page.

Use this command to specify the number of lines per page you require for your system printer.

The default page length is the American standard for 8.5 x 11: 58 lines per page.

Example:

```
START 191 * 66 #
```

Print 66 Lines per page

```
START 191 * 0 #
```

Never form-feed the printer (this is the default)

Default:

0 lines per page (never form feed printer)

Related CMDs:

- CMD 88*23 – Print Reporting Setups
- CMD 188*4 – Print Setup Changes for Reporting and Duress

CMD 192: CHANGE PROGRAMMING MODE TIMEOUT INTERVAL

Syntax: `START 192 * Time-out Time #`

Description:

To program stand-alone controllers, programming mode is invoked at a ScramblePad. Normally, CMD 99 is used to quit Programming Mode manually at the end of a programming session. However, if the operator forgets to quit programming mode, the controller will automatically time out and return to normal entry mode after 8 minutes without command activity on the programming ScramblePad.

Use this command to change the time-out interval from the 8 minute default to any interval from 2 - 20 minutes.

*Note: This setting does not affect the S*NAP PC.*

Example:

```
START 192 * 15 #
```

Change Programming Mode Time-out to 15 minutes

Default:

8 minutes

Related CMDs:

CMD 88*2 – Print System Information

CMD 188*4 – Print Setup Changes for Reporting and Duress

CMD 01, 13*0 – Change System (User 0) Code
CMD 02 – Add Programming Pass/word
CMD 99 – Quit Programming

CMD 193: SET HOST PHONE NUMBER

Syntax: `START 193 * N * Phone Number #`

Variables: N

1 First Number
2 Second Number
3 Third Number
4 Fourth Number

Description:

Use this command to configure up to four host phone numbers a controller at a remote site can call. Each phone number can contain up to 16 digits.

Most networks only have a single main site phone number; however, this feature accepts up to 4 phone numbers as alternate numbers which can be called if the first number is either busy or out-of-service.

The controller at the remote site will dial the first number first. If there is only one number programmed, it will continue to dial until the call has been completed. If a second, third or fourth number has been programmed into the controller, it will automatically rotate through the numbers until the call has been successfully completed. This allows for an emergency backup host to receive calls from remote sites if the primary host at the main site is either busy or off-line.

This command is part of the *Remote Site Management* feature set.

Examples:

```
START 193 * 1 * 17142509990 #
```

Sets Phone Number 1 to 714 250-9990

```
START 193 * 2 * 18005551212 #
```

Sets Phone Number 2 to 1 800 555-1212

Default:

None (no phone numbers are preset)

Related CMDs:

CMD 88*24 – Print Remote Site Management Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Modem Setups

CMD 90*2, 97*2, 97*4, 97*8 – Host Setup Commands
CMD 108 – Time Zone Control of Modem
CMD 194 – Select Tone or Pulse Dialing
CMD 195 – Change Host Call-Back

Alarm Setups

CMD 261 – Define Alarm Actions

CMD 194: SELECT TONE OR PULSE DIALING

Syntax: `START 194 * N #`

Variables: N

1 Tone Dialing
2 Pulse Dialing

Description:

This command enables the modem at the remote site to communicate with either a Tone or Pulse Dialing phone system.

This Command is part of the *Remote Site Management* feature set.

Examples:

```
START 194 * 2 #
```

Sets Modem to Pulse Dialing

Default:

Tone Dialing

Related CMDs:

CMD 88*24 – Print Remote Site Management Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Modem Setups

CMD 90*2, 97*2, 97*4, 97*8 – Host Setup Commands
CMD 108 – Time Zone Control of Modem
CMD 193 – Set Host Phone Number(s)
CMD 195 – Change Host Call-Back

Alarm Setups

CMD 261 – Define Alarm Actions

CMD 195: CHANGE HOST CALL-BACK

Syntax: `START 195 * N #`

Variables: N

0 Disable
1 Enable
2 Disable

Description:

Use this command to force an automatic call-back from the controller(s) at the remote site to the host at the main site whenever the host initiates a call to the remote site. This insures that the call originates from the host at the main site, not from an unknown host attempting an unauthorized logon to a controller at the remote site.

This command is part of the *Remote Site Management* feature set.

Some networks do not allow remote site management from multiple hosts. If this operation is needed, do not enable host call-back.

On some networks the remote site is billed for phone changes related to communications between it and the main site. Enable host call-back if this mode of operation is needed.

Comment:

In V6.5, you had to turn the host call-back feature on (“dialoutonly”), then use 198*4*0*0*0*0# to trigger the actual dial-back from the panel. There could be complications: if this feature was enabled but the host didn't send CMD 198*4, nothing would happen: it wouldn't let the host “log on.” With v6.6 and later, attempting to log on triggers a dial-back, exactly as if a 198*4 command were sent.

The host call back mode must also be enabled on the S*NAP PC under host setups.

Examples:

```
START 195 * 1 #
```

Enables Host Call Back

Default:

Disabled (195*2)

Related CMDs:

CMD 88*24 – Print Remote Site Management Setups

CMD 188*4 – Print Setup Changes for Reporting and Duress

Modem Setups

CMD 90*2, 97*2, 97*4, 97*8 – Host Setup Commands
CMD 108 – Time Zone Control of Modem
CMD 193 – Set Host Phone Number(s)
CMD 194 – Select Tone or Pulse Dialing

Alarm Setups

CMD 261 – Define Alarm Actions

CMD 200: CHANGE PRINTER LANGUAGE

Syntax: `START 200 * N #`

Variables: N

0 English
1 Unused
2 Dutch
3 Français
4 Español
5 Unused

Description:

The DIGI*TRAC controllers all include the capability of printing in different languages. The standard local parallel printer, as well as the optional remote serial printer using the Serial Communications Interface Board (SCIB), will both be affected by the language selection.

The change in printed language affects the presentation of all transactions, alarms, programming commands and responses and reports, but does not affect the system setup & status printouts. Switching between languages can be performed at any time and does not affect controller operation in any way.

Once a language is selected it is advisable to use Command 00 * 0 to print the entire built-in set of programming commands as a hard copy reference in the new language.

*Note: The Language change will not affect the S*NAP PC display or printer.*

Example:

```
START 200 * 2 #
```

Print Dutch

Default:

0 (English)

Related CMDs:

CMD 88*2 – Print System Information

CMD 204: DEFINE MASTER ACCESS ZONE (66-127)

Syntax: `START 204 * Standard Access Zone * Master Access Zone * Col. 1-8 #`

Description:

A master access zone (MAZ) can be defined with up to eight standard access zones assigned to it. This provides a convenient way for special access authority to be created for high level groups of users, such as corporate management requiring access to multiple locations throughout a site, region, or country.

To remove a standard access zone from a master access zone, use this command to redefine the specified master access zone.

The printed master access zone report appears as follows:

Standard Access Zones – Column								
MAZ	1	2	3	4	5	6	7	8
66	0	9	0	0	0	0	12	0
67	61	0	29	12	0	4	0	0

Note: Master Access Zone 66 has two standard access zones defined in Columns 2 and 7. Master Access Zone 67 has 4 standard access zones defined.

A master access zone consists of up to eight standard access zones, plus tag and alert flags. V6.6 and 6.6 provide up to four extension flags to handle SNUX conditions, two-person rules, and anti-passback options. In V7.0 these flags are moved to the user code records.

Two-person rule and anti-passback do not work in combination with each other for any Hirsch software using version 7.1.11. One person's passback status is updated but not the other.

The Special Needs Extended Unlock (SNUX) condition prolongs the interval when the door is unlocked. This is used for wheelchairs, deliverymen, or other requestors who generally take more time to enter or exit a door than an average individual. Door mode, door open, and door delay times can all be extended. This is used with CMD 282.

Example:

```
START 204 * 9 * 66 * 2 #
START 204 * 12 * 66 * 7 #
```

Define Master Access Zone 66 to include Standard Access Zone 9 in Column 2 and Standard Access Zone 12 To Column 7

Default:

None

Related CMDs:

CMD 88*15 – Print Master Access Zone Setups

CMD 188*6 – Print Setup Changes for Master Access Zones

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)

CMD 217: CLEAR ACCESS ZONE

Syntax:

```
START 217 * Access Zone #
START 217 * First Access Zone * Last Access Zone #
```

Description:

Any access zone—standard or master—can be cleared or erased with this command, except AZ0 and AZ65.

In V6.6 and later, you can also set a range of access zones to clear.

Example:

```
START 217 * 1 #
```

Clear Access Zone 1

```
START 217 * 23 * 27 #
```

Clear Access Zones 23 through 27

Default:

None

Related CMDs:

- CMD 88*5 – Print Standard Access Zone Setups
- CMD 88*15 – Print Master Access Zone Setups
- CMD 188*5 – Print Setup Changes for Standard Access Zones
- CMD 188*6 – Print Setup Changes for Master Access Zones

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)
CMD 249, 349 – Tag/Alert Access Zone

CMD 220: BATCH-ADD ACCESS USERS - ENROLL CARD ONLY (IDF 2)

Syntax:

```
START 220 * Starting Users No. * No. of Users * Access Zone #
Card
Card
 ..
 ..
 ..
Card
```

Description:

Use this command to enroll a sequence of card-only users. Batch-adding is a convenient way to enroll many users into the controller in a single programming session. It can be used to pre-add users to a controller for future issuance by adding them with Access Zone 0 (zero). When issued to a user, simply change the access zone from zero, no access, to the required access zone.

Any number of users can be added in sequence by using this command. Since this is a batch command, you don't have to reenter the entire command syntax between each new user of the same access zone. Once this batch-add command is started, each additional card is swiped in the reader in sequence until all new users are added.

Note: Be sure to watch the card reader status LED when enrolling each card. A rapid flicker means a bad card read has occurred and requires the misread card to be re-swiped.

Once each card is enrolled, a new user record is printed. You can verify that a card has been successfully enrolled by using CMD 316 to test a card and trigger a relay.

The users are added from the specified user number and fill in any available user number required to complete the process, skipping any existing users. The command automatically terminates when the specified number of new users has been enrolled or after the programming mode time-out expires or by using CMD 96.

Examples:

```
START 220 * 45 * 15 * 1 #
```

Swipe 15 Cards. Add 15 Card Only Access Users With Access Zone 1 Starting at User 45

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

Adding and Changing Users

CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 224 – Batch-Change Card for Existing Users (IDF 2, 5, 6, 7)
CMD 225 – Batch-Restore Users
CMD 310 – Add Access User Card Only (IDF 2)

CMD 223: BATCH-ENROLL CARD TO EXISTING USERS (IDF 5, 6, 7)

Syntax:

```
START 223 * Starting User Number * Ending User Number #
Card
Card
 ..
 ..
 ..
Card
```

Description:

This command enables batch-enrolling of cards for existing users. It is the second step in a two-step process: the first step auto-adds users through CMDs 320, 321, or 322. Batch-enrolling is a convenient way to enroll cards for many users in a single programming session without tedious, error-prone manual data entry.

Any number of user's cards can be enrolled in sequence by using this command.

Note: For convenience, you do not have to re-enter the entire command syntax between each user.

Once the batch-enroll command is started, each card to be enrolled is swiped in the reader until all users are enrolled. The command automatically terminates when the specified range of user's cards have been enrolled. This command can be terminated at any time using CMD 96.

Be sure to watch the card reader status LED when enrolling each card. A rapid flicker means a bad card read and requires the misread card to be re-swiped. cards are enrolled from the specified starting user number and affect all user numbers with cards over the specified range of users, skipping any non-card users within the range. To enroll one user specify that user's number as both the starting and ending number. The command automatically enrolls the card and card + code data for each multiple ID user format without further commands being required.

For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

Example:

```
START 223 * 230 * 300 #
```

Swipe 70 Cards. Enroll Cards To Users 230 – 300.

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding and Changing Users

CMD 220 – Batch-Add Access Users – Enroll Card-Only (IDF 2)
CMD 224 – Batch-Change Card for Existing Users (IDF 2, 5, 6, 7)
CMD 225 – Batch-Restore Users
CMD 313-315 – Add Access User (IDF 5-7)

CMD 224: BATCH-CHANGE CARD FOR EXISTING USERS (IDF 2, 5, 6, 7)

Syntax:

```
START 224 * Starting User Number * Ending User Number #
Card
Card
 ..
 ..
 ..
Card
```

Description:

This command enables you to batch-change of cards for existing users.

Batch-changing is a convenient way to re-card many users in a single programming session without tedious and error-prone manual data entry.

Any number of user's cards can be changed in sequence by using this command.

Note: For convenience, you do not have to re-enter the entire command syntax between each user.

Once this batch-change command is started, each card to be changed is swiped in the reader until all users are changed. The command automatically terminates when the specified range of user's cards have been changed. This command can be terminated at any time using CMD 96.

Note: Pay attention to the card reader status LED when enrolling each card. A rapid flicker means a bad card read and requires the misread card to be re-swiped.

Cards are changed from the specified starting user number and affect all user numbers with cards over the specified range of users, skipping any non-card users within the range. To change one user specify that user's number as both the starting and ending number.

For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

Examples:

```
START 224 * 500 * 500 #
```

Changes The Card To The New Card For User 500

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding and Changing Users

CMD 220 – Batch-Add Access Users – Enroll Card-Only (IDF 2)
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 225 – Batch-Restore Users
CMD 310 – Add Access User Card Only (IDF 2)

CMD 225: BATCH-RESTORE USERS

Syntax:

```
START 225 * User Function * ID Format * Access Zone #
ST UN * KPD-CODE #                      (IDF 1)
ST UN * CARD-CODE #                     (IDF 2)
ST UN * DUAL-CODE #                     (IDF 3)
ST UN * CARD-CODE * DUAL-CODE #         (IDF 4)
ST UN * KPD-CODE * DUAL-CODE #          (IDF 5)
ST UN * KPD-CODE * CARD-CODE #          (IDF 6/7)
```

where: ST = START and UN = User Number

Variables:

User Function

1	Access	15	Force OFF Release
2	Unlock	16	Lock Down
3	Relock	17	Lock Down Release
4	Momentary Single Mask	18	Lock Open
5	Mask	19	Lock Open Release
6	Unmask	20	System Password
7	Cancel Entry Delay	21	Executive Password
8	Start Exit Timer	22	Supervisor Password
9	Mask and Cancel Entry Delay	23	Operator Password
10	Start Exit Timer and Unmask	24	Service Password
11	Control Trigger	25	Alarm Cancel
12	Force ON	26	Watch Log
13	Force ON Release	27	Time Log
14	Force OFF	28	Deadman Timer

ID Format

1	Keypad Only (1 record)
2	Card Only (1 record)
3	Dual Only (1 record)
4	Card & Dual (2 records)
5	Keypad & Dual (2 records)
6	Keypad & Card (2 records)
7	Keypad & Card & Dual (3 records)

Effective with Version 7.0, all ID Formats will use just one record each.

Description:

This command enables you to batch-restore current users. It is designed to restore user records in a controller containing damaged, corrupted, or deleted records when manual re-entry of the original keypad code, card codes, and dual codes is required.

For example, if it is not possible to retrieve user cards to complete the restoral, this method restores the records so that the original cards would again be operational. It allows the manual entry of user records from a ScramblePad or a printed record listing the user codes.

Note: After either initial user programming or any subsequent user additions and deletions, make sure to print out all existing user codes and store them in a safe place.

To use this command:

1. Determine the user function, ID format, and access or control zone number for the first group of users.

2. Enter the command with the required information. The yellow LED 1 turns ON and a user code printout header prints on the line printer. This means the controller is in Batch-Restore Mode waiting for you to enter the user number and code information.
3. Enter the user number and code information. Use the proper syntax as determined by the IDF #. Enter all users sharing the same function, ID format, and zone during a batch session.
4. When done, use CMD 96 to terminate batch mode. The yellow LED 1 is now OFF. Repeat the process for each group of similar users.

You may also enter all users with similar IDFs during one batch-restore session, then use CMD 325 to change the function and zone for a range of users. For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

With V7.0 and later, all ID formats use just one record each.

Examples:

```
START 225 * 1 * 2 * 2 #
START 100 * 29746610 #
```

Restore Card Only Access to User 100 for Access Zone 2

Default:

None

Related CMDs:

- CMD 00*22 – Print Glossary With User Function & IDF List
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

Adding and Changing Users

CMD 220 – Batch-Add Access Users – Enroll Card-Only (IDF 2)
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 224 – Batch-Change Card for Existing Users (IDF 2, 5, 6, 7)
CMD 310 – Add Access User Card Only

CMD 235: CHANGE OCCUPANCY COUNT LIMITS

Syntax: `START 235 * N * Count #`

Variables: N

1 Minimum Count
2 Maximum Count

Description:

This command enables you to set occupancy count limits for an area controlled by entry and exit readers. You can set both a minimum and a maximum limit.

The maximum count can be set in a range from 0 (zero)–which is disabled–up to 32766.

When the area is occupied by one less than the minimum setting, an occupancy violation alarm occurs after a 20-second delay. As long as the occupancy remains below the minimum, the occupancy violation alarm will recur once every 2 minutes.

The maximum occupancy count is used to override and deny access to the controlled area by more users than the maximum count. If the maximum count is set to 50 the 51st authorized user will be denied access. Once the count falls below the maximum, additional authorized users may access the area. The maximum count may be set from 0 (zero), which is disabled, to the maximum user memory in the controller.

You can use the minimum and maximum counts set here to trigger control zones for special alarms, area annunciators, occupancy status signs, or other purposes using CMD 236.

Note: For the occupancy controls to work properly, passback control must be enabled for the same readers.

Example:

```
START 235 * 1 * 6 #
START 235 * 2 * 50 #
```

Set Min Count to 6 and Max Count to 50

Default:

Minimum = 2

Maximum = 0

Related CMDs:

CMD 88*27 – Print Occupancy Controls

CMD 188*9 – Print Setup Changes for Passback & User Management

CMD 236 – Trigger Control Zone on Change in Occupancy Count
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-person Access Rule

CMD 236: TRIGGER CONTROL ZONE ON CHANGE IN OCCUPANCY COUNT

Syntax: `START 236 * N * Control Zone #`

Variables: N

1 Change from 0 to 1
2 Change from 1 to 2
3 Change from 2 to 1
4 Change from 1 to 0
5 Count is at Minimum
6 Count is at Minimum Less 1
7 Count is at Minimum Plus 1
8 Count is at Maximum
9 Count is at Maximum Less 1

Description:

This command allows a standard or master control zone to be triggered on any of the above changes in occupancy count. It also uses the minimum and maximum counts set with CMD 235.

This command can be used to trip alarms, area annunciators, or occupancy status signs. It can also be used to automatically mask the interior alarms in a controlled area during a 'first person in' condition or unmask the area during a 'last person out' condition.

Example:

```
START 236 * 5 * 12 #
```

Trigger Control Zone 12 When Inside User Count Equals The Minimum Count

Default:

None (No Control Zones are triggered by occupancy count)

Related CMDs:

CMD 88*27 – Print Occupancy Controls

CMD 188*9 – Print Setup Changes for Passback & User Management

CMD 235 – Change Occupancy Count Limits
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-person Access Rule
CMD 435 – Define Occupancy Count Limits From Host
CMD 436 – Define Occupancy Count Control Zones From Host
CMD 437 – Define Occupancy, Passback, Two-Person

CMD 237: CHANGE OCCUPANCY THRESHOLD FOR AUTO-DISABLE OF 2-PERSON ACCESS RULE

Syntax: `START 237 * Number of Users Inside #`

Description:

Use this command to automatically change a controlled area from a 2-person access rule to a 1-person access rule based on the area's inside occupancy count. Some areas require 2-person open and 2-person close rules but allow 1-person access once the area is open. In other cases, the area may require 6 persons (3 sets of 2 persons) to be inside before switching to 1-person access.

The maximum count can be set from 0 (zero)–which is disabled–up to 32766.

Note: The setting can only be set on an even number of users: 2, 4, 6, 8, and so on.

Example:

```
START 237 * 6 #
```

Change from 2-Person to 1-Person at 6 Persons Inside

Default:

0 (disabled)

Related CMDs:

CMD 88*27 – Print Occupancy Controls

CMD 188*9 – Print Setup Changes for Passback & User Management

CMD 235 – Change Occupancy Count Limits
CMD 236 – Trigger Control Zone on Change in Occupancy Count
CMD 255 – Change 2-Person Access Rule
CMD 256 – Change 2-Person Access Rule Mode for Relay
CMD 257 – Disable 2-Person Access Rule During Time Zone
CMD 435 – Define Occupancy Count Limits From Host
CMD 436 – Define Occupancy Count Control Zones From Host
CMD 437 – Define Occupancy, Passback, Two-Person

CMD 238: SINGLE ZONE ACCESS

Syntax: `START 238 * N #`

Variables: N

0 OFF
1 ON

Description:

Use this command to specify that only a single access zone can occupy a controlled area at a time. You can authorize more than one access zone to use the same secure area; however, when the area is unoccupied and this command is enabled (ON), the first access zone to enter automatically excludes all other authorized access zones until the area is again unoccupied.

With CMD 238 enabled, when the area is occupied, access attempts by other authorized users of other valid access zones are overridden and denied.

Example:

```
START 238 * 1 #
```

Enable Single Zone Access Control

Default:

OFF

Related CMDs:

CMD 88*27 – Print Occupancy Controls

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)
CMD 435 – Define Occupancy Count Limits From Host
CMD 436 – Define Occupancy Count Control Zones From Host
CMD 437 – Define Occupancy, Passback, Two-Person

CMD 246: DEFINE PASSBACK ZONE (PZ AREA)

Syntax: `START 246 * N * PZFROM * PZINTO * Reader * Reader #`

Variables: N

1 Define Readers 1 - 16 specified as PZFROM goes to PZINTO
2 Define Readers 1 - 8 specified as PZFROM to PZINTO, and Readers 9 - 16 specified as PZINTO to PZFROM

PZFROM, PZINTO
0 Unknown, any, unrestricted
1 Outside the secured area(s)
2–63 Inside the secured area(s)

Reader
0 No reader
1-8 Reader specified: like CMD 03, the first Reader variable specifies readers 1 – 8 while the second Reader variable uses numbers 1 – 8 to specify readers 9 – 16.

Description:

In order to set up zoned passback areas, you must define both the Entry and Exit readers that separate different passback zones.

As an added convenience, option N = 2 enables automatic 'mirror-image' definition. Using this option, you can define your entry and exit readers simultaneously.

Example:

```
START 246 * 1 * 1 * 2 * 5 * 0 #
START 246 * 1 * 2 * 1 * 0 * 5 #
```

Define Reader 5 as an Entry Reader from PZ1 (Outside) to PZ2 (Inside), and Reader 13 as an Exit Reader from PZ2 to PZ1.

```
START 246 * 2 * 1 * 3 * 6 * 7 #
```

Define Reader 6 as an Entry Reader from PZ1 (Outside) to PZ3 (Inside), and Reader 15 as an Exit Reader from PZ3 to PZ1.

Related CMDs:

Passback Functions
CMD 03*7, 03*8, 03*9, 03*10 – Change Reader Functions (Passback)
CMD 43*9 – Forgive All Users at Door
CMD 47 – Forgive Access User
CMD 48 – Forgive Passback & Occupancy Count for All Users
CMD 146 – Disable Passback & Occupancy Control During Time Zone
CMD 235 – Change Occupancy Count Limits
CMD 236 – Trigger Control Zone on Change in Occupancy Count

Relay Settings
CMD 79 – Change Time for Alarm Relay

CMD 247: DEFINE READER THREAT LEVEL SETTINGS

Syntax: `START 247 * N * THREAT_LEVEL * Reader * Reader #`

Variables: **N**

0 Set current threat level. Default = 0
1 Set threat level threshold for disabling reader. Default = 99
2 Set threat level threshold for enforcing dual technology rule (that is, disable CCOTZ rule). Default = 99

Threat_Level
0-99 Available threat levels where 0 = no threat level and 99 = the highest priority.

Reader
0 No reader
1-8 Reader specified: like CMD 03, the first Reader variable specifies readers 1 – 8 while the second Reader variable uses numbers 1 – 8 to specify readers 9 – 16.

Description:

User grants and master control zones can change the system threat level between 0 and 99 for all sixteen reader addresses. This option enables you to change a specified reader's behavior depending on a specific threat level and also, using option 0, to set different readers to different initial threat levels.

Example:

```
START 247 * 1 * 60 * 2 * 5 #
```

Define Reader 2 and Reader 13 as disabled whenever the threat level reaches 60 or above. If the threat level reaches that point, no codes can be accepted at this reader, *regardless of the user's threat authority*.

```
START 247 * 2 * 40 * 3 * 6 #
```

Define Reader 3 and Reader 14 to discontinue the CCOTZ rule whenever the threat level reaches 40 or higher. If no CCOTZ rule has been programmed using CMD 104, this setting is ignored.

Related CMDs:

- CMD 34 * 9 – Print Users Inside
- CMD 88 * 2 – Print System Information
- CMD 88 * 2 – Print Setup Changes for Passback & User Management

Passback Functions
CMD 03*7, 03*8, 03*9, 03*10 – Change Reader Functions (Passback)
CMD 47 – Forgive Access User
CMD 48 – Forgive Passback & Occupancy Count for All Users
CMD 146 – Disable Passback & Occupancy Control During Time Zone
CMD 235 – Change Occupancy Count Limits
CMD 236 – Trigger Control Zone on Change in Occupancy Count

Relay Settings
CMD 79 – Change Time for Alarm Relay

CMD 249: TAG ACCESS ZONE

Syntax: `START 249 * N * Access Zone #`

Variables: N

0 Tag Access Zone NO
1 Tag Access Zone YES

Description:

Any access zone – standard or master – can be tagged with this command. When tagged, a tag alert alarm message will be printed on the system printer and the trouble alarm relay is triggered whenever a code assigned to the specified access zone is used at a ScramblePad or MATCH reader, regardless of whether access is granted or denied.

Example:

```
START 249 * 1 * 1 #
```

Tag Standard Access Zone 1

Default:

None

Related CMDs:

- CMD 88*5 – Print Standard Access Zone Setups
- CMD 88*15 – Print Master Access Zone Setups
- CMD 188*5 – Print Setup Changes for Standard Access Zones
- CMD 188*6 – Print Setup Changes for Master Access Zones

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

Tag and Alert Setups

CMD 49, 149 – Tag/Alert any User or Range of Users
CMD 349 – Alert Access Zone
CMD 449, 549 – Tag/Alert Control Zone

CMD 255: CHANGE 2-PERSON-ACCESS-RULE

Syntax: `START 255 * N * Seconds (1-100) #`

Variables: N

1 Granted Code Time Increment
2 Granted Access Time Threshold

Description:

This command is used to restrict access to 2 persons at a time in high security areas, or in areas where industrial safety is an issue. It requires that the requestors enter two different but valid access codes before the system grants access.

If both entry and exit ScramblePad/MATCH readers are installed at the access point, 2-person access rule is active in both directions of travel.

2-Person Access Rule is controlled by two time settings. A time increment in seconds is set for each granted access code. A time setting in seconds is also set to establish a threshold time that must be exceeded for access to be granted. If the time settings are correct, the threshold will be exceeded and access granted when two valid codes are entered in succession. If the first code's timer runs out before a second valid code is entered, access will be denied.

In V7.0 and later, you can specify both a time increment and time threshold using the same command line as shown in the second command syntax.

When the first valid code is entered at a 2-person access point the code timer starts counting down from its set maximum value towards zero. When a second valid access code is entered the two times are added together, and if their combined time exceeds the access grant threshold time setting, the door will unlock. If the combined total of the first code time and the second code time does not exceed the threshold time, the door will not unlock. This enables control over how much of a delay is allowed between the two code entries.

A formula that might help you to remember this is:

If,

$2x - t \geq y$

where,

x = granted code increment

t = the time the user actually takes to enter the code, and

y = the granted access threshold,

then access is granted.

The controller automatically checks to prevent a valid code from being entered twice in a row in order to grant access. 2-Person Access Rule Violation reports are printed if only one code is entered before the timeout, or if the same code is entered twice in a row. A violation triggers the tamper alarm relay, since this is considered an attempt to bypass the controller.

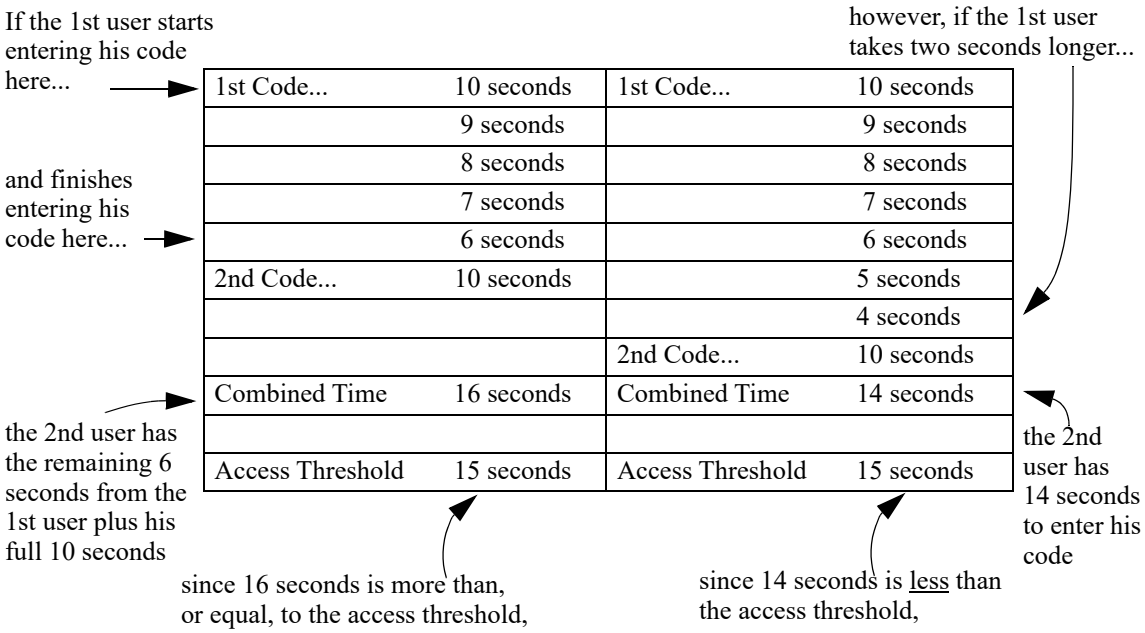
2-Person Access Rule can be disabled during specified time zones using CMD 257. This rule can also be combined with occupancy controls for even greater security.

Example:

```
START 255 * 1 * 10 #
START 255 * 2 * 15 #
```

Granted Code Increment is 10 seconds and the Granted Access Threshold is 15 seconds.

The previous example can follow one of two scenarios, depending on when the second user actually enters his/her access code as shown below.



1st Code...	10 seconds	1st Code...	10 seconds
	9 seconds		9 seconds
	8 seconds		8 seconds
	7 seconds		7 seconds
	6 seconds		6 seconds
2nd Code...	10 seconds		5 seconds
			4 seconds
		2nd Code...	10 seconds
Combined Time	16 seconds	Combined Time	14 seconds
Access Threshold	15 seconds	Access Threshold	15 seconds

To expedite things, we suggest that you formulate a time increment that is practical for entering codes into this door under any foreseeable situation, then apply the same time interval to the time threshold.

So, for example, if you specified that 10 seconds is a reasonable value for the granted code time increment, designate 10 seconds for the granted access time threshold.

So,

```
START 255 * 1 * 10 #
START 255 * 2 * 10 #
```

Default:

2-Person Rule Time Increment = 10 seconds

2-Person Rule Grant Threshold = 11 seconds

Related CMDs:

CMD 88*2 – Print System Information
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-person Access Rule
CMD 256 – Change 2-Person Access Rule Mode for Relay
CMD 257 – Disable 2-Person Access Rule During Time Zone
CMD 437 – Define Occupancy, Passback, Two-Person

CMD 256: CHANGE 2-PERSON-ACCESS-RULE MODE FOR RELAY

Syntax: `START 256 * N * Relay #`

Variables: N

0 OFF
1 ON

Description:

Use this command to select which door relays connected to a controller should operate during a 2-person rule condition. This mode of operation only applies to access codes, not to control codes. Since access codes and control codes can both affect the same relay, two entirely different modes of operation are possible on the same relay at the same time.

You can disable a 2-person rule during specified time zones using CMD 257. This rule can also be combined with passback controls for even greater security.

Example:

```
START 256 * 1 * 1 #
```

Changes Relay 1 to 2-Person Rule ON

Default:

OFF

Related CMDs:

CMD 88*7 – Print Relay Setups and Status
CMD 205 * 2 – Lesser 2-Person Control
CMD 205 * 3 – Executive 2-Person Override
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-person Access Rule
CMD 255 – Change 2-Person Access Rule
CMD 257 – Disable 2-Person Access Rule During Time Zone

CMD 257: DISABLE 2-PERSON-ACCESS-RULE DURING TIME ZONE

Syntax: `START 257 * Time Zone #`

Description:

Use this command to disable 2-person rule during a specified time zone. This enables a security or safety controlled area to operate in normal 1-person rule during high occupancy hours and to switch automatically to 2-person rule whenever operational conditions require.

Example:

```
START 257 * 1 #
```

Disable 2-Person-Access-Rule During Time Zone 1

Default:

Disabled during TZ 0 (Never)

Related CMDs:

CMD 88*2 – Print System Information

CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones

CMD 205 * 2 – Lesser 2-Person Control
CMD 205 * 3 – Executive 2-Person Override
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-person Access Rule
CMD 255 – Change 2-Person Access Rule
CMD 256 – Change 2-Person Access Rule Mode for Relay

Time Zone Setups

CMD 52, 54, 56, 154 – Define/Clear Standard, Master, Grand Master Time Zones

CMD 259: CHANGE SPECIAL MODES FOR LINE MODULE INPUT

Syntax: `START 259 * NN * 1/0 * Input #`

Variables: **NN**

1 Tamper Masked when Door Masked

1/0
0 Off
1 On

Description:

This command is used to select which door inputs operate with "Tamper Masked When Door Masked."

Example:

```
START 259 * 1 * 1 * 3 #
```

Changes Input 3 to Tamper Masked When Door Masked ON

Related CMDs:

CMD 88 * 7 – Print Relay Setups and Status

CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-Person Access Rule
CMD 255 – Change 2-Person Access Rule
CMD 257 – Disable 2-Person Access Rule During Time Zone

CMD 260: PRINT ACTION CONTROL BLOCKS

Syntax: `START 260 * ACB * [last ACB in range] #`

Description:

This command prints a single ACB, a range of ACBs, or a complete list of ACBs showing how specified alarms types take action. This includes information on which relays, if any, are triggered when they are active in the controller.

When only the first ACB argument is used, only a single ACB is specified, unless ACB = 0 in which case all ACBs are printed.

When both the first and optional second ACB argument are used, the first argument defines the first ACB in the range and the second argument defines the last ACB in the range.

For a complete list of ACBs and their default values, refer to Table 4-2 on page 4-188. Several new ACBs have been added for Version 7. These are written in *italics*.

The printout created by this command is self-explanatory. Use this printout to increase your understanding of system operation. Also, it's a good idea to print out the current ACB status before performing any ACB programming.

Note: V6.6 ACBs 41-72 have been reassigned in V7.0. In addition, several new ACBs have been created.

Example:

```
START 260 * 1 #
```

Prints ACB 1

```
START 260 * 0 #
```

Prints All ACBs

```
START 260 * 1 * 30 #
```

Prints ACBs 1 - 30

Default:

None

Related CMDs:

CMD 261 – Define Alarm Actions
CMD 262 – Alarm Condition Triggers Control Zone
CMD 263 – Reset Alarm Actions to Factory Setting

CMD 261: DEFINE ACTION CONTROL BLOCKS

Syntax: `START 261 * Action Control Block * Actions #`

Variables: Actions

0 No Action
1 Trigger Alarm Relay
2 Trigger Duress Relay
3 Trigger Tamper Relay
4 Trigger Trouble Relay
5 Dial Host
6 Log

Description:

This command changes how all types of alarms take action, such as which relays are triggered, or if they are triggered at all, when they are active in the controller. The Alarm Action Control Blocks (ACBs) are the means by which the controller knows what to do with each alarm event.

Note: Changing the ACBs must be done carefully and with careful planning to prevent unexpected performance changes.

Print the ACB chart with CMD 260 for a better understanding of system operation and before you program any ACB. The log selection determines whether the alarm condition reports to the local printer or, on the network, to a host PC program, like SAM, S*NAP, or Velocity.

A new version of this command is offered in V7.0 which allows all six of these options plus “Report as Alarm” (default on most of them) and have each option controlled by a time zone instead of a simple ON/OFF control.

Additional ACBs are found in V7.0 including RQE/MRQs, ‘Alarm Secure’ and ‘Network Active/Inactive’ conditions.

Example:

```
START 261 * 1 * 0 #
```

Alarm Action Control Block 1 Takes No Action

Defaults:

The following table provides all the Alarm Action Control Block defaults for both CMD 261 and 262.

Related CMDs:

CMD 260 – Print Alarm Action(s)

CMD 188*11 – Print Setup Changes for ACBs

Alarm Setups

CMD 262 – Alarm Condition Triggers Control Zone
CMD 263 – Reset Alarm Actions to Factory Setting

Relay Setups

CMD 79 – Change Time For Alarm Relay

The Action Control Block input mappings are shown in Table 4-2 starting on the next page. The ACBs added for Version 7 are noted in *red italics*.

ACB	Description	Alarm Type	Trigger on Secure? [1]
1-8	Alarm Input 1-8	general alarm	yes
9-16	Alarm Input 1-8 DOTL/AATL	general alarm	yes
17-24	Alarm Input 1-8 Tamper	general alarm	yes
25-40	Expansion Alarm Input 1-16	general alarm	yes
41-56	*Expansion Alarm Input 17-32 [Vn. 7.0]*	*general alarm*	*yes*
57-64	*Alarm Input 1-8 DOTL/AATL WARN [Vn. 7.0]*		*yes*
65-72	*Alarm Input 1-8 RQE/MRQ [Vn. 7.0]*		*yes*
73	Occupancy Violation	general alarm	
74	Line-Shorted	general alarm	
75	Duress	duress alarm	
76	Box Tamper	tamper alarm	yes
77-92	Kpd 1-16 Physical Tamper	tamper alarm	yes
93-108	Kpd 1-16 CODE Tamper	tamper alarm	yes
109	Tag Alert	trouble alarm	
110	Line Noise	general alarm	
111	Keypad Offline	trouble alarm	
112	Parallel Printer Offline	trouble alarm	yes
113	Serial Printer Offline	trouble alarm	yes
114	Passback Violation	general alarm	
115	UPS Fail	trouble alarm	yes
116	AC Fail	trouble alarm	yes
117	Membat Fail	trouble alarm	yes
118	UPS Low	trouble alarm	yes
119	Line Out-of-Spec	general alarm	
120	Line Open	general alarm	
121	Network Offline	trouble alarm	yes
122	Entry Delay Warning		
123	2-Person-Rule Violation	tamper alarm	

Table 4-2: ACB Settings

ACB	Description	Alarm Type	Trigger on Secure? [1]
124	Exit Delay Warning		yes
125	Modem Offline	trouble alarm	yes
126	Report Buffer Full	trouble alarm	
127	MATCH Reader Offline	trouble alarm	
CODE Denial Alarms:			
128	Deny: restricted address		
129	Deny: bad CODE		
130	Deny: restricted access zone		
131	Deny: restricted control zone		
132	Deny: restricted temporary days		
133	Deny: passback violation		
134	Deny: access CODE overridden at relay		
135	Deny: Use Count Exceeded		
136	Deny: Absentee Limit Count Expired		
137	Deny: Access Override by Sgl-Zone		
138	Deny: Paging Override		
139	Deny: Two-Person rule incomplete		
140	Deny: Incomplete Dual, no COTZ		
141	Deny: Can't unmask active inputs		
142	Deny: Day Count Exceeded		
143	Deadman Timer Expired		
144-159	Local Duress at reader 1-16		
160-167	Tagged User at Door 1-8 [Vn. 7.0]		
More CODE Denial Alarms:			
168-183	Deny: Local Reader 1-16		
184-185	Reserved		
186	Deny: User Disabled by Host		
187-189	Reserved		
190	Deny: Bad PIN (good card)		

Table 4-2: ACB Settings (Continued)

ACB	Description	Alarm Type	Trigger on Secure? [1]
191	Deny: Unknown CODE, Unknown Host		
192	Deny: Value Error		
193	Deny: Duress		
194	Deny: Threat Level		
195	Deny: Reader Disabled		
196	Deny: Code Tamper Lockout		
197	Deny: Host timed out, no Host Grant		
198	Deny: User Disabled by Code Tamper.		
199	Deny: restricted access zone (Never at this reader)		
200-207	Alarm Input 1-8 Line Fault [Vn. 7.0]		yes
208-223	*Expansion Alarm Input 1-16 DOTL/AATL* *These were ACBs 41-56 on Vn. 6.X*	*alarm*	*yes*
224-239	Expansion Alarm Input 17-32 DOTL/AATL	alarm	yes
240-255	*Expansion Alarm Input 1-16 Tamper* *These were ACBs 57-72 on Vn. 6.X*	*alarm*	*yes*
256-271	Expansion Alarm Input 17-32 Tamper [Vn. 7.0]	general alarm	yes
272-303	Expansion Alarm Input 1-32 Line Fault [Vn. 7.0]		yes
304-335	Expansion Alarm Input 1-32 DOTL/AATL WARN [Vn. 7.0]		yes
336-367	Expansion Alarm Input 1-32 RQE/MRQ [Vn. 7.0]		yes
368-383	Keypad 1 - 16 Sequential CODE Tamper Regular "Reserved" messages will also apply.	tamper alarm	yes
384	Reserved.		
385	Visitor Count Short		
386	Unescorted Visitor		
387	Denied by Host. Regular "Denied" messages will also apply.		
388-400	Reserved.		

Table 4-2: ACB Settings (Continued)

1. This indicates that the ACB can be triggered when secured as well as when active. For example, a DOTL can trigger an alarm both when it is active and when it is inactive (and the door is closed).

CMD 262: ACTION CONTROL BLOCK TRIGGERS CONTROL ZONE

Syntax: `START 262 * Action Control Block * Control Zone [*Control Zone On Secure] #`

Description:

This command enables you to trigger a control zone (SCZ or MCZ) using an alarm condition or other event. By triggering a control zone with an alarm condition, you can cause special control condition or annunciation to occur. When the ACB returns to its secure state, the control zone is inactivated.

An optional variable indicates when an ACB can turn control zone control off for a specified SCZ or MCZ.

Example:

```
START 262 * 1 * 192 #
```

Alarm Action Control Block 1 Triggers Control Zone 192

```
START 262 * 1 * 192 * 193 #
```

Alarm Action Control Block 1 triggers Control Zone 192 and initiates Control Zone 193 when the ACB returns to its secure value.

Defaults:

For a complete list of Alarm Action Control Block defaults, see Table 4-2 starting on page 4-188.

Related CMDs:

CMD 88*6, 88*16 – Print Standard, Master Control Zone Setups

CMD 260 – Print Action Control Block(s)

Alarm Setups

CMD 261 – Define Action Control Block(s)

CMD 263 – Reset Alarm Actions to Factory Setting

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

CMD 263: RESET ACTION CONTROL BLOCKS TO FACTORY SETTINGS

Syntax: `START 263 * Action Control Block #`

Description:

Use this command to reset the actions that occur when an alarm is active from the current values to the default factory setups for either a single ACB or all ACBs.

Enter a 0 (zero) to reset all ACBs.

Example:

```
START 263 * 0 #
```

Reset All Alarm Action Control Blocks To Factory Setups

Defaults:

For a complete list of Alarm Action Control Block defaults, see Table 4-1 starting on page 4-158.

Related CMDs:

CMD 260 – Print Alarm Action(s)
CMD 261 – Define Alarm Actions
CMD 262 – Alarm Condition Triggers Control Zone

CMD 270: CHANGE SUPERVISED LINE MODULE TYPE FOR LINE MODULE INPUT

Syntax: `START 270 * N * Line Module Input` (Version 6.6 and earlier)
`START 270 * N * Line Module Input [* LMI * ... * LMI] #` (Version 7)

Variables: N = Line Module Type

1 DTLM1/MELM1
2 DTLM2/MELM2
3 DTLM3/MELM3

Description:

This command is used to select the type of DTLM (DIGI*TRAC Line Module) or MELM (Miniature Embedded Line Module) being installed on each line module input. The factory default setting is set to DTLM2/MELM2. If a DTLM1/MELM1 is installed without changing the setting, it will function properly. If a DTLM3/MELM3 is being installed, the setting *must be changed* for proper operation.

DTLM1 / MELM1 – 1 Line Module Input

DTLM2 / MELM2 – 1 Line Module Input, 1 RQE Input

DTLM3 / MELM3 – 1 Line Module Input, 1 RQE Input, 1 Tamper Input

In V7.0 and later, you can specify two or more line module inputs in the same command line as shown above. In V6.6 or earlier, you can only specify one line module input per command statement.

This command is very important, because the controller cannot automatically detect what type of line module has been installed.

DTLM

The screw terminals on each DTLM are labeled as follows: HI LO is the terminal for connection to the DIGI*TRAC controller's line module input.

Observe polarity: HI to HI, LO to LO. The terminal labeled 1 is for the Alarm Sensor, the terminal labeled 2 is the RQE Device and the terminal labeled 3 is the Tamper Switch.

MELM

The flying leads on each MELM are color-coded as follows: White for HI and Black for LO.

Observe polarity: white to HI, Black to LO. The orange wires are for the Alarm Sensor, the blue for the RQE Device, and the green is for the Tamper Switch.

Examples:

```
START 270 * 3 * 1 #
```

Change Line Module To DTLM3 / MELM3 For Line Module Input 1

```
START 270 * 2 * 1 * 3 * 5 #
```

Change Line Module To DTLM2 / MELM2 For Line Module Inputs 1, 3, and 5

Default:

DTLM2

Related CMDs:

CMD 88*8 – Print Alarm Setups and Status

CMD 88*9 – Print Alarm Special Setups and Status

CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

CMD 70, 71, 72 – Enable/Disable/Change Selected Line Module Inputs
CMD 370 – Change Line Module Type for Expansion Line Module Input

CMD 273: DISABLE RQE DURING TIME ZONE

Syntax:

```
START 273 * Time Zone * Inputs # (DTLM2/3-MELM2/3 Required)
```

Description:

An RQE can be configured to not operate during a Time Zone. During that Time Zone, its behavior is comparable to the "RQE OFF" option on CMD 73*5.

Examples:

```
START 273 * 40 * 1 #
```

Change RQE On Door 1 To Be Disabled During Time Zone 40

```
START 273 * 65 * 3 #
```

Change RQE On Door 3 To Be Disabled During Time Zone 65, i.e. all the time.

Related CMDs:

CMD 88*10 – Print Door Setups and Status

CMD 188*12 – Print Setup Changes for Alarm & Sense Inputs

Alarm Setups

CMD 70-72 – Enable, Disable, Change Selected Line Module Input
CMD 74 – Change Door-Open-Too-Long Interval
CMD 75 – Door-Open-Too-Long Active While Door Unlocked (Yes/No)
CMD 76 – Mask Line Module Input During Time Zone
CMD 173 - Change Expansion RQE (Request To Exit)
CMD 270 - Change Line Module Type for Line Module Input

Relay Setups

CMD 80 - Change Door Time of Relay

CMD 274: CHANGE DOOR-OPEN-TOO-LONG WARNING

Syntax: `START 274 * DOTL Warning Time * Inputs # (DTLM2/3-MELM2/3 Required)`

Description:

The unauthorized opening of a door is reported as a Forced Entry. The door is also monitored for being held Open-Too-Long beyond an adjustable time delay of 0-8100 (0=Off) seconds. Both door alarm conditions print and trigger the Alarm Relay.

Note: The Door-Open-Too-Long Timer starts when its associated relay deactuates.

Examples:

```
START 274 * 15 * 12 #
```

Define DOTL Warning Delay as 15 seconds for Doors 1 & 2

Related CMDs:

CMD 88*10 - Print Door Setups and Status
CMD 188*12 - Print Setup Changes for Alarm & Sense Inputs

Alarm Setups
CMD 70-72 - Enable, Disable, Change Selected Line Module Input
CMD 73 - Change Selected RQEs (Request to Exit)
CMD 74 - Change Door-Open-Too-Long Interval
CMD 75 - Door-Open-Too-Long Active While Door Unlocked (Yes/No)
CMD 76 - Mask Line Module Input During Time Zone
CMD 174 - Change Expansion Door Open Too Long Time
CMD 270 - Change Line Module Type for Line Module Input
CMD 374 - Change Expansion Door Open Too Long Warning Time

Relay Setups
CMD 80 - Change Door Time of Relay
CMD 282 - Define Special Needs Unlock Extension Time

CMD 280: CHANGE DOOR DELAY TIMER FOR RELAY

Syntax: `START 280 * Seconds * Door #`

Description:

For special entrance or exit control applications, the door delay timer can be delayed from starting after a granted code, RQE, or time zone actuation. The delay duration can be set in the range 1 - 8100 seconds. This is especially useful for implementing delayed egress control on emergency exit doors where local building codes permit such controls to be installed. It is also useful for bank vaults, where unlock delays after correct codes are sometimes required.

Set delay time to 0 (zero) for no delay. This is the default value.

Example:

```
START 280 * 5 * 1 #
```

Delay Egress From Door 1 When RQE is Actuated For 5 Seconds

Default:

0 seconds (no delay)

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 88*10 – Print Door Setups and Status
- CMD 188*14 – Print Setup Changes for Relays

CMD 80 – Change Door Time of Relay
CMD 205 * 1 – Special Needs Extended Unlock
CMD 282 – Define Special Needs Unlock Extension Time

CMD 281: CHANGE CONTROL DELAY TIMER FOR RELAY

Syntax: `START 281 * Control Delay Timer * Relay #`

Description:

For special control applications, the control time of any relay can be delayed from starting after a granted control code, alarm trigger, or relay trigger. The control delay timer can be set in the range 1 - 8100 seconds.

Set delay time to 0 (zero) for no delay. This is the default value.

Example:

```
START 281 * 5 * 1 #
```

Delay Relay 1 Control Timer From Starting For 5 Seconds

Default:

0 seconds (no delay)

Related CMDs:

- CMD 88*7 – Print Relay Setups and Status
- CMD 188*14 – Print Setup Changes for Relays

CMD 81 – Change Control Time of Relay
CMD 381 – Change Control Delay for Expansion Relay

CMD 282: DEFINE SPECIAL NEEDS UNLOCK EXTENSION TIME

Syntax: `START 282 * N1 * N2 * N3 #`

Variables: N

N1 Door Delay extension time (0 - 8100 seconds)
N2 Door Mode extension time (0 - 8100 seconds)
N3 Door Open extension time (0 - 8100 seconds)

Description:

Use this command to extend the Door Delay, Door Mode, and/or Door-Open-Too-Long timers by a fixed amount, up to a limit of 8100 seconds. This command defines a time delay for special needs. Only those doors and relays defined for a specific access zone are affected. For example, if you have previously defined an access zone as SNUX (Special Needs Extended Unlock) using CMD 205, then this command specifies how many additional seconds the door will remain unlocked for the special case. This is particularly useful for wheelchairs, deliverymen, and other requestors who take more than the normal amount of time to enter or exit a door.

Door Delay extension time (N1) defines extra time allotted between the code/card entry and the door unlocking. This feature is particularly useful when there is distance between the keypad/reader and the door.

Door Mode extension time (N2) defines extra time allotted for unlock—how long the controller keeps this door/relay unlocked.

Door Open extension time (N3) defines extra time allotted before the controller issues a DOTL condition. This controls the amount of time you're actually allowed to prop open the door past the normal time.

Maximum extension time for each option is 8100 seconds (2:15:00). Don't use this feature to extend relay times past that limit.

Only use this command when an access code is used. The access zone will determine whether or not to use the time extensions. If the door's base door delay time is 0 and the access zone's flag is set for SNUX, whatever has been specified as the additional time to be added will be used as the delay. However, if the door's base door mode time is 0 or if the base door open time is 0, the corresponding extension will not apply.

Example:

```
START 282 * 0 * 15 * 0 #
```

Keeps the door unlocked for an additional 15 seconds

```
START 282 * 0 * 0 * 33 #
```

Delays issuing a DOTL for an additional 33 seconds

```
START 282 * 0 * 30 * 200 #
```

Give the special-needs users an extra 30 seconds to get the door open, enabling them to prop the door open 200 seconds longer than the typical access user. (Door Delay extension is set to 0, so whatever door delay time has been set still applies.)

Default:

0 seconds (no delay)

Related CMDs:

CMD 88*7 – Print Relay Setups and Status
CMD 81 – Change Control Time of Relay
CMD 205 - Define Access Zone Extensions
CMD 381 – Change Control Delay for Expansion Relay

CMD 283: CHANGE TIMER FOR RELAY IN 1/4 SECOND

Syntax: `START 283 * NN * Time (in 1/4-second) * Relay #`

Variables: NN

1 Control Mode Time (see also CMD 81)
2 Control Delay Time (see also CMD 281)
3 Door Mode Time (see also CMD 80)
4 Door Delay Time (see also CMD 280)

Time
0 - 32400 where 32400 means 8100 seconds.
4 = 1 second, 240 = 60 seconds = 1 minute, 14400 = 3600 seconds = 1 hour

Description:

Use this command to change the specified timers interval from whole seconds to quarter-seconds. This enables you to fine-tune timing down to quarter-seconds.

Example:

```
START 283 * 2 * 21 * 1 #
```

Delay Relay 1 Control Timer From Starting For 5.25 Seconds

Related CMDs:

CMD 88*7 – Print Relay Setups and Status

CMD 188*14 – Print Setup Changes for Relays

CMD 81 – Change Control Time of Relay
CMD 381 – Change Control Delay for Expansion Relay

CMD 284: CHANGE EXTENDED ACCESS TIMES FOR RELAY

Syntax: `START 284 * NN * Time (in Minutes) * Relay #`

Variables: **NN**

1 Extended Time Maximum (0-1440 min)
2 Extended Access Warning Time (0-15 min)

Description:

Use this command to change extended access times for specified relays. This enables qualified operators to prolong the time a designated relay actuates before it deactuates. This allows persons with disabilities and special needs to enter an area at their own speed.

Example:

```
START 284 * 2 * 4 * 1 #
```

Set Relay 1 Expansion Access Timer Warning to 4 minutes

Related CMDs:

CMD 88*7 - Print Relay Setups and Status

CMD 188*14 - Print Setup Changes for Relays
CMD 81 - Change Control Time of Relay
CMD 381 - Change Control Delay for Expansion Relay

CMD 301: ADD EXPANSION LINE MODULE INPUT OR RELAY TO STANDARD CONTROL ZONE

Syntax: `START 301 * Expansion LMI / Expansion Relay * SCZ #`

Description:

Use this command to add expansion line module inputs (LMI) or expansion relays to standard control zones (SCZ). This enables control codes to either mask expansion LMIs or to trigger, force, or lock down/open expansion relays.

A standard control zone must be defined before expansion LMIs or relays can be added to it (see CMD 45).

LMIs and relays can share the same control zone as shown in the example below. If you have defined both an Expansion LMI1 and Expansion Relay 1 then specifying a '1' as your first argument adds both to Control Zone 1; the system interprets this apparent ambiguity without trouble: depending on what type of code is assigned to Control Zone 1, the system determines if alarms are masked (by using an alarm control code type) or if relays are actuated (using a relay control code type). Separate control zones can be assigned to alarm control codes and to relay control codes if desired or required.

Example:

```
START 301 * 1 * 1 #
```

Add Expansion Line Module Input and/or Expansion Relay 1 To Standard Control Zone 1

Default:

None

Related CMDs:

- CMD 88*6 – Print Standard Control Zone Setups
- CMD 88*16 – Print Master Control Zone Setups
- CMD 188*7 – Print Setup Changes for Standard Control Zones

Control Zone Setups

CMD 45 – Define Standard Control Zone
CMD 302 – Remove Expansion Line Module Input or Relay from Standard Control Zone

CMD 302: REMOVE EXPANSION LINE MODULE INPUT OR RELAY FROM STANDARD CONTROL ZONE

Syntax: `START 302 * Expansion LMI / Expansion Relay * SCZ #`

Description:

Use this command to remove expansion line module inputs (LMIs) or expansion relays from standard control zones (SCZ). This changes how control codes mask expansion LMIs or trigger, force, or lock down/open expansion relays.

Example:

```
START 302 * 1 * 1 #
```

Remove Expansion Line Module Input And/Or Relay 1 From Standard Control Zone 1

Default:

None

Related CMDs:

- CMD 88*6, 88*16 – Print Standard, Master Control Zone Setups
- CMD 188*7 – Print Setup Changes for Standard Control Zones

CMD 45 – Define Standard Control Zone
CMD 301 – Add Expansion Line Module Input or Relay to Standard Control Zone

CMD 303: CHANGE TIME ZONE OF STANDARD CONTROL ZONE

Syntax: `START 303 * Time Zone * Standard Control Zone #`

Description:

Use this command to change the time zone associated with a standard control zone (SCZ) from its original (current) value. CMD 303 enables you to change the TZ associated with the SCZ using CMD 45. Set the time zone to a standard, master, or grand master time zone.

You can also disable a currently-active SCZ using this command. Simply change the current time zone to 0 (Zero), Never.

Note: A Time Zone is only used to restrict the command when a Control Zone will be activated by a Card or Code. The Tiime Zone does not effect the triggering of a Control Zone by an input or an alarm.

Example:

```
START 303 * 1 * 1 #
```

Change Time Zone of Standard Control Zone 1 to Time Zone 1

Default:

None

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*6 – Print Standard Control Zone Setups
- CMD 188*7 – Print Setup Changes for Standard Control Zones

Control Zone Setups

CMD 45 – Define Standard Control Zone
CMD 305 – Define Time Zone for Master Control Zone

Time Zone Setups

CMD 52, 54, 56, 154, 454 – Define/Clear Standard, Master, Grand Master Time Zones

CMD 304: DEFINE MASTER CONTROL ZONE (192-255)

Syntax:
```
START 304 * NN * Standard Control Zone * Master Control Zone #
START 304 * MCZ * NN * Value * ... * Value #
```

Variables: **NN**

1	Trigger Relays
2	Clear Relays
3	Mask Alarms
4	Unmask Alarms
5	Unlock Doors
6	Relock Doors
7	Force ON Relays
8	Force ON Release of Relays
9	Force OFF Relays
10	Force OFF Release of Relays
11	Lock Down Relays
12	Lock Down Release of Relays
13	Lock Open Relays
14	Lock Open Release of Relays
15	Annunciate Readers
16	Cancel Entry Delay
17	Start Exit Timer
18	Unmask Alarms if all secure
19	Partial Unmask
20	Set Threat Level
21	Turn on ScramblePad LEDs
22	Turn off ScramblePad LEDs

Description:

CMD 305, Define Time Zone for Master Control Zone, must be invoked before a master control zone can operate. Use CMD 40 to add a control user to trigger a master control zone.

Master control zones enable the setup of either simple or sophisticated controls to be triggered by a single control code entered at an authorized ScramblePad/MATCH reader, or triggered by a line module input or relay. One common use of this feature is to put a single facility, or area within a facility, into night or day operation mode with a single code entry. For instance, the last person leaving a building equipped with an M8 controller and 16 expansion line module inputs could unmask all alarms, lock all doors, and lock down the vault room with a single 'Night Code' at the building exit's ScramblePad/MATCH reader.

Annunciate Readers is a special option that sounds the specified ScramblePad's alarm annunciators for 5 beeps. This can be used to signal that a special event is beginning, that a special meeting is taking place, or that all employees should leave the building within a specified number of minutes.

Partial Unmask the system to unmask all inputs in the specified control zone previously detected as secure. All unsecured inputs are left masked.

V7.0 and later offers a variation on this command. It enables you to set every field in a master control zone you require. It uses this syntax:

```
304 * MCZ * NN * Value * ... * Value #
```

In addition to the twenty NN fields listed above, you can also set the time zone (CMD 305), tag/alert flags (CMD 449/CMD 549), link control zone (CMD 307), and link access zone (CMD 307).

Note: A Time Zone is only used to restrict the command when a Control Zone will be activated by a Card or Code. The Tiime Zone does not effect the triggering of a Control Zone by an input or an alarm.

Example:

```
START 304 * 3 * 1 * 192 #
START 304 * 5 * 2 * 192 #
```

Mask all line module inputs assigned to Standard Control Zone 1 and Unlock all doors assigned to Standard Control Zone 2 when a Code assigned to Master Control Zone 192 is used.

Default:

None

Related CMDs:

- CMD 88*6 – Print Standard Control Zone Setups
- CMD 88*16 – Print Master Control Zone Setups
- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 188*8 – Print Setup Changes for Master Control Zones

Control Zone Setups

CMD 45 – Define Standard Control Zone
CMD 303 – Change Time Zone of Standard Control Zone
CMD 305 – Define Time Zone for Master Control Zone
CMD 306 – Clear Master Control Zone
CMD 449 – Tag Control Zone
CMD 549 – Alert Control Zone

CMD 305: DEFINE TIME ZONE FOR MASTER CONTROL ZONE

Syntax: `START 305 * Time Zone * Master Control Zone #`

Description:

Use this command to set or change the time zone for a master control zone.

You must assign a time zone other than TZ0 to a master control zone or it won't work.

Note: A time zone is only used to restrict the command when a control zone will be activated by a card or code. The tiime zone does not effect the triggering of a control zone by an input or an alarm.

Example:

```
START 305 * 16 * 250 #
```

Define Time Zone 16 for Master Control Zone 250

Default:

None

Related CMDs:

- CMD 88*3, 88*4, 88*14 – Print Standard, Master, Grand Master Time Zones
- CMD 88*16 – Print Master Control Zone Setups
- CMD 188*8 – Print Setup Changes for Master Control Zones

Control Zone Setups

CMD 304 – Define Master Control Zone
CMD 306 – Clear Master Control Zone
CMD 307 – Define Access Zone for Master Control Zone

Time Zone Setups

CMD 52, 54, 56, 154, 454 – Define/Clear Standard, Master, Grand Master Time Zones

CMD 306: CLEAR MASTER CONTROL ZONE

Syntax:

```
START 306 * Master Control Zone #
START 306 * First MCZ * Last MCZ #
START 306 * First MCZ * Last MCZ * 1 #
```

Description:

A Master Control Zone can be cleared or erased with this command. In Version 6.6 you can also specify a range of master control zones.

This does not clear the Link Access Zone or Link Control Zone fields as defined in CMD 307.

To perform a complete clear:

```
START 306 * MCZ #
START 307 * 0 * 0 * MCZ #
```

To clear a range of master control zones use:

```
START 306 * First MCZ * Last MCZ #.
```

This variation is available on V6.6 and later only.

To clear the link access zone and link control zones, use:

```
START 306 * First MCZ * Last MCZ * 1 #
```

This variation is available on V6.6 and later only.

If you only need to clear one master control zone, list it twice as “first and last” values.

Example:

```
START 306 * 250 #
```

Clear Master Control Zone 250

```
START 306 * 235 * 240 * 1#
```

Clear Master Control Zones 235-240 including new Link fields

Default:

None

Related CMDs:

- CMD 88*16 – Print Master Control Zone Setups
- CMD 188*8 – Print Setup Changes for Master Control Zones

CMD 304 – Define Master Control Zone

CMD 307: DEFINE LINKED ZONES FOR MASTER CONTROL ZONE

Syntax: `START 307 * Access Zone * Linked Control Zone * Master Control Zone #`

Description:

Use this command to program Master Control Zones that can be triggered by Control Code. This is done by defining a Linked Master Control Zone.

Note: This command only works with CCM 6.6. CCM 7.0 and later does not utilize this command.

If a particular door is associated with this AZ, then all of the tasks defined for this Master Control Zone (in CMD 304) are carried out. This is useful for setting in motion a cascade of events if certain conditions are met, particularly for elevator installations and medical cabinets where several actions must be triggered by one request at a designated Access Zone.

If a door/relay attempts to execute a Master Control Zone that is linked, and if the Master Control Zone is allowed by the Time Zone but is locked out via the Access Zone, the Controller will pull up the linked Master Control Zone and follow the linked tasks.

Discussion:

One of the most powerful DIGI*TRAC feature is the ability to program Master Control Zones that can be triggered by a control code. Suppose that you have a user with one control code and you want different Master Control Zones to be triggered depending on where and when the card is used.

First, set up the control code to trigger the first Master Control Zone of the sequence. Make a note of the Access Zone numbers corresponding to where and when each Master Control Zone will be triggered, then issue the following command:

```
307 * AZ * LCZ * MCZ #
```

Suppose you set up Master Control Zones 192 – 195 and define Access Zones 51 – 54 as areas where they can be used. Set Master Control Zone 192 as the zone triggered by the control code, then write the following sequence:

```
307 * 51 * 193 * 192 #
307 * 52 * 194 * 193 #
307 * 53 * 195 * 194 #
307 * 54 * 0 * 195 #
```

Once this sequence is entered, when the user enters the specified control code at the Reader (R) and Time (T) specified by the Access Zone, this sequence of events results:

```
if (access_zone_ok (51, R, T)) then trigger MCZ 192
else if (access_zone_ok (52, R, T)) then trigger MCZ 193
else if (access_zone_ok (53, R, T)) then trigger MCZ 194
else if (access_zone_ok (54, R, T)) then trigger MCZ 195
else do nothing
```

The controller will automatically detected and prohibit looping. For instance, if you were to use this line

```
307 * 54 * 193 * 195 #
```

in the preceding example, it would be rejected as invalid since that would link MCZ 195 back to MCZ 193.

The Master Control Zone's existing Time Zone control is still checked. We recommend using Time Zone 65 in linked Master Control Zone situations because if the Time Zone is not active, it won't proceed down the link to the next Master Control Zone in the chain.

Example:

```
307 * 51 * 193 * 192 #
307 * 52 * 194 * 193 #
307 * 53 * 195 * 194 #
307 * 54 * 0 * 195 #
```

Set up Master Control Zones 192 – 195 and define Access Zones 51 – 54 as areas where they can be used. Set Master Control Zone 192 as the zone triggered by the control code.

Default:

None

Related CMDs:

CMD 88*16 – Print Master Control Zone Setups

CMD 188*8 – Print Setup Changes for Master Control Zones

CMD 304 – Define Master Control Zone
CMD 305 – Define Time Zone for Master Control Zone
CMD 306 – Clear Master Control Zone

CMD 310: ADD ACCESS USER CARD ONLY (IDF 2)

Syntax: `START 310 * User Number * Access Zone * Card #`

Description:

Use this command to add one new access user with a card only (ID Format 2) to the controller's database. This new user is required to enter a card only to gain entry into a locked security area. To add the new user and card, select an unused user number, assign it to the appropriate access zone and swipe the card in the reader.

The MATCH reader must be connected to a ScramblePad in order to program the controller. Use a DIGI*TRAC Enrollment Station located at the system printer for convenient programming, or use a dual technology reader installed at a door.

If you are using this command to enroll a prox card at a DS47L-SPX, use the enrolling procedure described in "Card Enrollment Methods" starting on page 3-31.

For a detailed discussion of available IDFs, see "ID Formats (IDF)" on page 3-24.

If you're using S*NAP, only execute this command from the Virtual System Manager using an SMES S*NAP MATCH Enrollment Station.

Examples:

```
START 310 * 110 * 2 * Swipe Card #
```

Add Card Only Access User Number 110 To Access Zone 2

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 19-22, 311-315, 320-322 – Add Access Users
CMD 220 – Batch-Add Access Users – Enroll Card-Only (IDF 2)
CMD 316 – Test Card During Programming

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 311: ADD ACCESS USER CARD+CODE (IDF 3)

Syntax: `START 311 * User Number * Code * Access Zone * Card #`

Description:

Use this command to add one new access user with a card + code (dual technology) combination (IDF 3) to the controller. This user is required to enter both a card and a code to gain entry to a locked security area.

To add a user, select an unused user number, enter a code, specify the appropriate access zone, then swipe the selected card. A new user record is created and printed on completion of a successful command.

If you're using this command to enroll a prox card at a DS47L-SPX, use the enrolling procedure described in "Card Enrollment Methods" starting on page 3-31.

For a detailed discussion of IDFs, see "ID Formats (IDF)" on page 3-24.

If you're using S*NAP, you can only execute this command from the Virtual System Manager using an SMES MATCH Enrollment Station. It can also be issued directly from the SMES.

Examples:

```
START 311 * 2 * 334821 * 6 * Swipe Card #
```

Add Card + Code (Dual) Access User Number 2 With Code 334821 To Access Zone 6

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 19-22, 310, 312-315, 320-322 – Add Access Users

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions

CMD 16, 23 – Delete Any User, Range of Users

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)

CMD 204 – Define Master Access Zone (66-127)

CMD 312: ADD ACCESS USER WITH CARD & CARD + CODE (IDF 4)

Syntax: `START 312 * User Number * Code * Access Zone * Card #`

Description:

Use this command to add a new multiple ID format (IDF) user—in this case, IDF4. A multiple IDF user is any user who can use more than one ID for access at controlled doors.

IDF4 enables a user to enter a card only at a card reader-controlled door and a card + code on a dual technology-controlled door.

In V6.6 and earlier, IDF4 places two user records in the controller memory. The specified user number must be an even number (such as 2, 4, 10). Therefore a controller with a memory maximum of 1000 users can store a maximum of 500 IDF4 users.

In V7.0 and later, all ID formats use just one record each.

Passback controls track the use of all IDs simultaneously.

If you are using this command to enroll a prox card at a DS47L-SPX, use the enrolling procedure described in “Card Enrollment Methods” starting on page 3-31.

For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

If you’re using S*NAP, this command can be executed from the Virtual System Manager using an SMES MATCH Enrollment Station. It can also be issued directly from the SMES.

Example:

```
START 312 * 166 * 7360026 * 1 * Swipe Card#
```

Add Access User 166 With Code 7360026 & Card to Access Zone 1

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 19-22, 310, 311, 313-315, 320-322 – Add Access Users
CMD 104 – Enable Card Only at Dual Technology Reader during Time Zone
CMD 316 – Test Card During Programming

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 313: ADD ACCESS USER WITH CODE & CARD+CODE (IDF 5)

Syntax: `START 313 * User Number * Code * Access Zone * Card #`

Description:

Use this Command to add a new multiple ID format (IDF) User. A multiple ID user is anyone who can use more than one ID for access at controlled doors. In this case, the multiple ID format is IDF5.

IDF5 enables a user to enter a code only at a ScramblePad-controlled door and a card + code at a dual technology-controlled door.

Since this command assigns the same access zone to both IDs, the code also works on a dual technology reader. If you don't want this, use CMD 12 to change the access zone of the code-only user number to the required access zone.

In V6.6 and earlier, IDF5 uses two user records in the controller memory and the user number specified must be an even number (2, 4, 6). Therefore a controller with a memory maximum of 1000 users can store a maximum of 500 IDF5 users.

In V7.0 and later, all ID formats use just one record each.

Passback controls track the use of all IDs simultaneously.

If you are using this command to enroll a prox card at a DS47L-SPX, use the enrolling procedure described in "Card Enrollment Methods" starting on page 3-31.

For a discussion of IDFs, see "ID Formats (IDF)" on page 3-24.

If you're using S*NAP, execute this command from the Virtual System Manager using an SMES MATCH Enrollment Station. It can also be issued directly from the SMES.

Example:

```
START 313 * 702 * 1038891 * 41 * Swipe Card #
```

Add Access User 702 With Code 1038891 & Card To Access Zone 41

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 19-22, 310-312, 314, 315, 320-322 – Add Access Users
CMD 104 – Enable Card Only at Dual Technology Reader during Time Zone

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 224 – Batch-Change Card for Existing Users (IDF 2, 5, 6, 7)

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 314: ADD ACCESS USER WITH CODE & CARD (IDF 6)

Syntax: `START 314 * User Number * Code * Access Zone * Card #`

Description:

Use this Command to add a new multiple ID format (IDF) User. A multiple ID user is anyone who can use more than one ID for access at controlled doors. In this case, the multiple ID format is IDF6.

IDF6 enables a user to enter a code only on a ScramblePad-controlled door and a card only on a card reader-controlled door.

In V6.6 and earlier, this format uses two user records in the controller memory and the specified user number must be an even number (2, 4, 6). Therefore a controller with a memory maximum of 1000 users can store a maximum of 500 IDF6 users.

In V7.0 and later, all IDFs use only a single record.

Passback controls track the use of all IDs simultaneously.

If you are using this command to enroll a prox card at a DS47L-SPX, use the enrolling procedure described in “Card Enrollment Methods” starting on page 3-31.

For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

If you’re using S*NAP, execute this command from the Virtual System Manager using an SMES MATCH Enrollment Station. You can also issue it directly from the SMES.

Example:

```
START 314 * 4 * 6670 * 12 * Swipe Card #
```

Add Access User Number 4 With Code 6670 & Card To Access Zone 12

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 19-22, 310-313, 315, 320-322 – Add Access Users

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 224 – Batch-Change Card for Existing Users (IDF 2, 5, 6, 7)
CMD 316 – Test Card During Programming

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 315: ADD ACCESS USER WITH CODE & CARD & CARD+CODE (IDF 7)

Syntax: `START 315 * User Number * Code * Access Zone * Card #`

Description:

Use this Command to add a new multiple ID format (IDF) User. A multiple ID user is anyone who can use more than one ID for access at controlled doors. In this case, the multiple ID format is IDF7.

IDF7 enables a user to enter a code only at a ScramblePad-controlled door, a card only at a card reader-controlled door, and a card + code at a dual technology-controlled door.

Code only will also work on a dual technology reader. If this arrangement is not wanted, use CMD 12 to change the access zone of the code only user number to an appropriate access zone.

In V6.6 and earlier, IDF7 uses three user records in the controller memory. For this reason, the specified user number must be divisible by four in order to allow all three user numbers to be stored consecutively. Therefore, a controller with a maximum of 1000 users in its memory can have a maximum of 250 IDF7 users.

In V7.0 and later, all ID formats use just one record each.

Passback controls track the use of all IDs simultaneously.

If you are using this command to enroll a prox card at a DS47L-SPX, use the enrolling procedure described in “Card Enrollment Methods” starting on page 3-31.

For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

If you’re using S*NAP, execute this command from the Virtual System Manager using an SMES MATCH Enrollment Station. You can also issue this command directly from the SMES.

Examples:

```
START 315 * 8 * 1428990 * 1 * Swipe Card #
```

Add Access User Number 8 With Code 1428990 & Card To Access Zone 1

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 10, 19-22, 310-314, 320-322 – Add Access Users
CMD 104 – Enable Card Only at Dual Technology Reader during Time Zone
CMD 316 – Test Card During Programming

Changing and Deleting Users

CMD 11-13, 325 – Change User(s) Codes, Zones, and/or Functions
CMD 16, 23 – Delete Any User, Range of Users
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 224 – Batch-Change Card for Existing Users (IDF 2, 5, 6, 7)

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 316: TEST CARD DURING PROGRAMMING

Syntax: `START 316 * Card #`

Description:

Use this Command to test a card while in Programming Mode. This command emulates the use of a card at a card reader. Different responses occur when the card is tested, depending on whether the card is

- already enrolled or not
- encoded or improperly encoded
- belongs to a currently active / inactive access zone.

If the card was successfully enrolled and is assigned to a currently active access zone, the card reader responds with a single flash of its LED, the ScramblePad responds with a single flash of its green LED, and the door relay in the system will trigger.

If the card is assigned to a currently inactive access zone, the card reader responds with a single flash of its green LED indicating a successful card read. The ScramblePad responds with a single flash of both its green and red LEDs followed by a second flash of its red LED, then a tone to indicate Access Denied.

If the card has not yet been enrolled in the controller, the card reader responds with two bursts of its green LED, the ScramblePad flashes both green and red LEDs followed by the red LED and a tone to indicate Access Denied.

If the card is improperly encoded or damaged, the card reader responds with a long burst of rapid flashing on its green LED and the ScramblePad flashes its red LED and beeps to indicate an invalid card.

*Note: This Command cannot be executed from S*NAP Software.*

Examples:

```
START 316 * Card #
```

Tests Card During Programming

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
CMD 310 – Add Access User Card Only (IDF 2)

CMD 320: AUTO-ADD ACCESS USERS WITH CODE & CARD+CODE (IDF 5)

Syntax: `START 320 * Starting User Number * Number of Users * Access Zone #`

Description:

Use this command to automatically add a specified number of new multiple ID format users. A multiple ID user is any user who can use more than one ID for access at controlled doors. In this case, the multiple ID format is IDF5.

IDF5 enables a user to enter a code only on a ScramblePad-controlled door and a card + code on a dual technology-controlled door.

Using this command, code only users can also access dual technology readers. If you don't want this arrangement, use CMD 12 to change the access zone of the code only user number to an appropriate access zone.

In V6.6 and earlier, IDF5 uses two user records in the controller memory and the starting user number specified must be an even number (2, 4, 6). Therefore a controller with a memory maximum of 1000 users can store a maximum of 500 IDF5 users.

In V7.0 and later, all IDFs use only one record each.

Passback controls track the use of all IDs simultaneously.

This command automatically generates a code and requires the use of CMD 223 to add the card to the user record. This is useful because, even if card delivery is delayed, the building can be secured by immediately issuing codes only until cards arrive and can be issued.

For a discussion of IDFs, see "ID Formats (IDF)" on page 3-24.

Examples:

```
START 320 * 100 * 10 * 4 #
```

Add 10 Access Users Starting At User Number 100 To Access Zone 4

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding and Changing Users

CMD 10, 19-22, 310-315, 321, 322 – Add Access Users

CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)

CMD 204 – Define Master Access Zone (66-127)

CMD 321: AUTO-ADD ACCESS USERS WITH CODE & CARD (IDF 6)

Syntax: `START 321 * Starting User Number * Number of Users * Access Zone #`

Description:

Use this command to automatically add a specified number of new multiple ID format users. A multiple ID user is any user who can use more than one ID for access at controlled doors. In this case, the multiple ID format is IDF6.

IDF6 enables a user to enter a code only on a ScramblePad-controlled door and a card only on a card reader-controlled door.

In V6.6 and earlier, IDF6 uses two user records in the controller memory and the starting user number specified must be an even number (2, 4, 6). Therefore a controller with a memory maximum of 1000 users can store a maximum of 500 IDF5 users.

In V7.0 and later, all IDFs use only one card record.

Passback controls track the use of all IDs simultaneously.

This command automatically generates a code and requires the use of CMD 223 to add the card to the user record. This is useful because, even if card delivery is delayed, the building can be secured by immediately issuing codes only until cards arrive and can be issued.

For a discussion of IDFs, see “ID Formats (IDF)” on page 3-24.

Example:

```
START 321 * 200 * 25 * 2 #
```

Auto-Add 25 Access Users Starting At User Number 200 To Access Zone 2

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding and Changing Users

CMD 10, 19-22, 310-315, 320-322 – Add Access Users
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 316 – Test Card During Programming

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 322: AUTO-ADD ACCESS USERS WITH CODE & CARD & CARD+CODE (IDF 7)

Syntax: `START 322 * Starting User Number * Number of Users * Access Zone #`

Description:

Use this command to automatically add a specified number of new multiple ID format users. A multiple ID user is any user who can use more than one ID for access at controlled doors. In this case, the multiple ID format is IDF7.

IDF7 enables a user to enter a code only on a ScramblePad-controlled door, a card only on a card reader-controlled door, and a card + code on a dual technology-controlled door.

Code only works on a dual technology reader. If you don't want this arrangement, use CMD 12 to change the access zone of the code only user number to an appropriate access zone.

In V6.6 and earlier, IDF7 uses three user records in the controller memory. For this reason, the specified user number must be divisible by four in order to allow all three user numbers to be stored consecutively. Therefore, a controller with a maximum of 1000 users in its memory can only hold a maximum of 250 IDF7 users.

In V7.0 and later, all IDFs use only one card record.

Passback controls track the use of all IDs simultaneously.

This command automatically generates a code and requires the use of CMD 223 to add the card to the user record. This is useful because, even if card delivery is delayed, the building can be secured by immediately issuing codes only until cards arrive and can be issued.

For a discussion of IDFs, see "ID Formats (IDF)" on page 3-24.

Example:

```
START 322 * 664 * 10 * 17 #
```

Auto-Add 10 Access Users Starting At User Number 664 To Access Zone 17

Default:

None

Related CMDs:

CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes

Adding and Changing Users

CMD 10, 19-22, 310-315, 320, 321 – Add Access Users
CMD 223 – Batch-Enroll Card to Existing Users (IDF 5, 6, 7)
CMD 316 – Test Card During Programming

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

CMD 325: CHANGE RANGE OF USERS TO NEW FUNCTION AND ZONE

Syntax: `START 325 * Starting User Number * Ending User Number * Function * Access Zone /Control Zone #`

Variables: **Function**

1	Access
2	Unlock
3	Relock
4	Momentary Single Mask
5	Mask
6	Unmask
7	Cancel Entry Delay
8	Start Exit Timer
9	Mask and Cancel Entry Delay
10	Start Exit Timer and Unmask
11	Control Trigger
12	Force ON
13	Force ON Release
14	Force OFF
15	Force OFF Release
16	Lock Down
17	Lock Down Release
18	Lock Open
19	Lock Open Release
20	System Password
21	Executive Password
22	Supervisor Password
23	Operator Password
24	Service Password
25	Alarm Cancel
26	Watch Log
27	Time Log
28	Deadman Timer
29	Manual Holiday
30	Test Secure
31	Unmask If Secure
32	Function Group
34	Extended Access

Description:

Use this command to change a range of users from one function to another. You can change or leave the access zone or control zone as well.

This command is used to convert automatically-generated access users into control users of a specified function.

Example:

```
START 325 * 100 * 150 * 4 * 2 #
```

Change Users 100 to 150 To Momentary Mask Users For Control Zone 2

Default:

None

Related CMDs:

CMD 35, 36, 38*8, 330 – Print User, Users, or Family of Users with Codes

Adding Users

CMD 02 – Add Programming Pass/word
CMD 10, 19-22, 310-315, 320-322 – Add Access Users
CMD 15, 40-42, 44 – Add Control Users

Changing Users

CMD 425 – Change User(s) Codes, Zones, and/or Functions

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

CMD 330: PRINT SETUPS AND STATUS BY PRINTOUT STYLE FOR FAMILIES OF USERS

Syntax: `START 330 * NN * STYLE * Starting User Number * Ending User Number #`

Variables: **NN**

1 All Users
2 Momentary Access
3 Unlock / Relock
4 All Access
5 Control
6 Lock Down / Lock Open
7 Alarm Mask / Unmask / Cancel / Deadman
8 Passwords
9 Users Inside
10 Tagged Users
11 Alerted Users
12 Temporary-Day Users
13 Use Count Users
14 Absentee Rule Users
15 Unreconstructed Records

STYLE

1 User Codes
2 User Temporary-Days
3 Use Count (also prints *Temp Days and Absentee Info* where needed)
4 Absentee Rule
5 User Tracking Status
6 Deadman Time
7 Option Flags
8 Print All Fields

Description:

Use this command to print a single user or a range of users, by family—the NN user functions—and formatted in a specified report STYLE.

All Version 7 options are marked in *italics*.

S*NAP Note: For Style 1, User Codes, to be displayed, the setup for S*NAP must have codes set to 'Reveal'.

Example:

```
START 330 * 4 * 1 * 50 * 60 #
```

Print Access Users 50 - 60 With Codes

Default:

None

Related CMDs:

CMD 30, 31, 33, 34 – Print User, Users, Users by Zone, or Family of Users Without Codes

CMD 35, 36, 38*8 – Print User, Users, or Family of Users with Codes

CMD 345: CLEAR STANDARD CONTROL ZONE

Syntax:

```
START 345 * Standard Control Zone #
START 345 * First SCZ * Last SCZ #
```

Description:

Use this command to clear a standard control zone. In V6.6 and later, you can clear a range of standard control zones using the variant syntax.

Example:

```
START 345 * 1 #
```

Clear Standard Control Zone 1

```
START 345 * 2 * 8 #
```

Clear Standard Control Zones 2 – 8

Default:

None

Related CMDs:

- CMD 88*6 – Print Standard Control Zone Setups
- CMD 188*7 – Print Setup Changes for Standard Control Zones
- CMD 45 – Define Standard Control Zone

CMD 349: ALERT ACCESS ZONE

Syntax: `START 349 * N * Access Zone #`

Variables: N

0 Alert Access Zone NO
1 Alert Access Zone YES

Description:

Use this command to notify all users of a specified access zone—standard or master—that a special condition exists—such as a message is waiting, a new code is being issued, a briefing is scheduled, or a meeting is required.

The alert is sounded at the ScramblePad where the user entered their code. The alert is 4 short beeps of the ScramblePad's alarm annunciator.

The alert sounds when any user of the specified zone enters their code at any ScramblePad connected to the controller. An alert cannot be sounded at a MATCH reader since it has no audible alarm device.

The alert message does not trigger any relays.

Example:

```
START 349 * 1 * 1 #
```

Alerts Access Zone 1

Default:

None

Related CMDs:

- CMD 88*5 – Print Standard Access Zone Setups
- CMD 88*15 – Print Master Access Zone Setups
- CMD 188*5 – Print Setup Changes for Standard Access Zones
- CMD 188*6 – Print Setup Changes for Master Access Zones
- CMD 260 – Print Alarm Action(s)

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

Tag and Alert Setups

CMD 49, 149 – Tag/Alert any User or Range of Users
CMD 249 – Tag Access Zone
CMD 449, 549 – Tag/Alert Control Zone

CMD 350: AUTO-DELETE ON EXPIRATION FOR USERS

Syntax: `START 350 * N * Starting User Number * Ending User Number #`

Variables: N

0 OFF
1 ON

Description:

Use this command to automatically delete a user record from the controller whenever it reaches one of these user limits: use count, absentee rule, or temporary day limit.

This keeps the maximum amount of memory available for adding new users; however, this can also prevent a user from being identified when they attempt access after they have been disabled by reaching a predefined user limit.

Example:

```
START 350 * 1 * 901 * 910 #
```

Auto-Delete Users 901 - 910 On Expiration

Default:

None

Related CMDs:

CMD 330*12, 330*13, 330*14 – Print Setups and Status for Families of Users
CMD 351 – Use Count Mode for Users
CMD 352 – Set Use Count for Users
CMD 353 – Absentee Rule Mode for Users
CMD 354 – Set Max Days Absent for Users
CMD 355 – Forgive Absentee Users
CMD 356 – Temporary Day Mode for Users
CMD 357 – Set Days for Temporary-Day Users

CMD 351: USE COUNT MODE FOR USERS

Syntax: `START 351 * N * Starting User Number * Ending User Number #`

Variables: N

0 OFF
1 ON

Description:

Use this command to enable use count limiting over a specified range of users.

Use CMD 352 to set the use count for a specified range of users. Only those users enabled for use count here can be specified in CMD 352.

Example:

```
START 351 * 1 * 25 * 50 #
```

Change Use Count Mode To On For Users 25 Through 50

Default:

OFF

Related CMDs:

CMD 330*13 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 352 – Set Use Count for Users

CMD 352: SET USE COUNT FOR USERS (1 - 255 Uses)

Syntax: `START 352 * Use Count * Starting User Number * Ending User Number #`

Description:

Use this command to set the maximum number of uses, Use Count, allowed for a range of users. To restrict a single user by use count, set the starting and ending user number the same.

Set the use count in a range from 1 to 31 uses for Version 6.6 or earlier; set range from 1 to 255 uses for Version 7.

For example, setting the use count to 1 specifies that a designated user can only use a card or code once. Each time the specified user is granted access, the use count goes down by one. When the count reaches zero, the user can no longer use their ID to access a building.

Any attempt to use an ID with an expired use count causes a use count violation. The controller prints the user number that caused the violation.

Use Count limits can be set for any function user. Use CMD 350 to auto-delete a user on use count expiration, if required. Use Count mode, CMD 351, must be set to ON before setting the use count.

Users limited by use count cannot also be limited by absentee use (CMDs 353 - 354); however, a user specified as a temporary-day user (CMD 356) can also have a use count limit set.

Example:

```
START 352 * 1 * 25 * 50 #
```

Set Use Count To 1 For Users 25 - 50

Default:

none

Related CMDs:

CMD 330*13 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 351 – Use Count Mode for Users

CMD 353: ABSENTEE RULE MODE FOR USERS (1 - 255 Days)

Syntax: `START 353 * N * Starting User Number * Ending User Number #`

Variables: N

0 OFF
1 ON

Description:

Use this command to enable day count limiting over the specified range of users. For Version 6.6 and earlier the range is 1 - 63; for Version 7, the range is 1 - 255.

Users must be qualified for absentee rule here before an actual limit can be set in CMD 354.

Example:

```
START 353 * 1 * 100 * 110 #
```

Set Absentee Rule For Users 100 - 110 to ON

Default:

OFF

Related CMDs:

CMD 330*14 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 354 – Set Max Days Absent for Users
CMD 355 – Forgive Absentee Users

CMD 354: SET MAX DAYS ABSENT FOR USERS

Syntax: `START 354 * Max Days Absent * Starting User Number * Ending User Number #`

Description:

Use this command to set the maximum number of days, Day-Count, a specified user is allowed without entering a keypad code or MATCH code.

To specify a single user's day-count, set the starting and ending user number to the same value.

Set the day count in a range from 1 – 63 days for Version 6.6 and earlier or 1 – 255 for Version 7.

If a code is used every day, the day-count stays at its maximum setting. However, each day that the designated code is not used, the day-count goes down by one. When the count reaches zero, the user's code is disabled and can no longer be used. Any attempt to use a code with an expired day-count will cause a day-count violation report and the controller prints the user number that caused the violation. Absentee Rule Mode, CMD 353, must be set to ON (NN = 1) before you can set the maximum number of absent days here.

Use CMD 350 to auto-delete a user upon absentee day-count expiration, if desired.

Users limited by use count (CMD 351 - 352) cannot also be limited by absentee-use; however, a user specified as a temporary-day user (CMD 356) can also have an absentee-count limit set.

Example:

```
START 354 * 30 * 500 * 600 #
```

Set Max Days Absent For Users 500 Through 600 To 30 Days

Default:

None

Related CMDs:

CMD 330*14 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 353 – Absentee Rule Mode for Users
CMD 355 – Forgive Absentee Users

CMD 355: FORGIVE ABSENTEE USERS

Syntax: `START 355 * Starting User Number * Ending User Number #`

Description:

Use this command to restore the maximum number of days absent to the original setting for a range of users. To restore a single user's max days, set the starting and ending user number the same.

Each user's day count is maintained in the user record. When this command is issued, the user's max day count will be restored to the original number of days set in the user record.

If a different number of days is required, use CMD 354 to set a new maximum day count value for a user or range of users.

Example:

```
START 355 * 10 * 10 #
```

Forgive Absentee User 10 To Max Day Setting

```
START 355 * 10 * 16 #
```

Forgive Absentee Users 10 through 16 To Max Day Setting

Default:

None

Related CMDs:

CMD 330*14 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 353 – Absentee Rule Mode for Users
CMD 354 – Set Max Days Absent for Users

CMD 356: TEMPORARY DAY MODE FOR USERS

Syntax: `START 356 * N * Starting User Number * Ending User Number #`

Variables: N

0 OFF
1 ON

Description:

Use this command to enable temporary day use over a specified range of users.

It enables you to pre-authorize a code for use on specified future days and forbids use before then. Once the last authorized day expires, the code is disabled. Any attempt to use a code that has expired causes a day-use violation and the controller prints the user number that caused the violation.

Use CMD 357 to define the temporary days themselves. Only users qualified through this command for temporary day mode can be specified for designated temporary days using CMD 357.

Use CMD 350 to auto-delete a user on temporary-day expiration, if required.

Example:

```
START 356 * 1 * 25 * 50 #
```

Change Temporary-Day Mode For Users 25 Through 50 To ON

Default:

OFF

Related CMDs:

CMD 330*12 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 357 – Set Days for Temporary-Day Users

CMD 357: SET DAYS FOR TEMPORARY-DAY USERS

Syntax: `START 357 * Starting User Number * Ending User Number * Days This Week * [Days Next Week] #`

Description:

User this command to define which days of this week and next week a code is authorized for. This user management command enables a code to be pre-authorized for use on the specified future days and prevents use before then.

Once the last authorized day expires, the code is disabled. Any attempt to use a code that has expired will cause a day-use violation and print the user number that caused the violation.

Use CMD 350 to auto-delete a user on temporary-day expiration, if required.

Temporary-day limited users cannot also be limited by absentee rule; however, a user limited by temporary-day can also be limited by use count.

You must qualify a user for temporary day mode using CMD 356 before this command will work.

Version 7.0 replaces this command with a 'Day Count' option. In order to allow a user access on 'Saturday/Sunday This week and Next week', the user's access zone will need to use Sat/Sun-only Time Zones and a Day Count of 14 will let the code run for two weeks. To set the number of days, use CMD 352.

Example:

```
START 357 * 60 * 90 * 67 * 67 #
```

Set Days To Saturday and Sunday This Week And Next Week For Users 60 - 90

Default:

None

Related CMDs:

CMD 330*12 – Print Setups and Status by Printout Style for Families of Users
CMD 350 – Auto-Delete on Expiration for Users
CMD 356 – Temporary Day Mode for Users

CMD 358: SET DEADMAN TIMER

Syntax: `START 358 * User Number * Time #`

Description:

Use this command to set the deadman timer for each deadman user. Set the timer in a range from 0 - 65,000 seconds. Each deadman user requires two deadman codes:

- a code to start the timer
- a code to stop the timer

The start code's time is set for the length of time required to complete the assigned task. The stop code's time is set to 0 (zero) seconds.

When you enter a code with a time of 0 seconds, it forces the deadman timer to 0 (zero) and cancels the count down, avoiding an alarm.

If the deadman timer counts down to zero before a stop code is entered, a deadman timer expiration alarm is reported to both the system printer and alarm relay.

Example:

```
START 358 * 444 * 60 #
```

Set User 444's Deadman Timer for 60 Seconds

```
START 358 * 100 * 0 #
```

Cancels User 100's Deadman Timer

Default:

None

Related CMDs:

CMD 330*7 – Print Setups and Status by Printout Style for Families of Users
CMD 44*4 – Add Keypad Special Control User

CMD 370: CHANGE LINE MODULE FOR EXPANSION LINE MODULE INPUT

Syntax: `START 370 * N * Expansion Line Module Input #`

Variables: N = Line Module Type

1 DTLM1/MELM1
2 DTLM2/MELM2
3 DTLM3/MELM3

Description:

Use this command to select the type of DTLM or MELM DIGI*TRAC line module being installed on each expansion line module input. The factory default setting is DTLM2/MELM2. If a DTLM1/MELM1 is installed, the system will function properly without changing the default setting.

Note: If a DTLM3 or MELM3 is being installed, the setting must be changed for proper operation.

Here are the inputs provided for each line module type:

DTLM1/MELM1 - 1 Line Module Input

DTLM2/MELM2 - 1 Line Module Input, 1 RQE Input

DTLM3/MELM3 - 1 Line Module Input, 1 RQE Input, 1 Tamper Input

DTLM

The screw terminals on each DTLM are labeled as follows: HI LO is the terminal for connection to the DIGI*TRAC controller's Line Module Input.

Observe polarity: HI to HI, LO to LO. The terminal labeled 1 is for the Alarm Sensor, the terminal labeled 2 is the RQE Device and the terminal labeled 3 is the Tamper Switch.

MELM

The flying leads on each MELM are color coded as follows: White for HI and Black for LO.

Observe polarity: White to HI, Black to LO. The Orange wires are for the Alarm Sensor, the Blue for the RQE Device, and the Green is for the Tamper Switch.

Examples:

```
START 370 * 3 * 8 #
```

Changes Line Module To DTLM3/MELM3 For Expansion Input 8

Default:

DTLM2/MELM2

Related CMDs:

CMD 88*20 – Print Expansion Alarm/RQE Setups and Status

CMD 88*21 – Print Expansion Alarm Special Setups and Status

CMD 270 – Change Line Module Type for Line Module Input

CMD 373: DISABLE EXPANSION RQE DURING TIME ZONE

Syntax: `START 373 * Time Zone * Expansion RQE #`

Description: An Expansion RQE can be configured to not operate during a Time Zone. During that Time Zone, its behavior is comparable to the "RQE OFF" option on CMD 173*3.

Examples:

```
START 373 * 1 * 1 #
```

Change Expansion RQE 1 to be Disabled During Time Zone 1.

Related CMDs:

- CMD 88*20 – Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 – Print Expansion Alarm Special Setups and Status
- CMD 88*22 – Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 – Print Setup Changes for Expansion Line Module Inputs

Alarm Setups

CMD 170, 171 – Enable, Disable Expansion Line Module Input
CMD 172 – Change Expansion Line Module Input
CMD 174 – Change Expansion Door Open Too Long Time
CMD 175 – Expansion DOTL Active While Input Unlocked
CMD 176 – Mask Expansion Line Module Input during Time Zone

CMD 374: CHANGE EXPANSION DOOR OPEN TOO LONG WARNING TIME

Syntax: `START 374 * DOTL Warning Time * Expansion Input #`

Description:

Any Expansion Alarm Input may be set up to report as a door. The unauthorized opening of a door is reported as a Door Forced Open. The door is also monitored for being held Open-Too-Long beyond an adjustable time delay of 0-8100 (0=Off) seconds. Both door alarm conditions report on the printer and trigger the Alarm Relay.

Note: The Door-Open-Too-Long Timer starts at the end of the Door Mode Timer. Example: If the Door Unlock Timer is set to 6 seconds and the door is held open, the DOTL Timer starts after the 6 second door unlock time expires. If the DOTL Timer is set to 10 seconds the alarm will sound after 16 seconds total time has expired.

Example:

```
START 374 * 15 * 1 #
```

Define DOTL Warning Delay To 15 Seconds For Expansion Input 1

Related CMDs:

- CMD 88*10 - Print Door Setups and Status
- CMD 88*20 - Print Expansion Alarm/RQE Setups and Status
- CMD 88*21 - Print Expansion Alarm Special Setups and Status
- CMD 88*22 - Print Expansion Line Module Input Door Setups and Status
- CMD 188*13 - Print Setup Changes for Expansion Line Module Inputs

CMD 74 - Change Door-Open-Too-Long Interval
CMD 170, 171 - Enable, Disable Expansion Line Module Input
CMD 172 - Change Expansion Line Module Input
CMD 173 - Change Expansion RQE (Request To Exit)
CMD 174 - Change Expansion Door Open Too Long Time
CMD 175 - Expansion DOTL Active While Input Unlocked
CMD 176 - Mask Expansion Line Module Input during Time Zone
CMD 274 - Change Door Open Too Long Warning Time
CMD 282 - Define Special Needs Unlock Extension Time

CMD 381: CHANGE CONTROL DELAY TIMER FOR EXPANSION RELAY

Syntax: `START 381 * Control Delay Timer * Expansion Relay #`

Description:

For special control applications, you can delay the control time of any expansion relay from starting after a granted code, alarm trigger, or relay trigger. The delay can range from 1 to 8,100 seconds.

Set delay time to 0 (zero) for NO delay.

Example:

```
START 381 * 5 * 1 #
```

Delay Expansion Relay 1 Control Timer From Starting For 5 Seconds

Default:

0 seconds (no delay)

Related CMDs:

- CMD 88*18 – Print Expansion Relay Setups and Status
- CMD 88*28 – Print Virtual Relay Setups and Status
  CMD 281 – Change Control Delay for Relay

CMD 383: CHANGE TIMER FOR EXPANSION RELAY IN 1/4 SECOND

Syntax: `START 383 * NN * Time (in 1/4-second) * Relay #`

Variables: NN

1 Control Mode Time
2 Control Delay Time

Time
0 - 32400 where 32400 means 8100 seconds.
4 = 1 second, 240 = 60 seconds = 1 minute, 14400 = 3600 seconds = 1 hour

Description:

Use this command to change the specified timers interval from whole seconds to quarter-seconds for the expansion relay designated. This enables you to fine-tune timing down to quarter-seconds for each designated expansion relay.

Example:

```
START 383 * 2 * 21 * 1 #
```

Delay Expansion Relay 1 Control Timer From Starting For 5.25 Seconds

Related CMDs:

CMD 88*7 – Print Relay Setups and Status

CMD 188*14 – Print Setup Changes for Relays

CMD 81 – Change Control Time of Relay
CMD 381 – Change Control Delay for Expansion Relay

CMD 405: DEFINE CUSTOM CARD READER CONFIGURATION

Syntax: `START 405 * NN * DIGMAP [Up to 32 digits] #`

Variables: **NN**
Reader number, 1-16, or 0 to set all card readers.

DIGMAP
A series of two-digit numbers, all strung together. If you want to pass through the first eight digits of a card's raw data, use 0102030405060708. To reset in order to generate MATCH codes instead of customized codes, set DIGMAP variable to 0. You cannot set one of these individual two-digit numbers higher than **39**.

Description:

This command enables the host to set up a customized card reader, assuming that the MATCH board connected to the card reader supports this feature.

This command is used to select a subset of 8 – 16 digits out of the card code received from the card reader.

Examples:

```
START 405 * 3 * 01020304050607080900 #
```

Define Card Reader 3 to use the first 9 digits of the card data, followed by a 0 digit as the card number. (Same as 010203040506070809 because zeroes are padded on the end.)

```
START 405 * 0 * 0102030411121314 #
```

Use the first 4 digits, skip the next 6 digits, and use digits 11-14 as the card's 8-digit card code, for all of the card readers.

```
START 405 * 13 * 0000010203040506 #
```

Use the card's first 6 digits as the card code, but pad it with two leading zeros.

```
START 405 * 0 * 0 #
```

Reset all card readers from card reader mapping to normal MATCH code generation.

Related CMDs:

- CMD 88*11 – Print Keypad/Match Setups and Status
- CMD 188*3 – Print Setup Changes for Keypad/MATCH

CMD 03 – Change Selected Keypad/Match Functions
CMD 17 – Define Standard Access Zone
CMD 103 – Change Selected MATCH Functions
CMD 104 – Enable CARD/CODE-Only At Dual Technology Reader During Time Zone

*03*3 – Programming Functions*
CMD 01, 02 – Add or Change Programming Codes

*03*4 – Control Functions*
CMD 45 – Define Standard Control Zone

*03*7, 03*8, 03*9, 03*10 – Passback Functions*
CMD 46 – Change Passback Mode
CMD 146 – Disable Passback and Occupancy Control During Time Zone

CMD 420: ENABLE/DISABLE USERS SPECIAL OPTIONS

Syntax: `START 420 * NN * 1/0 * First User * Last User #`

Variables: NN

1	Temp Days Rule
2	Use Count Rule
3	Absentee Rule
4	Global User
5	Disabled
6	Auto-Delete
7	Alert
8	Tag
9	2-Person A
10	2-Person B
11	2-Person Exec Override
12	SNUX
13	Exec Passback Override
14	XDAT status
15-19	Reserved
20	Disabled by Code Tamper

1 / 0

1	Enable
0	Disable

Description:

Use this command to define special option flags. All options enable/disable a specific flag bit in Message 118 except for Temp Days, Use Count, Absentee Rule, and the 2-Person options which affect 2 bits each. If first and last user are the same number, only one user is specified.

The fully-compliant V7.0 front-end host can use the new V7.0 Code Record Download feature in lieu of this command.

If you are using S*NAP, selecting Reveal Codes in the S*NAP setups causes codes to print. Secure these printouts.

Example:

```
START 420 * 11 * 1 * 01 * 02 #
```

Users 01 and 02 are enabled for two-person executive override.

Related CMDs:

- CMD 30, 31, 34 - Print User, Users, or Family of Users Without Codes
- CMD 32 - Print First Available User Number
- CMD 35, 36, 38, 330 - Print User, Users, or Family of Users with Codes
- CMD 37 - Print User given Code

Changing and Deleting Users

CMD 16, 23 - Delete Any User, Range of Users
CMD 425 - Change User To New Function And Zone
CMD 421 - Set Users Special Options

Access Zone Setups

CMD 17, 24, 117 - Define Standard Access Zone (1-64)
CMD 204 - Define Master Access Zone (66-127)

Control Zone Setups

CMD 45, 304 - Define Standard, Master Control Zone

CMD 421: SET USERS SPECIAL OPTIONS

Syntax: `START 421 * First User * Last User * NN * VALUE(S)... #`

Variables: NN

1 - Code Type. (See also CMD 425.)
2 - Zone. (See also CMD 425.)
4 - DAY/USE Counter. (See also CMD 352, CMD 354, CMD 357.)
8 - DAY/USE Limit. (See also CMD 352, CMD 354, CMD 357.)
16 - Threat Authority
32 - PZ
64 - Globalize this. Update other controllers on network. No value specified.

Description: Assuming a given extracurricular option is enabled in the controller, this command lets the host system set the values. Reallocation initializes all data, so it's important to enable all the features you intend to use before sending the data with this command.

Selecting 'Reveal Codes' in the S*NAP Setups will cause Codes to print. Secure these printouts.

Example:

```
START 421 * 345 * 346 * 32 * 2#
```

Enables users 345 and 346 for predefined special options inside PZ 2.

Related CMDs:

CMD 30, 31, 34 - Print User, Users, or Family of Users Without Codes
CMD 32 - Print First Available User Number
CMD 35, 36, 38, 330 - Print User, Users, or Family of Users with Codes
CMD 37 - Print User given Code
CMD 423 - Print Users Extra Curricular Data

Changing and Deleting Users
CMD 16, 23 - Delete Any User, Range of Users
CMD 425 - Change User To New Function And Zone
CMD 420 - Enable/Disable Users Special Options

Access Zone Setups
CMD 17, 24, 117 - Define Standard Access Zone (1-64)
CMD 204 - Define Master Access Zone (66-127)

Control Zone Setups
CMD 45, 304 - Define Standard, Master Control Zone

CMD 422: SET USERS CUSTOM ACCESS ZONE

Syntax: `START 422 * User * Reader * Time Zone [* Time Zone...] #`

Description:

Use this command to assign special access zones to specific users.

Standard Access Zones allow different users to share the same access privileges. A standard access zone consists of a time zone for every door or reader.

For example:

Reader	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Door	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Time Zone	0	0	13	14	13	0	22	31	0	0	65	65	65	0	22	41

Ordinarily, this combination of time zones per reader would be assigned to a standard access zone, numbered from 1 – 64, then an access user would be defined using that SAZ number.

Certain customers, however, may want some of their users (or, possibly, all of their users) enrolled with their own personal access combination. For example, a customer might have a special user who has almost the same access as everyone else but needs special privileges on special occasions; or a consultant who requires access to an assortment of areas but only for brief periods of time; or an airline agent who suddenly must have access to three gates ordinarily used by a competing airline.

This new situation might change the SAZ for this user to something more like this example:

Reader	1	2	3	4	5	**6**	7	8	**9**	**10**	11	12	13	**14**	15	16
Door	1	2	3	4	5	**6**	7	8	**1**	**2**	3	4	5	**6**	7	8
Time Zone	0	0	13	14	13	**33**	22	31	**33**	**33**	65	65	65	**33**	22	41

The access zone information—timezones for each reader—can then be downloaded per user. Of course, this reduces the total user capacity. Users assigned individual access zones can take up twice as much space in controller memory; therefore only half as many users can be enrolled. However, this only applies to those users with this feature enabled.

To enroll a user with a Custom Access Zone, set their regular Access Zone to 0 and use CMD 422 to add the custom access information. Signify the reader the designated user can access during the specified time zone in this way:

```
422 * 4 * 0 * 51 #
```

This example indicates that user 4's custom access is set at Reader 1 during Time Zone 51. Notice that Reader 1 is indicated by 0, so that readers are specified in the form:

```
(Reader #) - 1
```

You can specify more than one reader or door by adding new arguments to a string. Each new argument represents an additional time zone and assumes the next reader/door in the sequence. For example:

```
422 * 4 * 0 * 51 * 51 * 51 #
```

indicates that the next two readers—in this case, Readers 2 and 3—also accept User 4's access at Time Zone 51.

To specify another time zone for the same user and reader, you must create a new command line. For example:

```
422 * 3 * 2 * 51 #
```

```
422 * 3 * 2 * 52
```

indicates that User 3 has access at Reader 3 during both Time Zones 51 and 52.

Assuming an access zone is enabled at the controller, this command lets the host system set the values. Reallocation initializes all data, so it's important to enable all the features you intend to use before sending the data with this command.

The fully-compliant V7.0 front-end host may use the new V7.0 Extracurricular Data Record Download feature in lieu of this command.

Example:

```
START 422 * 5 * 0 * 65 * 65 * 65 * 65 #
START 422 * 5 * 8 * 4 * 4 * 4 * 4 #
```

Sets User 5's Custom Access to Time Zone 65 at Readers 1 – 4 and Time Zone 4 at Readers 9 – 12.

Related CMDs:

- CMD 30, 31, 34 – Print User, Users, or Family of Users Without Codes
- CMD 32 – Print First Available User Number
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 - Print User given Code

Changing and Deleting Users

CMD 16, 23 – Delete Any User, Range of Users
CMD 425 – Change User To New Function And Zone
CMD 420 – Enable/Disable Users Special Options

Access Zone Setups

CMD 17, 24, 117 – Define Standard Access Zone (1-64)
CMD 204 – Define Master Access Zone (66-127)

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

CMD 423: PRINT USERS EXTRACURRICULAR DATA

Syntax: `START 423 * Starting User Number * Ending User Number #`

Description:

Use this command to print users' extracurricular data by entering the starting and ending user number.

We recommend that you secure this information after printing.

Example:

```
START 423 * 101 * 152 #
```

Print Extracurricular Data for Users 101– 152

Related CMDs:

- CMD 30, 31, 34 – Print User, Users, or Family of Users Without Codes
- CMD 35, 36, 38, 330 – Print User, Users, or Family of Users with Codes
- CMD 37 – Print User given Code
- CMD 425 – Define Users Extra Curricular Data

Changing and Deleting Users

CMD 16, 23 – Delete Any User, Range of Users

CMD 425: CHANGE RANGE OF USERS TO NEW FUNCTION AND ZONE

Syntax: `START 425 * Starting User No. * Ending User No. * Function * Access/Control Zone #`

Variables: **Function**

0. Access	20. Lock Open
1. Control Trigger	21. Lock Open Release
2. Unlock	22. Momentary Single Mask
3. Alarm Cancel	24. Watch Log
6. Mask	25. Time Log
7. Unmask	26. Cancel Entry Delay
8. System Password	27. Start Exit Timer
9. Executive Password	28. Mask and Cancel Entry Delay
10. Supervisor Password	29. Start Exit Timer and Unmask
11. Operator Password	30. Deadman Timer
12. Service Password	34. Indexed Command *
13. Relock	35. Pre-Arm Status
14. Force ON	36. Conditional Unmask
15. Force ON Release	37. Function Group
16. Force OFF	39. Extended Access
17. Force OFF Release	43. Partial Unmask (Force Arm)
18. Lock Down	46. Set Security (Threat) Level
19. Lock Down Release	

* Indexed commands, Function 34, consist of these Access/ Control Zone arguments equivalents:

1-4	Manual Holidays	9	Forgive All Users
5-8	Unholidays	10	Count Users Inside

To assign a function group, defined using CMD 426, to a range of users, use subcommand 37.

Description:

Use this command to change a range of users from one function to another. The access zone or control zone can be left alone or changed as well. This command is used to convert automatically generated access users into control users of a specified function.

The fully-compliant V7.0 front-end host can use the new V7.0 Code Record Download feature in lieu of this command.

Example:

```
START 425 * 100 * 150 * 22 * 2 #
```

Change Users 100 to 150 To Momentary Mask These Users For Control Zone 2

```
START 425 * 25 * 50 * 37 * 24 #
```

Assign Users 25 through 50 to Function Group 24.

Related CMDs:

CMD 427 – List Function Groups
CMD 325 – Change User(s) Codes, Zones, and/or Functions
CMD 420 – Enable/Disable Users Special Options
CMD 421 – Set Users Special Options
CMD 426 – Define Function Group

CMD 426: DEFINE FUNCTION GROUP

Syntax: `START 426 * Function Group ID [* Function * Access/Control Zone * Code Extension] #`

Variables: **Function**

0. Access	21. Lock Open Release
1. Control Trigger	22. Momentary Single Mask
2. Unlock	24. Watch Log
3. Alarm Cancel	25. Time Log
6. Mask	26. Cancel Entry Delay
7. Unmask	27. Start Exit Timer
8. System Password	28. Mask and Cancel Entry Delay
9. Executive Password	29. Start Exit Timer and Unmask
10. Supervisor Password	30. Deadman Timer
11. Operator Password	34. Indexed Command
12. Service Password	35. Pre-Arm Status
13. Relock	36. Conditional Unmask
14. Force ON	39. Extended Access
15. Force ON Release	43. Partial Unmask
16. Force OFF	46. Set Threat Level
17. Force OFF Release	
18. Lock Down	128-174. Same as 0 – 46, but Zone should be taken from XDAT's n^{th} parameter byte.
19. Lock Down Release	
20. Lock Open	

Indexed Commands: Zone 1-4=Manual Holidays, 5-8=Unholidays, 9=Forgive All Users, 10=Clear Code Tamper, 11=Count Users This Side, 12=Count Users Otherside.

Description:

Use this command either to define a Function Group code extension or to clear a function group and reset it for a new definition. A Function Group usually consists of at least two code extensions and associated function and zone numbers. Code extensions can consist of 0, 1, or 2 digits.

CMD 426 * 0 # will clear all Function Groups. CMD 426 * N # where N = 1–255 will clear/define Function Group N.

Function Group IDs are in the range of 0 – 255 where 0 = all function groups.

Assign code extensions to perform specific access/control zone functions for a specified function group.

Once defined, you assign users to function groups using CMD 425 through Function 37.

Example:

```
START 426 * 13 * 0 * 65 #
```

Set Default for Function Group 13 to 'Access, AZ 65.'

Related CMDs:

CMD 427 – List Function Group
CMD 325 – Change User(s) Codes, Zones, and/or Functions
CMD 420 – Enable/Disable Users Special Options
CMD 421 – Set Users Special Options
CMD 425 – Change User(s) Codes, Zones, and/or Functions

CMD 427: LIST FUNCTION GROUP

Syntax:

```
START 427 * 0 # (List all)
START 427 * Function Group ID #
START 427 * Function Group ID * Function Group ID #
```

Description:

This Command is used to list one or more function groups.

To list all currently defined function groups, enter this command argument:

```
CMD 427 * 0 #
```

To list a specific function group, enter this syntax:

```
CMD 427 * N #
```

To list a range of function groups, use this syntax:

```
CMD 427 * First * Last #
```

Example:

```
START 427 * 1 * 3 #
```

List Function Groups 1-3.

Related CMDs:

CMD 325 – Change User(s) Codes, Zones, and/or Functions
CMD 420 – Enable/Disable Users Special Options
CMD 421 – Set Users Special Options
CMD 425 – Change User(s) Codes, Zones, and/or Functions
CMD 426 – Define Function Group

CMD 449: TAG CONTROL ZONE

Syntax: `START 449 * N * Control Zone #`

Variables: N

0 Tag Control Zone NO
1 Tag Control Zone YES

Description:

You can tag any control zone, standard or master, using this command. When tagged, a tag alert alarm message is printed on the system printer and the trouble alarm relay is triggered whenever a code assigned to the specified control zone is used at a ScramblePad/MATCH reader, regardless of whether the control code is granted or denied.

Example:

```
START 449 * 1 * 1 #
```

Tag Standard Control Zone 1

Default:

None

Related CMDs:

CMD 88*6, 88*16 – Print Standard, Master Control Zone Setup

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

Tag and Alert Setups

CMD 49, 149 – Tag/Alert any User or Range of Users
CMD 249, 349 – Tag/Alert Access Zone
CMD 549 – Alert Control Zone

CMD 454: DEFINE MASTER OR GRAND MASTER TIME ZONE 66-149

Syntax:

```
START 454 * MTZ/GTZ * Standard or Master Time Zone #
START 454 * MTZ/GTZ * TZ * TZ #
START 454 * MTZ/GTZ * TZ * TZ * TZ #
START 454 * MTZ/GTZ * TZ * TZ * TZ * TZ #
START 454 * MTZ/GTZ * TZ * TZ * TZ * TZ * TZ #
START 454 * MTZ/GTZ * TZ * TZ * TZ * TZ * TZ * TZ * TZ #
START 454 * MTZ/GTZ * TZ * TZ * TZ * TZ * TZ * TZ * TZ * TZ #
```

Description:

Use this command to define master (MTZ) and grand master (GTZ) time zones as complex multiple time zones.

Time zones can restrict the use of codes when used to define an access zone, or regulate the automatic scheduling of an event when used to define a control zone. Most of these time zones include only one set of start and stop times along with a set of valid days. However, when more complex time controls are required, you can assign

- ❑ any combination of standard time zones (up to a maximum of eight) as master time zones
- ❑ any combination of standard or master time zones (up to a maximum of eight) as grand master time zones

Rather than go through a laborious process of writing a whole series of MTZ and GTZ commands, this command enables you to assign up to eight TZs or MTZs in the same line. Unspecified columns are left blank.

To help you plan these complex time zones, use the worksheets in Appendix A.

Examples:

```
START 454 * 68 * 8 * 25 #
```

Define Master Time Zone 68 as the time zone matrix shown below.

MTZ/GTZ	Time Zones - Column							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
MTZ68	8	25	0	0	0	0	0	0
GTZ140	70	7	6	5	4	3	2	1

```
START 454 * 140 * 70 * 7 * 6 * 5 * 4 * 3 * 2 * 1 #
```

Defines Grand Master Time Zone 140 as shown in the matrix above.

Related CMDs:

CMD 17 – Define Standard Access Zone
CMD 45 – Define Standard Control Zone
CMD 50 – Set Date & Day Of The Week
CMD 51 – Set Time
CMD 52 – Define Standard Time Zone
CMD 76 – Mask Alarm Input During Time Zone
CMD 82 – Time Zone Control Of Relay
CMD 88 – Print System Setups and Status
CMD 154 – Define Grand Master Time Zone

CMD 460: PRINT ACTION CONTROL BLOCKS

Syntax:
```
START 460 * Single Action Control Block #
START 460 * First ACB * Last ACB #
```

Description:

Use this command to print the characteristics of action control blocks (ACBs). These indicate how alarms take action—including which relays are triggered and when the ACBs are active in the system.

You can print the characteristics of a single ACB, a range of ACBs, or all ACBs as required. Select 0 (zero) as the single action control block argument to print *all* control blocks.

Only ACBs that are *not* set to their defaults are printed.

In V7.0, ACBs 41-72 have been reassigned from their V6.x assignments. In addition, V7.0 introduces several new ACBs.

A complete list of the Action Control Blocks are included under CMD 260.

Examples:

```
START 460 * 1 #
```

Prints ACB 1

```
START 460 * 0 #
```

Print all ACBs

```
START 460 * 6 * 13 #
```

Print ACBs 6 through 13

Related CMDs:

CMD 260 – Print Alarm Action(s)

Alarm and ACB Setups

CMD 261 – Define Action Control Block
CMD 262 – Action Control Block Triggers Control Zone
CMD 263 – Reset Action Control Blocks to Factory Setting
CMD 461 – Action Control Block Options

CMD 461: ACTION CONTROL BLOCK OPTIONS

Syntax: `START 461 * First ACB * Last ACB * NNNN * Value(s) #`

Variables: NNNN

1	Trigger Control Zone
4	Trigger Control Zone on Secure
16	General Alarm TZ
32	Duress Alarm TZ
64	Tamper Alarm TZ
128	Trouble Alarm TZ
256	Dial TZ
512	Log TZ
1024	Log Low Priority TZ

This variable is additive, meaning that up to nine actions can be stipulated by NNNN. Add variables to represent the included actions. For example, Trigger CZ (1) and General Alarm TZ (16) would render a variable of 17.

Description:

Use this command to trigger a control zone using an action control block (ACB) or other event, thereby causing special control conditions or annunciation to occur.

In V7.0, the time zone field of the specified control zone is used to determine whether the control zone is actually triggered.

Example:

```
START 461 * 1 * 2 * 513 * 4 * 5 #
```

Set 'Trigger Control Zone' in ACBs 1-2 to a value of 4, and 'Log TZ' to 5. Remember NN is additive where: 513 = 1 (Trigger Control Zone) + 512 (Log TZ).

Related CMDs:

- CMD 88*6, 88*16 – Print Standard, Master Control Zone Setups
- CMD 260 – Print Alarm Action(s)
- CMD 460 – Print Action Control Blocks

Alarm and ACB Setups

CMD 261 – Define Action Control Block
CMD 262 – Action Control Block Triggers Control Zone
CMD 263 – Reset Action Control Blocks to Factory Setting

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

CMD 479: CHANGE TIME FOR ALARM RELAYS

Syntax: `START 479 * Time1 [* Time2 * Time3 * Time4] #`

Variables:

Time1	General Alarms
Time2	Duress Alarms
Time3	Tamper Alarms
Time4	Trouble Alarms

Description:

DIGI*TRAC controllers have one or four dedicated alarm relays. A timer can be set for each of these relays, from 0 (zero)—do not actuate on alarm—to 8100 seconds.

Controllers with a single alarm relay use the same four alarm timers to trip the relay. Each timer is set individually. If any of the four alarm timers is active, the relay actuates. If you need to set one or more of the four conditions to *not* trip the relay, set its timer to zero.

This setup is used for special interface tasks like configuring digital communicators that transmit any of the four system action control blocks—general alarms on Relay 1, duress alarms on Relay 2, tamper alarms on Relay 3, or trouble alarms on Relay 4—to a monitored central station alarm company. Another task would be tripping local annunciation systems at a central guard station.

The general alarm relay is tripped by any of these conditions: Door Forced or Held Open, Input Tamper, Input Shorted, Noisy, Open, and Out-of-Spec, Occupancy and Passback Violations, and Deadman Timer Expired.

The duress alarm relay is tripped by a user entering their code with a duress digit at a keypad.

The tamper alarm relay is triggered by Box Tamper, ScramblePad/MATCH Reader Physical Tamper and Code Tampering.

The trouble alarm relay is tripped by power failures, battery problems, inactive networks, offline keypads, MATCHs, printers or modems, Report Buffer Threshold Exceeded, and Tag Alerts.

The fully-compliant V7.0 front-end host may use CMD 479 to replace CMD 79, thereby reducing the total number of commands sent to the controller.

Example:

```
START 479 * 10 #
```

Changes all four Alarm Relay Actuation Times To 10 Seconds

```
START 479 * 10 * 20 * 30 * 40 #
```

Changes Alarm Relay Actuation Times To 10 Seconds for General, 20 for Duress, 30 for Tamper, and 40 for Trouble.

Related CMDs:

CMD 88*2 – Print System Information

CMD 188*14 – Print Setup Changes for Relays

CMD 08 – Change Duress Alarm Mode
CMD 77 – Change Code/ID Tamper
CMD 261 – Define Action Control Block

CMD 549: ALERT CONTROL ZONE

Syntax: `START 549 * N * Control Zone #`

Variables: N

0 Alert Control Zone NO
1 Alert Control Zone YES

Description:

Alert a Control Zone is utilized to notify all Users of the specified Control Zone, Standard or Master, that a special condition exists such as: a message is waiting, a new Code is to be issued, a briefing is scheduled, a meeting is required, etc. The Alert is sounded at the ScramblePad Keypad where the User enters their Code as 4 short beeps of the ScramblePad Keypad's Alarm Annunciator. An Alert cannot be sounded at a MATCH reader since it has no audible alarm device.

The Alert message does not trigger any relays.

Example:

```
START 549 * 1 * 1 #
```

Alerts Control Zone 1

Default:

None

Related CMDs:

CMD 88*6, 88*16 – Print Standard, Master Control Zone Setup

Control Zone Setups

CMD 45, 304 – Define Standard, Master Control Zone

Tag and Alert Setups

CMD 49, 149 – Tag/Alert any User or Range of Users
CMD 249, 349 – Tag/Alert Access Zone
CMD 449 – Tag Control Zone

Host-Based Commands

While there are several host-based commands—those commands which must be sent by a host computer and routed through an XBox—only two of them are significant and can be used in any way at all by a qualified operator. These are CMD 98 and CMD 198.

For more host-based commands, refer to the *S*NET Gateway (XBox) Programmer's Reference* (ADD001-0301).

Both commands are explained on the following pages.

CMD 98: UPDATE/DOWNLOAD SETUP COMMANDS

Syntax: `98 * NN * P1 * P2 * P3 * P4`

Description:

This command can only be used between the host and controller with the XBox as intermediary, not between a ScramblePad and controller. For this reason it is available through the diagnostic window in SAM, the command line in S*NAP, the TestTool utility in MOMENTUM, and Velocity.

This command is used to upload to or download from the controller various values which speed up the operation of the DIGI*TRAC system.

For more information on host-based commands, refer to the *S*NET Gateway (XBox) Programmer's Reference* (ADD001-0899).

Variables:

NN Sub-Command

P1 – P4 Parameters: decimal numbers in the range 0 - 65535 for 16-bit parameters. Currently there are 25 sub-commands. (Where required, decimal ranges are specified for each subcommand.)

Discussion:

This command specifies a large number of subcommands, each of which is issued by the Host PC for translation by the XBox.

CAUTION **Use of these subcommands should be limited to those administrators/installers thoroughly conversant with the Hirsch system. Incorrect use of these commands can crash the system resulting in loss of all data and necessitate a cold start.**

The specific command used here is dictated by *NN* as determined by the following:

Sub-Command 1—Simulate CODE Entry

Access Class Functions

Parameter	Usage
P1	0 = Access
	2 = Unlock
	13 = Relock
P2	1 - 8 = Door Number
P3	0 - 65535 = Low word UID
P4	0 - 65535 = High word UID

Control Class Functions

Parameter	Usage
P1	1 = Control Trigger
	6 = Alarm Mask
	7 = Alarm Unmask
	14 = Force On
	15 = Force On Release
	16 = Force Off
	17 = Force Off Release
	18 = Lock Down
	19 = Lock Down Release
	20 = Lock Open
	21 = Lock Open Release
	22 = Momentary Mask
	26 = Entry Delay Cancel
	27 = Exit Timer Start
	28 = Mask Alarm/Entry Delay Cancel
	29 = Unmask Alarm/Exit Timer Start
P2	0 = Don't Care
P3	1 - 191 = Control Zone (1 - 255 for Control Trigger)
P4	0 - 65535 = Low word UID
P5	0 - 65535 = High word UID

Miscellaneous Function

Parameter	Usage
P1	3 = Alarm Cancel
P2 - P4	0 = Don't Care

Host Denial Functions

Parameter	Usage
P1	129 - 156 = Host Denial. 128 + Disposition
P2	1 - 16 = Reader (Door)
P3	0 - 65535 = Low UID word, if applicable
P4	0 - 65535 = High UID word, if applicable

Sub-Command 2—Alarm Cancel Button

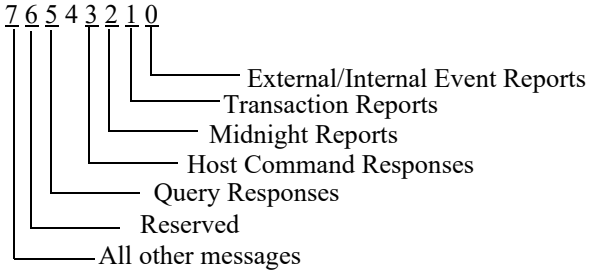
Parameter	Usage
P1	0 = Disable Button
	1 = Enable Button
P2 - P4	0 = Don't Care

Sub-Command 3—Return Alarm Relay State

Parameter	Usage
P1 - P4	0 = Don't Care

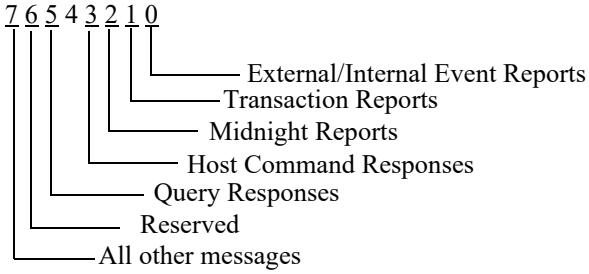
Sub-Command 4—Host Message Filters

Parameter	Usage
P1	Bit Flags:
P2 - P4	0 = Don't Care



Sub-Command 5—Local Printer Filters

Parameter	Usage
P1	Bit Flags:
P2 - P4	0 = Don't Care



Sub-Command 6—Open/Close low-priority host buffer (in DT controller)

Parameter	Usage
P1	0 = Close Buffer
	1 = Open Buffer
P2 - P4	0 = Don't Care

Sub-Command 7—Set Default HES Key

Parameter	Usage
P1	Bits 0 - 15
P2	Bits 16 - 31
P3	Bits 32-47
P4	Bits 48-63

! CAUTION **Use this subcommand only with extreme caution. Incorrect use of this command can crash the system and lead to loss of all data.**

Sub-Command 8—Not Used

Sub-Command 9—Set Host Password

Parameter	Usage
P1	Bits 0 - 15
P2	Bits 16 - 31
P3	Bits 32-47
P4	Bits 48-63

! CAUTION **Use this subcommand only with extreme caution. Incorrect use of this command can crash the system and lead to loss of all data.**

Sub-Command 10—Return ROM Signature

Parameter	Usage
P1 - P4	0 = Don’t Care

Sub-Command 11—System CODE Reset Button

Parameter	Usage
P1	0 = Disable Button
	1 = Enable Button
P2 - P4	0 = Don't Care

Sub-Command 12—Host Logoff

Parameter	Usage
P1 - P4	0 = Don’t Care

Sub-Command 13—Set Time

Parameter	Usage
P1	BCD Hour (12 Dec → 12H)

Parameter	Usage
P2	BCD Minute (15 Dec → 15H)
P3	BCD Second (30 Dec → 30H)
P4	0 = Don't Care

The values are sent in an unusual format using the decimal equivalent of hex. For instance, to specify 18, you convert it to its equivalent hex value, 12. For example, to set the time to 12:31:10, you would use 98*13*18*49*16*00#. This code segment shows how the format is derived and can be used by a third-party developer:

```
format_time_cmd(char buf[], int hr, int min, int sec)
{
hr += 6*(hr/10);
min += 6*(min/10);
sec += 6*(sec/10);
sprintf(cmd, "98*13*%d*%d*%d*0#",
hr,min,sec);
}
```

Note: Do not use this command unless you need to include it in code for a host program. Normally, use CMDs 50 and 51 to set time.

Sub-Command 14—Set Date

Parameter	Usage
P1	BCD Month (December → 12H)
P2	BCD Day (15th → 15H)
P3	BCD Year (1993 → 93H)
P4	0 = Don't Care

The values are sent in an unusual format using the decimal equivalent of hex. For instance, to set the year to 2010, you would take the last two digits (10) and convert them to its equivalent hex value, in this case A; if the hex value is a letter, you would then reconvert the hex value, A for example, to its decimal value, 16. For example, to set the date to Dec. 31, 2010, you would use 98*14*18*49*16*00#. This code segment shows how the format is derived and can be used by a third-party developer:

```
format_date_cmd(char buf[], int mm, int dd, int yy)
{
mm += 6*(mm/10);
dd += 6*(dd/10);
yy += 6*((yy%100)/10);
sprintf(cmd, "98*14*%d*%d*%d*0#",
mm,dd,yy);
}
```

Note: Do not use this command unless you need to include it in code for a host program. Normally, use CMD 50 to set a date.

Sub-Command 15—Request Date and Time

Parameter	Usage
P1 - P4	0 = Don’t Care

Sub-Command 16—Network Buffer

Parameter	Usage
P1	0 = Close Buffer
	1 = Open Buffer
P2 - P4	0 = Don't Care

Sub-Command 17—Super Status Request

Parameter	Usage
P1	0 = Return All Status
	1 = Base Relay Status
	2 = Expansion Relay Status
	3 = Keypad Status
	4 = Time Zone 0-63
	5 = Time Zone 64-127
	6 = Time Zone 128-149
	7 = Base Alarm Input Status
	8 = Exp. Alarm Input 1-8 Status
	9 = Exp. Alarm Input 9-16 Status
	10 = Alarm Relay/Lights Power/Printer Status
	11 = Std. Input/Battery/AC Power Voltages
	12 = Expansion Input Voltages
	13 = Host Signature
P2 - P4	0 = Don't Care

Sub-Command 18—Host Restore Setup

Parameter	Usage
P1 - P4	0 = Don’t Care

This command initializes

- all Standard, Master and Grand TZs
- all ACBs
- all Standard Access Zones, Master Access Zones
- standard Control Zones and all Master Control Zones

to their default values. This usually means clearing every field to 00.

Sub-Command 19—Force User Passback Location

Parameter	Usage
P1	0 = User Number
P2	0 = New Location
P3 - P4	0 = Don't Care

Sub-Command 20—Jam Inside User Count

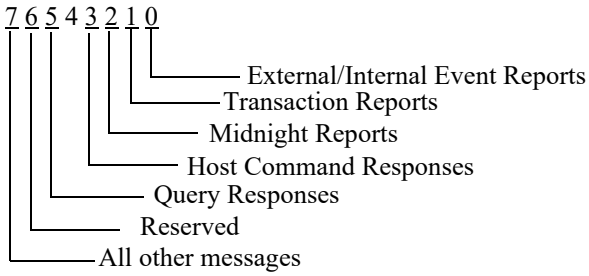
Parameter	Usage
P1	0 = New Inside User Count
P2 - P4	0 = Don't Care

Sub-Command 21—Host Text Insertion

Parameter	Usage
P1 - P4	Text / CR / Null

Sub-Command 22—Terminal Report Configuration

Parameter	Usage
P1	Bit Flags:



P2 - P4	0 = Don't Care

Sub-Command 23—Set Host Signature

Parameter	Usage
P1	0 - 65535 – First Signature Element
P2	0 - 65535 – Second Signature Element
P3	0 - 65535 – Third Signature Element
P4	0 - 65535 – Fourth Signature Element

Sub-Command 24—Keypad Programming Command Echo

Parameter	Usage
P1	0 = Echo Off
	1 = Echo On
P2 - P4	0 = Don't Care

Sub-command 25—Send First Alarm Info

Parameter	Usage
P1 - P4	0 = Don't Care

Sub-command 26—Reset Setups

Parameter	Usage
P1 - P4	0 = Don't Care

This subcommand initializes the following settings to their default values:

- all keypad and MATCH reader setups
- all relay, expansion relay, alarm input, and expansion input setups
- alarm relay times and alarm relay mapping
- PIN generation length
- programming mode timeout
- code tamper time settings
- default duress digit
- host timeout time
- SCIB baud rate settings
- 2-code rule settings
- occupancy count min inside settings.

Sub-Command 27—Clear user database

Parameter	Usage
P1 - P4	0 = N/A

Sub-Command 28—Set Configuration Options

Parameter	Usage
P1	0 - 255 = config1
P2	0 - 255 = config2
P3	0 - 255 = config3
P4	0 - 255 = config4

config1 and *config2* are defined bit by bit below. Each bit name is also specified.

config1 BIT 0 = Six-second system CODE Reset, ON = Enabled.
Note: If OFF, be careful you don't accidentally cold start the controller.
MCRENA.

BIT 1 = One-Second Alarm Cancel, ON = Enabled. ACNENA.

BIT 2 = Duress Mode. ON = Enable duress alarm handling. ENDUMF.

BIT 3 = Duress Generation Mode. ON = Enroll codes with duress digits. (Doesn't apply to code record downloads.) DRGEN.

BIT 4 = Bypass “no such hardware” errors. ON = Bypass, OFF = Check equipment before commands that use base or expansion relays, inputs, and other hardware. NOEQPERR.

BIT 5 = Bypass CODE conflict checking. ON = Bypass, OFF = check every CODE (and CARD) for conflicts before adding to user database. NOVLDT.

BIT 6 = Shorter “Auto Gen” CODE printout. Only applies to CMD 22 and related commands.
OFF = output all CODES to printer as they are generated. GENTIM.

BIT 7 = Show CODES on printer each time a user is added. ON = displays CODE record with PIN and CARD visible. SHOWCD.

config2 BIT 0 = SEKENA.
BIT 1 = EDMENA.
BIT 2-5 = Reserved.
BIT 6 = SEKBUG.
BIT 7 = ALMBUG.

Sub-Command 29—Global I/O Force On Relay From Host

Parameter	Usage
P1	0 - 8 – Relay to ‘Force On’
P2	0 - 64 – Expansion/Virtual Relay to ‘Force On’
P3	0 - 8 – Relay to ‘Force On Release’
P4	0 - 64 – Expansion/Virtual Relay to ‘Force On Release’

Sub-Command 30—Trigger Alarm or Event Condition

Parameter	Usage
P1	1 - 3 – where 3 = Alarm
P2	0 - 60 – Event Subtype
P3	0 - 255 – First parameter
P4	0 - 65535 – Second parameter

Sub-Command 31—Enable Self-Enrollment Kit

Parameter	Usage
P1	0 = disable, 1 = enable
P2 - P4	N/A

This subcommand requires special enrollment kit hardware.

Sub-Command 32—Expand Event Reporting Buffers

Parameter	Usage
P1	1 - 65520 Desired size of host event reporting buffer
P2	1 - 65520 Desired size of host alarm reporting buffer
P3	1 - 65520 Desired size of local printer report buffer
P4	1 - 65520 Desired size of local “alarm cancel” buffer

If the buffer in question has been expanded already, specifying a lower number will not truncate the buffer. Numbers will be rounded up to the next multiple of 780.

Sub-Command 33 - Set or Request Relay/Input States

Parameter	Usage
P1	1 - 3 – where: 1 = Enable specified inputs for input state change reporting. See also 05*9*1. Automatically requests state from previously-disabled inputs. 2 = Request input states from the designated inputs. Doesn't change which inputs have state changes enabled. 3 = Request relay states.
P2	0 - 255 – bit mask for alarms 1 - 8
P3	0 - 65535 – bit mask for expansion inputs 1 - 16
P4	0 - 65535 – bit mask for expansion inputs 17 - 32

Sub-Command 34—OR in Configuration Options

Parameter	Usage
P1	0-255 – bit mask to 'or' into config1
P2	0-255 – bit mask to 'or' into config2
P3	0-255 – bit mask to 'or' into config3
P4	0-255 – bit mask to 'or' into config4

config1 and *config2* are defined bit by bit below. Each bit name is also specified.

config1 BIT 0 = Six-second system CODE Reset, ON = Enabled.
Note: If OFF, be careful you don't accidentally cold start the controller.
MCRENA.

BIT 1 = One-Second Alarm Cancel, ON = Enabled. ACNENA.

BIT 2 = Duress Mode. ON = Enable duress alarm handling. ENDUMF.

BIT 3 = Duress Generation Mode. ON = Enroll codes with duress digits. (Doesn't apply to code record downloads.) DRGEN.

BIT 4 = Bypass “no such hardware” errors. ON = Bypass, OFF = Check equipment before commands that use base or expansion relays, inputs, and so on. NOEQPERR.

BIT 5 = Bypass CODE conflict checking. ON = Bypass, OFF = check every CODE (and CARD) for conflicts before adding to user database. NOVLDT.

BIT 6 = Shorter “Auto Gen” CODE printout. Only applies to CMD 22 and related commands.
OFF = output all CODES to printer as they are generated. GENTIM.

BIT 7 = Show CODES on printer each time a user is added.
ON = displays CODE record with PIN and CARD visible. SHOWCD.

config2 BIT 0 = SEKENA (see CMD 98*31).
BIT 1 = EDMENA.
BIT 2 = Enable globalized user management. GLOBUM
BIT 3 = Enable globalized relays. GLOBRY
BIT 4 & 5 reserved
BIT 6 = SEKBUG.
BIT 7 = ALMBUG.

Sub-Command 35—Set Reporting Options

Parameter	Usage
P1	0-255 rptopf1
P2	0-255 rptopf2
P3	0-255 rptopf3
P4	0-255 rptopf4

See also CMD 406.

Sub-Command 36—OR in Reporting Options

Parameter	Usage
P1	0-255 bit mask to 'or' into rptopf1
P2	0-255 bit mask to 'or' into rptopf2
P3	0-255 bit mask to 'or' into rptopf3
P4	0-255 bit mask to 'or' into rptopf4

The bit values for rptopf are provided below together with the respective bit names. Also shown in parentheses are the commands which these host functions replace or for which they substitute.

dbflag1 1 (BIT 0) = Wait for DUAL (non-COTZ) behavior. When an unknown card is presented, start Scramblepad and wait for PIN before rejecting the combination. (See also dbstat1.) WTDUAL
2 (BIT 1) = Immediate COTZ behavior. When in COTZ mode, accept or reject cards immediately. (Cards that are only enrolled as DUAL would be denied as "Incomplete Dual." Invalid cards will be denied as invalid.) IMCOTZ
4 (BIT 2) = XDAT enabled. See also BIT 7.
8 (BIT 3) = Host Grant support. HOSTGR
16 (BIT 4) = Short Pins.
32 (BIT 5) = Allow code record download overwrite. REFRESH.
64 (BIT 6) = Reserved.
128 (BIT 7) = Allocate XDAT record for every user. XDATALL

dbflag2 BIT 0,1 = XTOKEN support.
4 (BIT 2) = XZONE.
8 (BIT 3) = XDATES.
16 (BIT 4) = XASSET - enable tracking.
32 (BIT 5) = XRPT
64 (BIT 6) = reserved.
128 (BIT 7) = reserved.

See also CMD 406.

Sub-Command 37—Set All Message Filters

Parameter	Usage
P1	0-255 hprocm
P2	0-255 pprocm
P3	0-255 tprocm
P4	0-255 kprocm

See also Sub-Commands 4, 5, 22.

Sub-Command 38—OR in Database Processing Options

Parameter	Usage
P1	0-255 bit mask to 'or' into dbflag1
P2	0-255 bit mask to 'or' into dbflag2
P3	0-255 bit mask to 'or' into dbflag3
P4	0-255 bit mask to 'or' into dbflag4

rptopf1 BIT 0 = Enable state change reporting of TZ control of relay (TZRYRP, CMD 05*6)
BIT 1 = Time Zone State Change Reporting (TZSCRP, CMD 05*5)
BIT 2 = Enable reporting of Time Zone control of alarm masking (TZMSRP, CMD 05*7)
BIT 3 = New S*Xnet features (MOM, CMD 05*10)
BIT 4 = V7.0 S*Xnet features. Always on. (If it's off, you won't get this message.) (CMD 198*6, CMD 05*11)
BIT 5 = Enable keypad command echo. REPBOP.
(CMD 98*16, CMD 97*5)
BIT 6 = Command Echo Enabled CMDECHO. (CMD 97*7, CMD 98*24)
BIT 7 = HSTECHO.
Host Note: *A default value of 48 is suggested.*

rptopf2 BIT 0 = Enable Midnight reporting (MIDNITERPT, CMD 107, 97*9)
BIT 1 = Enable MCZ reporting. (RPTMCZ)
BIT 2 = Internal Event reporting enable flag. (IERPTG, CMD 05*2)
BIT 3 = External Event reporting enable flag. (EERPTG, CMD 05*3)
BIT 4 = Transaction reporting enable flag (TRRPTG, CMD 05*4)
BIT 5 = Relay State Change Reporting Flag (RYSCRP, CMD 05*1)
BIT 6 = Invalid Code Reporting (INVCOD/invldcoderpt, CMD 109)
BIT 7 = Reserved.
Host Note: *A default value of 88 is suggested.*

Sub-Command 39—Test DS47 Annunciator

Parameter	Usage
P1	1-16 Reader number of keypad
P2	1-7 Test to perform
P3	0-65535 See below
P4	0-15 See below

The tests currently available are:

1. Display value of P3 on the keypad
2. Beep P3 (1-12) times; value of P4 controls the tone. (1=low, 7=high; 8=long low, 15=long high)
3. Scramble-Up
4. Start Up, Unscrambled
5. Beep test
6. Falling beep test
7. Display “123 456 789" (no “0”)
8. Display “111 222 333 4”
9. Display “007” on second row

   *Note: These four ‘display on LEDs’ options test the same feature in the DS47, but exercise different DIGI*TRAC firmware paths.*

10. Disable Start key for 255 seconds
11. Enable Start key

12. Send test text message to MRCB annunciator channel
13. Test Card LED drive lines

*Note: If you use 98*39*RDR*11*7*7#, use 98*39*RDR*11*8*8# to end the test.*

Sub-Command 40—Execute Control Function

Parameter	Bit	Usage
P1	1	Control Trigger
	6	Alarm Mask
	7	Alarm Unmask
	14	Force On
	15	Force On Release
	16	Force Off
	17	Force Off Release
	18	Lock Down
	19	Lock Down Release
	20	Lock Open
	21	Lock Open Release
	22	Momentary Mask
P2	0 - 8	Base relay or alarm input
P3	0 - 64	Expansion relay or alarm input
P4	0	0 - 65535 Low word UID
P5	0	0 - 65535 High word UID

Sub-Command 41—Turn On/Off Config Flags

P1	Usage	P2	Usage
1	config1	1	System CODE Reset Button Enable
		2	Alarm Cancel Button Enable
		3	Duress Alarm Handling
		4	Duress CODE Generation
		5	Bypass ‘No Such Hardware’ Errors. NOEQPERR.
		6	Bypass CODE Conflict Checking
		7	Auto-Gen Summaries Only. GENTIM.
		8	Show CODES when added. SHOWCD.
2	config2	1	SEKENA.
		2	EDMENA.
		3	Globalized User Management. GLOBUM.

		4	Globalized Relays and MCZ's. GLOBRY.
5	rptopf1	1	TZ Relay Control State Changes
		2	Time Zone State Changes
		3	Time Zone Alarm Control Reporting
		4	MOM S*Xnet Features. SXNET.
		5	Vn. 7 S*Xnet Features. SXNET2.
		6	Event Host Buffer Open
		7	Command Echo. CMDECHO.
		8	Print SNET Messages. SNETPRN.
6	rptopf2	1	Midnight Reports
		2	MCZ Reporting (for troubleshooting). RPTMCZ.
		3	Internal Events
		4	External Events
		5	Transaction Reporting
		6	Relay State Changes
		7	Invalid Code Reporting
		8	RPTACB Reporting (for troubleshooting). RPTACB.
7	rptopf3	1	Reserved. SKIPDUP.
9	dbflag1	1	WTDUAL.
		2	IMCOTZ.
		3	XDAT.
		4	Host Grant Support. HOSTGR.
		5	Short PINs
		6	Allow CODE Record Download Overwrite.
		8	XDATALL
10	dbflag2	3	XDAT
13	pprocm Printer Msg Filters	1	External/Internal Events
		2	Transaction Reports
14	hprocm Host Msg Filters	3	Midnight Reports
		4	Command Responses
15	tprocm Terminal Msg Filters	5	Command Completes
		6	Query Responses

16	kprocm Keypad Msg Filters	7	Title Messages
		8	Other Messages
17	mdmopf1	1	Modem control: Use Pulse Dialing instead of Tone? PULSEDIAL.
		2	Modem control: dial host (call back) instead of accepting incoming logins? CALLBACK.
		3	Reserved. HANGUPOK.
		4	Reserved. INCBAUD.

Sub-Command 42—Allocate User Database

Parameter	Usage
P1	0-65535 Desired minimum number of users. Low word.
P2	0-2 High word of min user allocation
P3	0 NA
P4	0 NA

Sub-Command 43—Reset Buffer Pointers

Parameter	Usage
P1	3 Reset Host Alarm and Host Event Buffer Pointers 255 Reset all Host, Printer, and Globalization Buffer Pointers
P2	0 Reserved
P3	0 Reserved
P4	0 Reserved

Sub-Command 44—Forgive Physical Zone Users, Reset Inside User Count

Forgive all users that are in the designated PZ's. If GLOBALUM is set, tell the other controllers on the XBox to do the same.

Parameter	Usage
P1	0-63 First PZ
P2	0-63 Last PZ. (If P1 > P2, it uses P1.)
P3	0 Reserved
P4	0 Reserved

Examples:

To clear the entire User Database and reset the Master CODE to 123:

```
98 * 27 * 0 * 0 * 0 * 0 #
```

To unlock Door 3:

```
98 * 1 * 2 * 3 * 0 * 0 #
```

To relock Door 7:

```
98 * 1 * 13 * 7 * 0 * 0 #
```

To turn off command responses (during command upload):

```
98 * 1 * 4 * 151 * 0 * 0 #
```

To turn on command responses (after command upload):

```
98 * 1 * 4 * 159 * 0 * 0 #
```

To enable the Self-Enrollment Kit, Access Zone 65, and Reader 2:

```
90 * 2 #
97 * 10 * 0 * 2 * 65 * 0 #
98 * 31 * 1 * 0 * 0 * 0 #
```

To enlarge the Scramble*Net event buffer to 20,000 events (actually 20,280) and 2,000 (actually 2,340) alarms:

```
98 * 32 * 20000 * 2000 * 0 * 0#
```

To lock open (energize) Base Relay 2 and Expansion Relay 33:

```
98 * 40 * 20 * 2 * 33 * 0 #
```

To turn on SNET MSG Printing and turn off Command Echo:

```
98 * 41 * 5 * 8 * 1 * 0 #
98 * 41 * 5 * 7 * 0 * 0 #
```

To log off the Host:

```
98 * 12 * 0 * 0 * 0 * 0 #
```

Related CMDs:

CMD 198 - Host-Only Commands

CMD 198: HOST-GENERATED COMMANDS

Syntax: `198 * N * P1 * P2 * P3 * P4`

Description:

This command can only be used between the host and controller with the XBox as intermediary, not between a ScramblePad and controller. For this reason it is available through the diagnostic window in SAM, the command line in S*NAP, the TestTool utility in MOMENTUM, and Velocity.

This command is used to upload to or download from the controller advanced values which speed up the operation of the DIGI*TRAC system.

For more information on host-based commands, refer to the *S*NET Gateway (XBox) Programmer's Reference* (ADD001-0899).

Variables:

N	Single-digit sub-command number
P1 – P4	Decimal number in the range 0 - 65535

Discussion:

This command incorporates a number of subcommands which can be issued by the Host PC for translation by the XBox.

CAUTION **Use of these subcommands should be limited to those administrators and installers thoroughly conversant with the Hirsch system. Incorrect use of these commands can crash the system resulting in loss of all data and necessitate a cold start.**

The specific command used here is dictated by the variable N as determined by the following:

Sub-Command 1—Hello, Trigger Self ID Message Build

Parameter	Usage
P1 - P4	0 = Don't Care

Sub-Command 2—Logon

Parameter	Usage
P1	PW1 Decimal number for password bytes 0 - 1
P2	PW2 Decimal number for password bytes 2 - 3
P3	PW3 Decimal number for password bytes 4 - 5
P4	PW4 Decimal number for password bytes 6 - 7

Sub-Command 3—Reload Default HES keys

Parameter	Usage
P1 - P4	0 = Don't Care

Sub-Command 4—Trigger Modem Dial-Back

Parameter	Usage
P1 - P4	0 = Don't Care

Sub-Command 5—Hello, Self-ID Message, New Protocol

Parameter	Usage
P1 - P4	0 = Don't Care

Sub-Command 6—Log on, New Protocol

Parameter	Usage
P1	PW1 Decimal number for password bytes 0 & 1
P2	PW2 Decimal number for password bytes 2 & 3
P3	PW3 Decimal number for password bytes 4 & 5
P4	PW4 Decimal number for password bytes 6 & 7

Sub-Command 7—Turn on/off Global Relay

Parameter	Usage
P1	Master Controller Address
P2	Global Relay Identifier
P3	Relay Status Word (RSTT1,2)
P4	n/a

Sub-Command 8—Update Globalized User

Sub-Command 9—Set Security Level

Parameter	Usage
P1	Security Level ("Threat Level") Range is 0 - 99
P2	Readers to set: 255 = set readers 1-8 65535 = set all readers
P3	n/a
P4	n/a

Sub-Command 10—Log on, New Protocol, Hold Events

Parameter	Usage
P1	PW1 Decimal number for password bytes 0 - 1
P2	PW2 Decimal number for password bytes 2 - 3
P3	PW3 Decimal number for password bytes 4 - 5
P4	PW4 Decimal number for password bytes 6 - 7

Sub-Command 11—Global User Update
(for CMD 421)

Parameter	Usage
P1	reserved
P2	reserved
P3	reserved
P4	reserved

Sub-Command 12—Global Forgive Physical Zone Users, Reset Inside User Counts
(for CMD 98*44)

Parameter	Usage
P1	0 - 63 = first PZ
P2	0 - 63 = last PZ
P3	n/a
P4	n/a

Related CMDs:

CMD 98 - Host-Only Commands

CMD 435: DEFINE OCCUPANCY COUNT LIMITS FROM HOST

Syntax: `START 435 * FirstPZ * LastPZ * mininside * maxinside * 2mndsblthr #`

Variables:

mininside	Minimum Count
maxinside	Maximum Count
2mndsblthr	Occupancy Threshold For Auto-Disable Of 2-Person Access Rule

Description:

Using this command enables you to set occupancy count limits for an area controlled by entry and exit readers. You can set both a minimum and a maximum limit. The default is set to a minimum of 2 and a maximum of 0 (zero) none.

When the area is occupied by one less than the minimum setting, an occupancy violation alarm occurs after a 20-second delay. As long as the occupancy remains below the minimum, the occupancy violation alarm recurs every 2 minutes.

The maximum occupancy count is used to override and deny access to the controlled area by more users than the maximum count. If the maximum count is set to 50 the 51st authorized user is denied access. Once the count falls below the maximum, additional authorized users may access the area. You can set the maximum count in a range of 0 (zero) meaning disabled up to the maximum user memory of the system.

You can use both minimum and maximum counts to trigger control zones for special alarms, area annunciators, occupancy status signs, or other purposes using CMD 436.

Set the occupancy threshold for auto-disable of two-person rule using CMD 437.

All unspecified fields are set to 00.

For the occupancy controls to work, you must enable passback control for the same readers.

Example:

```
START 435 * 23 * 25 * 6 * 50 #
```

Set Minimum Count to 6 people and Maximum Count to 50 people for PZ 23 through 25

Related CMDs:

CMD 88*27 – Print Occupancy Controls

CMD 188*9 – Print Setup Changes for Passback & User Management

Occupancy Commands

CMD 235 – Change Occupancy Count Limits
CMD 236 – Trigger Control Zone on Change in Occupancy Count
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-Person Access Rule
CMD 238 – Single Zone Access
CMD 436 – Define Occupancy Count Control Zones From Host
CMD 437 – Define Occupancy, Passback, Two-Person

CMD 436: DEFINE OCCUPANCY COUNT CONTROL ZONES FROM HOST

Syntax: `START 436 * FirstPZ * LastPZ * CZ1 * CZ2 * CZ3 * CZ4 * CZ5 * CZ6 * CZ7 * CZ8 * CZ9 #`

Variables:

CZ1 Change from 0 to 1
CZ2 Change from 1 to 2
CZ3 Change from 2 to 1
CZ4 Change from 1 to 0
CZ5 Count is at the minimum
CZ6 Count is at the minimum less 1
CZ7 Count is at the minimum plus 2
CZ8 Count is at the maximum
CZ9 Count is at the maximum less 1

Description:

Use this command to trigger a standard or master control zone when a change in occupancy count occurs for the associated physical zones (PZ). The minimum and maximum occupancy limits is defined for these physical zones (FirstPZ * LastPZ) in the previous command, CMD 435.

You can use this command to trip alarms, area annunciators, or occupancy status signs. It can also be used to automatically mask the interior alarms in the controlled area on the 'first person in' and unmask the area on the 'last person out.'

Make sure to set all unspecified fields to 00.

The fully-compliant V7.0 front-end host may use CMD 435 and CMD 436 to replace CMDs 235, 236, and 237, thereby reducing the total number of commands sent to the controller to set up occupancy controls.

Example:

```
START 436 * 23 * 25 * 0 * 0 * 0 * 0 * 12 #
```

Trigger Control Zone 12 when the inside user count equals the minimum count for PZ 23 through 25. Using the example shown in CMD 435, this minimum count for PZ 23 - 25 would be defined as 6 people.

Related CMDs:

CMD 88*27 – Print Occupancy Controls

CMD 188*9 – Print Setup Changes for Passback & User Management

Occupancy Commands
CMD 235 – Change Occupancy Count Limits
CMD 236 – Trigger Control Zone on Change in Occupancy Count
CMD 237 – Change Occupancy Threshold for Auto-Disable of 2-person Access Rule
CMD 238 – Single Zone Access
CMD 435 – Define Occupancy Count Limits From Host
CMD 437 – Define Occupancy, Passback, Two-Person

CMD 450: SET DATE AND TIME FROM THE HOST

Syntax: `START 450 * YYYYMMDD * Day Of The Week * HHMMSS #`

Description:

Use this command to set the controller's date, day of the week, and time through the connected host computer.

Setting the date and day of the week sets the system clock / calendar for accurate access restriction, automatic event scheduling, and transaction reporting using the system printer or SCRAMBLE*NET.

The accuracy of all time-controlled functions depends on this setting.

Set the day of the week for the current day using this format:

Date:	January	= Month 01
	February	= Month 02
	March	= Month 03
	April	= Month 04
	May	= Month 05
	June	= Month 06
	July	= Month 07
	August	= Month 08
	September	= Month 09
	October	= Month 10
	November	= Month 11
	December	= Month 12

Day:	Monday	= Day 1
	Tuesday	= Day 2
	Wednesday	= Day 3
	Thursday	= Day 4
	Friday	= Day 5
	Saturday	= Day 6
	Sunday	= Day 7

Set the time in 24-hour format, HHMMSS, like this:

Time:	000000 = Midnight	120000 = Noon
	010000 = 1 AM	130000 = 1 PM
	020000 = 2 AM	140000 = 2 PM
	030000 = 3 AM	150000 = 3 PM
	040000 = 4 AM	160000 = 4 PM
	050000 = 5 AM	170000 = 5 PM
	060000 = 6 AM	180000 = 6 PM
	070000 = 7 AM	190000 = 7 PM
	080000 = 8 AM	200000 = 8 PM
	090000 = 9 AM	210000 = 9 PM
	100000 = 10 AM	220000 = 10 PM
	110000 = 11 AM	230000 = 11 PM

If you're using S*NAP, this command sets the time in each controller, not in the PC. Use S*NAP setup commands to set the PC time.

Example:

```
START 50 * 20000101 * 6 * 120000 #
```

Set The Date To January 1, 2000, Saturday, 12:00:00 Noon

Related CMDs:

 CMD 88*1 – Print Date, Time, Version Number

 CMD 188*1 – Print Setup Changes for Date, Time, Version Number

Date, Time, and Holidays

CMD 50 - Set Date and Day of the Week
CMD 51 - Set Time
CMD 57-59 - Define, Clear Holidays
CMD 98*13, 98*14 - Set Time, Date

Time Zone Setups

CMD 52, 54, 454 - Define/Clear Standard Time Zone

CMD 457: DEFINE HOLIDAY(S) FROM THE HOST

Syntax:

```
START 457 * NN * Year * MMDD #
START 457 * NN * Year * MMDD * MMDD#
```

Variables: **NN**

0	Clear any and all holidays for given date or range of dates.
1234	Set holidays for given date or range of dates. Use '1234' to set all 4 holiday tables.
5	Set daylight savings time 'spring forward' and 'fall back' dates.

Year

00-99	Corresponds to years 2000–2099.
2099-2999	Alternatively, you can specify a 4-digit year.

MMDD Month and day for the specified year.

Description:

Version 7 has four Holiday Tables, each with two years of 366 days and a pair of Daylight Savings Time change dates. **NN** controls the Holiday Table for which a particular date is set.

The four Holiday Tables allow for applications such as half-day holidays, multiple tenants who recognize different holidays, and flexible work schedules.

- ❏ Half-Day Holidays – Instead of having one Time Zone all workday, define a Time Zone with one Holiday Table for the half day that the company will be open and a Time Zone with another Holiday Table for the half day the company will be closed. Put them together in a Master Time Zone for regular days and holidays. For a half day holiday, use the Holiday Table you selected for your half-day Time Zone.
- ❏ Multiple Tenants – For two or more tenants sharing the same security system. Each tenant will use a different Table.
- ❏ Flex Schedules – If, for example, you need to set up two schedules, each with every other Friday off, and put users in two different groups, each with their own Access Zone. Each group will be assigned to a different Holiday Table. Set each group's table to be a Holiday every other Friday.

When setting up Time Zones, select Day 8 to indicate that the Time Zone will be in effect even during the Holiday Schedules you select. When you do not select Day 8, the time zone will NOT be in effect during the Holiday Schedules you select. Time Zones will ignore any holidays not in the Holiday Schedule selected for that Time Zone.

Unplanned Holidays, such as snow days and fire evacuations, can be defined and updated immediately.

All Holidays defined for the previous year are deleted at year's end.

Note: On the Daylight Savings Time "fall back" date (old "Holiday 32")—the date when the time falls back from 02:00AM to 01:00AM—there will be one hour of overlap in the recorded or printed history log for that date. In other words, there will be two one-hour periods from 01:00 to 02:00 hours recorded for that date.

Examples:

```
START 457 * 1 * 00 * 0101 #
```

Define January 1, 2000 as a holiday in Holiday Table 1

```
START 457 * 2 * 2000 * 0101 #
```

Define January 1, 2000 as a holiday in Holiday Table 2 (and clears it from Holiday Table 1,3,4 if present).

```
START 457 * 5 * 2000 * 0415 * 1031 #
```

Define Daylight Savings change dates for April 15, 2000 (forward 1 hour), and October 31, 2000 (back 1 hour).

```
START 457 * 12 * 2000 * 1224 * 1231 #
```

Define Dec. 24-31, 2000 as holidays in both Holiday Tables 1 and 2.

```
START 457 * 2 * 2000 * 1224 #
START 457 * 1 * 2000 * 1225 * 1231 #
```

Defines Dec. 24, 2000 as a holiday in Holiday Table 2, and Dec. 25-31 as holidays in Holiday Table 1. (You might have "Holiday Table 1" set up for full-day holidays and "Holiday Table 2" set up for "Half-Day Holidays".)

```
START 457 * 1 * 2000 * 1225 #
START 457 * 2 * 2000 * 1224 #
START 52 * 3 * 0800 * 1200 * 12345 * 1 #
START 52 * 4 * 1200 * 1700 * 12345 * 12 #
START 454 * 66 *3 *4 #
```

Half-Day Holiday – Holiday Schedule 1 includes full-day holidays. Holiday Schedule 2 includes half-day holidays. Time Zone 3 includes mornings, except full-day holidays. Time Zone 4 includes afternoons, except half- or full-day holidays. Master Time Zone 66 contains morning and afternoon time zones.

```
START 457 * 1 * 2000 * 0107 #
START 457 * 2 * 2000 * 0114 #
START 457 * 1 * 2000 * 0121 #
START 457 * 2 * 2000 * 0128 #
```

Flexible Schedule – Groups with Holiday Schedule 1 have “holidays” or days off on the first and third Fridays of January. Groups with Holiday Schedule 2 have days off on the second and fourth Fridays of January.

Related CMDs:

CMD 50 – Set Date & Day Of The Week
CMD 52 – Define Standard Time Zone
CMD 59 – Clear All Holidays
CMD 88 – Print System Setups and Status

Factory Setup & Printout

5

This Page Left Intentionally Blank

Factory Setup Guide

When you use CMD 88, the DIGI*TRAC controller returns a list of the current setups and status for the component(s) you requested. If your controller is linked to a printer, the result of your query is printed out; if you are linked to a host PC, the results are displayed on the screen. Whichever output method you select, the generated list presents a lot of material in a compressed form. While most of the information presented there is self-explanatory, some of it may require explanation. To fully understand what these lists and forms mean, refer to the specific commands in this section.

The following pages show the complete System Setup and Status Report for a DIGI*TRAC Model 8. This report is printed by executing the CMD 88*0. You may also print just individual parts of the report by choosing different variables in the CMD 88. The values shown on the following pages reflect the factory default setups in a Controller newly shipped from the factory or immediately after a cold start of the system. Following the factory default report is a listing of each subcategory and the commands used to change each one. Only make those changes to the factory defaults you feel are necessary to meet the requirements of your system. CMD 88 and its variables are:

ST 88 * NN #

0 - Complete System Setups and Status
1 - Date, Time, Version Number
2 - System Information
3 - Standard Time Zone
4 - Master Time Zone
5 - Standard Access Zone
6 - Standard Control Zone
7 - Relays
8 - Alarm/RQE Inputs
9 - Alarm Special Setups and Status
10 - Doors
11 - Keypads/MATCH Readers
12 - MATCH
13 - Holidays
14 - Grand Master Time Zones
15 - Master Access Zones
16 - Master Control Zones
17 - Detailed Relay Status Only
18 - Expansion Relays
19 - Detailed Expansion Relay Status Only
20 - Expansion alarm/RQE Inputs
21 - Expansion Alarm Special Setups and Status
22 - Expansion Line Module Input Door Setups
23 - Reporting Setups
24 - Remote Site Management Setups
25 - System Power Status (of AC power, standby battery, and memory battery)
26 - Transactions Since Midnight
27 - Occupancy Controls
28 - Virtual Relays
29 - Detailed Virtual Relay Status Only
30 - HEC Factory Diagnostics
31 - Special Needs Unlock Extension
32 - Special Keypad / MATCH Setups
33 - Special MATCH Card Mapping
34 - Additional Special Keypads / MATCH Setups
50 - ACBs

51 - Who's Inside (Passback Zones)
52 - Function Groups

The order of topics below is that provided when you use CMD 88 * 0. The command variable you would use to display a specific section of the data is shown in the left margin.

Note: Neither the command in bold nor the commentary appears in the data readout.

CMD 88 * 0 - Complete Setups

This lists the complete printout generated when you send the 88 * 0 command. The bold does not appear in the printout.

```
***
<HIRSCH M1>  Ver 7.78.5 *** cdbb000225

00:21:50 - Sat - 01 Jan 2000
Max Users = 01024  Total Users = 00001
Users Inside (PZ 2) = 00000

Cmd> 88 * 2 #
* System Information
Configuration: 4 Relays - 64 Expansion Relays - 0 Alarm Relays
4 Inputs - 0 Expansion Inputs
Options:
SPIB - Baud Rate=9600-8-N-1
Onboard Users - 416 KB - 6K Users
Long RAM
Max Users = 01024 allocated, limit= 04352
Network Inactive
1 Active Keypads 1 Active MATCH Readers
Auto-Generation CODE Length = 7 - Standard card length = 8
Language = 0 (English)
Current Duress Digit = 9
Duress Alarm Mode Disabled
Duress CODE Generation Mode Disabled
CODE Tamper Time Penalty = 20
CODE Tamper Alarm Threshold = 50
CODE Tamper Lockout = 1 min
Programming Mode Timeout = 8
Alarm Relay Times:
General = 60 Map to: Relay 4
Duress = 60 Map to: Relay 4
Tamper = 60 Map to: Relay 4
Trouble = 60 Map to: Relay 4
System CODE Reset Button Enabled
Alarm Cancel Button Enabled
Report Buffer = Open
Report Buffer Size= 1560/ 1560/  780
Alarm Buffer Size = 1560

Cmd> 88 * 3 #
Standard Time Zone Setups and Status
  #       Start       End  MTWTFSSH 1234
  0: From 00:00  to  00:00 -------- ---- Inactive
 65: From 00:00  to  24:00 XXXXXXXX XXXX Active

Cmd> 88 * 4 #
Master Time Zone Setups and Status
    |  <- Standard Time Zones ->
TZM |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |
----+----+----+----+----+----+----+----+----+
 66 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 | Inactive
```

```
Cmd> 88 * 5 #
Standard Access Zone Setups
   |  |  |        <-Time Zones->         |
AZS|TG|AL| R1| R2| R3| R4| R9|R10|R11|R12|
  0|--|--| - | - | - | - | - | - | - | - |
 65|--|--| 65| 65| 65| 65| 65| 65| 65| 65|

Cmd> 88 * 6 #
Standard Control Zone Set Ups
 CZS| TZ | TAG|ALRT| ONBOARD  |
  0 |  0 | -- | -- |   None   |

Expansion Relays or Inputs:
              1111111 11122222 22222333 33333334 44444444 45555555 55566666
CZS| 12345678 90123456 78901234 56789012 34567890 12345678 90123456 78901234
 0 | -------- -------- -------- -------- -------- -------- -------- --------

Cmd> 88 * 7 #
Relay Setups and Status
RY |OP/ | 2 | DOOR | DOOR |CONTRL| CTRL ||ACT|DIS|CLR|TRG|RTG|DUCFFTTZZLL|
#  | RPT|MAN| TIME | DELAY| TIME | DELAY|RESTS| TZ| TZ| TZ| CZ|CZ|TLTNFADADDO|
  1|Door|OFF|    6s|    0s|    6s|    0s| OFF |  0|  0|  0|  0| 0|-----------|
  2|Ctrl|OFF|    6s|    0s|    6s|    0s| OFF |  0|  0|  0|  0| 0|-----------|
  3|Ctrl|OFF|    6s|    0s|    6s|    0s| OFF |  0|  0|  0|  0| 0|-----------|
  4|Ctrl|OFF|    6s|    0s|    6s|    0s| OFF |  0|  0|  0|  0| 0|-----------|

Cmd> 88 * 8 #
Alarm Setups and Status
INP|CONTACT|TIM| TZ |CTL |DSBL|TRG|RTG|ACT|DIS|    |LINE | CONTACT
 #  |NRMALLY|ZON|MSKD|MSKD|NOW |CZ |CZ |CZ |CZ |VOLT|MODE |   IS
  1| Closed|  0| -- | -- | -- |  0|  0|  0|  0|0.00|DTLM2|Open Ckt
  2| Closed|  0| -- | -- | -- |  0|  0|  0|  0|0.00|DTLM2|Open Ckt
  3| Closed|  0| -- | -- | -- |  0|  0|  0|  0|0.00|DTLM2|Open Ckt
  4| Closed|  0| -- | -- | -- |  0|  0|  0|  0|0.00|DTLM2|Door X |RQE file://|

Cmd> 88 * 9 #
Alarm Special Setups and Status
   | Entry/Exit Delay |      |DOTL |MAX  | TZ |   |INP|     |
INP|ENTRY|EXIT |  TZ  |  TZ  |WARN |DOOR | UN-|fg1|STA|LINE |
 #  |DELAY|DELAY|DIS EE|DISRQE|TIME |EXTND|MASK|   |CHG|MODE |
  1|   0 |   0 |   0  |   0  |    0|00:00|  0 |  0|   |DTLM2|
  2|   0 |   0 |   0  |   0  |    0|00:00|  0 |  0|   |DTLM2|
  3|   0 |   0 |   0  |   0  |    0|00:00|  0 |  0|   |DTLM2|
  4|   0 |   0 |   0  |   0  |    0|00:00|  0 |  0|   |DTLM2|

Cmd> 88 * 10 #
Door Setups and Status
DOOR| DOOR|DOOR | DOTL| DOTL | AUTO |   |RQE|RQE|LINE | CONTACT
 #  | TIME|DELAY| SECS|ALWAYS|RELOCK|RQE|RLY|RTG|MODE |   IS
  1 |    6|    0|   12|  --  | Open |OFF| - | - |DTLM2|Open Ckt
  2 |    6|    0|   12|  --  | Open |OFF| - | - |DTLM2|Open Ckt
  3 |    6|    0|   12|  --  | Open |OFF| - | - |DTLM2|Open Ckt
  4 |    6|    0|   12|  --  | Open |OFF| - | - |DTLM2|Door X |RQE file://|
```

```
Cmd> 88 * 11 #
Keypad / MATCH Setups and Status
  |   |   |   |   |Stt|   |   |   |   |Yel|Y- |GRN|GFl|           |
  |Onl|Acc|Ctl|Prg|req|Scr|Sil|Red|Grn|#1 |ACF|RLY|DDy|Passback PZ|
01| - | X | X | X | X | - | - | - | - | - | - | - | - |00 00 Unlim|
02| X | X | X | X | X | - | - | - | - | - | - | - | - |00 00 Unlim|
03| - | X | X | X | X | - | - | - | - | - | - | - | - |00 00 Unlim|
04| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
05| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
06| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
07| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
08| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
09| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
10| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
11| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
12| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
13| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
14| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
15| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|
16| - | X | X | X | X | X | - | - | - | - | - | - | - |00 00 Unlim|

Cmd> 88 * 12 #
Match Setups and Status
    | On-|Ch2|  |Ch 1|Ch 2| Reader  |Ch1|Ch2|Phys|Rly|Ch1|Ch2|Ch1|Ch2|
ADDR|line|Ena|Vn|COTZ|COTZ|Interface|LED|LED|Tmpr|LED|Kpd|Kpd|Rdr|Rdr|
----|----|---|--|----|----|---------|---|---|----|---|---|---|---|---|
  1 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  2 | XX | X |32|  0 |  0 |   ABA   | - | - | -- | - | X | - | X | X |
  3 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  4 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  5 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  6 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  7 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  8 | -- |   |  |  0 |  0 |         | - | - | -- | - | - | - | - | - |
  9 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 10 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 11 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 12 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 13 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 14 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 15 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |
 16 | -- |   |  |  0 |    |         | - |   | -- | - | - |   | - |   |

Cmd> 88 * 13 #
Holidays
Year=0000
Year=0000

Cmd> 88 * 14 #
Grand Master Time Zone Setups and Status
    |      <- Master Time Zones ->
TZG |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |
----+----+----+----+----+----+----+----+----+
130 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 | Inactive


Cmd> 88 * 15 #
Master Access Zone Setups
              |  <- Standard Access Zones ->
 AZM | TAG|ALRT|  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |
-----+----+----+----+----+----+----+----+----+----+----+
  66 | -- | -- |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |
```

```
Cmd> 88 * 16 #
Master Control Zone Setups and Status
CZM|   |    |    |TRIG|CLR |    | UN | UN | RE |FORC| RE |FORC| RE |
 # | TZ| TAG|ALRT|RYS |RYS |MASK|MASK|LOCK|LOCK| ON |LEAS|OFF |LEAS|
---+---+----+----+----+----+----+----+----+----+----+----+----+----+
192|  0| -- | -- |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |
---+---+----+----+----+----+----+----+----+----+----+----+----+----+
   |THR|    |MCZ |LOCK| RE |LOCK| RE |KPD |ENTR|EXIT|COND|PART|GLOB|
   |LVL| AZ |LINK|DOWN|LEAS|OPEN|LEAS|ANNC|CNCL|STRT|UMSK|UMSK| ID |
   +---+----+----+----+----+----+----+----+----+----+----+----+----+
   |  0| 65 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |
   +---+----+----+----+----+----+----+----+----+----+----+----+----+

Cmd> 88 * 17 #
Detailed Relay Status
RY | DOOR|     |CNTRL|FORCE|FORCE|  TZ |  TZ |  CZ |  CZ | LOCK| LOCK|OPER-|
#  |TIMER|UNLOK|TIMER|  ON | OFF | ACT | DIS | ACT | DIS | DOWN| OPEN|ATION|NOW
  1|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  2|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  3|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  4|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off

Cmd> 88 * 18 #
Expansion Relay Setups and Status
XRY|CONTRL|CONTRL|     |ACT|DIS|CLR|TRG|RTG|UCFFTTZZLL|
#  | TIME | DELAY|RESTS| TZ| TZ| TZ| CZ| CZ|LTNFADADDO|

Expansion Relays not Available

Cmd> 88 * 19 #
Detailed Expansion Relay Status
RY |CNTRL|FORCE|FORCE|  TZ |  TZ |  CZ |  CZ | LOCK| LOCK|OPER-|
#  |TIMER|  ON | OFF | ACT | DIS | ACT | DIS | DOWN| OPEN|ATION|NOW
Expansion Relays not Available

Cmd> 88 * 20 #
Expansion Alarm Inputs not Available

Cmd> 88 * 21 #
Expansion Alarm Inputs not Available

Cmd> 88 * 22 #
Expansion Alarm Inputs not Available

Cmd> 88 * 23 #
* Reporting Setups
TZ |TZ |TZ |SNT|SNT|RPT|CMD|SNT|MID|MCZ|INT|EXT|TRN|RLY|INV|ACB|
RLY|SC |ALM|MOM|Vn7|BUF|ECH|PRN|NIT|RPT|EVN|EVN|RPT|RPT|COD|RPT|
 X | X | X | - | - | X | X | X | - | - | X | X | X | - | - | - |231  28
 Access |  RQE   |Prnt|SNIB|Tran|Evnt|Grnt|Rpt Buf|Page|
Grant Rp|Grant Rp|Dis |Dis |Dis |Dis |Dis | Thresh|Len |
12345678|12345678|  0 |  0 |  0 |  0 |  0 |     0 |  0 |
     |I/E|TRN|MID|CMD|CMD|QRY|TTL|GEN|
     |EVS|RPT|NIT|RSP|END|RPT|HDR|MSG|
Print| X | X | X | X | X | X | X | X |
Host | X | X | - | X | X | X | X | X |
Term | X | X | X | X | X | X | X | X |
Kpd  | X | X | X | X | X | X | X | X |
Printer Page Length = 0
M.C|Alm|Dur|Drs|NEq|No |Gen|Sho|SEK|EDM|GLB|GLB| . | . |SEK|ALM|
res|Cnc|Alm|Gen|Err|Vld|Tim|COD|ENA|ENA|USR|RLY| . | . |BUG|BUG|
 X | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
WT |IM | X |HST|SHR|RFR|HST|XDT|xdt|xdt|xdt|xdt|xdt|xdt|xdt|xdt|
 - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
```

```
Cmd> 88 * 24 #
* Remote Site Management Setups

Host Phone Numbers:
1) None
2) None
3) None
4) None
Dial-Host:
Tone Dialing
Dial-Host at Start of Time Zone 0
Postpone Dial-Host During Time Zone 0
Cancel Dial-Host During Time Zone 0
Disable Answer During Time Zone 0
Host Call-Back Disabled

Cmd> 88 * 25 #
* System Power Status

Main power = 29.71
UPS Battery = 26.67 0.00
Memory Battery = 4.15

Cmd> 88 * 26 #
* Transactions Since Midnight:

Access 0
Control 1
Programming Commands 28
Lost Reports 0
Denials 0
Alarms 8

0 Communication Errors on Reader 1
0 Communication Errors on Reader 2
0 Communication Errors on Reader 3
0 Communication Errors on Reader 4
0 Communication Errors on Reader 5
0 Communication Errors on Reader 6
0 Communication Errors on Reader 7
0 Communication Errors on Reader 8
0 Communication Errors on Reader 9
0 Communication Errors on Reader 10
0 Communication Errors on Reader 11
0 Communication Errors on Reader 12
0 Communication Errors on Reader 13
0 Communication Errors on Reader 14
0 Communication Errors on Reader 15
0 Communication Errors on Reader 16

Cmd> 88 * 27 #
* Occupancy Controls

Passback Mode -> OFF
Occupancy Violation Reporting Disabled
Passback Disabled During Time Zone 0
2-Person Rule Time Increment = 10
2-Person Rule Grant Threshold = 11
Control Zones Triggered on Occupancy Count Changes
PZ |on |on |on |on |Min|Min|Min|Max|Max|Min Users |Max Users | 2-Person |
   |0-1|1-2|2-1|1-0|   | -1| +1|   | -1|  Inside  |  Inside  |Dis. Thr. |
  2|  0|  0|  0|  0|  0|  0|  0|  0|  0|     00002|     00000|     00000|
Single Zone Access Mode is OFF
```

```
Cmd> 88 * 28 #
Virtual Relay Setups and Status
XRY|CONTRL|CONTRL|     |ACT|DIS|CLR|TRG|RTG|UCFFTTZZLL|
#  | TIME | DELAY|RESTS| TZ| TZ| TZ| CZ| CZ|LTNFADADDO|
  1|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  2|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  3|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  4|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  5|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  6|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  7|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  8|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
  9|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 10|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 11|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 12|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 13|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 14|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 15|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 16|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 17|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 18|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 19|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 20|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 21|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 22|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 23|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 24|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 25|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 26|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 27|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 28|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 29|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 30|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 31|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 32|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 33|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 34|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 35|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 36|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 37|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 38|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 39|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 40|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 41|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 42|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 43|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 44|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 45|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 46|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 47|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 48|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 49|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 50|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 51|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 52|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 53|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 54|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 55|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 56|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 57|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 58|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 59|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 60|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 61|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
```

```
 62|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 63|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|
 64|   24s|    0s| OFF |  0|  0|  0|  0|  0|----------|

Cmd> 88 * 29 #
Detailed Virtual Relay Status
RY |CNTRL|FORCE|FORCE|  TZ |  TZ |  CZ |  CZ | LOCK| LOCK|OPER-|
#  |TIMER|  ON | OFF | ACT | DIS | ACT | DIS | DOWN| OPEN|ATION|NOW
  1|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  2|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  3|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  4|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  5|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  6|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  7|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  8|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
  9|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 10|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 11|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 12|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 13|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 14|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 15|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 16|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 17|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 18|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 19|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 20|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 21|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 22|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 23|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 24|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 25|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 26|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 27|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 28|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 29|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 30|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 31|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 32|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 33|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 34|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 35|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 36|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 37|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 38|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 39|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 40|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 41|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 42|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 43|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 44|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 45|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 46|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 47|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 48|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 49|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 50|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 51|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 52|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 53|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 54|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 55|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 56|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 57|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
```

```
 58|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 59|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 60|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 61|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 62|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 63|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off
 64|  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |  -- |Norml|Off

Cmd> 88 * 30 #
HEC Factory Diagnostics
8819
*VM
84E2 00 00 05 23 46 01 00 00 00 00 00 00 00 00 00
84F2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8502 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8512 00 20 00 00 01 01 00 00 00 02 0A 40 08 00 00 00
8522 00 03 FF 02 58 00 08 00 00 00 00 00 00 83 40 05
8532 01 01 00 00 00 1A 45 02 FF 00 00 D5 02 00 00 E9
8542 03 67 00 00 00 00 01 0E 03 00 00 07 00 40 40 00
8552 00 AB 18 EE 2C EE 2C F0 00 04 00 00 FF 00 08 08
8562 0B 03 00 0D 02 03 02 0A 00 0B 00 0D 02 02 00 00
8572 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8582 00 00 00 00 00 00 00 00 00 00 00 60 85 00 00 00
8592 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
85A2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
85B2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
85C2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
85D2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20
*NVM
8857 00 00 00 00 FF FB FF 08 FF 00 00 00 00 00 00 00
8867 00 00 00 00 00 00 00 00 00 00 0A 0B 00 00 00 09
8877 00 00 00 00 FE 00 00 00 00 5F 80 00 80 00 00 00
8887 60 C0 00 00 04 04 04 04 03 00 00 00 00 00 01 14
8897 32 3C 00 3C 00 3C 00 3C 00 00 00 00 E7 1C 00 00
88A7 00 00 00 00 00 03 05 00 08 01 51 74 01 7B 00 7B
88B7 00 7B 00 7B 00 7B 00 7B 00 7B 00 7B 00 00 00 00
88C7 00 00 00 00 00 59 24 00 06 01 03 00 20 7B 00 7B
88D7 00 7B 00 7B 00 00 00 00 00 07 08 00 00 00 00 00
88E7 00 01 00 00 00 04 00 00 03 00 01 02 03 00 00 00
88F7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8907 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 04
8917 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8927 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
8937 00 00 FF 00 00 00 00 00 00 00 00 00 00 00 00 20
8947 00 00 00 01 00 08 00 00 00 00 00 00 00 00 59 24
*S
873F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
874F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
875F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
876F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
877F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
878F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
879F 00 00 00 60 00 91 4B E5 1F 1C 00 1A 00 B4 7D 79
87AF 40 69 40 49 0C 7C 40 87 79 40 AD 08 54 17 1A 00
87BF BD 19 44 06 1A 00 B4 7D 06 03 17 19 02 00 73 18
87CF 8E 07 1A 00 B4 7D 06 03 29 18 25 18 19 18 E8 07
87DF 2C 0C 79 40 69 40 7C 40 87 03 4E 86 45 12 4E 86
87EF C3 33 4E 86 01 01 AA 85 02 20 06 03 E8 41 00 FF
87FF 13 85 9C 41 08 20 00 0A D3 05 09 88 06 03 21 0A
880F 08 08 87 4E 00 05 08 0D 71 4E 11 4B 04 4B 69 2F
881F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
882F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
883F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
884F 00 00 0F 08 08 0F 08 06 00 00 00 00 FF FB FF 08
```

```
Cmd> 88 * 31 #
Special Needs Unlock Extension Times
Door Delay Extension (sec) = 0
Door Mode Extension  (sec) = 0
Door Open Extension  (sec) = 0

Cmd> 88 * 32 #
Special Keypad / Match Setups
   |SLN|   |TPR|   |   |DNY|ALT|ANN|INS|   |CRD|   |THR|DIS|CTZ|
   |TPR|   |DIS|   |   |DUR|RDR|DSP|DSP|LCD|MAP|   |LVL|LVL|DIS|
  1| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  2| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  3| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  4| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  5| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  6| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  7| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  8| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
  9| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 10| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 11| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 12| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 13| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 14| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 15| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|
 16| - | - | - | - | - | - | - | - | - | - | - | - |  0| 99| 99|

Cmd> 88 * 33 #
Custom Card Map Setups
  1 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  2 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  3 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  4 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  5 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  6 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  7 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  8 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  9 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 10 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 11 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 12 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 13 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 14 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 15 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 16 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
```

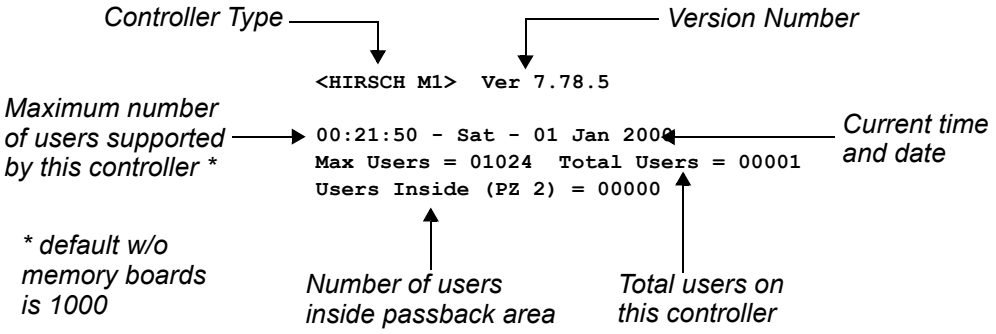
Command Descriptions

Each of the 88 commands is described here. They are presented in numerical order. The command which changes a specific default is shown in **bold** to the left of the displayed data.

Comments and notes about the specific lines or fields of data are shown in callouts. Some items which appear here show the current status of your system and cannot be changed with just a command number. In such cases, no command reference is provided.

Note: In most cases, an x indicates the function or feature is enabled; a dash, -, indicates the feature is disabled.

CMD 88 * 1 - Date, Time, Version Number



CMD 88 * 2 - System Information

```
                * System Information
                Configuration: 4 Relays - 64 Expansion Relays - 0 Alarm Relays
                4 Inputs - 0 Expansion Inputs
                Options:
                SPIB - Baud Rate=9600-8-N-1
                Onboard Users - 416 KB - 6K Users
                Long RAM
                Max Users = 01024 allocated, limit= 04352
                Network Inactive
                1 Active Keypads 1 Active MATCH Readers
      CMD 18    Auto-Generation CODE Length = 7 - Standard card length = 8
     CMD 200    Language = 0 (English)
      CMD 07    Current Duress Digit = 9
      CMD 08    Duress Alarm Mode Disabled
      CMD 09    Duress CODE Generation Mode Disabled
   CMD 77 * 1   CODE Tamper Time Penalty = 20
   CMD 77 * 2   CODE Tamper Alarm Threshold = 50
   CMD 77 * 0   CODE Tamper Lockout = 1 min
     CMD 192    Programming Mode Timeout = 8
                Alarm Relay Times:
CMD 78, 79 * 1  General = 60 Map to: Relay 4
CMD 78, 79 * 2  Duress = 60 Map to: Relay 4
CMD 78, 79 * 3  Tamper = 60 Map to: Relay 4
CMD 78, 79 * 4  Trouble = 60 Map to: Relay 4
   CMD 97 * 6   System CODE Reset Button Enabled
   CMD 44 * 1   Alarm Cancel Button Enabled
     CMD 140    Report Buffer = Open
     CMD 140    Report Buffer Size= 1560/ 1560/  780
     CMD 140    Alarm Buffer Size = 1560
```

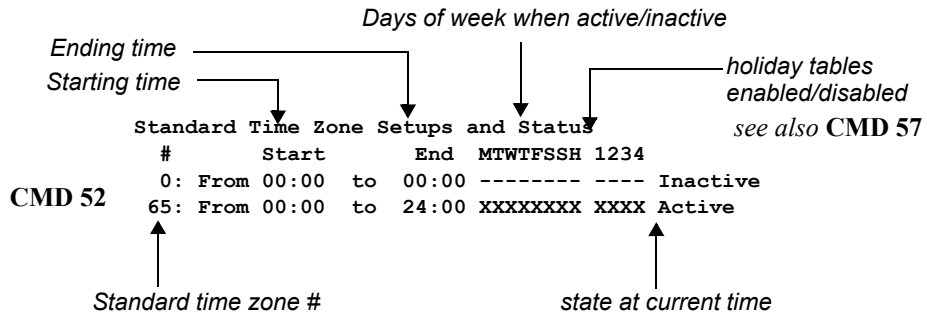
varies by system

current network status

see also CMDs 225, 325, 425

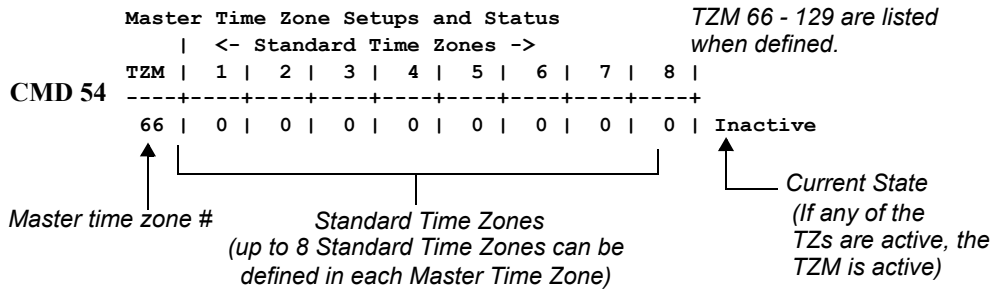
see also CMD 406

CMD 88 * 3 - Standard Time Zone Setups and Status

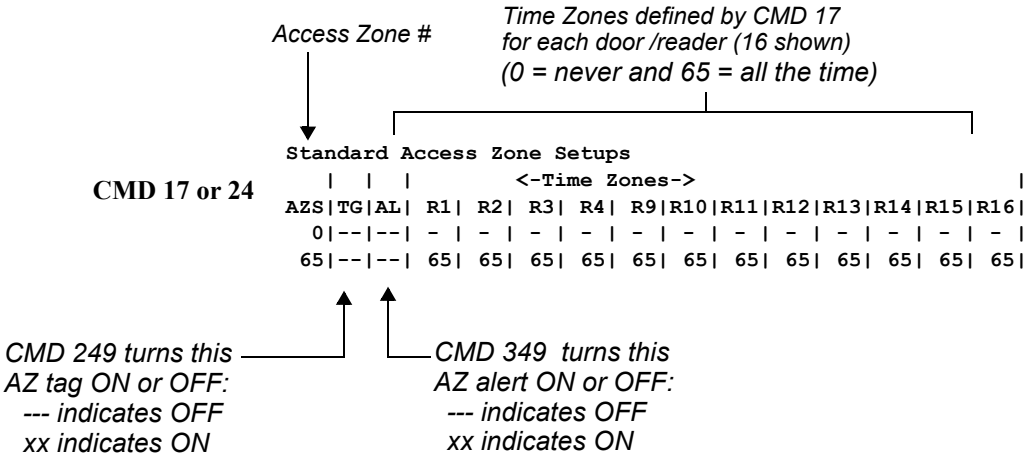


0 and 65 cannot be redefined; 1 - 64 may be defined.
Once defined, they are listed here.

CMD 88 * 4 - Master Time Zone Setups and Status



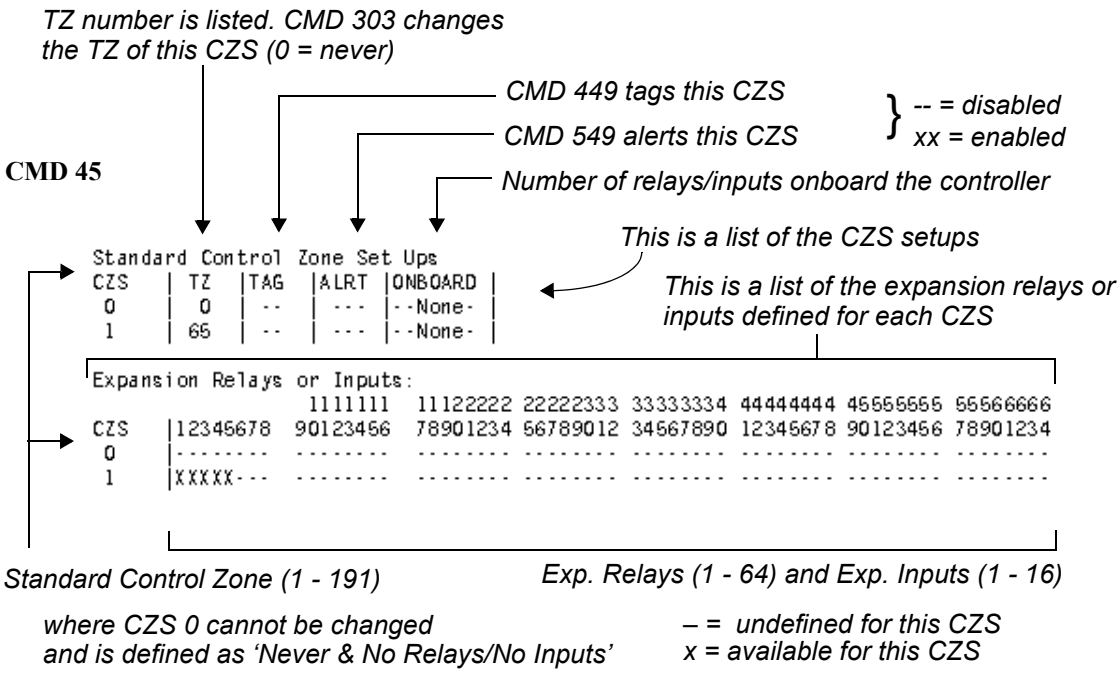
CMD 88 * 5 - Standard Access Zone Setups



The M1N will show 1 door, the M2 will show 4 doors, and the M8 shows 8 doors.

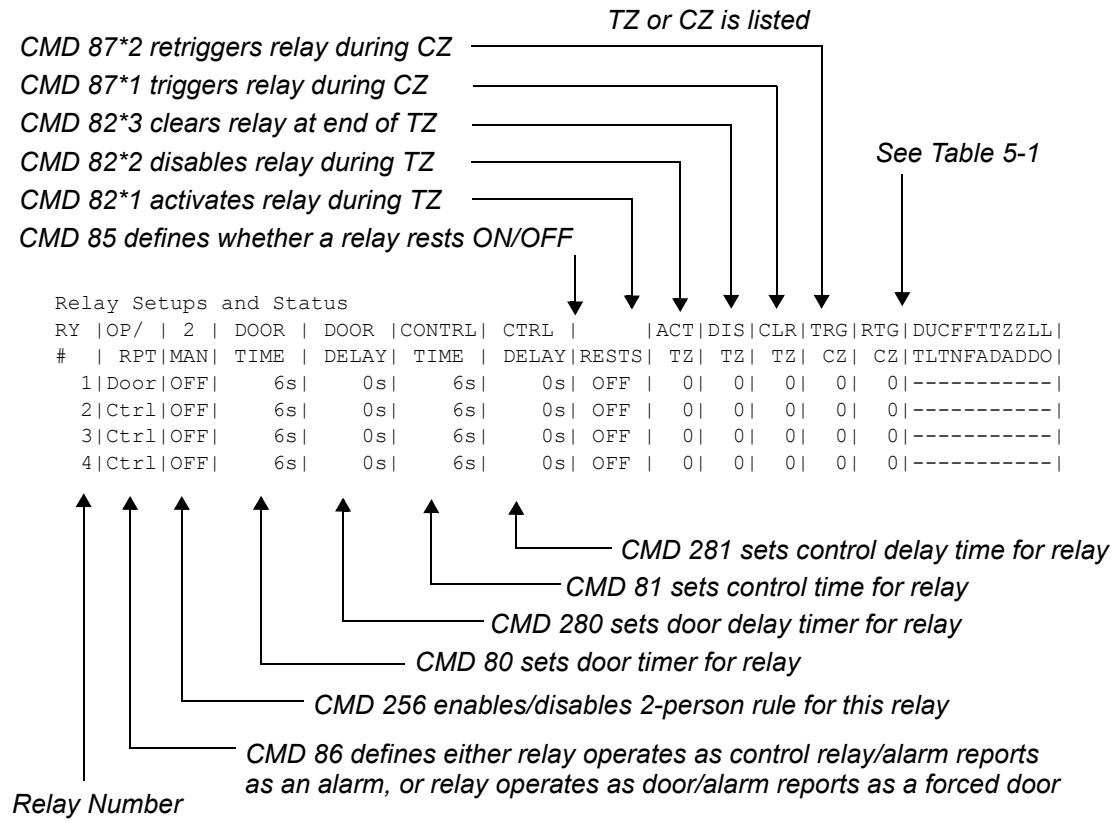
AZS 0 and AZS 65 are the ends of the Access Zone range. AZS0 means the doors are always unavailable while AZS65 indicates that the door is always available.

CMD 88 * 6 - Standard Control Zone Setups



In the preceding example, CZS 1 has five expansion relays/inputs defined.

CMD 88 * 7 - Relays Setups and Status

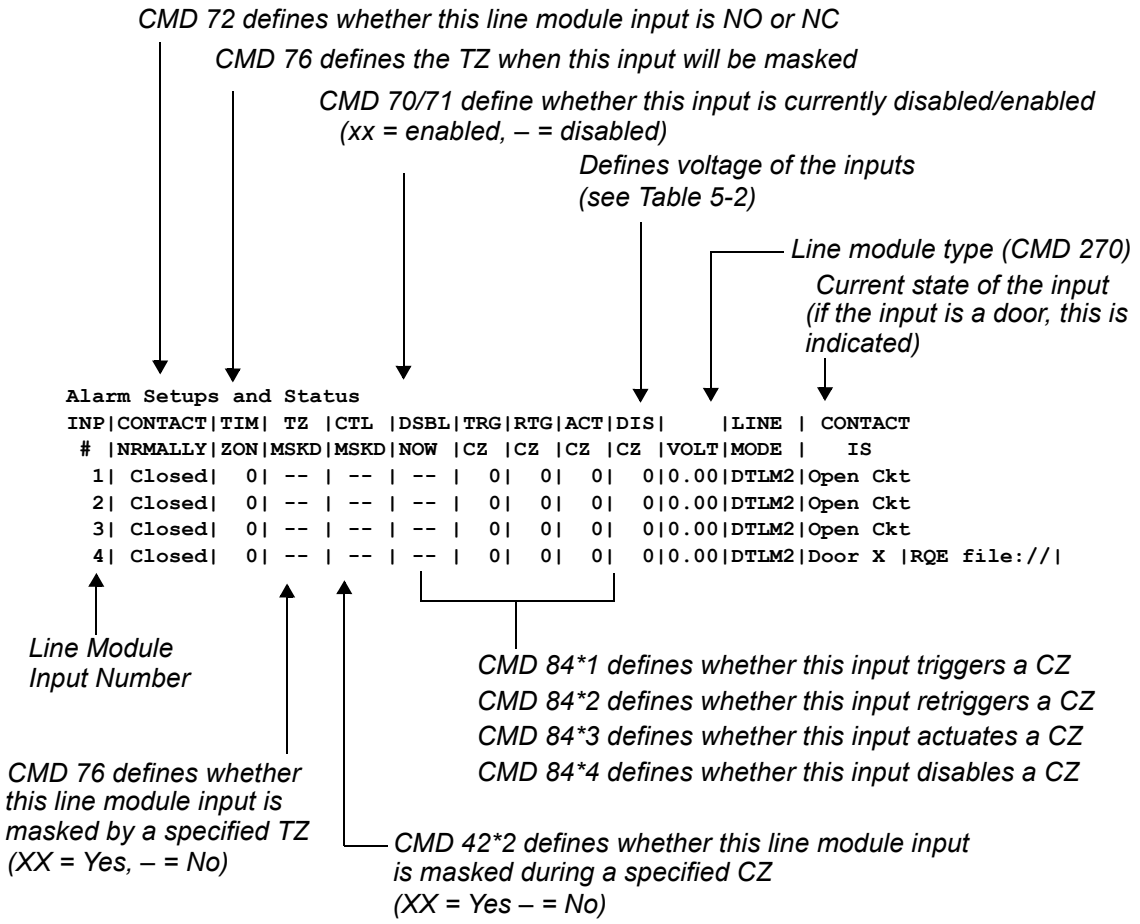


These abbreviations indicate why a specific relay is under control by the controller. There will be an 'X' under the category currently controlling the relay. Priority is also shown here, where DT (door timer) is the lowest priority and LO (lock open) is the highest. There may be an 'X' under more than one category, in which case the 'X' furthest to the right is the operation currently controlling the relay.

DT	Door Timer
UL	Unlock
CT	Control Timer
FN	Force On
FF	Force Off
TA	Time Zone Actuated
TD	Time Zone Disabled
ZA	Control Zone Actuated
ZD	Control Zone Disabled
LD	Lock Down
LO	Lock Open

Table 5-1: Relay Condition Abbreviations

CMD 88 * 8 - Alarm Setups and Status



The 88*8 command includes alarm status voltage ratings for each input. These voltages depend on the line module connected and the condition being signalled. In most cases, if you know the device (DTLM/MELM) attached to the controller, you can determine what the status of the line module is. Table 5-2 should help you determine this:

Min	Typical	Max	Door Reported As
DTLM1/MELM3 Voltage			
0.00	0.00	0.51	Open
0.55	—	0.78	Out-of-Spec
0.82	1.04	1.21	Door //
1.25	—	2.77	Out-of-Spec
2.81	3.02	3.16	Door X
3.20	—	4.88	Out-of-Spec
4.92	—	5.00	Short
DTLM2/MELM2 Voltage			
0.00	0.00	0.51	Open
0.55	—	0.78	Out-of-Spec
0.82	1.04	1.21	Door // RQE //
1.25	—	2.77	Out-of-Spec
2.81	3.02	3.16	Door X RQE //
3.20	—	3.55	Out-of-Spec
3.59	3.82	4.02	Door // RQE X
4.06	—	4.34	Out-of-Spec
4.38	4.64	4.80	Door X RQE //
4.84	—	4.88	Out-of-Spec
4.92	—	5.00	Short
DTLM3/MELM3 Voltage			
0.00	0.00	0.51	Open
0.12	—	0.20	Out-of-Spec
0.23	0.35	0.47	Door // RQE // Tmpr //
0.51	—	1.21	Out-of-Spec
1.25	1.37	1.48	Door X RQE // Tmpr //
1.52	—	1.88	Out-of-Spec
1.91	2.07	2.15	Door // RQE X Tmpr //
2.19	—	2.54	Out-of-Spec
2.58	2.71	2.81	Door X RQE X Tmpr //
2.85	—	2.97	Out-of-Spec
3.01	3.17	3.24	Door // RQE // Tmpr X
3.28	—	3.44	Out-of-Spec
3.48	3.60	3.71	Door X RQE // Tmpr X

Table 5-2: Alarm Status Input Voltage Ranges

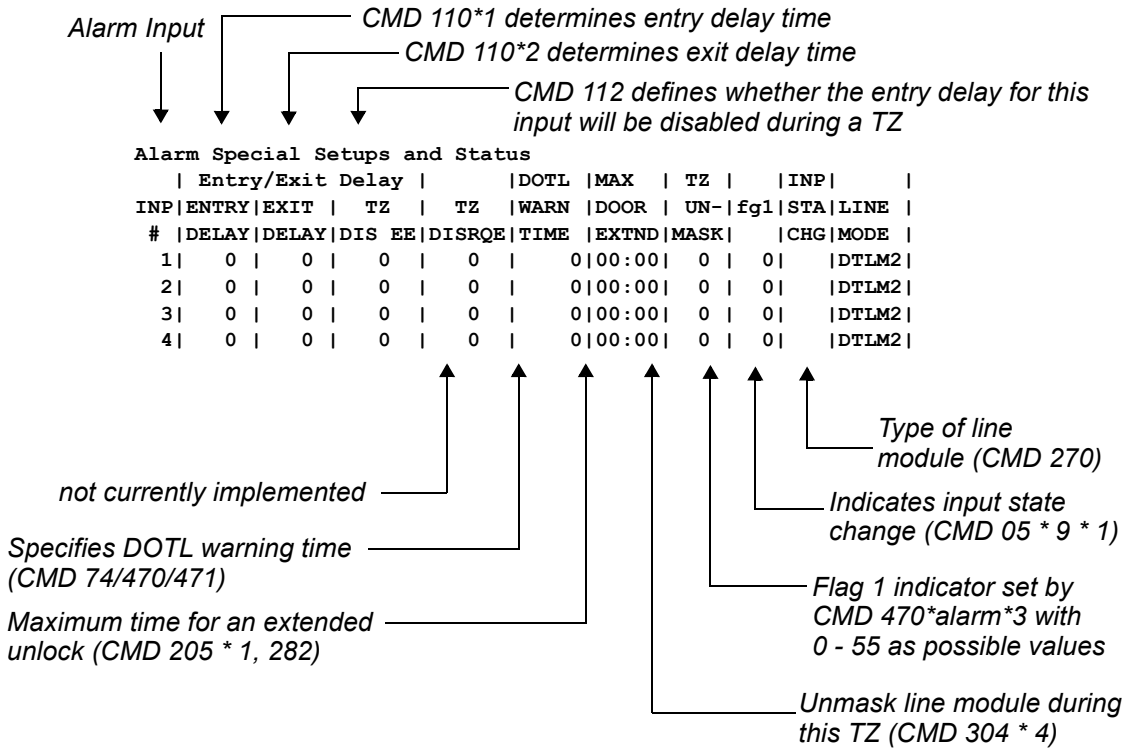
Min	Typical	Max	Door Reported As
3.75	—	3.75	Out-of-Spec
3.79	3.93	4.02	Door // RQE X Tmpr X
4.06	—	4.10	Out-of-Spec
4.14	4.24	4.38	Door X RQE X Tmpr X
4.41	—	4.65	Out-of-Spec
4.69	—	5.00	Short

Table 5-2: Alarm Status Input Voltage Ranges (Continued)

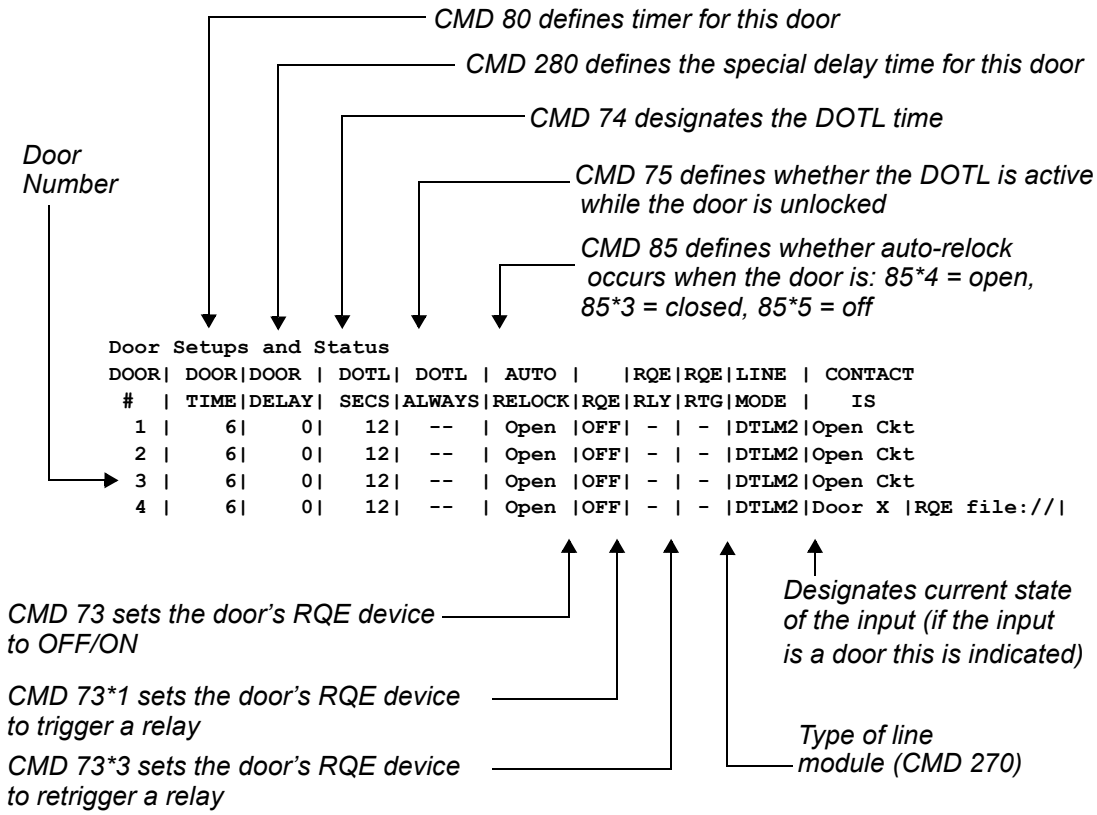
where:

// = open
X = closed

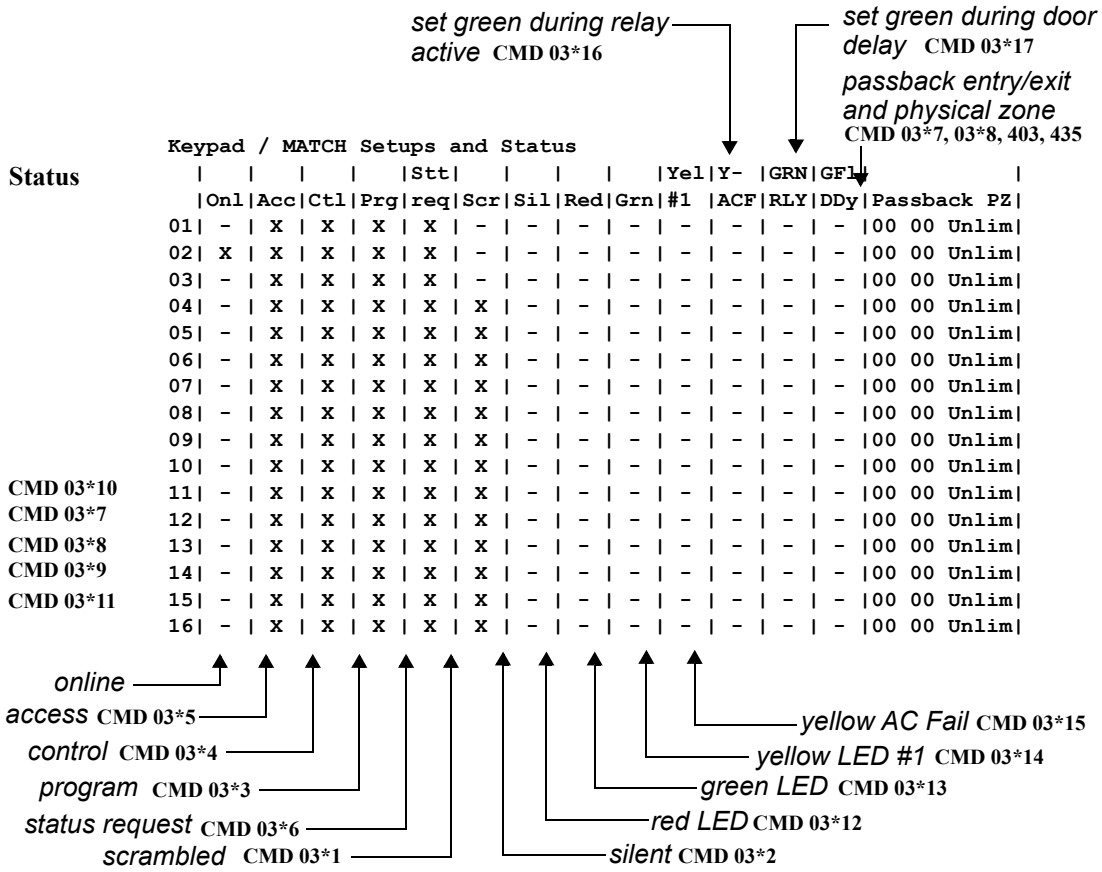
CMD 88 * 9 - Alarm Special Setups and Status



CMD 88 * 10 - Door Setups and Status



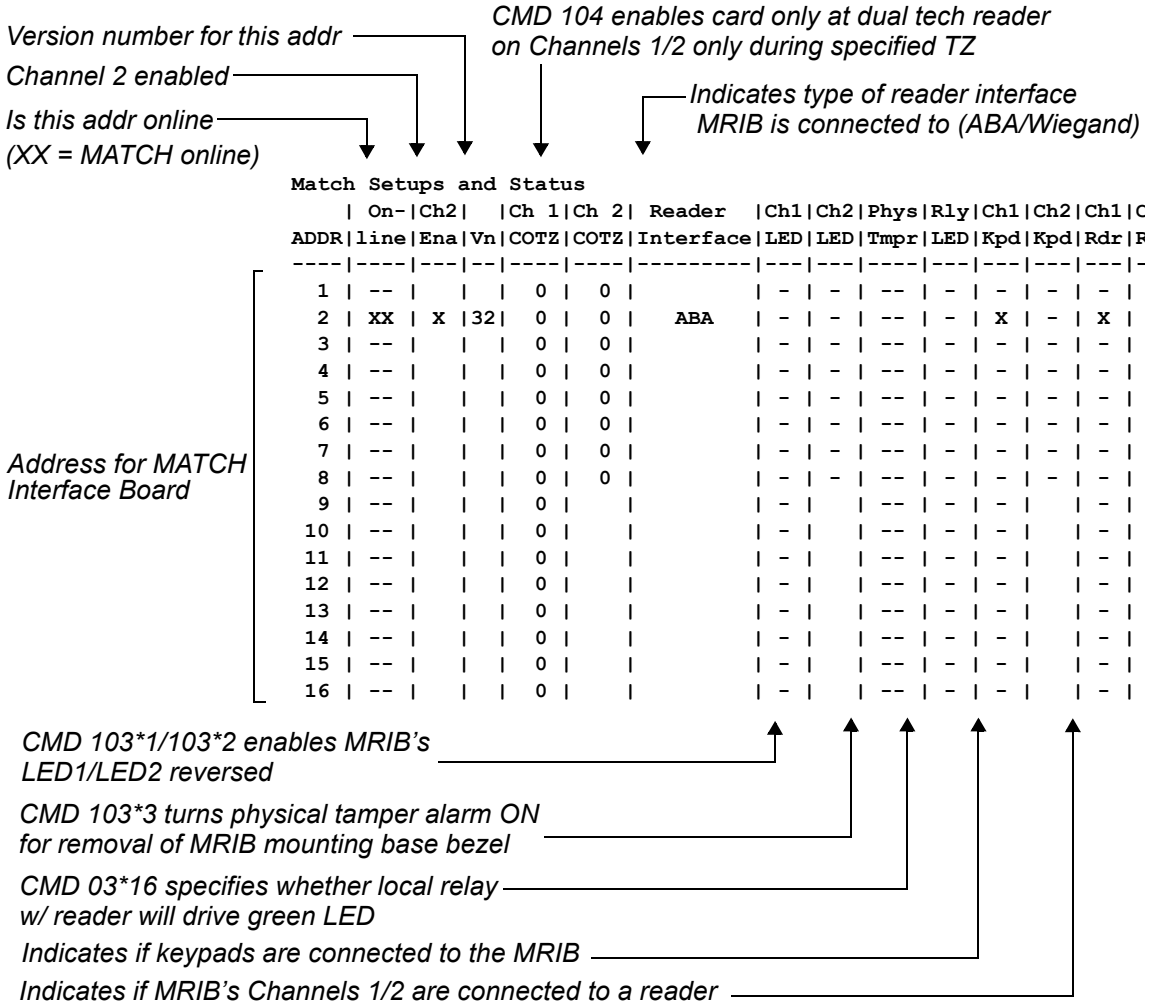
CMD 88 * 11 - Keypad Setups and Status



X = feature ON for ScramblePad or MRIB

– = feature OFF for ScramblePad or MRIB

CMD 88 * 12 - MATCH Setups and Status

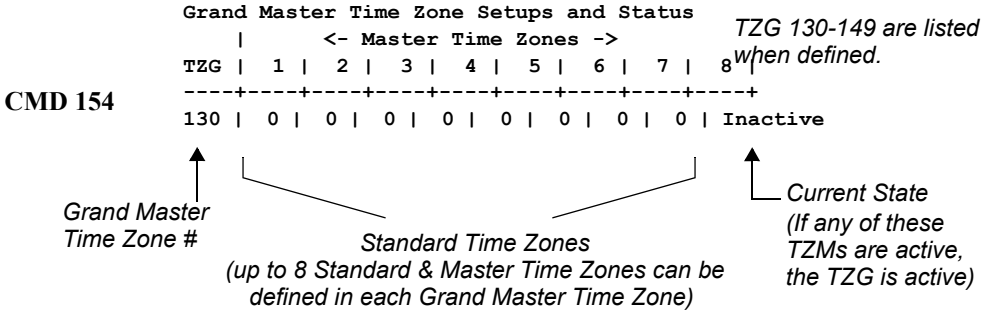


Match Setups and Status

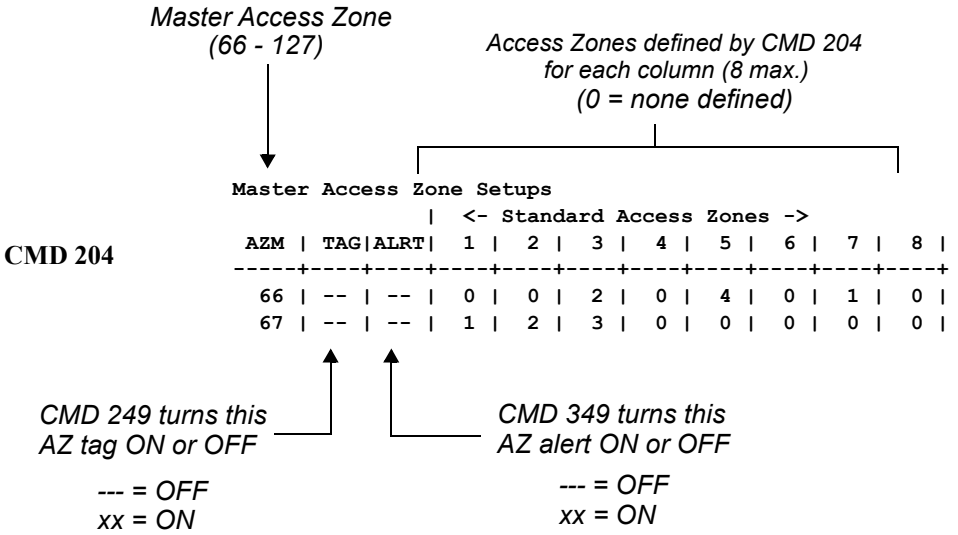
ADDR	On-line	Ch2 Ena	Vn	Ch 1 COTZ	Ch 2 COTZ	Reader Interface	Ch1 LED	Ch2 LED	Phys Tmpr	Rly LED	Ch1 Kpd	Ch2 Kpd	Ch1 Rdr	C
1	--			0	0		-	-	--	-	-	-	-	
2	XX	X	32	0	0	ABA	-	-	--	-	X	-	X	
3	--			0	0		-	-	--	-	-	-	-	
4	--			0	0		-	-	--	-	-	-	-	
5	--			0	0		-	-	--	-	-	-	-	
6	--			0	0		-	-	--	-	-	-	-	
7	--			0	0		-	-	--	-	-	-	-	
8	--			0	0		-	-	--	-	-	-	-	
9	--			0			-		--	-	-		-	
10	--			0			-		--	-	-		-	
11	--			0			-		--	-	-		-	
12	--			0			-		--	-	-		-	
13	--			0			-		--	-	-		-	
14	--			0			-		--	-	-		-	
15	--			0			-		--	-	-		-	
16	--			0			-		--	-	-		-	

CMD 88 * 13 - Holidays

CMD 88 * 14 - Grand Master Time Zone Setups and Status

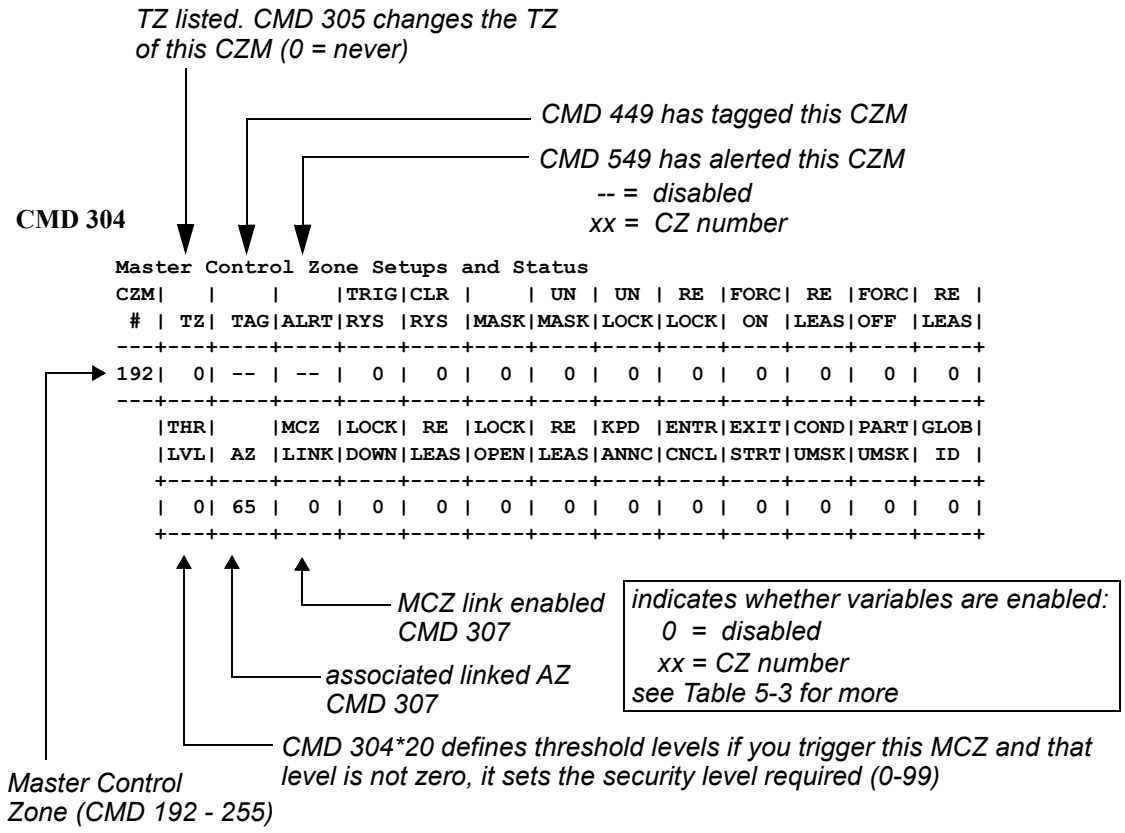


CMD 88 * 15 - Master Access Zone Setups



In the preceding example, notice how Master Zone 66 has three Standard Access Zones defined (Columns 3, 5, and 7) while Master Zone 67 has three AZSs defined (columns 1, 2, and 3).

CMD 88 * 16 - Master Control Zone Setups and Status

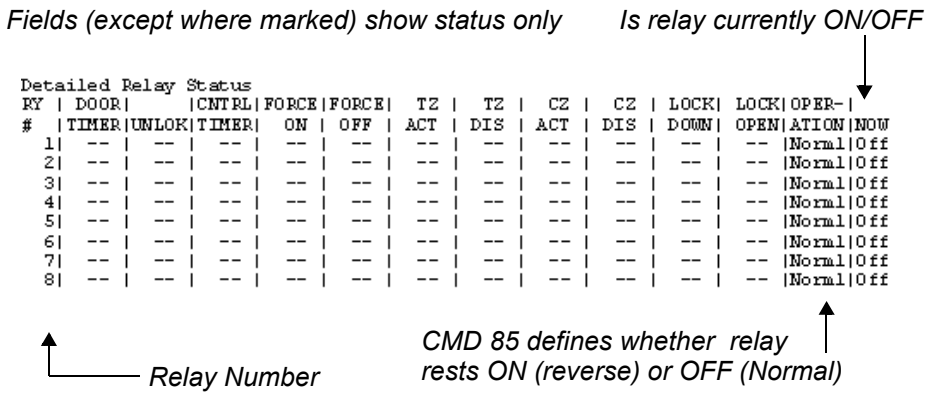


The variable abbreviations in the previous printout are:

TRIG RYS	304 * 1	Trigger Relays
CLR RYS	304 * 2	Clear Relays
MASK	304 * 3	Mask Alarms
UNMASK	304 * 4	Unmask Alarms
UNLOCK	304 * 5	Unlock Doors
RELOCK	304 * 6	Relock Doors
FORC ON	304 * 7	Force ON Relays
RELEAS	304 * 8	Force ON Release of Relays
FORC OFF	304 * 9	Force OFF Relays
RELEAS	304 * 10	Force OFF Release of Relays
LOCK DOWN	304 * 11	Lock Down Relays
RELEAS	304 * 12	Lock Down Release of Relays
LOCK OPEN	304 * 13	Lock Open Relays
RELEAS	304 * 14	Lock Open Release of Relays
KPD ANNC	304 * 15	Annunciate Readers
ENTR CNCL	304 * 16	Cancel Entry Delay
EXIT STRT	304 * 17	Start Exit Timer
COND UMSK	304 * 18	Unmask Alarms if all secure
PART UMSK	304 * 19	Partial Unmask
GLOB ID	304 * 20	Set Security Clearance Level

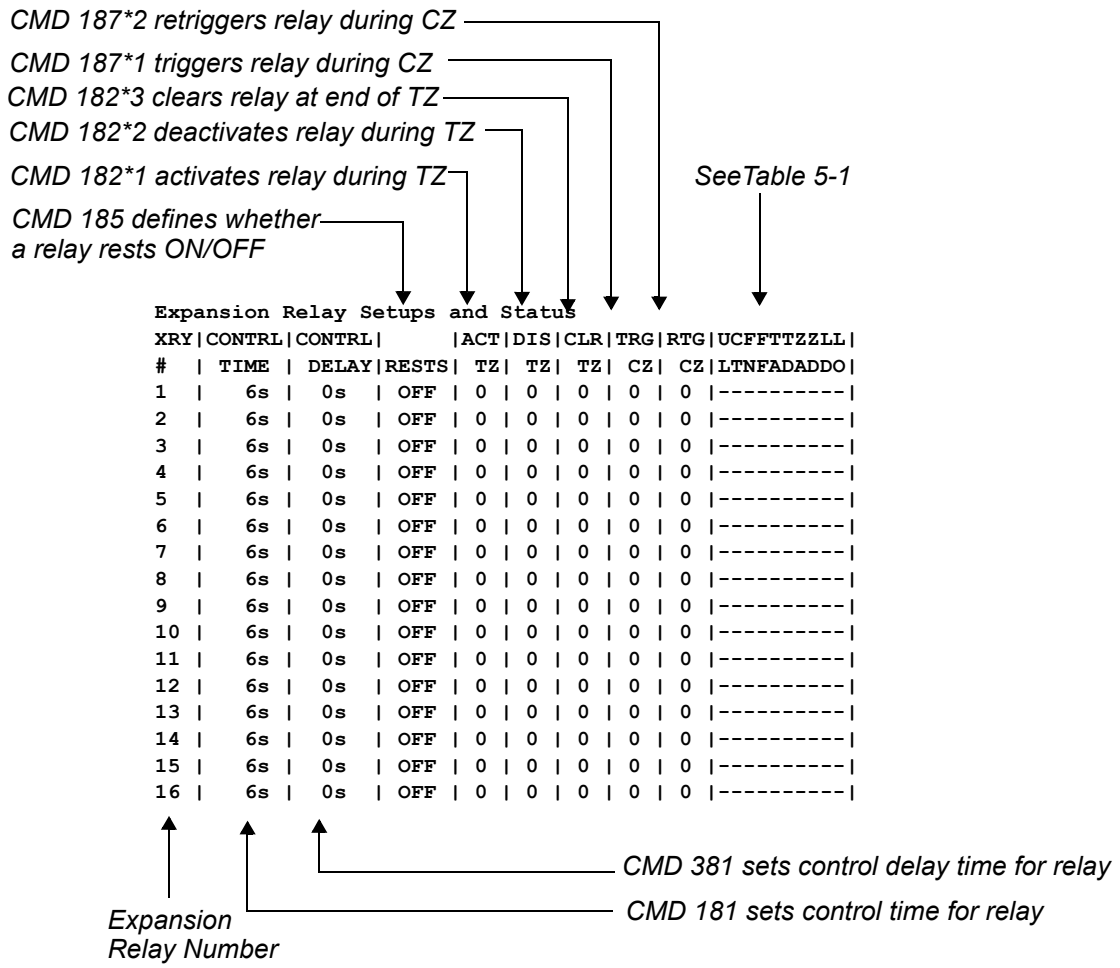
Table 5-3: Variable Abbreviations

CMD 88 * 17 - Detailed Relay Status Only



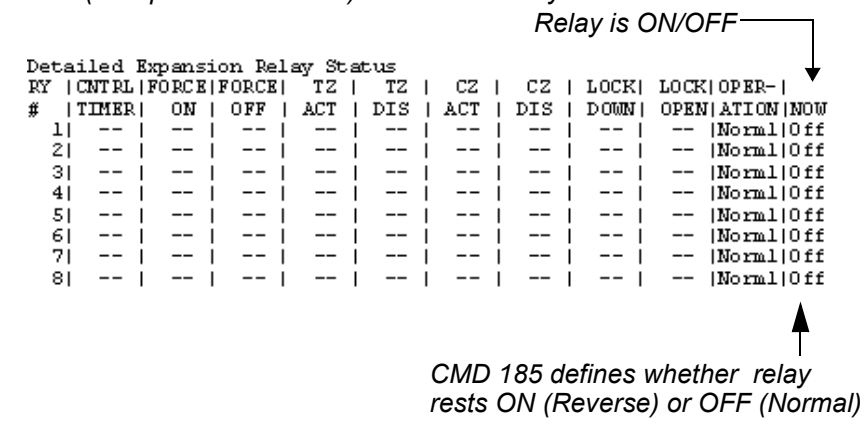
For a list of abbreviations and their meanings, see Table 5-1 on page 5-16. There will be an ‘On’ under the category currently controlling the relay. Priority is also shown here, where DT is the lowest priority and LO is the highest. There may be an ‘On’ under more than one category in which case the ‘On’ furthest to the right is the operation currently controlling the relay.

CMD 88 * 18 - Expansion Relay Setups and Status



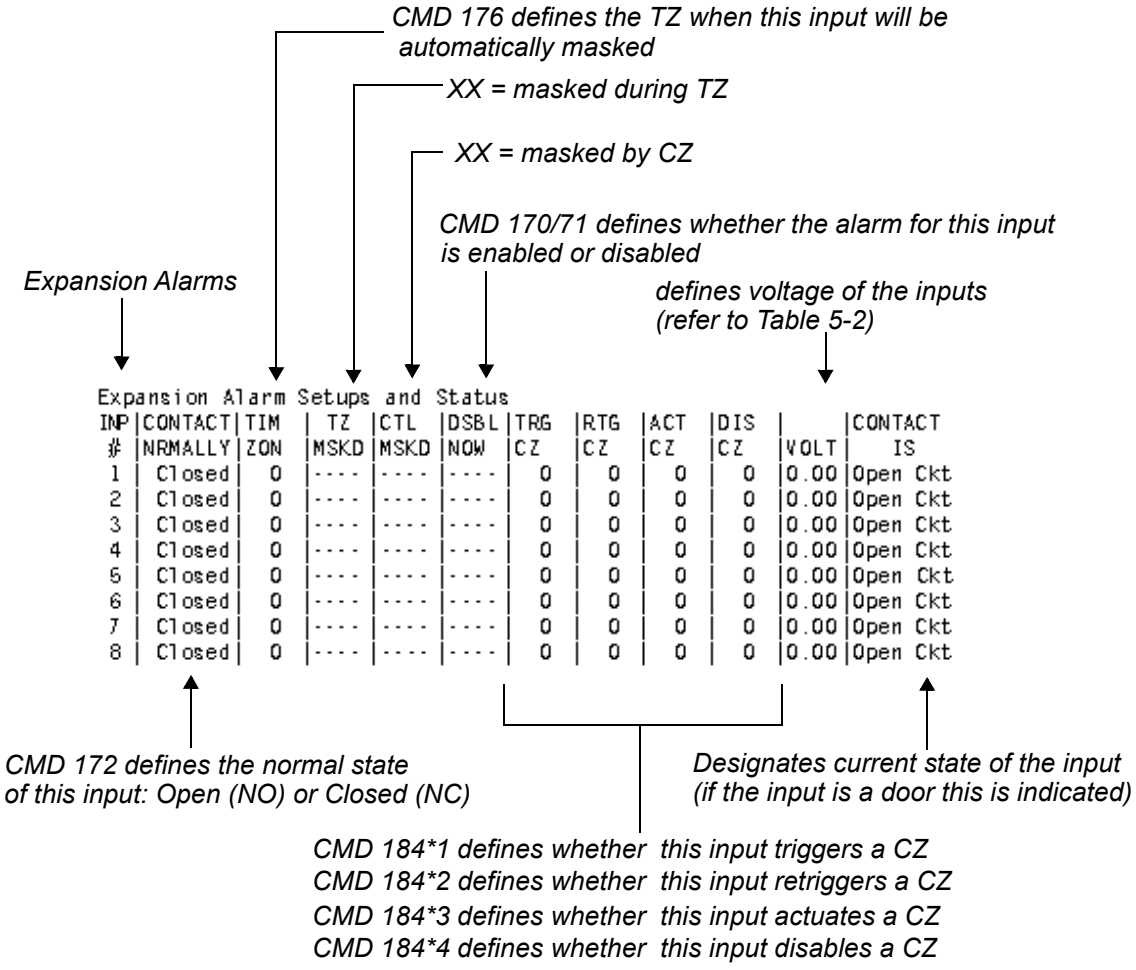
0 = no action for this relay, otherwise actual TZ or CZ number will appear. If no expansion relays are available, the message 'Expansion Relays not Available' will appear below the table headings.

CMD 88 * 19 - Detailed Expansion Relay Status Only



For a list of abbreviations and their meanings, see Table 5-1 on page 5-16. There will be an 'On' under the category currently controlling the relay. Priority is also shown here, where DT is the lowest priority and LO is the highest. There may be an 'On' under more than one category in which case the 'On' furthest to the right is the operation currently controlling the relay.

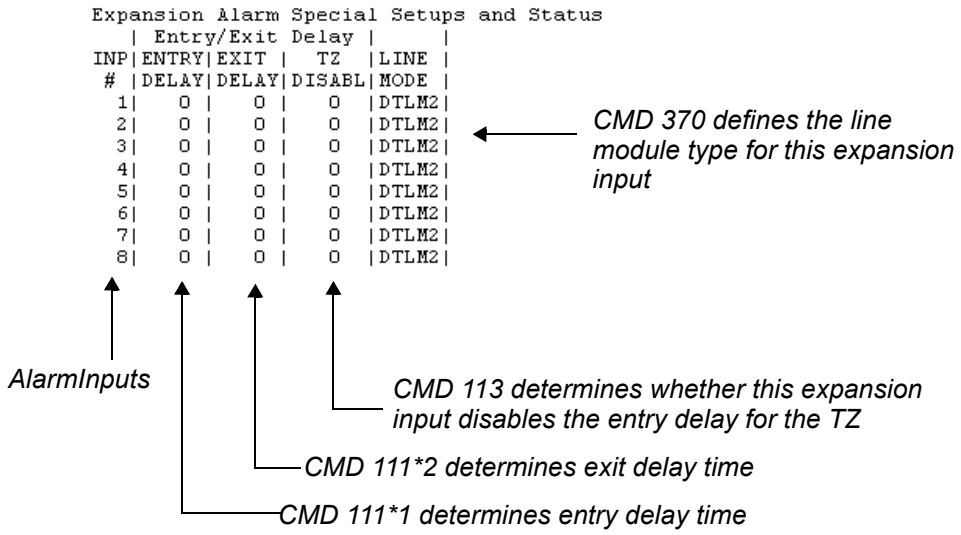
CMD 88 * 20 - Expansion Alarm Setups and Status



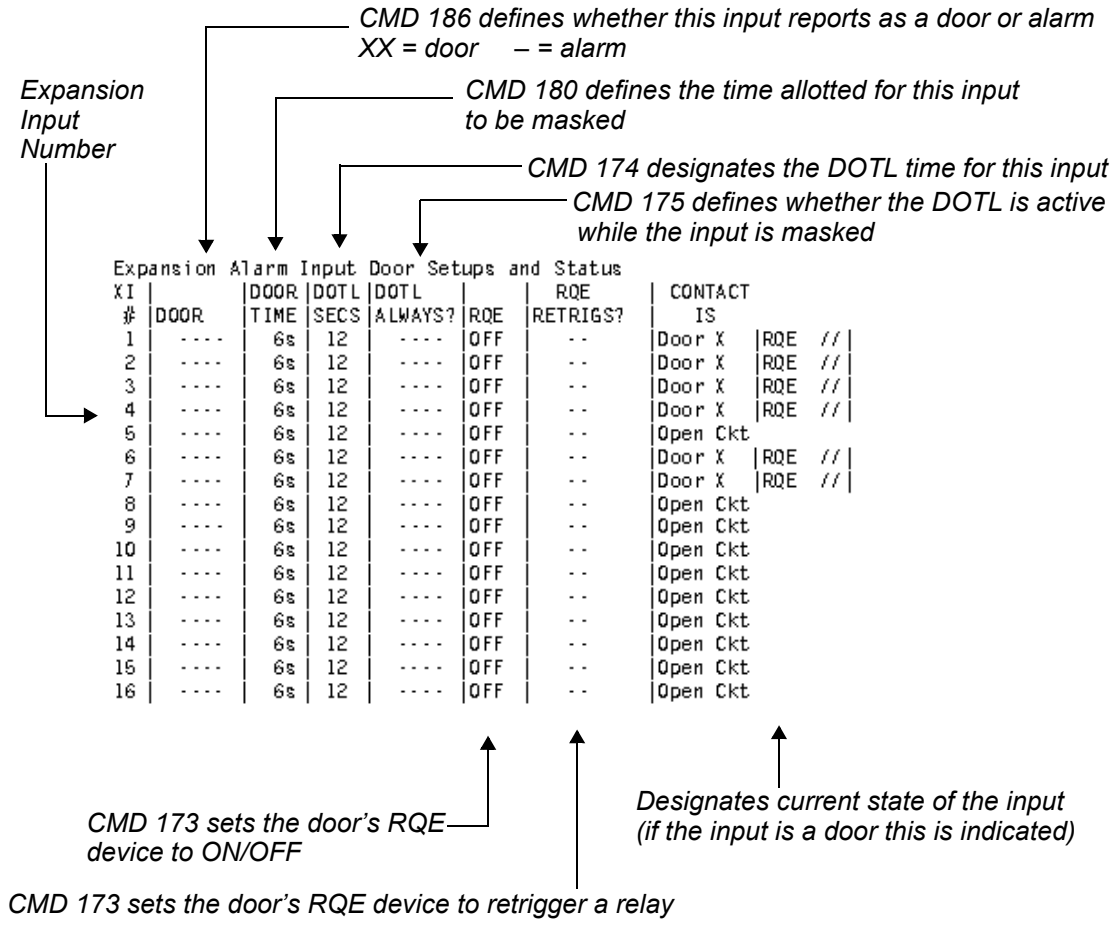
Expansion Alarm Setups and Status

INP #	CONTACT NRMALLY	TIM ZON	TZ MSKD	CTL MSKD	DSBL NOW	TRG CZ	RTG CZ	ACT CZ	DIS CZ	VOLT	CONTACT IS
1	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
2	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
3	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
4	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
5	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
6	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
7	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt
8	Closed	0	----	----	----	0	0	0	0	0.00	Open Ckt

CMD 88 * 21 - Expansion Alarm Special Setups and Status



CMD 88 * 22 - Expansion Line Module Input Door Setups and Status



CMD 88 * 23 - Reporting Setups

see Table 5-4 below for definitions and command controls

Each Door # is included in grant reports.

X = enabled
- = disabled

```
* Reporting Setups

TZ |TZ |TZ |SNT|SNT|RPT|CMD|SNT|MID|MCZ|INT|EXT|TRN|RLY|INV|ACB|
RLY|SC |ALM|MOM|Vn7|BUF|ECH|PRN|NIT|RPT|EVN|EVN|RPT|RPT|COD|RPT|
 X | X | X | - | - | X | X | X | - | - | X | X | X | - | - | - |

 Access |  RQE   |Prnt|SNIB|Tran|Evnt|Grnt|Rpt Buf|Page|
Grant Rp|Grant Rp|Dis |Dis |Dis |Dis |Dis | Thresh|Len |
12345678|12345678|  0 |  0 |  0 |  0 |  0 |     0 |  0 |

     |I/E|TRN|MID|CMD|CMD|QRY|TTL|GEN|
     |EVS|RPT|NIT|RSP|END|RPT|HDR|MSG|
Print| X | X | X | X | X | X | X | X |
Host | X | X | - | X | X | X | X | X |
Term | X | X | X | X | X | X | X | X |
Kpd  | X | X | X | X | X | X | X | X |

Printer Page Length = 58

M.C|Alm|Dur|Drs|NEq|No |Gen|Sho|SEK|EDM|GLB|GLB| . | . | - | - |
res|Cnc|Alm|Gen|Err|Vld|Tim|COD|ENA|ENA|USR|RLY| . | . | - | - |
 X | X | - | - | - | - | - | - | - | - | - | - | - | - | - | - |

WT |IM | X |HST|SHR|CRD| - | - |xdt|xdt|xdt|xdt|xdt|xdt|xdt|xdt|
DUA|COT|DAT|GR |PNS|OVW| - | - | - | - | - | - | - | - | - | - |
 - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
```

TZ RLY	05 * 6	Time zone relay control state changes reporting enabled
TZ SC	05 * 5	Time zone state changes reporting enabled
TZ ALM	05 * 7	Time zone input mask state changes reporting enabled
SNT MOM	05*10*1	MOMENTUM S*NET features enabled
SNT Vn7	198*6	CCM Version 7.0 S*NET features enabled
RPT BUF	98*16, 97*2/*5	Event report buffer is open/closed
CMD ECH	98*24	Command echo on / off
SNT PRN	98*41	Print S*NET messages
MID NIT	107	Midnight reports enabled
MCZ RPT	98*41*6*2	Master control zone reporting enabled
INT EVN	05*2	Internal events reporting enabled
EXT EVN	05*3	External events reporting enabled
TRN RPT	98*41*5*5	Transaction reporting enabled
RLY RPT	98*41*5*6	Relay state changes reporting enabled
INV COD	98*41*5*7	Invalid CODE reporting enabled
ACB RPT	98*41*5*8	ACB report enabled
Access Grant Rp	06*1, 403	Access grant report enabled/disabled for available doors
RQE Grant Rp	06*2	RQE grant report enabled/disabled for available doors

Table 5-4: Report Abbreviations and Meanings

Prnt Dis	105*1, 406	Printer disabled during TZ
SNIB Dis	105*2	SNIB disabled during TZ
Tran Dis	106*1	Transaction reporting disabled during TZ
Evnt Dis	106*2	Event reporting disabled during TZ
Grnt Dis	106*3	Granted transaction reporting only disabled during TZ
Rpt Buf Thres	140	Report buffer alarm threshold
Page Len	191	Printer page length
I/E EVS	98*5*13*1	Internal/external event reporting enabled
TRN RPT	98*41*5*13*2	Transaction reporting enabled
MID NIT	98*41*5*14*3	Midnight reporting enabled
CMD RSP	98*41*5*14*4	Command responses reporting enabled
QRY RPT	98*41*5*15*6	Query Reporting enabled
TTL HDR	98*41*5*16*7	Title messages enabled
GEN MSG	98*41*5*16*8	All other messages enabled
M.C. res	98*41*1*1	System code reset button enabled
Alm Cnc	98*41*1*2	Alarm cancel button enabled
Dur Alm	98*41*1*3	Duress alarm handling enabled
Drs Gen	98*41*1*4	Duress generation enabled
NEq Err	98*41*1*5	Bypass no such hardware error reporting enabled
No Vld	98*41*1*6	Bypass code conflict checking reporting enabled
Gen Tim	98*41*1*7	Shorter “auto gen” code printout
Sho COD	98*41*1*8	Show codes on printer each time a user is added
SEK ENA	98*41*2*1	SEK enabled
GLB USR	98*41*2*2	Globalized user management
GLB RLY	98*41*2*3	Globalized Relays and MCZ's
WT DUA	98*41*9*1	Wait for dual technology
IM COT	98*41*9*2	IMCOTZ flag1
XDAT	98*41*9*3	XDAT flag1
HST GR	98*41*9*4	Host grant support
SHR PNS	98*41*9*5	Short PINs enabled
CRD OVW	98*41*9*6	Allow code record download overwrite

Table 5-4: Report Abbreviations and Meanings (Continued)

CMD 88 * 24 - Remote Site Management Setups

```
                * Remote Site Management Setups

                Host Phone Numbers:
CMD 193 * 1     1) None
CMD 193 * 2     2) None
CMD 193 * 3     3) None
CMD 193 * 4     4) None
                Dial-Host:
CMD 194         Tone Dialing
CMD 108 * 1     Dial-Host at Start of Time Zone 0
CMD 108 * 2     Postpone Dial-Host During Time Zone 0
CMD 108 * 3     Cancel Dial-Host During Time Zone 0
CMD 108 * 4     Disable Answer During Time Zone 0
CMD 195         Host Call-Back Disabled
```

states provided for all time zones defined

CMD 88 * 25 - System Power Status

```
Main power = 28.661
UPS Battery = 27.84 27.022
Memory Battery = 4.323
```

Main Power Normal Range: 29V - 28V; AC Fail at 27.5V

1st Reading = Voltage Under Charge
2nd Reading = Open Cell Voltage
UPS Battery Normal Range: 28V - 24V
UPS Battery Low: 24V - 17V
UPS Fail: Below 17V
Weak Battery will show High Charge, but Open Cell Voltage will be low.
Dead Battery or if has short, will show Voltage Under Charge below 17V.

Memory Battery Normal Range: 3.47V - 4.5V
Replace if below 3.47V.

CMD 88 * 26 - Transactions Since Midnight

```
* Transactions Since Midnight:

Access 0
Control 1
Programming Commands 28
Lost Reports 0
Denials 0
Alarms 8

0 Communication Errors on Reader 1
0 Communication Errors on Reader 2
0 Communication Errors on Reader 3
0 Communication Errors on Reader 4
0 Communication Errors on Reader 5
0 Communication Errors on Reader 6
0 Communication Errors on Reader 7
0 Communication Errors on Reader 8
0 Communication Errors on Reader 9
0 Communication Errors on Reader 10
0 Communication Errors on Reader 11
0 Communication Errors on Reader 12
0 Communication Errors on Reader 13
0 Communication Errors on Reader 14
0 Communication Errors on Reader 15
0 Communication Errors on Reader 16
```

Reports for each reader installed

CMD 88 * 27 - Occupancy Controls

CMD 46, 437*1 Passback Mode -> OFF
CMD 46 Occupancy Violation Reporting Disabled
CMD 146 Passback Disabled During Time Zone 0
CMD 255*1 2-Person Rule Time Increment = 10
CMD 255*2 2-Person Rule Grant Threshold = 11
CMD 236 Control Zones Triggered on Occupancy Count Changes

see Table 5-5

```
PZ |on |on |on |on |Min|Min|Min|Max|Max|Min Users |Max Users | 2-Person
   |0-1|1-2|2-1|1-0|   | -1| +1|   | -1|  Inside  |  Inside  |Dis. Thr.
 2|  0|  0|  0|  0|  0|  0|  0|  0|  0|     00002|     00000|     0000
```

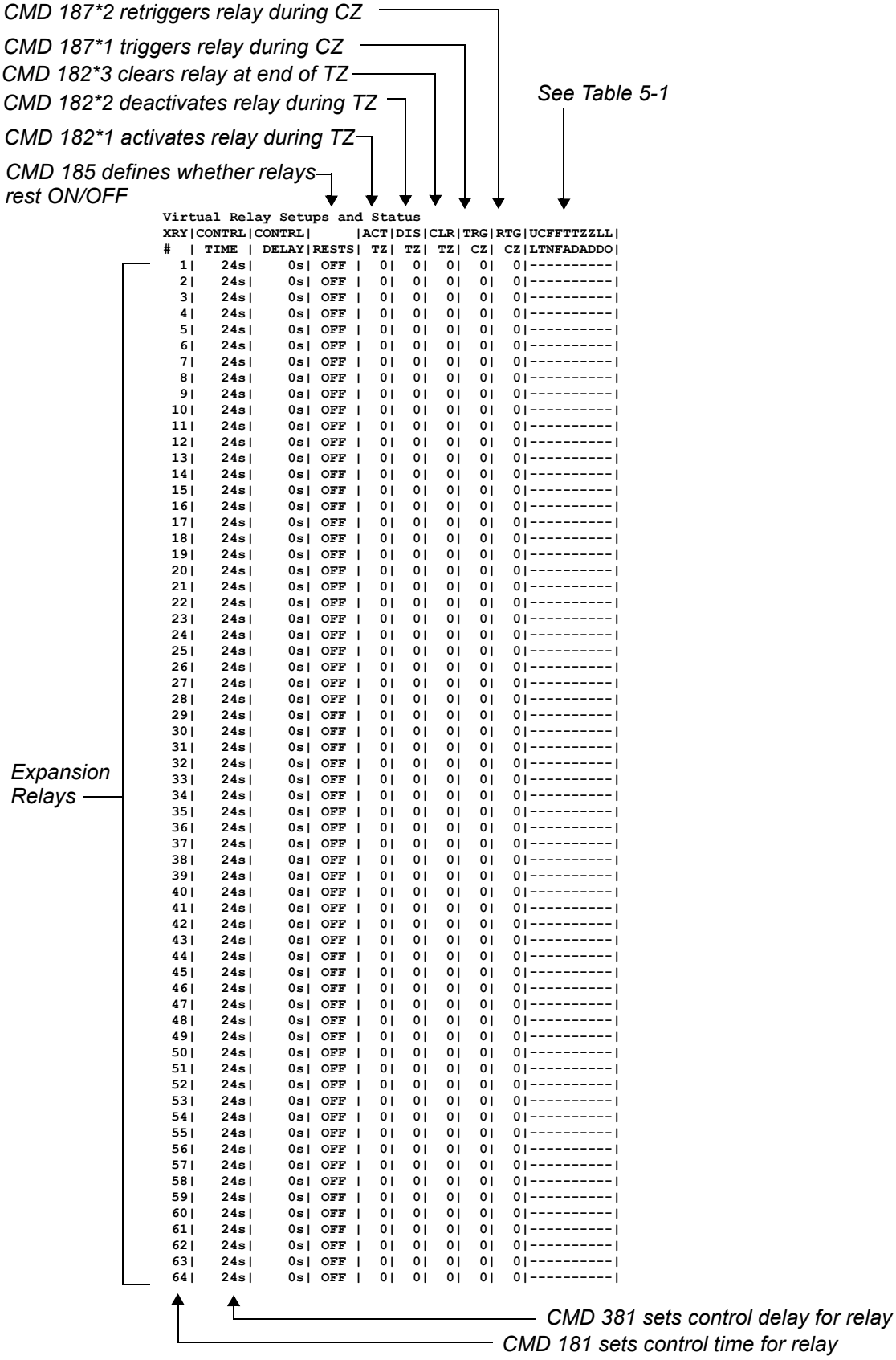
CMD 238 Single Zone Access Mode is OFF

The variables in this table are defined below:

PZ	421	Physical Zones
on 0-1	236*1	CZ triggered on change from 0 person to 1
on 1-2	236*2	CZ triggered on change from 1 person to 2
on 2-1	236*3	CZ triggered on change from 2 persons to 1
on 1-0	236*4	CZ triggered on change from 1 person to 0
Min	236*5	CZ triggered when count is at minimum
Min-1	236*6	CZ triggered when count is at minimum less 1
Min+1	236*7	CZ triggered when count is at minimum plus 1
Max	236*8	CZ triggered when count is at maximum
Max-1	236*9	CZ triggered when count is at maximum minus 1
Min Users Inside	235*1	Minimum users allowed inside
Max users inside	235*2	Maximum users allowed inside
2-Person Dis. Thr.	237	2-Person auto-disable occupancy threshold

Table 5-5: Occupancy Control Variables

CMD 88 * 28 - Virtual Relay Setups and Status



Virtual Relay Setups and Status

XRY #	CONTRL TIME	CONTRL DELAY	RESTS	ACT TZ	DIS TZ	CLR TZ	TRG CZ	RTG CZ	UCFFTTZZLL LTNFADADDO
1	24s	0s	OFF	0	0	0	0	0	----------
2	24s	0s	OFF	0	0	0	0	0	----------
3	24s	0s	OFF	0	0	0	0	0	----------
4	24s	0s	OFF	0	0	0	0	0	----------
5	24s	0s	OFF	0	0	0	0	0	----------
6	24s	0s	OFF	0	0	0	0	0	----------
7	24s	0s	OFF	0	0	0	0	0	----------
8	24s	0s	OFF	0	0	0	0	0	----------
9	24s	0s	OFF	0	0	0	0	0	----------
10	24s	0s	OFF	0	0	0	0	0	----------
11	24s	0s	OFF	0	0	0	0	0	----------
12	24s	0s	OFF	0	0	0	0	0	----------
13	24s	0s	OFF	0	0	0	0	0	----------
14	24s	0s	OFF	0	0	0	0	0	----------
15	24s	0s	OFF	0	0	0	0	0	----------
16	24s	0s	OFF	0	0	0	0	0	----------
17	24s	0s	OFF	0	0	0	0	0	----------
18	24s	0s	OFF	0	0	0	0	0	----------
19	24s	0s	OFF	0	0	0	0	0	----------
20	24s	0s	OFF	0	0	0	0	0	----------
21	24s	0s	OFF	0	0	0	0	0	----------
22	24s	0s	OFF	0	0	0	0	0	----------
23	24s	0s	OFF	0	0	0	0	0	----------
24	24s	0s	OFF	0	0	0	0	0	----------
25	24s	0s	OFF	0	0	0	0	0	----------
26	24s	0s	OFF	0	0	0	0	0	----------
27	24s	0s	OFF	0	0	0	0	0	----------
28	24s	0s	OFF	0	0	0	0	0	----------
29	24s	0s	OFF	0	0	0	0	0	----------
30	24s	0s	OFF	0	0	0	0	0	----------
31	24s	0s	OFF	0	0	0	0	0	----------
32	24s	0s	OFF	0	0	0	0	0	----------
33	24s	0s	OFF	0	0	0	0	0	----------
34	24s	0s	OFF	0	0	0	0	0	----------
35	24s	0s	OFF	0	0	0	0	0	----------
36	24s	0s	OFF	0	0	0	0	0	----------
37	24s	0s	OFF	0	0	0	0	0	----------
38	24s	0s	OFF	0	0	0	0	0	----------
39	24s	0s	OFF	0	0	0	0	0	----------
40	24s	0s	OFF	0	0	0	0	0	----------
41	24s	0s	OFF	0	0	0	0	0	----------
42	24s	0s	OFF	0	0	0	0	0	----------
43	24s	0s	OFF	0	0	0	0	0	----------
44	24s	0s	OFF	0	0	0	0	0	----------
45	24s	0s	OFF	0	0	0	0	0	----------
46	24s	0s	OFF	0	0	0	0	0	----------
47	24s	0s	OFF	0	0	0	0	0	----------
48	24s	0s	OFF	0	0	0	0	0	----------
49	24s	0s	OFF	0	0	0	0	0	----------
50	24s	0s	OFF	0	0	0	0	0	----------
51	24s	0s	OFF	0	0	0	0	0	----------
52	24s	0s	OFF	0	0	0	0	0	----------
53	24s	0s	OFF	0	0	0	0	0	----------
54	24s	0s	OFF	0	0	0	0	0	----------
55	24s	0s	OFF	0	0	0	0	0	----------
56	24s	0s	OFF	0	0	0	0	0	----------
57	24s	0s	OFF	0	0	0	0	0	----------
58	24s	0s	OFF	0	0	0	0	0	----------
59	24s	0s	OFF	0	0	0	0	0	----------
60	24s	0s	OFF	0	0	0	0	0	----------
61	24s	0s	OFF	0	0	0	0	0	----------
62	24s	0s	OFF	0	0	0	0	0	----------
63	24s	0s	OFF	0	0	0	0	0	----------
64	24s	0s	OFF	0	0	0	0	0	----------

CMD 88 * 29 - Detailed Virtual Relays

These categories are the same as those for CMD 88*19 indicating software settings for all programmable relays whether they are connected or not.

Detailed Virtual Relay Status

RY #	CNTRL TIMER	FORCE ON	FORCE OFF	TZ ACT	TZ DIS	CZ ACT	CZ DIS	LOCK DOWN	LOCK OPEN	OPER-ATION	NOW
1	--	--	--	--	--	--	--	--	--	Norml	Off
2	--	--	--	--	--	--	--	--	--	Norml	Off
3	--	--	--	--	--	--	--	--	--	Norml	Off
4	--	--	--	--	--	--	--	--	--	Norml	Off
5	--	--	--	--	--	--	--	--	--	Norml	Off
6	--	--	--	--	--	--	--	--	--	Norml	Off
7	--	--	--	--	--	--	--	--	--	Norml	Off
8	--	--	--	--	--	--	--	--	--	Norml	Off
9	--	--	--	--	--	--	--	--	--	Norml	Off
10	--	--	--	--	--	--	--	--	--	Norml	Off
11	--	--	--	--	--	--	--	--	--	Norml	Off
12	--	--	--	--	--	--	--	--	--	Norml	Off
13	--	--	--	--	--	--	--	--	--	Norml	Off
14	--	--	--	--	--	--	--	--	--	Norml	Off
15	--	--	--	--	--	--	--	--	--	Norml	Off
16	--	--	--	--	--	--	--	--	--	Norml	Off
17	--	--	--	--	--	--	--	--	--	Norml	Off
18	--	--	--	--	--	--	--	--	--	Norml	Off
19	--	--	--	--	--	--	--	--	--	Norml	Off
20	--	--	--	--	--	--	--	--	--	Norml	Off
21	--	--	--	--	--	--	--	--	--	Norml	Off
22	--	--	--	--	--	--	--	--	--	Norml	Off
23	--	--	--	--	--	--	--	--	--	Norml	Off
24	--	--	--	--	--	--	--	--	--	Norml	Off
25	--	--	--	--	--	--	--	--	--	Norml	Off
26	--	--	--	--	--	--	--	--	--	Norml	Off
27	--	--	--	--	--	--	--	--	--	Norml	Off
28	--	--	--	--	--	--	--	--	--	Norml	Off
29	--	--	--	--	--	--	--	--	--	Norml	Off
30	--	--	--	--	--	--	--	--	--	Norml	Off
31	--	--	--	--	--	--	--	--	--	Norml	Off
32	--	--	--	--	--	--	--	--	--	Norml	Off
33	--	--	--	--	--	--	--	--	--	Norml	Off
34	--	--	--	--	--	--	--	--	--	Norml	Off
35	--	--	--	--	--	--	--	--	--	Norml	Off
36	--	--	--	--	--	--	--	--	--	Norml	Off
37	--	--	--	--	--	--	--	--	--	Norml	Off
38	--	--	--	--	--	--	--	--	--	Norml	Off
39	--	--	--	--	--	--	--	--	--	Norml	Off
40	--	--	--	--	--	--	--	--	--	Norml	Off
41	--	--	--	--	--	--	--	--	--	Norml	Off
42	--	--	--	--	--	--	--	--	--	Norml	Off
43	--	--	--	--	--	--	--	--	--	Norml	Off
44	--	--	--	--	--	--	--	--	--	Norml	Off
45	--	--	--	--	--	--	--	--	--	Norml	Off
46	--	--	--	--	--	--	--	--	--	Norml	Off
47	--	--	--	--	--	--	--	--	--	Norml	Off
48	--	--	--	--	--	--	--	--	--	Norml	Off
49	--	--	--	--	--	--	--	--	--	Norml	Off
50	--	--	--	--	--	--	--	--	--	Norml	Off
51	--	--	--	--	--	--	--	--	--	Norml	Off
52	--	--	--	--	--	--	--	--	--	Norml	Off
53	--	--	--	--	--	--	--	--	--	Norml	Off
54	--	--	--	--	--	--	--	--	--	Norml	Off
55	--	--	--	--	--	--	--	--	--	Norml	Off
56	--	--	--	--	--	--	--	--	--	Norml	Off
57	--	--	--	--	--	--	--	--	--	Norml	Off
58	--	--	--	--	--	--	--	--	--	Norml	Off
59	--	--	--	--	--	--	--	--	--	Norml	Off
60	--	--	--	--	--	--	--	--	--	Norml	Off
61	--	--	--	--	--	--	--	--	--	Norml	Off
62	--	--	--	--	--	--	--	--	--	Norml	Off
63	--	--	--	--	--	--	--	--	--	Norml	Off
64	--	--	--	--	--	--	--	--	--	Norml	Off

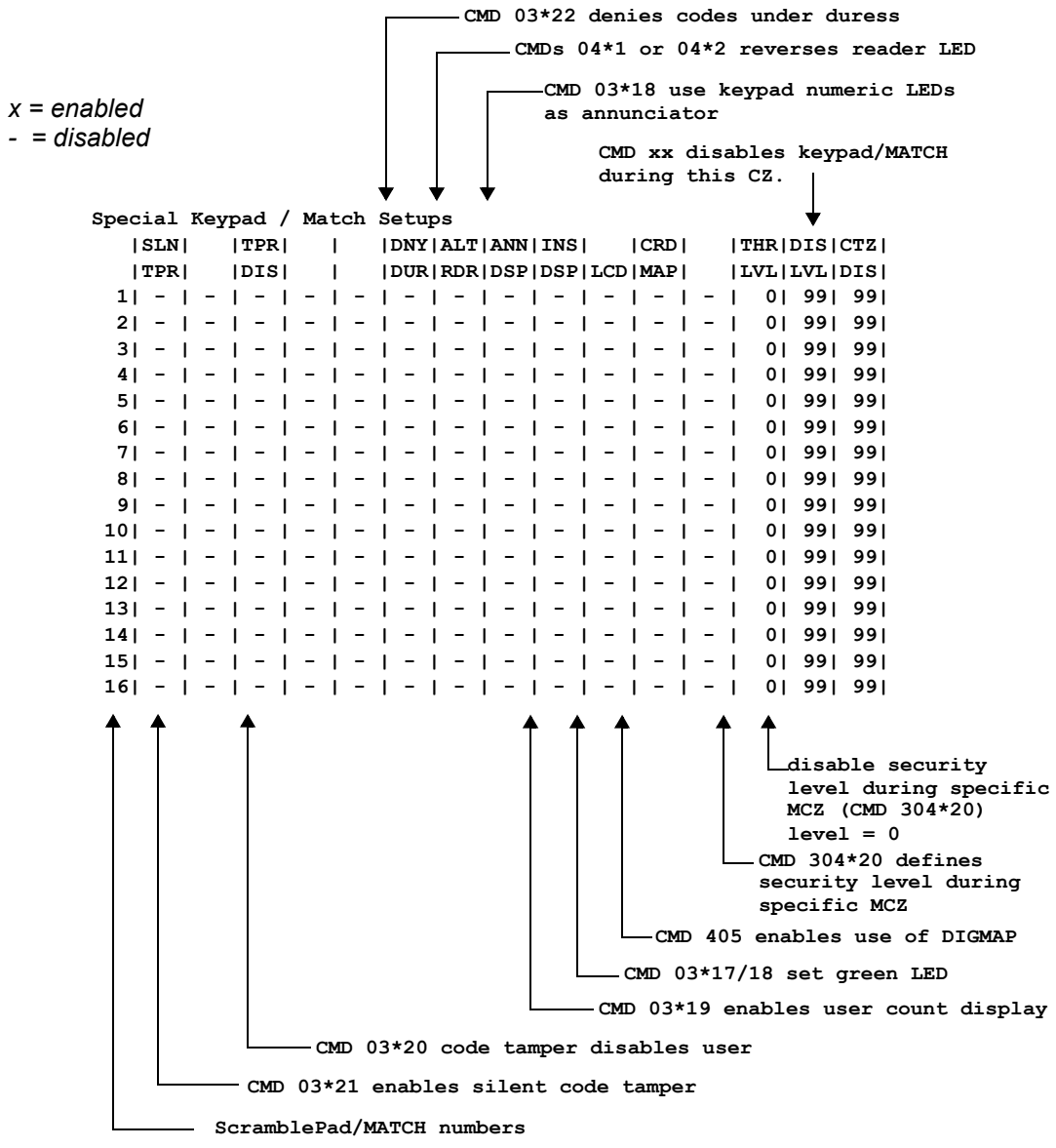
CMD 88 * 30 - HEC Factory Diagnostics

For Hirsch engineering only. Do not use.

CMD 88 * 31 - Special Needs Unlock Extension Times

```
Special Needs Unlock Extension Times
Door Delay Extension (sec) = 0 <---- CMD 282 * N
Door Mode Extension  (sec) = 0 <---- CMD 282 * 0 * N
Door Open Extension  (sec) = 0 <---- CMD 282 * 0 * 0 * N
```

CMD 88 * 32 - Special Keypad / MATCH Setups



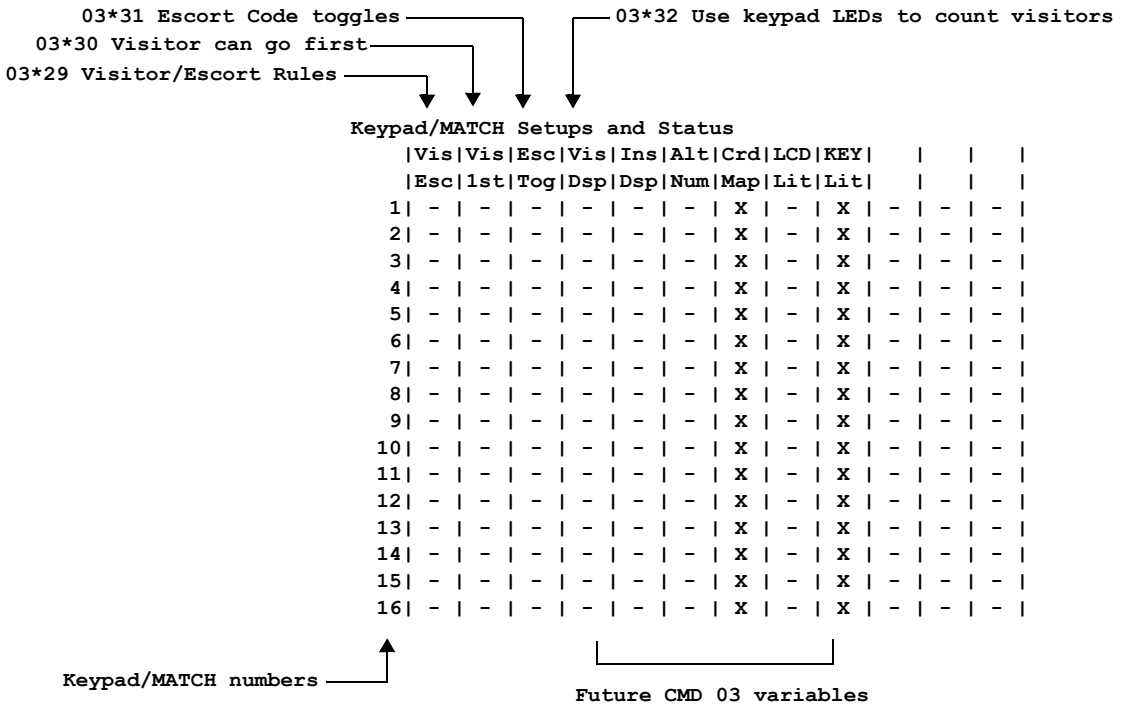
CMD 88 * 33 - Custom Card Map Setups

This table is defined by the custom card DIGMAP specifications for a specific MATCH reader created through the use of CMD 405. This command enables the host to set up a customized card reader, assuming that the MATCH board connected to the card reader supports this feature. This command is used to select a subset of 8 – 16 digits out of the card code received from the card reader.

```
Custom Card Map Setups
  1 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  2 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  3 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  4 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  5 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  6 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  7 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  8 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
  9 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 10 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 11 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 12 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 13 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 14 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 15 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
 16 |  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
```

CMD 88 * 34 - Additional Keypads / MATCH Setup & Status

This table is lists setups and status for all additional keypads as well as MATCHs detected by the controller. Up to 16 additional keypads and MATCHs can be detailed here.



This report is not included when you issue CMD 88*0.

Print Setup Guide

Use a 188 command to return a list of commands and their arguments used to program components since cold start. This is different from CMD 88 which prints out a list of factory default settings and status conditions for each requested system component. For example, if the system administrator programmed a new date using CMD 50, then this command plus the arguments used to set the new date (such as 50 * 011098 * 4 #) would be printed out if either 188 * 0 or 188 * 1 were specified.

This command is particularly useful for troubleshooting a system, since it provides the programmer with an opportunity to review all commands entered since cold start and ascertain whether the commands were entered correctly.

If your controller is linked to a printer, the result of your query is printed out.

The following pages show a representative list of commands that might be used to program a DIGI*TRAC Model 8. The report is printed by executing the Command 188*0. You may also print individual parts of the report by selecting different variables.

The general syntax for CMD 188 is:

```
ST 188 * NN #
```

where:

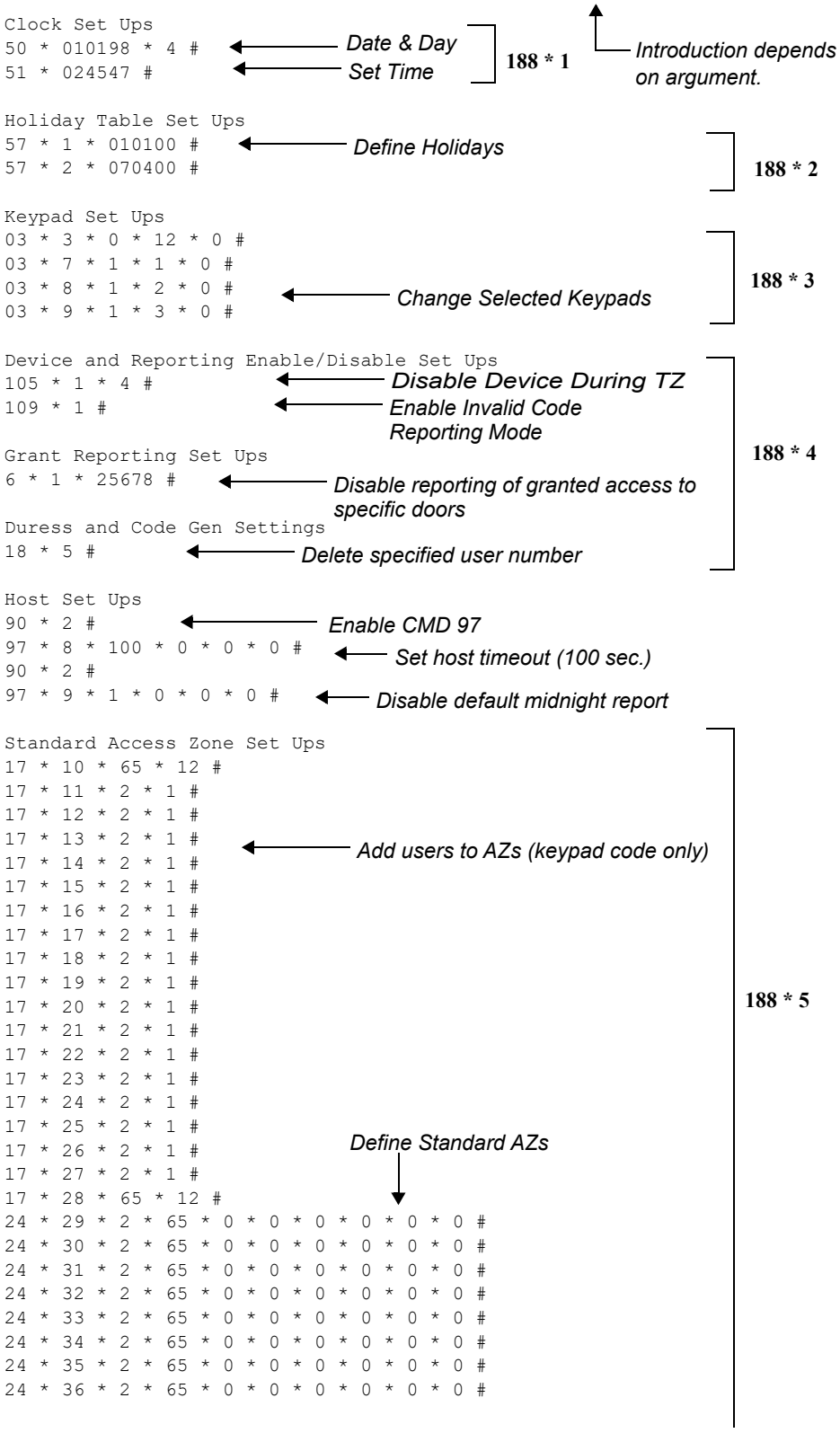
NN	Value	Commands Printed
0	Complete System Setups and Status	All
1	Date, Time, Version Number	CMD 50 - 51
2	Holidays	CMD 57 - 59
3	Keypad and MATCH	CMD 3, 103 - 104
4	Reporting and Duress	CMD 05-09, 18, 105-109, 140, 191-195
5	Standard Access Zones	CMD 17, 24, 117, 201, 203, 217, 249, 349
6	Master Access Zones	CMD 204, 217, 249, 349
7	Standard Control Zones	CMD 45, 301-303, 345
8	Master Control Zones	CMD 304-308
9	Passback & User Management	CMD 46, 146, 235-238, 255-257
10	Time Zones	CMD 52, 54, 56, 154
11	Alarm Action Control Blocks	CMD 261
12	Alarm & Sense Inputs	CMD 70-77, 84, 110, 112, 270
13	Expansion Line Module Inputs	CMD 111, 113, 170-176, 180, 184, 186
14	Relays	CMD 79-83, 85-87, 280-281
15	Expansion Relays	CMD 181-183, 185, 187

The order of topics below is that provided when you use CMD 188 * 0. The command variable you would use to display a specific section of the data is shown in the margin.

Note: Neither the command in bold nor the commentary appears in the printout.

The following example lists an entire printout as it would be generated if the user specified 188 * 0. If a user specifies one of the other arguments, then only designated portions of this list would appear. Each part is explained briefly on the following pages.

```
188*0#.  This is a Master dump of your System Setups.
Keep it in a safe place. You can restore your Setups from a cold start
using this printout, plus a list of CODEs & passwords. Good luck.

Clock Set Ups
50 * 010198 * 4 #
51 * 024547 #

Holiday Table Set Ups
57 * 1 * 010100 #
57 * 2 * 070400 #

Keypad Set Ups
03 * 3 * 0 * 12 * 0 #
03 * 7 * 1 * 1 * 0 #
03 * 8 * 1 * 2 * 0 #
03 * 9 * 1 * 3 * 0 #

Device and Reporting Enable/Disable Set Ups
105 * 1 * 4 #
109 * 1 #

Grant Reporting Set Ups
6 * 1 * 25678 #

Duress and Code Gen Settings
18 * 5 #

Host Set Ups
90 * 2 #
97 * 8 * 100 * 0 * 0 * 0 * 0 #
90 * 2 #
97 * 9 * 1 * 0 * 0 * 0 * 0 #

Standard Access Zone Set Ups
17 * 10 * 65 * 12 #
17 * 11 * 2 * 1 #
17 * 12 * 2 * 1 #
17 * 13 * 2 * 1 #
17 * 14 * 2 * 1 #
17 * 15 * 2 * 1 #
17 * 16 * 2 * 1 #
17 * 17 * 2 * 1 #
17 * 18 * 2 * 1 #
17 * 19 * 2 * 1 #
17 * 20 * 2 * 1 #
17 * 21 * 2 * 1 #
17 * 22 * 2 * 1 #
17 * 23 * 2 * 1 #
17 * 24 * 2 * 1 #
17 * 25 * 2 * 1 #
17 * 26 * 2 * 1 #
17 * 27 * 2 * 1 #
17 * 28 * 65 * 12 #
24 * 29 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 30 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 31 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 32 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 33 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 34 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 35 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 36 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 * 0 #
```



```
24 * 37 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 38 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 39 * 2 * 65 * 0 * 0 * 0 * 0 * 0 * 0 #
17 * 40 * 2 * 1 #
17 * 41 * 2 * 1 #
17 * 42 * 2 * 1 #
17 * 43 * 2 * 1 #
24 * 44 * 2 * 1 * 0 * 0 * 0 * 0 * 0 * 0 #
17 * 45 * 2 * 1 #
17 * 46 * 2 * 1 #
17 * 47 * 2 * 1 #
17 * 48 * 2 * 1 #
17 * 49 * 2 * 1 #
17 * 50 * 2 * 1 #
17 * 51 * 2 * 1 #
17 * 52 * 2 * 1 #
17 * 53 * 2 * 1 #
17 * 54 * 2 * 1 #
17 * 55 * 2 * 1 #
17 * 56 * 65 * 1 #
17 * 57 * 2 * 1 #
24 * 58 * 65 * 2 * 0 * 0 * 0 * 0 * 0 * 0 #
24 * 60 * 2 * 1 * 0 * 0 * 0 * 0 * 0 * 0 #
204 * 12 * 66 * 1 #
204 * 30 * 66 * 2 #
204 * 12 * 67 * 1 #
204 * 25 * 67 * 2 #
```

Define Master AZs

188 * 5

```
Standard Control Zone Set Ups
45 * 1 * 3 * 123 #
45 * 2 * 2 * 4567 #
```

Define Standard CZs

188 * 6

```
Master Control Zone Set Ups
304 * 1 * 1 * 192 #
305 * 65 * 192 #
307 * 0 * 192 #
304 * 2 * 2 * 193 #
305 * 65 * 193 #
307 * 0 * 193 #
307 * 0 * 194 #
307 * 0 * 195 #
307 * 0 * 196 #
307 * 0 * 197 #
307 * 0 * 198 #
307 * 0 * 199 #
307 * 0 * 200 #
307 * 0 * 201 #
307 * 0 * 202 #
307 * 0 * 203 #
307 * 0 * 204 #
307 * 0 * 205 #
307 * 0 * 206 #
307 * 0 * 207 #
307 * 0 * 208 #
307 * 0 * 209 #
307 * 0 * 210 #
307 * 0 * 211 #
307 * 0 * 212 #
307 * 0 * 213 #
307 * 0 * 214 #
307 * 0 * 215 #
307 * 0 * 216 #
```

Define Master CZs
Define TZ for Master CZ

188 * 7

Define AZ for Linked and Master CZs

188 * 8

```
307 * 0 * 217 #
307 * 0 * 218 #
307 * 0 * 219 #
307 * 0 * 220 #
307 * 0 * 221 #
307 * 0 * 222 #
307 * 0 * 223 #
307 * 0 * 224 #
307 * 0 * 225 #
307 * 0 * 226 #
307 * 0 * 227 #
307 * 0 * 228 #
307 * 0 * 229 #
307 * 0 * 230 #
307 * 0 * 231 #
307 * 0 * 232 #
307 * 0 * 233 #
307 * 0 * 234 #
307 * 0 * 235 #
307 * 0 * 236 #
307 * 0 * 237 #
307 * 0 * 238 #
307 * 0 * 239 #
307 * 0 * 240 #
307 * 0 * 241 #
307 * 0 * 242 #
307 * 0 * 243 #
307 * 0 * 244 #
307 * 0 * 245 #
307 * 0 * 246 #
307 * 0 * 247 #
307 * 0 * 248 #
307 * 0 * 249 #
307 * 0 * 250 #
307 * 0 * 251 #
307 * 0 * 252 #
307 * 0 * 253 #
307 * 0 * 254 #
307 * 0 * 255 #
```

Define AZ for Linked and Master CZs

188 * 8

```
Passback and User Management Set Ups
46 * 2 #
```

Change Passback Mode

188 * 9

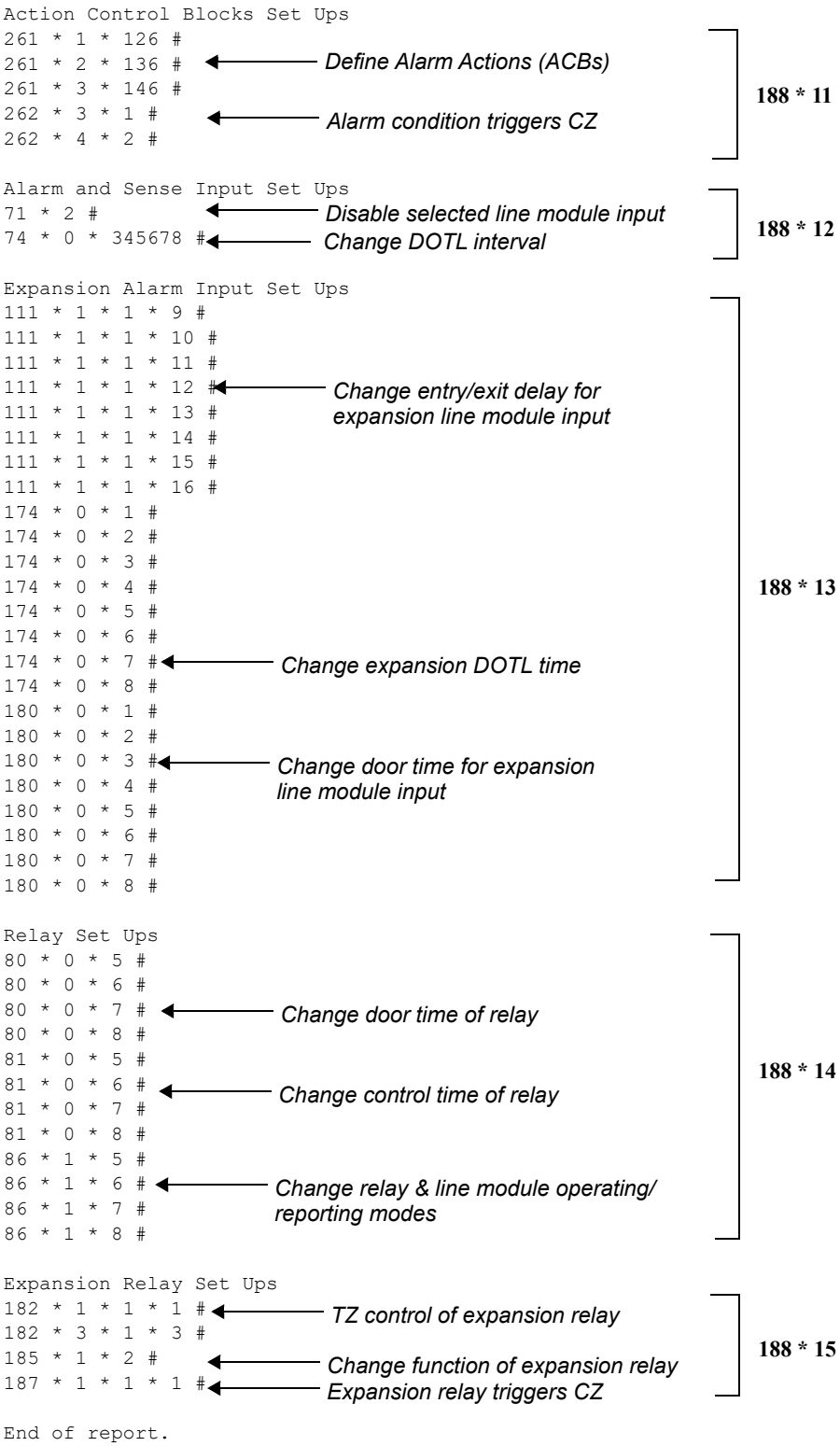
```
Standard Time Zone Set Ups
52 * 1 * 0630 * 1930 * 12345 #
52 * 2 * 0600 * 2000 * 1234567 #
52 * 3 * 0830 * 1800 * 12345 #
52 * 4 * 1100 * 1400 * 12345 #

Master Time Zone Set Ups
54 * 1 * 66 * 1 #
54 * 3 * 66 * 2 #
54 * 4 * 67 * 1 #

Grand Time Zone Set Ups
154 * 66 * 130 * 1 #
154 * 67 * 130 * 2 #
```

Define Standard TZ

Define Master TZ

Define Grand Master TZ

188 * 10


Action Control Blocks Set Ups
261 * 1 * 126 #
261 * 2 * 136 #
261 * 3 * 146 #
262 * 3 * 1 #
262 * 4 * 2 #
Define Alarm Actions (ACBs)
Alarm condition triggers CZ
188 * 11
Alarm and Sense Input Set Ups
71 * 2 #
74 * 0 * 345678 #
Disable selected line module input
Change DOTL interval
188 * 12
Expansion Alarm Input Set Ups
111 * 1 * 1 * 9 #
111 * 1 * 1 * 10 #
111 * 1 * 1 * 11 #
111 * 1 * 1 * 12 #
111 * 1 * 1 * 13 #
111 * 1 * 1 * 14 #
111 * 1 * 1 * 15 #
111 * 1 * 1 * 16 #
174 * 0 * 1 #
174 * 0 * 2 #
174 * 0 * 3 #
174 * 0 * 4 #
174 * 0 * 5 #
174 * 0 * 6 #
174 * 0 * 7 #
174 * 0 * 8 #
180 * 0 * 1 #
180 * 0 * 2 #
180 * 0 * 3 #
180 * 0 * 4 #
180 * 0 * 5 #
180 * 0 * 6 #
180 * 0 * 7 #
180 * 0 * 8 #
Change entry/exit delay for expansion line module input
Change expansion DOTL time
Change door time for expansion line module input
188 * 13
Relay Set Ups
80 * 0 * 5 #
80 * 0 * 6 #
80 * 0 * 7 #
80 * 0 * 8 #
81 * 0 * 5 #
81 * 0 * 6 #
81 * 0 * 7 #
81 * 0 * 8 #
86 * 1 * 5 #
86 * 1 * 6 #
86 * 1 * 7 #
86 * 1 * 8 #
Change door time of relay
Change control time of relay
Change relay & line module operating/ reporting modes
188 * 14
Expansion Relay Set Ups
182 * 1 * 1 * 1 #
182 * 3 * 1 * 3 #
185 * 1 * 2 #
187 * 1 * 1 * 1 #
TZ control of expansion relay
Change function of expansion relay
Expansion relay triggers CZ
188 * 15
End of report.

Printout Guide

DIGI*TRAC Systems are designed to utilize a local dot matrix line printer to provide real time reports of transactions, events and alarms. There are a variety of Commands that affect the printer. Each of these Commands will be detailed in this Printout Guide along with examples of the resulting printed reports where appropriate.

Note: Laser and inkjet printers are not supported.

Context-Sensitive Printed Help

DIGI*TRAC systems provide context-sensitive printed help on the system printer. If an operator makes an error during the Command entry process, the system will print an error message followed by the correct Command syntax. This capability can also be used to print the syntax of an infrequently-used Command by entering the Command number followed by several * keys. This forces a Command error and the controller will print the desired Command syntax.

Command Printed Responses

The system will also print a Command response upon Command execution. These printouts are valuable for confirming the result of the programming Command just issued. For example, when changing the unlock time of a door, the relay setup and status report will automatically be printed to confirm the change. In addition, whenever a new user is added or an existing user is deleted, one of several styles of user report will be automatically printed.

CMD 10 Add Access User - Keypad Only - Printed Report

For example, the report for the command 10*100*2495*65 might be:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00100.        Access         .KPD .1. 65.Unknown . No  . No  .
User Added/Updated
```

CMD 22 Add Access Users - Keypad Only - Printed Report

For example, the report for the command 22*1*8*2 might be:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00001.        Access         .KPD .1.  2.4519015 . -
00002.        Access         .KPD .1.  2.2585000 . -
00003.        Access         .KPD .1.  2.1775304 . -
00004.        Access         .KPD .1.  2.8959517 . -
00005.        Access         .KPD .1.  2.7302450 . -
00006.        Access         .KPD .1.  2.4597448 . -
00007.        Access         .KPD .1.  2.4615568 . -
00008.        Access         .KPD .1.  2.9162988 . -
Auto-Generation Done
```

Note: 8 Users GeneratedSecure These Printouts. Note that when automatically generating new users with keypad codes, the codes will be printed out for issuance. These printouts must be securely stored or destroyed. Printouts listing codes can be printed on Command by an authorized operator.

CMD 16 Delete A User - Printed Report

For example, the report to the command 16*6 might be:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00006.    <unused record>
```

CMD 00 Print Lists of Commands

This Command allows the system operator to print a list of Commands by category or in total. This Command is useful for printing a substitute manual or programming guide from the system's permanent memory in case the printed manual is not available.

```
System Commands
------------------------------------------------------------
Print Lists of Commands PW 12345
ST 00 * NN #
0 - All Commands
1 - System Commands
2 - Program User Commands
3 - Auto-Program User Commands
4 - Program Multiple ID User Commands
5 - Program Control User Commands
6 - User Management Commands
7 - Print Users without CODE Commands
8 - Print Users with CODE Commands
9 - Time Control Commands
10- Access Zone Commands
11- Control Zone Commands
12- Duress Commands
13- Alarm / RQE Commands
14- Expansion Alarm Commands
15- Keypad / MATCH Commands
16- Rel Commands
17- Expansion Relay Commands
- Report Commands
19- Rete Site Management Commands
20- Print System Setups and Status
21- Maintenance
22- Glossary
```

Print Users without CODE Commands

CMD 30 Print User without CODE

This Command prints a single user record without listing the CODE. For example, the report to the command 30*100 might be:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00100.        Access         .KPD .1. 65.Unknown . No  . No  .
```

CMD 31 Print Users without CODE

This Command prints a range of user records without listing the CODE. For example, the response to the command 31*1*15 might be:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00001.        Access         .KPD .1.  2.Unknown . No  . No  .
00002.        Access         .KPD .1.  2.Unknown . No  . No  .
00003.        Access         .KPD .1.  2.Unknown . No  . No  .
00004.        Access         .KPD .1.  2.Unknown . No  . No  .
00005.        Access         .KPD .1.  2.Unknown . No  . No  .
00006.        Access         .KPD .1. 65.Unknown . No  . No  .
00007.        Access         .KPD .1.  2.Unknown . No  . No  .
00008.        Access         .KPD .1.  2.Unknown . No  . No  .
00009.        Access         .KPD .1. 65.Unknown . No  . No  .
00010.        Access         .KPD .1. 65.Unknown . No  . No  .
00011.        Access         .KPD .1. 65.Unknown . No  . No  .
00012.        Access         .KPD .1. 65.Unknown . No  . No  .
00013.        Access         .KPD .1. 65.Unknown . No  . No  .
00014.        Access         .KPD .1. 65.Unknown . No  . No  .
00015.        Access         .KPD .1. 65.Unknown . No  . No  .
```

CMD 32 Print First Available User Number From Specified Starting User Number

This Command prints the first unused user record from the specified starting user number. This Command is used to assist the operator in selecting the next available user within a range to manually add a new user. For example, the response to the command 32*100 might be:

```
First Available User Number = 105
```

CMD 33 Print Users Given Access Zone Or Control Zone

This Command is used to print a list of users organized by their Access Zone or Control Zone. For example, the response to the command 33*1*65 might be:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00000.      SYSTEM CODE      .KPD .1. 65.   n/a  . No  . No  .
00006.        Access         .KPD .1. 65.Unknown . No  . No  .
00009.        Access         .KPD .1. 65.Unknown . No  . No  .
00010.        Access         .KPD .1. 65.Unknown . No  . No  .
00011.        Access         .KPD .1. 65.Unknown . No  . No  .
00012.        Access         .KPD .1. 65.Unknown . No  . No  .
00013.        Access         .KPD .1. 65.Unknown . No  . No  .
00014.        Access         .KPD .1. 65.Unknown . No  . No  .
00015.        Access         .KPD .1. 65.Unknown . No  . No  .
00016.        Access         .KPD .1. 65.Unknown . No  . No  .
00017.        Access         .KPD .1. 65.Unknown . No  . No  .
00018.        Access         .KPD .1. 65.Unknown . No  . No  .
00019.        Access         .KPD .1. 65.Unknown . No  . No  .
00039.        Access         .KPD .1. 65.Unknown . No  . No  .
00040.        Access         .KPD .1. 65.Unknown . No  . No  .
00041.        Access         .KPD .1. 65.Unknown . No  . No  .
00042.        Access         .KPD .1. 65.Unknown . No  . No  .
00100.        Access         .KPD .1. 65.Unknown . No  . No  .
00150.        Unlock         .KPD .1. 65.   n/a  . No  . No  .
00151.        Relock         .KPD .1. 65.   n/a  . No  . No  .
```

CMD 34 Print Families of Users without CODE

This Command is used to print a list of users organized by function, status, or by location within the security boundary of a Passback controlled system. For example, the response to the command 34*1*0*999 filters for force on/off functions:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00200.        Control        .KPD .1.  1.   n/a  . No  . No  .
00400.       Force Off       .KPD .1.  8.   n/a  . No  . No  .
00401.   Force Off Release   .KPD .1.  8.   n/a  . No  . No  .
00500.       Force On        .KPD .1.  4.   n/a  . No  . No  .
00501.   Force On Release    .KPD .1.  4.   n/a  . No  . No  .
End Printout
```

In an example, the response to the line 34*7*0*999 filters for masking/unmasking functions:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00700.      Alarm Mask       .KPD .1. 23.   n/a  . No  . No  .
00701.     Alarm Unmask      .KPD .1. 23.   n/a  . No  . No  .
End Printout
```

In yet another example, the response to the line 34*8*0*999 filters for system code:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00000.      SYSTEM CODE      .KPD .1. 65.   n/a  . No  . No  .
End Printout
```

Print Users with CODE Commands

CMD 35 Print User with Code

This Command prints a single user record with the CODE listed. For example, the response to the command 35*100 might be:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00100.        Access         .KPD .1. 65.123456  . -
```

or, to the command 35*106:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00106.       Force On        .KPD .1. 50.222     . -
```

CMD 36 Print Users with CODE

This Command prints a range of user records with the codes listed. For example, the response to the command 36*100*999 might be:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00100.         Access         .KPD .1. 65.2495    . 5
00150.         Unlock         .KPD .1. 65.24951   . 5
00151.         Relock         .KPD .1. 65.24952   . 5
00200.         Control        .KPD .1.  1.26549   . 5
00201.       Lock Down        .KPD .1.  3.582141  . 5
00202.   Lock Down Release    .KPD .1.  3.582142  . 5
00300.       Lock Open        .KPD .1. 12.671461  . 5
00301.   Lock Open Release    .KPD .1. 12.671462  . 5
00400.       Force Off        .KPD .1.  8.915461  . 5
00401.   Force Off Release    .KPD .1.  8.915462  . 5
00500.       Force On         .KPD .1.  4.6397451 . 5
00501.   Force On Release     .KPD .1.  4.6397452 . 5
00700.      Alarm Mask        .KPD .1. 23.24959   . 5
00701.     Alarm Unmask       .KPD .1. 23.24950   . 5
```

CMD 37 Print User Given CODE

This Command is used to confirm a user number when the user's code is known. For example, the response to the command 37*2495 might be:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00100.         Access         .KPD .1. 65.2495    . 5
```

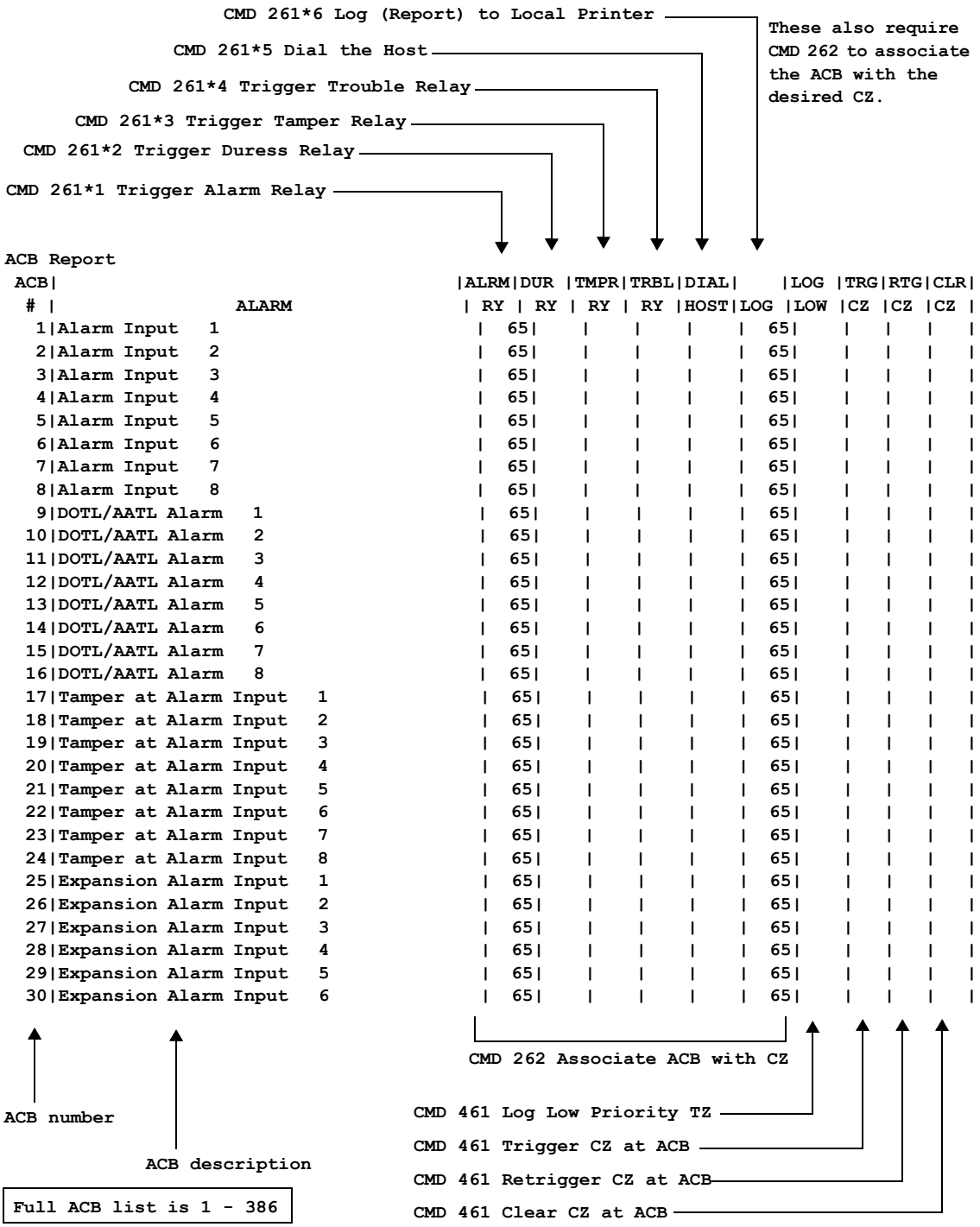
CMD 38 Print Families of Users with CODE

This Command is used to print a list of users organized by function. In addition, a list of users can be printed sorted by CODE. For example, the response to the command 38*2*0*20 might be:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00001.         Access         .KPD .1.  2.4519015 . -
00002.         Access         .KPD .1.  2.2585000 . -
00003.         Access         .KPD .1.  2.1775304 . -
00004.         Access         .KPD .1.  2.8959517 . -
00005.         Access         .KPD .1.  2.7302450 . -
00006.         Access         .KPD .1. 65.8948004 . -
00007.         Access         .KPD .1.  2.4615568 . -
00008.         Access         .KPD .1.  2.9162988 . -
00009.         Access         .KPD .1. 65.7447730 . -
00010.         Access         .KPD .1. 65.1897559 . -
00011.         Access         .KPD .1. 65.1625276 . -
00012.         Access         .KPD .1. 65.0331532 . -
00013.         Access         .KPD .1. 65.2574616 . -
00014.         Access         .KPD .1. 65.2335917 . -
00015.         Access         .KPD .1. 65.6015300 . -
00016.         Access         .KPD .1. 65.4448447 . -
00017.         Access         .KPD .1. 65.7532591 . -
00018.         Access         .KPD .1. 65.7324882 . -
00019.         Access         .KPD .1. 65.5601928 . -
00020.         Access         .KPD .1.  3.8886000 . -
End Printout
```

CMD 260 Print Alarm Actions

This printout is lists all of the system's internal alarm conditions and how they are configured to report when active. This printout shows changes to setups of specific line module inputs or system alarms and how they report when actuated. The example below lists only the first 30 ACBs.



Refer to CMD 261 starting on page 4-187 for a complete list of ACBs.

CMD 330 Print Setups and Status by Printout Style for Families of Users

This Command is capable of printing a list of users by function and by Style. User reports include the status of Temporary-Days, the status of Use-Count, the status of Absentee Rule, and the current Passback location with tagged and alerted conditions. For example, the response to the command 330*1*1*1*15 which filters by user codes might be:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE  |DUR|
-----+----------------------+----+-+---+--------+---|
00001.        Access         .KPD .1.  2.4519015 . -
00002.        Access         .KPD .1.  2.2585000 . -
00003.        Access         .KPD .1.  2.1775304 . -
00004.        Access         .KPD .1.  2.8959517 . -
00005.        Access         .KPD .1.  2.7302450 . -
00006.        Access         .KPD .1. 65.8948004 . -
00007.        Access         .KPD .1.  2.4615568 . -
00008.        Access         .KPD .1.  2.9162988 . -
00009.        Access         .KPD .1. 65.7447730 . -
00010.        Access         .KPD .1. 65.1897559 . -
00011.        Access         .KPD .1. 65.1625276 . -
00012.        Access         .KPD .1. 65.0331532 . -
00013.        Access         .KPD .1. 65.2574616 . -
00014.        Access         .KPD .1. 65.2335917 . -
00015.        Access         .KPD .1. 65.6015300 . -
End Printout
```

Or, the response to the command 330*1*3*40*49 which filters by use-count might be:

```
Use-Count
                                        |Use|
User#|   User Function     | ID |F| Z |Cnt|Cnt|DEL|
-----+----------------------+----+-+---+---+---+---|
00040.        Access         .KPD .1. 65.Yes.  6.Yes.
00041.        Access         .KPD .1. 65.Yes.  6.Yes.
00042.        Access         .KPD .1. 65.Yes.  6.Yes.
00043.        Access         .KPD .1.  4.Yes.  0.Yes.
00044.        Access         .KPD .1.  4.Yes.  0.Yes.
00045.        Access         .KPD .1.  4.No .  0.Yes.
00046.        Access         .KPD .1.  4.No .  0.Yes.
00047.        Access         .KPD .1.  4.No .  0.Yes.
00048.        Access         .KPD .1.  4.No .  0.Yes.
00049.        Access         .KPD .1.  4.No .  0.Yes.
End Printout
```

Or, the response to the command 330*1*4*40*50 which filters by absentee rule might be:

```
Absentee Rule
User#|     User Function     | ID |F| Z |Mode |Max Days|Current |DEL|
-----+----------------------+----+-+---+-----+--------+--------+---|
00040.        Access         .KPD .1. 65. No  .        .        .Yes.
00041.        Access         .KPD .1. 65. No  .        .        .Yes.
00042.        Access         .KPD .1. 65. No  .        .        .Yes.
00043.        Access         .KPD .1.  4. No  .        .        .Yes.
00044.        Access         .KPD .1.  4. Yes .   45   .   45   .Yes.
00045.        Access         .KPD .1.  4. Yes .   45   .   45   .Yes.
00046.        Access         .KPD .1.  4. Yes .   45   .   45   .Yes.
00047.        Access         .KPD .1.  4. Yes .   45   .   45   .Yes.
00048.        Access         .KPD .1.  4. Yes .   60   .   60   .Yes.
00049.        Access         .KPD .1.  4. Yes .   60   .   60   .Yes.
00050.        Access         .KPD .1.  4. No  .        .        .No .
End Printout
```

Or, the command 330*1*5*1*10 which filters by user tracking status:

```
User Tracking Status
User#|     User Function     | ID |F| Z |PassBack| Tag |Alert|
-----+----------------------+----+-+---+--------+-----+-----|
00001.        Access          .KPD .1.  2.Unknown . No  . No  .
00002.        Access          .KPD .1.  2.Unknown . No  . No  .
00003.        Access          .KPD .1.  2.Unknown . Yes . No  .
00004.        Access          .KPD .1.  2.Unknown . No  . Yes .
00005.        Access          .KPD .1.  2.Unknown . No  . Yes .
00006.        Access          .KPD .1. 65.Unknown . Yes . Yes .
00007.        Access          .KPD .1.  2.Unknown . Yes . No  .
00008.        Access          .KPD .1.  2.Unknown . No  . No  .
00009.        Access          .KPD .1. 65.Unknown . No  . Yes .
00010.        Access          .KPD .1. 65.Unknown . No  . Yes .
```

Or, the command 330*1*6*1*10 which filters by Deadman Timer:

```
Deadman Timer
User#|     User Function     | ID |F| Z |Deadman Timer|
-----+----------------------+----+-+---+-------------|
00001.        Access          .KPD .1.  2.     n/a     |
00002.        Access          .KPD .1.  2.     n/a     |
00003.        Access          .KPD .1.  2.     n/a     |
00004.        Access          .KPD .1.  2.     n/a     |
00005.        Access          .KPD .1.  2.     n/a     |
00006.        Access          .KPD .1. 65.     n/a     |
00007.        Access          .KPD .1.  2.     n/a     |
00008.        Access          .KPD .1.  2.     n/a     |
00009.        Access          .KPD .1. 65.     n/a     |
00010.        Access          .KPD .1. 65.     n/a     |
End Printout
```

Or, the command 330*2*2*50*59 which filters by User Temporary Days:

```
User Temporary-Days
                                          |Tmp|  Temp Days   |
User     User Function     | ID |F| Z |Use|MTWTFSSMTWTFSS|DEL|
-----+----------------------+----+-+---+---+--------------+---|
00050.        Access          .KPD .1.  4.Yes.XX-----XX-----.No .
00051.        Access          .KPD .1.  4.Yes.XX-----XX-----.No .
00052.        Access          .KPD .1.  4.Yes.XX-----XX-----.No .
00053.        Access          .KPD .1.  4.Yes.XX-----XX-----.No .
00054.        Access          .KPD .1.  4.Yes.-XXX---XX-----.No .
00055.        Access          .KPD .1.  4.Yes.-XXX---XX-----.No .
00056.        Access          .KPD .1.  4.Yes.-XXX---XX-----.No .
00057.        Access          .KPD .1.  4.Yes.-------XX-----.No .
00058.        Access          .KPD .1.  4.Yes.-------XX-----.No .
00059.        Access          .KPD .1.  4.Yes.-------XX-----.No .
End Printout
```

Or, finally, the command 330*1*1*1*10 which filters by User Codes:

```
User CODEs
User#|     User Function     | ID |F| Z |  CODE   |DUR|
-----+----------------------+----+-+---+---------+---|
00001.        Access          .KPD .1.  2.4519015 . -
00002.        Access          .KPD .1.  2.2585000 . -
00003.        Access          .KPD .1.  2.1775304 . -
00004.        Access          .KPD .1.  2.8959517 . -
00005.        Access          .KPD .1.  2.7302450 . -
00006.        Access          .KPD .1. 65.8948004 . -
00007.        Access          .KPD .1.  2.4615568 . -
00008.        Access          .KPD .1.  2.9162988 . -
00009.        Access          .KPD .1. 65.7447730 . -
00010.        Access          .KPD .1. 65.1897559 . -
End Printout
```

Report Commands

These Commands change the way in which the system printer operates and what is printed. The Factory printer setup allows the system to print virtually every transaction, event, alarm and internal change of state possible. This information is invaluable when first setting up a system and when troubleshooting an improperly operating system. However, during normal system operation, many owners want to reduce the amount of information printed. These Commands allow that as well as other reporting controls.

CMD 05 Reporting Modes

This Command is used to disable the printing of relay state changes, normally not required during system operation. Internal and external events can also be disabled from printing. Refer to the Glossary for a complete list of all internal and external events. All transactions from users entering codes or cards as well as RQE requests can be disabled with this Command. See the next Command for eliminating granted transactions only while letting denied transaction print. Time Zone controlled state changes of system operational modes, relays and line module input masking may also be disabled from printing.

CMD 06 Disable Report of Grants on Selected Doors

This Command is used to disable the printing of granted user transactions on a door by door basis. It does not disable denied transactions. If an authorized user attempts access at the wrong door or at the wrong time and is denied, it will be printed. RQE, Request-To-Exit, transactions can be disabled on a door by door basis if desired.

CMD 105 Disable Device During Time Zone

This Command disables the printer from printing anything at all during the specified Time Zone. This reduces the quantity of printed records from time periods when printed records are not required, but enables printed records to be collected during more sensitive time periods. This Command also prevents data from being logged in the system's internal history buffer. The S*NIB may also be disabled during a specified Time Zone, thus taking the system off-line from the SCRAMBLE*NET.

CMD 106 Disable Reporting During Time Zone

This Command disables the printing of all user transactions, either granted or denied, or system events during the specified Time Zone. It does not disable the printing of alarms.

CMD 107 Daily Report Printing

This Command disables the several page long daily system status report. This report is normally printed each and every midnight Monday through Saturday. On Sunday at midnight, a more complete weekly status report is printed.

CMD 109 Invalid CODE Reporting

This Command enables the printing of invalid codes when they are entered at a keypad. This may prove useful for detecting users attempting to guess another valid code using a systematic approach, or may disclose a user making errors by transposing digits in their code. It will also print the resulting MATCH code from an invalid card.

CMD 140 Set Report Buffer Alarm Threshold

This Command establishes how many reports are held in the system's internal buffer memory, either the standard ONBOARD memory, or the optional expanded memory, before the system will replace them with newer reports.

CMD 88 Print System Setups and Status

This Command is used during system setup, programming and troubleshooting. It enables individual sections of the system's setups to be printed, such as alarm setups or relay set-ups, Time Zone or Access Zone setups.

The following table lists all CMD 88 variables with their meaning:

88*	Use	Select this variable to:
0	Complete System Setups and Status	Print the complete list.
1	Date, Time, Version Number	Print only the current date, system time, and the CCM version number.
2	System Information	Print a short list of information about the system configuration and optional equipment installed.
3	Standard Time Zones	Print a table of any programmed Standard Time Zones.
4	Master Time Zones	Print a table of any programmed Master Time Zones.
5	Standard Access Zones	Print a table of Standard Access Zones with their active status.
6	Standard Control Zones	Print a table of any programmed Standard Control Zones.
7	Relays	Print a table of base relays, their setups and their current status.
8	Alarm / RQE Inputs	Print a table of base line module inputs and RQE setups with current status.
9	Alarm Special Setups and Status	Print a table of base alarm special setups, such as entry/exit delays.
10	Doors	Print a table of relay and alarm setups specific to a door, with door management functions, operation and status.
11	Keypads/MATCH	Print a table of Keypad/MATCH setups and on-line status.
12	MATCH	Print a table of MATCH Reader Interface Board setups and status.
13	Holidays	Print a list of any unexpired programmed Holidays by date.
14	Grand Master Time Zones	Print a table of any programmed Grand Master Time Zones.
15	Master Access Zones	Print a table of any programmed Master Access Zones.
16	Master Control Zones	Print a table of any programmed Master Control Zones.

88*	Use	Select this variable to:
17	Detailed Relay Status Only	Print an expanded table of current relay status, and is most useful for troubleshooting. See the Relay Status Guide for more information and examples.
18	Expansion Relays	Print a table of the setups and status of expansion relays.
19	Detailed Expansion Relay Status Only	Print an expanded table of current expansion relay status, and is most useful for troubleshooting.
20	Expansion Alarm / RQE Inputs	Print a table of expansion line module inputs and RQE setups with status.
21	Expansion Alarm Special Setups and Status	Print a table of expansion alarm special setups, such as entry/exit delays.
22	Expansion Line Module Input Door Setups	Print a table of expansion line module input setups specific to door monitoring, with door management functions, operation and status.
23	Reporting Setups	Print a summary of all the setups pertaining to report Commands.
24	Remote Site Management Setups	Print a summary of all the setups pertaining to Remote Site Management.
25	System Power Status	Print the power status of the primary power supply, the UPS Battery and the memory protection battery.
26	Transactions Since Midnight	List the total number of access transactions, control transactions, and alarms since last midnight. It also lists any lost reports. These are reports that the buffer could not contain because of buffer overrun, or printer off-line.
27	Occupancy Control	List the occupancy control setups including minimum, maximum settings.
28	Virtual Relays	List the 64 virtual non-physical relays that are in the system.
29	Detailed Virtual Relays	Print the detailed setups of any virtual relays used in the system.
30	HEC Factory Diagnostics	List diagnostic data for factory use only.

See the Factory Setup Guide for the complete 88 * 0 printout and all its subsections.

CMD 191 Change Page Length For Printer

This Command sets the page length for the printer from 40 to 100. This allows for 4A paper sizes and others to be used.

CMD 200 Change Printer Language

This Command changes the printer language between English, German, Dutch, French, Spanish and Italian.

Application Examples

6

This Page Intentionally Left Blank

Introduction

This chapter provides application examples which help you plan security for your own site. These examples include a large variety of devices and show you how they can fit into a Hirsch DIGI*TRAC system.

Hirsch offers a complete line of security control systems which can provide everything from simple one door access control to total facility control including:

- ❑ Access control
- ❑ Alarm monitoring
- ❑ Elevator control
- ❑ Parking control
- ❑ Energy management
- ❑ Lighting control
- ❑ Input monitoring
- ❑ Relay control
- ❑ Network control & management

In the following examples, these conventions are used for specifying cable types:

TSP	Twisted Shielded Pair (Stranded) (used for DTLMs/MELMs)
TP	Twisted Pair (Locks and Strikes)
2TSP	2-Twisted Shielded Pairs (Stranded) (for ScramblePads/MATCHs)

Note: For wire size and distance limitations, refer to Chapter 7.

Application Examples

The following examples apply to many, if not most, of the security situations encountered. In these examples, we start at the simplest examples and proceed to the more complex. No matter how sophisticated the security needs, Hirsch typically has a solution.

The examples provided are:

The preceding examples employ standard DIGI*TRAC command language for configuration.

To learn how these same configurations might function within the Velocity™ environment, refer to the Application Notes available on the Hirsch website.

Example 1:

Entry ScramblePad: Single Door – with Duress Option

Objectives:

- ❑ Limit building access to business hours for most employees.
- ❑ Allow 24 hour building access for management
- ❑ Require all users to enter a code when entering the building.
- ❑ Log all after-hours access transactions.
- ❑ Initiate an alarm signal when the door is forced open or propped open.
- ❑ Give to all users the capability to send silent duress alarms to the security center by entering an additional duress digit.

Solution:

This example is one of the most basic configurations supported by Hirsch. A DIGI*TRAC Controller is used to control the door. (The programming can be performed from the ScramblePad.) The ScramblePad enables exit and entry to the building. A printer connected to the Controller records events as they take place. A power supply is required for the electric door lock. This example also includes a panic touch bar. This Request-to-Exit (RQE) device is connected to the controller (DIGI*TRAC M2) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

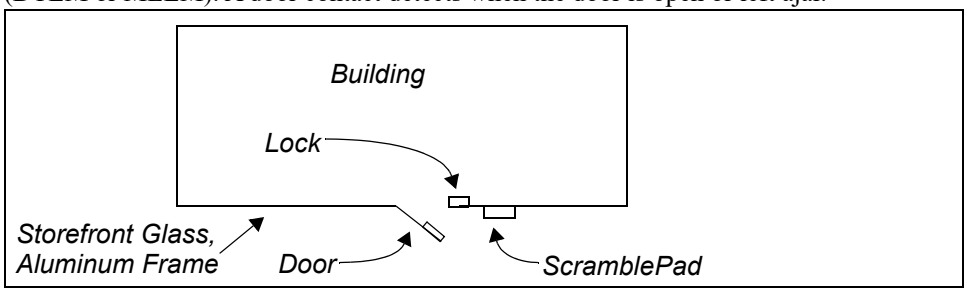


Figure 6-1: Single Door Building Access (Top View)

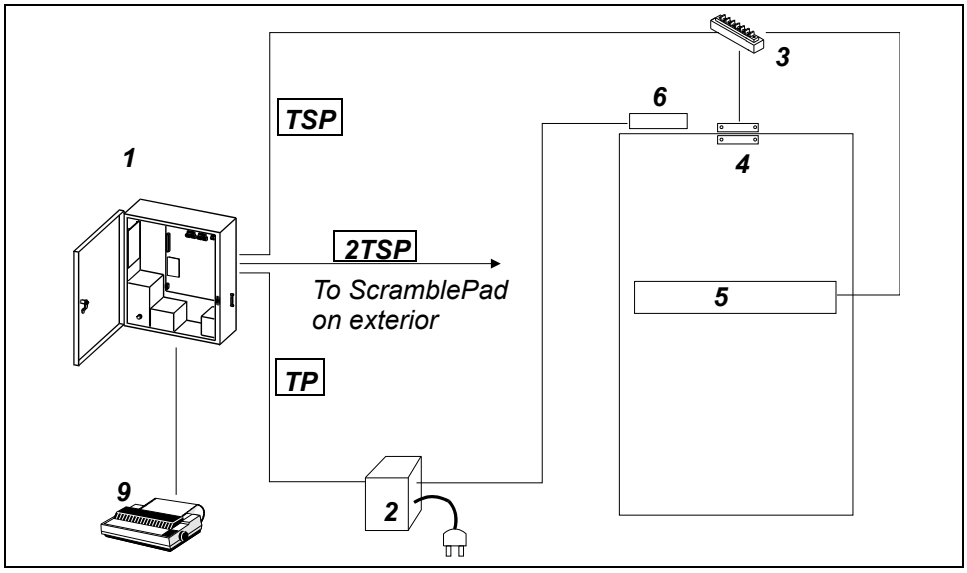


Figure 6-2: Single Door Building Access (Interior View)

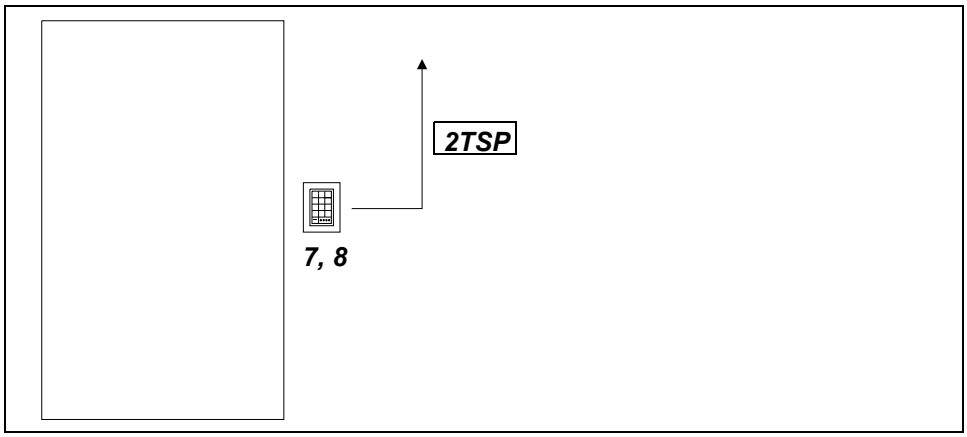


Figure 6-3: Single Door Building Access (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	MB5
8	Identification Device	DS37L-HI ScramblePad
9	Printer	PR1 Parallel printer

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
09	Generate codes with duress digit
08	Enable duress alarm mode
10	Add access user – code only

Example 2:

Entry & Exit ScramblePads: Single Door – with Anti-Passback, Who's Inside

Objectives:

- ❑ Limit building access to secured area during business hours for most employees.
- ❑ Allow 24 hour access for management.
- ❑ Require all users to enter a code when entering or exiting.
- ❑ Log all entry and exit transactions.
- ❑ Deny access to any user who did not use the card during their last entry or exit.
- ❑ Initiate an alarm signal when the door is forced open or propped open.
- ❑ Generate a list of all users currently inside.

Solution:

This example shows requirements for a secure area. This area can be either a building or a room. A DIGI*TRAC Controller is used to control the door. (The programming can be performed from one of the ScramblePads.) One ScramblePad enables entry to and a second ScramblePad enables exit from the secured area. A printer connected to the Controller records events as they take place. A power supply is required for the electric door lock. This example also includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (a DIGI*TRAC M1N, M2, or M8) by a line module (DTLM or MELM). Using the RQE instead of a code will cause an alarm when the door is opened. A door contact detects when the door is open or left ajar.

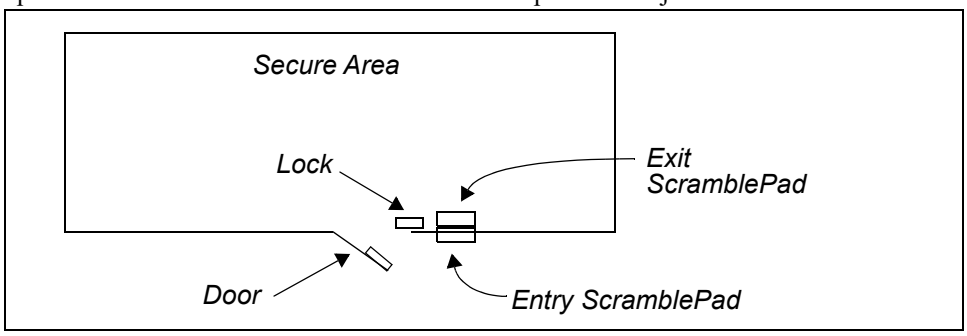


Figure 6-4: Single Door Secured Access (Top View)

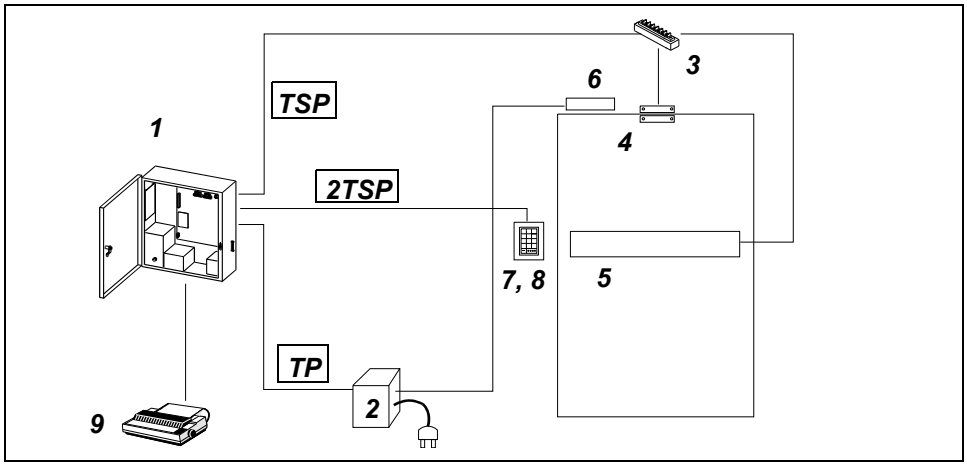


Figure 6-5: Single Door Secured Access (Interior View)

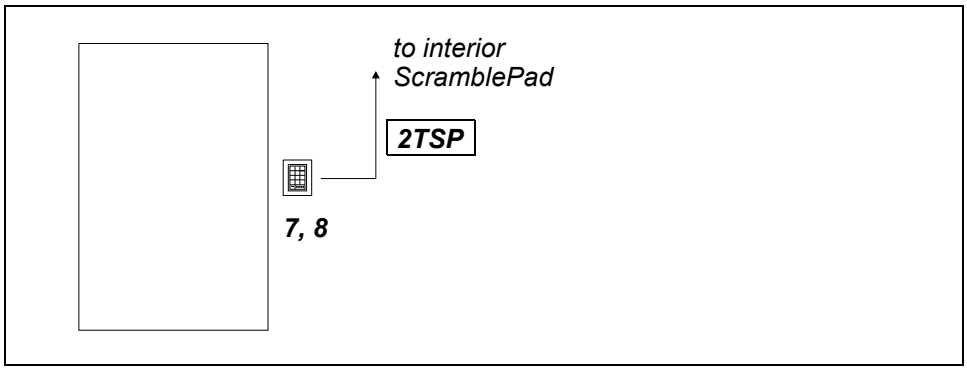


Figure 6-6: Single Door Secured Control (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	MB5 exterior, UMK (w/MB2) interior
8	Identification Device	DS37L-HI ScramblePad, exterior side of door DS37L ScramblePad, interior side of door
9	Printer	PR1 Parallel printer

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry/exit ScramblePad
46	Change Passback Mode
10	Add access user – code only
34	List all users inside

Example 3:

Entry Card Reader: Single Door – with 1st Person In Unlock, Timed Relock

Objectives:

- ❑ Limit building access to business hours for most employees.
- ❑ Allow 24 hour access for management.
- ❑ Cards used between 08:00 – 16:59, Monday – Friday will unlock the door until 17:00 the same day. At 17:00, the system will automatically relock the door.
- ❑ Require all users to use card when entering.
- ❑ First cards used after hours will momentarily unlock door
- ❑ Log all after-hours access transactions.
- ❑ Initiate an alarm signal when the door is forced open or propped open.

Solution:

This example uses a card reader as the access device rather than the ScramblePad. A DIGI*TRAC Controller is used to control the door. A Card Enrollment Station is also situated at this same location. A Card Reader is located at the entrance. A MATCH Reader Interface Board (MRIB) is mounted above the ceiling near the door and connects the Card Reader to the Controller. A printer connected to the Controller records events as they take place. A power supply is required for the magnetic door lock. This example also includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (an M1N, M2, or M8) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

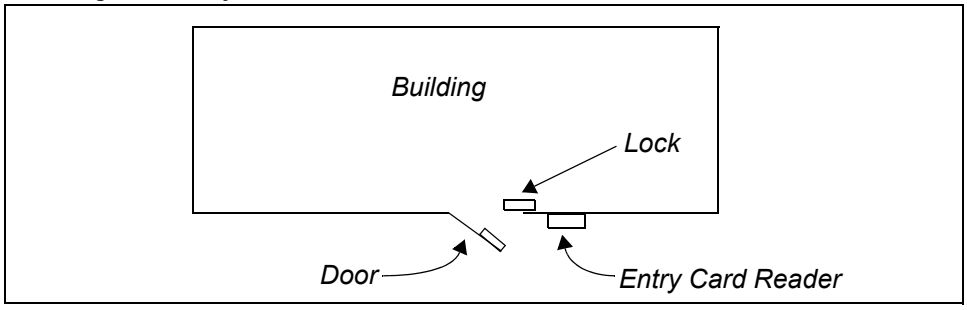


Figure 6-7: Single Door Card Reader (Top View)

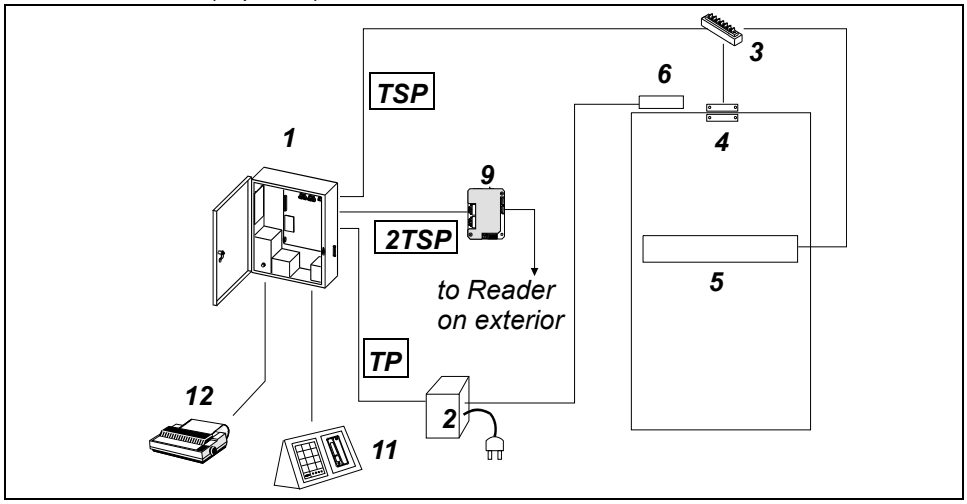


Figure 6-8: Single Door Card Reader (Interior View)

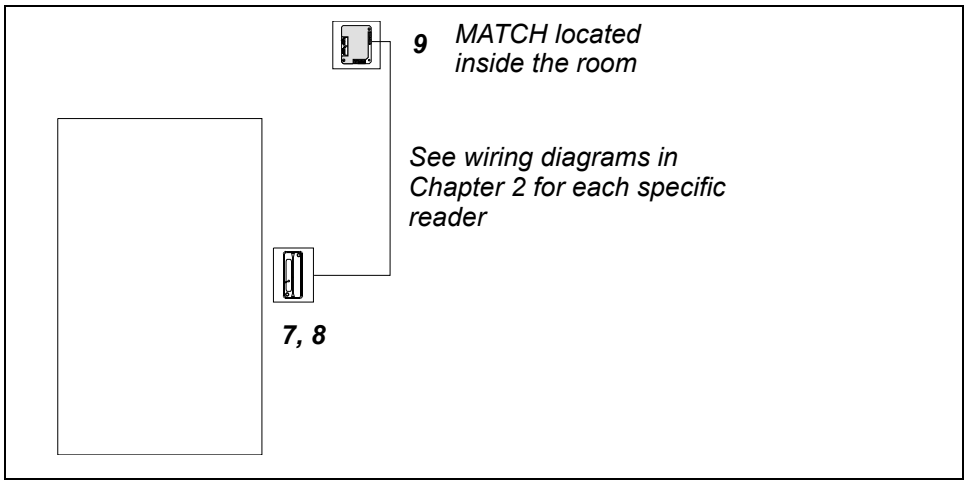


Figure 6-9: Single Door Card Reader (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	As required
8	Identification Device	CR12L mag stripe reader, weather resistant
9	Card Reader Interface	MRIB (secure side)
10	Cards	IDC 10 Magnetic Stripe Cards
11	Card Enrollment Station	DMES-M
12	Printer	PR1 Parallel Printer

Software Programming Commands

Command	Meaning
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
73	Define exit device function
45	Define control zone
304	Define master control zone
305	Select time zone for master control zone
82	Relay clear after end of time zone

Command	Meaning
87	Relay trigger control zone
310	Add access card user

Example 4:

Entry & Exit Card Readers: Single Door – Who's Inside

Objectives:

- ❑ Limit access to secured area during business hours for most employees.
- ❑ Allow 24 hour access for management
- ❑ Log all entry and exit transactions.
- ❑ Require all users to use card when entering and exiting.
- ❑ Initiate an alarm signal when the door is forced open or propped open.
- ❑ Generate a list of all users currently inside.

Solution:

This example uses card readers as the access devices to and from a secure area. A DIGI*TRAC Controller is used to control the door. A Card Enrollment Station is also situated at this same location. Card Readers are located on both sides of the door. The MRIB assembly is mounted on the back of this entry card reader (MR11LA), connecting both Card Readers to the Controller. A printer connected to the Controller records events as they take place. A power supply is required for the magnetic door lock. This example also includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (an M1N, M2, or M8) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

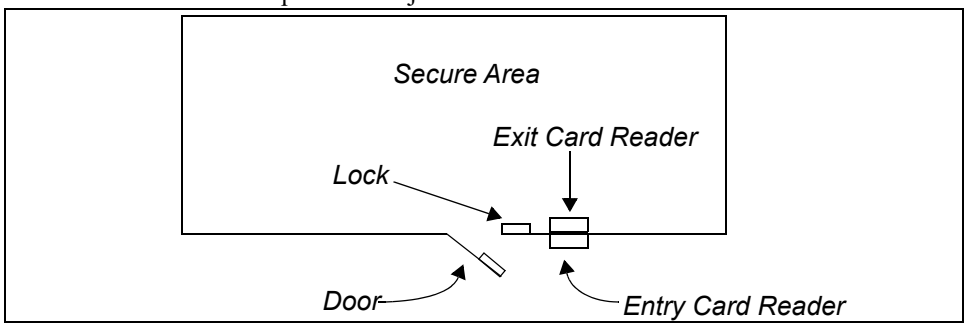


Figure 6-10: Single Door Card Readers Secured Access (Top View)

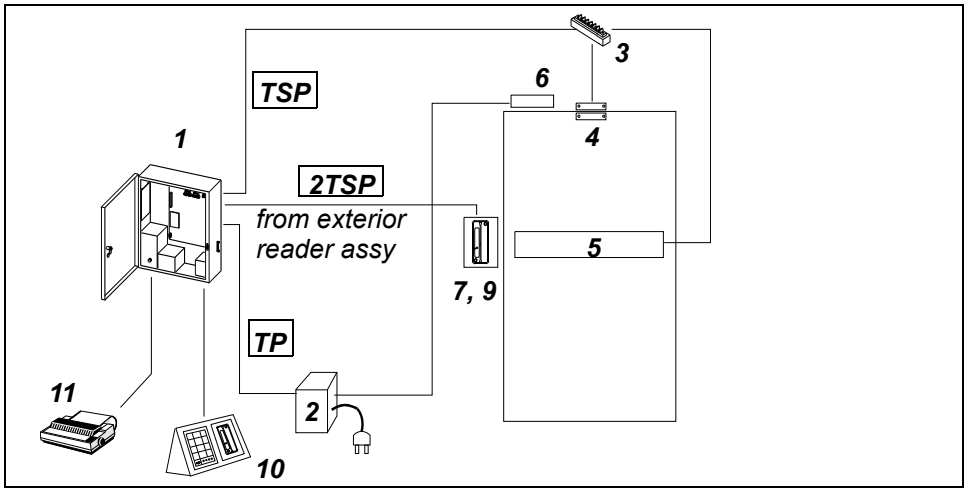


Figure 6-11: Single Door Card Readers Secured Access (Interior View)

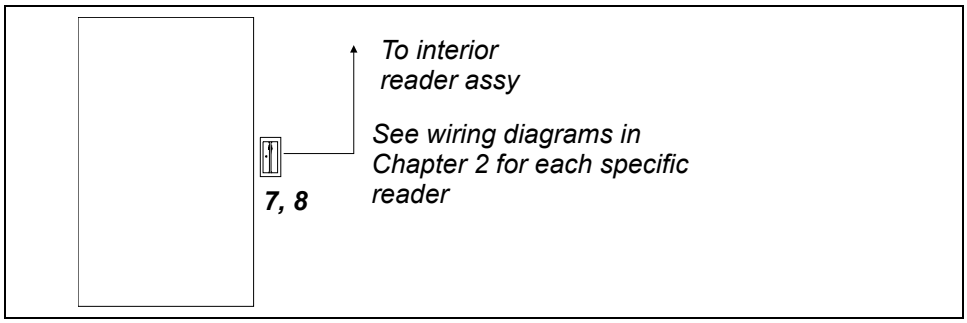


Figure 6-12: Single Door Card Readers Secured Access (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	MB1 or MB2, each side of door
8	Identification Device	MR11LA magnetic stripe reader, entry side
9	Identification Device	CR11LA magnetic stripe reader, exit side
10	Card Enrollment Station	DMES-M
11	Printer	PR1 Parallel Printer
	Cards	IDC 10 Magnetic Stripe Cards

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry-exit reader
310	Add access user – Card only
34	List all users inside
46	Set passback mode to report, forgive

Example 5:

Dual Technology Entry: Single Door

Objectives:

- ❑ Limit access to secured area during business hours for most employees.
- ❑ Require dual (card + code) to gain access and card only to exit.
- ❑ Allow 24 hour access for management
- ❑ Log all entry transactions.
- ❑ Initiate an alarm signal when the door is forced open or propped open.

Solution:

This example uses a combination of card readers and ScramblePads to access a secured area. In this example, a ScramblePad and card reader are mounted on the entry side of the door. A DIGI*TRAC Controller is used to control the door. A Card Enrollment Station is also situated at this same location. The MR11LA Card Reader includes an MRIB assembly to which both the CR11LA Card Reader and the ScramblePad are connected. This unit is wired to the controller. A printer connected to the Controller records events as they take place. A power supply is required for the magnetic door lock. This example also includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (an M1N, M2, or M8) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

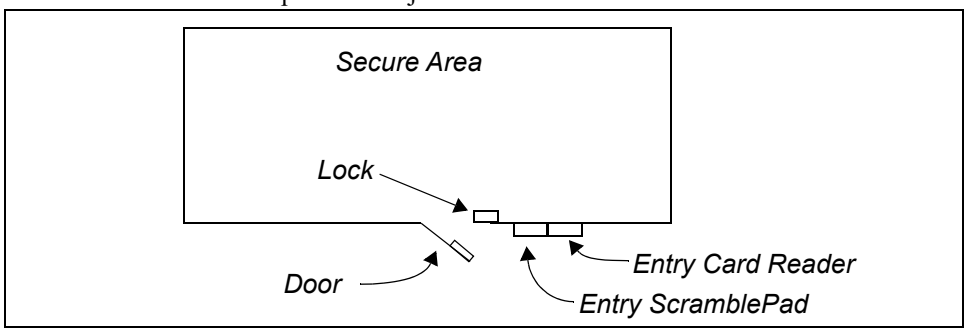


Figure 6-13: Single Door ScramblePad/Card Readers Secured Access (Top View)

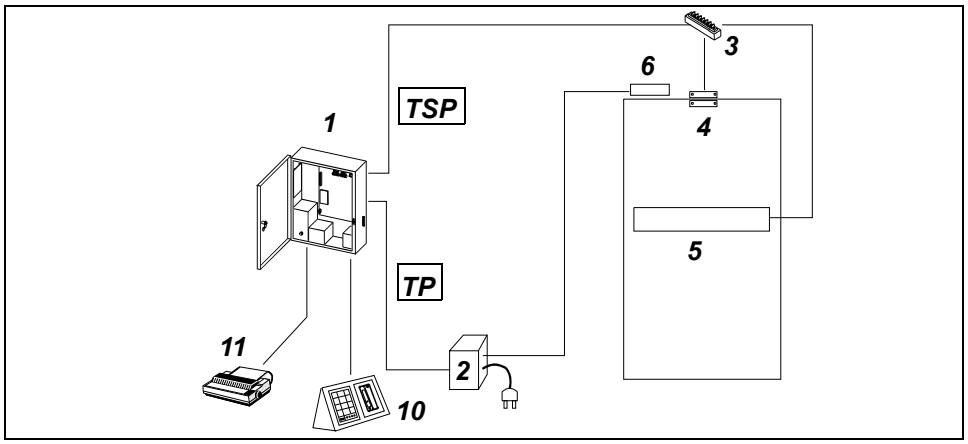


Figure 6-14: Single Door ScramblePad/Card Reader Secured Access (Interior View)

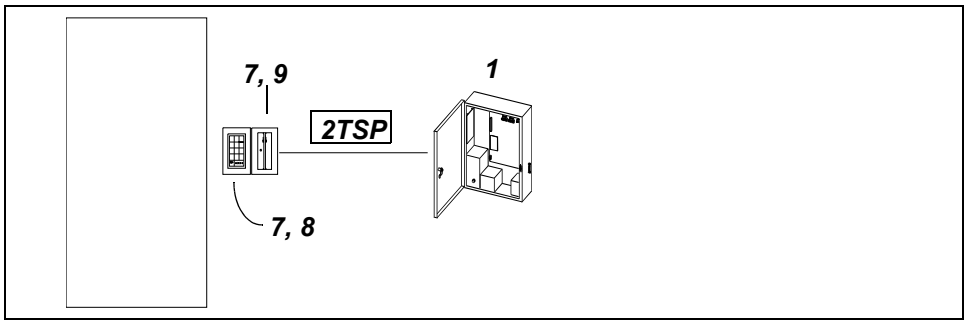


Figure 6-15: Single Door ScramblePad/Card Reader Secured Access (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	MB1 or MB2
8	Identification Device, Keypad	DS37L ScramblePad, entry side
9	Identification Device, Reader	MR11LA magnetic stripe reader, entry side
10	Card Enrollment Station	DMES-M
11	Printer	PR1 Parallel Printer
	Cards	IDC 10 Magnetic Stripe Cards

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry-exit reader
311	Add access user – card + code

Example 6:

Dual Technology Entry, Dual Technology Exit: Single Door

Objectives:

- ❑ Limit access to secured area during business hours for most employees.
- ❑ Require dual (card + code) to gain access or to exit.
- ❑ Allow 24 hour access for management
- ❑ Log all entry and exit transactions.
- ❑ Initiate an alarm signal when the door is forced open or propped open.
- ❑ Generate a list of all users currently inside.

Solution:

This example uses dual card readers and ScramblePads on both sides of a door into a secured area. A DIGI*TRAC Controller is used to control the door. A Card Enrollment Station is also situated at this same location. Card Readers are located on both sides of the door. The MRIB assembly is mounted in a J-Box above the ceiling, connecting both Card Readers and ScramblePads to the Controller. A printer connected to the Controller records events as they take place. A power supply is required for the magnetic door lock. This example also includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (a DIGI*TRAC M1, M2, or M8) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

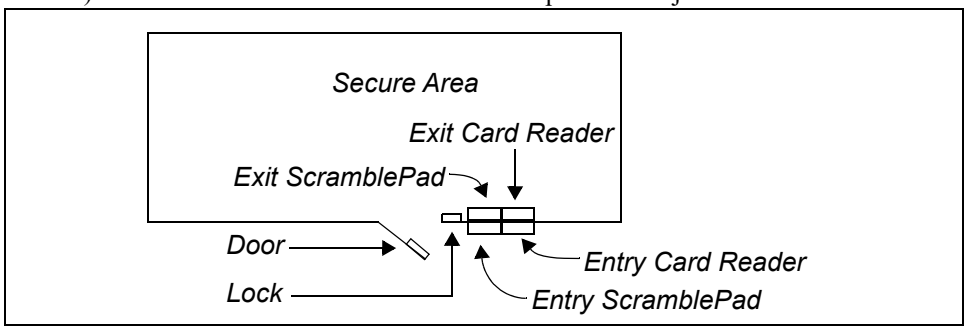


Figure 6-16: Single Door Dual ScramblePads/Readers Secured Access (Top View)

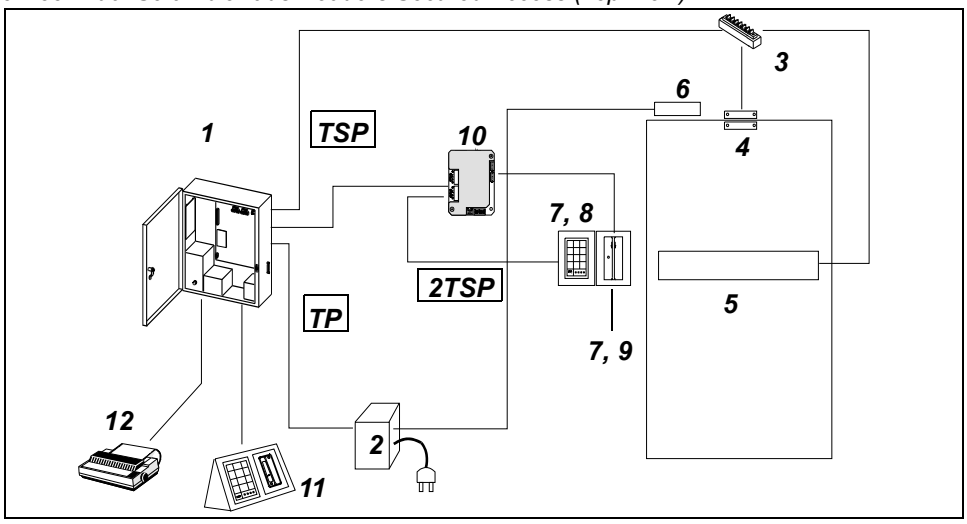


Figure 6-17: Single Door Dual ScramblePads/Readers Secured Access (Interior View)

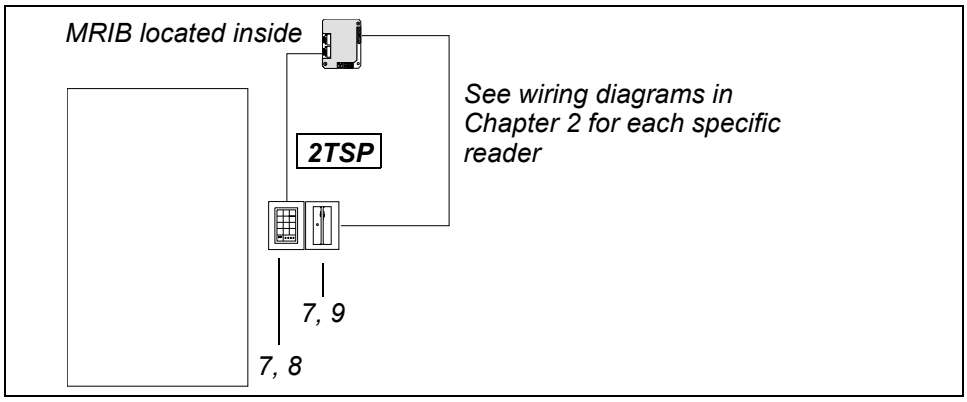


Figure 6-18: Single Door Dual ScramblePads/Readers Secured Access (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	MB1 or MB2, each side of door
8	Identification Device, Keypad	DS37L ScramblePad, each side of door
9	Identification Device, Reader	CR11LA magnetic stripe reader, exit side
10	Identification Device, Reader	MR11LA, secure side
11	Card Enrollment Station	DMES-M
12	Printer	PR1 Parallel Printer
	Magnetic Stripe Cards	IDC 10

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry-exit reader
311	Add access user – card + code
34	List all users inside

Example 7:

Dual Technology Entry, Card Reader Exit: Single Door – 2-Person Rule

Objectives:

- ❑ Limit access to secured area during business hours for most employees.
- ❑ Require two person identification before door releases.
- ❑ Require dual (card & code) to gain access and card only to exit.
- ❑ Allow 24 hour access for management
- ❑ Log all entry and exit transactions.
- ❑ Initiate an alarm signal when the door is forced open or propped open.
- ❑ Generate a list of all users currently inside.

Solution:

This example uses the two-person rule: two people have to enter their cards/codes before the door releases. With the hardware in place, the two-person rule is activated through programming. The entry side has both a card reader and ScramblePad. The exit side has a card reader. A Card Enrollment Station is also situated at this same location. The MRIB assembly is mounted in a J-Box above the ceiling, connecting both Card Readers and the ScramblePad to the Controller. A printer connected to the Controller records events as they take place. A power supply is required for the magnetic door lock. For emergency exit, this example includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (a DIGI*TRAC M1N, M2, or M8) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

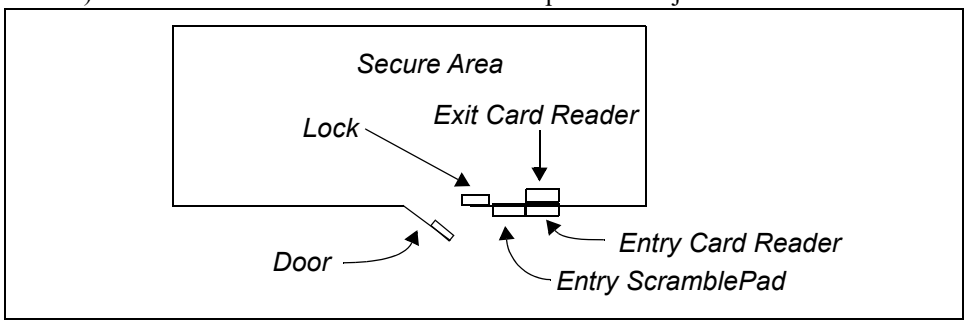


Figure 6-19: Readers/ScramblePad Two-Person Rule (Top View)

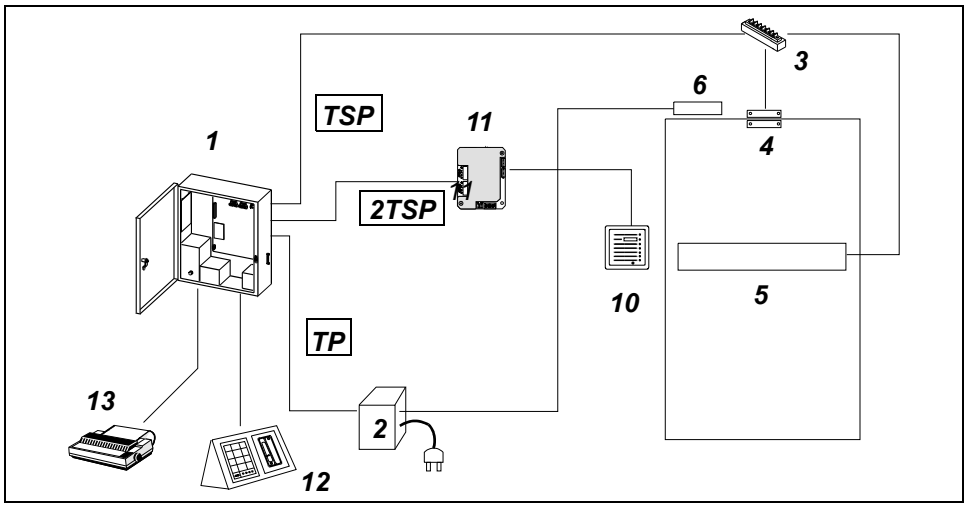


Figure 6-20: Readers/ScramblePad Two-Person Rule (Interior View)

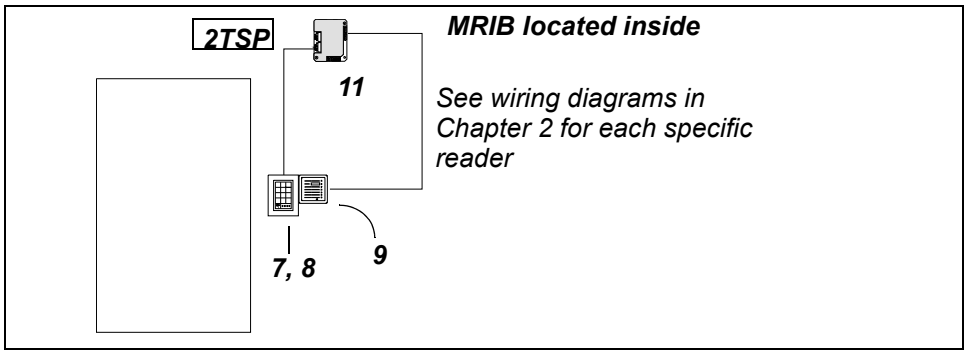


Figure 6-21: Readers/ScramblePad Two-Person Rule (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device	Panic Touch bar
6	Electric Door Lock	Magnetic lock
7	Mounting Hardware	MB1 or MB2, entry side
8	Identification Device, Keypad	DS37L ScramblePad, entry side
9	Identification Device, Reader	CR21L HID Proximity reader, entry side
10	Identification Device, Reader	CR21L HID Proximity reader, exit side
11	Card Reader Interface	MRIB, secure side
12	Printer	PR1 Parallel Printer
13	Card Enrollment Station	DMES-M
	Cards	IDC 20-125 Proximity card

Software Programming Commands

CMD	Meaning	CMD	Meaning
73	Define exit device function	03	Define entry-exit reader
80	Define door unlock time (1 - 8100 sec.)	256	Enable two-person rule at selected door
74	Define door-open-too-long interval (1 - 8100 sec)	255	Define time allowed between first and second user identification
85	Define relock function	312	Add access user - card + code
52	Define time zone	34	List all users inside
17	Define access zone	46	Set passback mode to report, forgive

Example 8:

Dual Technology Entry, Card Reader Exit: Single Door – 2-Person Rule with Alarm Control, PIR Masking, Who's Inside

Objectives:

- ❑ Limit access to secured area during business hours for most employees.
- ❑ Require two person identification before door releases.
- ❑ Require dual (card + code) to gain access and card only to exit.
- ❑ Allow 24 hour access for management
- ❑ Log all entry and exit transactions.
- ❑ Inside alarm points (PIR) automatically disarm when entry door is unlocked.
- ❑ Inside alarm points rearm by using arming code on entry ScramblePad
- ❑ Initiate an alarm signal when the door is forced open or propped open.
- ❑ Generate a list of all users currently inside.

Solution:

This example uses the two-person rule with alarm point control: deactivation of the alarm on valid entry; activation of alarm with valid code. With the hardware in place, the two-person rule and alarm control are both implemented through programming. The entry side has both a card reader and ScramblePad. The exit side has a reader. A DIGI*TRAC Controller is used to program and control the door. A Card Enrollment Station is also situated at this same location.

The MRIB assembly is mounted in a J-Box above the ceiling, connecting both Card Readers and the ScramblePad to the Controller. A printer connected to the Controller records events as they take place. A power supply is required for the magnetic door lock. This example also includes an exit panic touch bar as a Request-to-Exit (RQE) device connected to the controller (an M1N, M2, or M8) by a line module (DTLM or MELM). A door contact detects when the door is open or left ajar.

Motion detectors on the secure side are unmasked when the area is unoccupied and are automatically masked when the correct code and card are entered at the entry. The detectors are manually unmasked again when all occupants have exited.

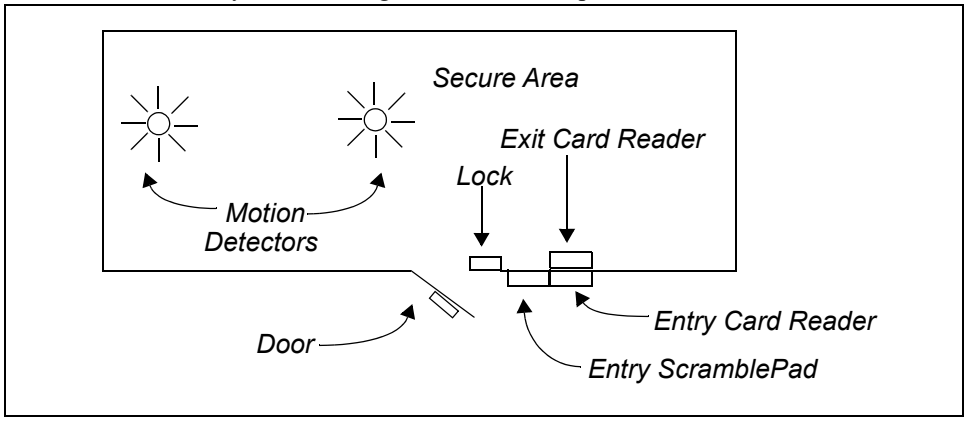


Figure 6-22: Readers/ScramblePad Two-Person Rule (Top View)

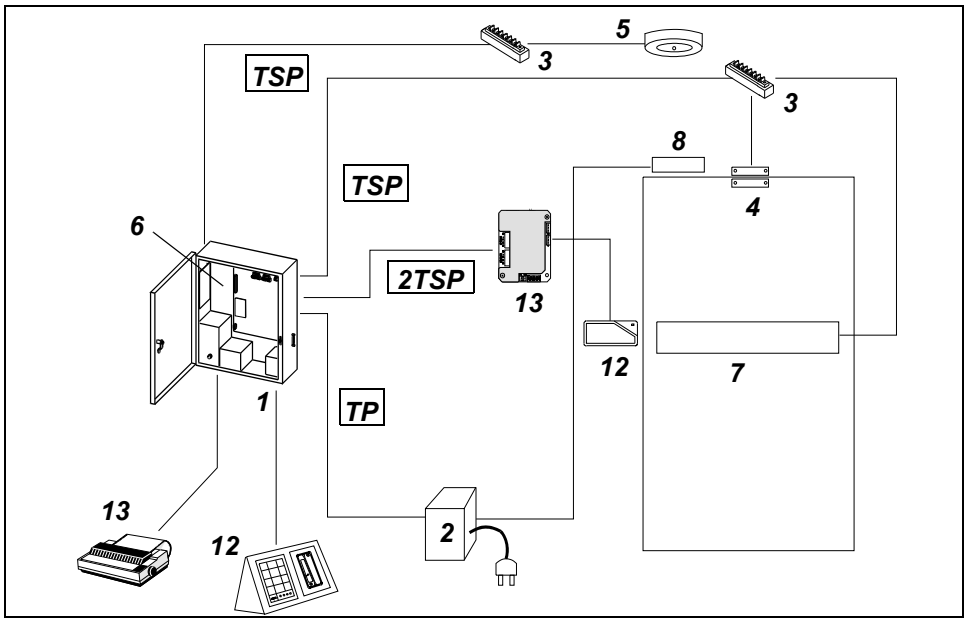


Figure 6-23: Readers/ScramblePad Two-Person Rule (Interior View)

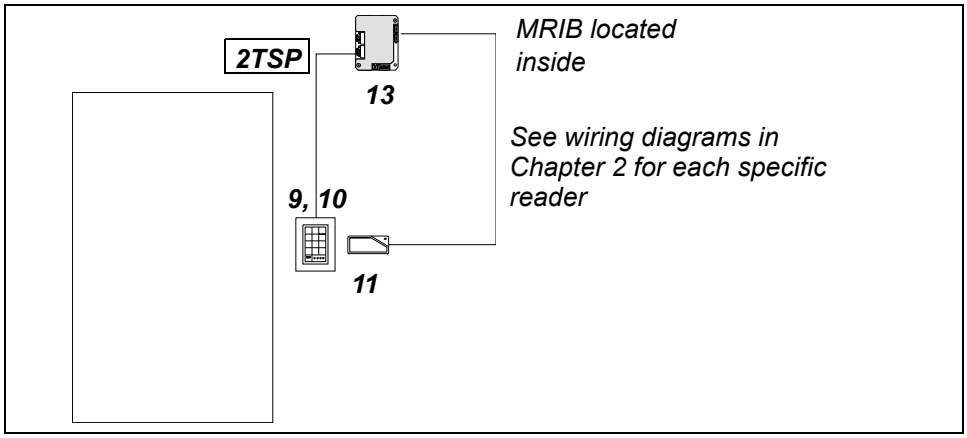


Figure 6-24: Readers/ScramblePad Two-Person Rule (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8, M2, or M1N
2	Door Lock Power Supply	PS2
3	Line Module	DTLM3/MELM3
4	Door Contact	Magnetic Switch
5	Interior Alarm Device	PIR motion detector
6	Alarm Expansion Board	AEB8
7	RQE Device	Panic Touch bar
8	Electric Door Lock	Magnetic lock

No.	Device Type	Hirsch Product
9	Mounting Hardware	MB1 or MB2, entry side
10	Identification Device, Key-pad	DS37L ScramblePad, entry side
11	Identification Device, Reader	CR31L Wiegand swipe reader, entry side
12	Identification Device, Reader	CR31L Wiegand swipe reader, exit side
13	Card Reader Interface	MRIB
14	Card Enrollment Station	DMES-U with CR31L
15	Printer	PR1 Parallel Printer
	Cards	IDC 30 Wiegand cards

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry-exit reader
256	Enable two-person rule at selected door
255	Define time allowed between first and second user identification
45	Define control zone
301	Add expansion alarm point to control zone
304	Define master control zone
305	Select time zone for master control zone
87	Select door relay to trigger master control zone
42	Add alarm unmask code
312	Add access user - card + code
34	List all users inside
46	Set passback mode to report, forgive

Example 9:

Card Reader Entry: Turnstile & Handicap Side Door – Unlock During Business Hours

Objectives:

- ❑ Free building access during business hours, no credentials required.
- ❑ Allow 24 hour access to management
- ❑ After hours entry requires credential.
- ❑ Restrict side door entry to handicapped users.
- ❑ Log all after hours access transactions.
- ❑ Initiate an alarm signal when the side door is forced open or propped open.
- ❑ Limit after hours entry to one person per credential at turnstile.
- ❑ Free exit through either door.

Solution:

As shown in Chapter 2, there are several types of turnstiles: half-height, full-height, and optical. Access control can be handled in any one of the ways shown in Examples 1-8. Turnstiles are frequently used for common area access, such as airports or lobbies. For handicapped users, a side door is available. In the event of an emergency, the side door opens automatically. A card reader entry is provided. The MRIBs are mounted in a J-Box above the ceiling, connecting each Card Readers to the Controller.

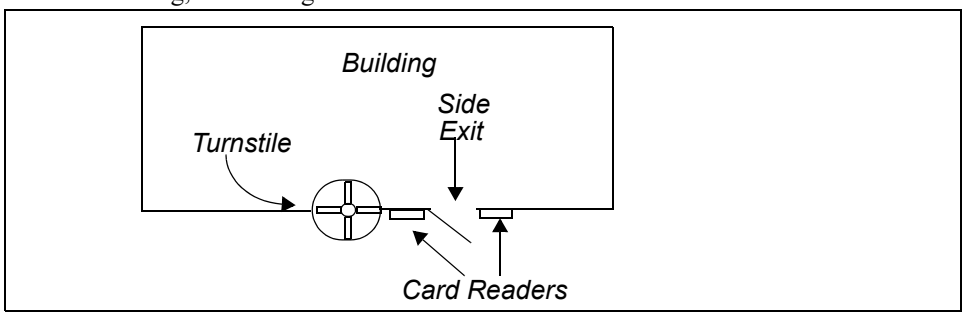


Figure 6-25: Turnstile (Top View)

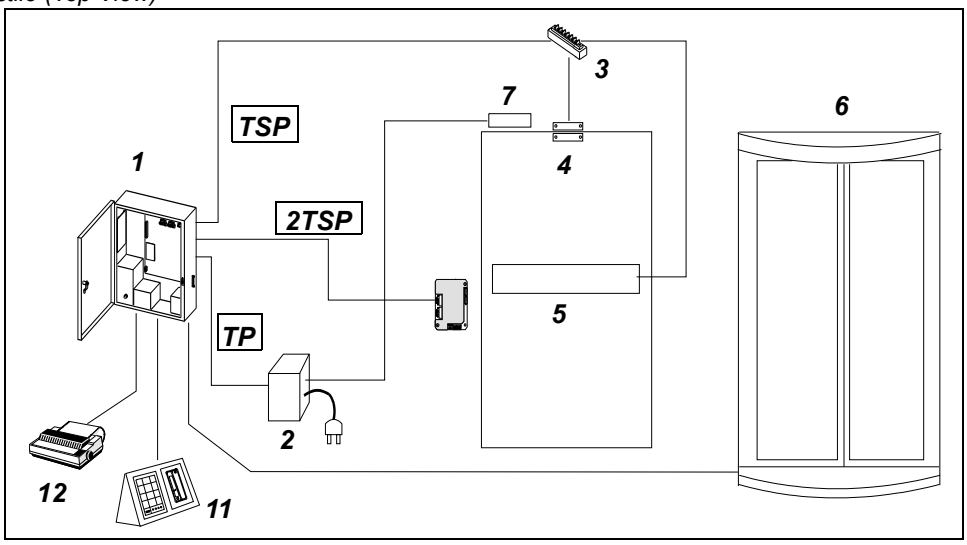


Figure 6-26: Turnstile (Interior View)

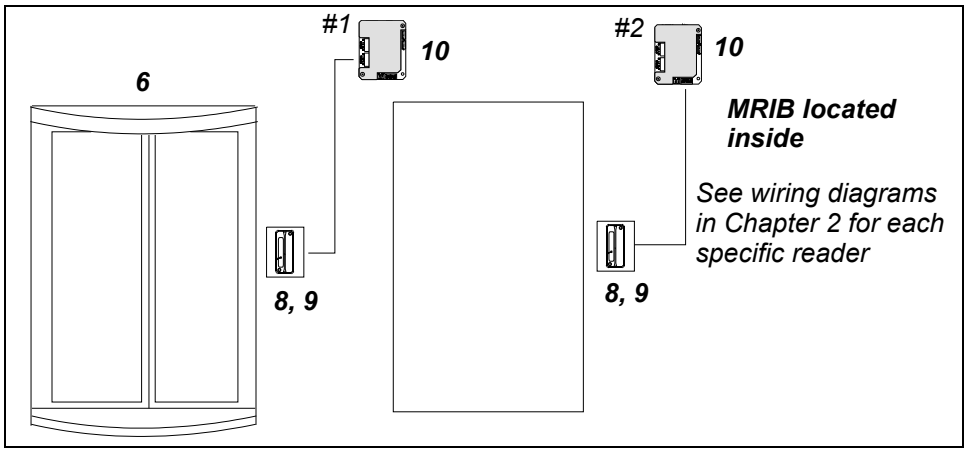


Figure 6-27: Turnstile (Exterior View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8 or M2
2	Door Lock Power Supply	PS2
3	Line module	DTLM2/MELM2
4	Door Contact	Magnetic Switch
5	RQE Device, Side Door	Panic Touch Bar
6	Exit Device, Rotating Door	N.O. contact
7	Electric Door Lock	Magnetic lock
8	Mounting Hardware	As required
9	Identification Device	CR12L magnetic stripe reader, weather resistant
10	Card Reader Interface	MRIB
11	Card Enrollment Station	DMES-M
12	Printer	PR1, parallel printer
	Magnetic Stripe Cards	IDC 10

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
82	Time Zone control of relays
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
310	Add access users - card only

Example 10:

ScramblePad Entry: Parking Gate - Logging, Lot Full Control

Objectives:

- ❑ Restrict parking lot access to authorized vehicles.
- ❑ Limit number of vehicles in parking lot.
- ❑ Automatically register all vehicles entering and exiting parking area.
- ❑ Automatically actuate “Lot Full” sign when the lot is full.
- ❑ Automatically disable vehicle entry when the lot is full.
- ❑ Automatically deactivate “Lot Full” sign when exiting vehicles make space available.
- ❑ Automatically allow vehicles to enter until the lot is full again.
- ❑ Report number of parked vehicles.

Solution:

This example demonstrates the parking gate. This serves to monitor the entry/exit of traffic to a parking lot or structure. It resembles a simple door configuration.

Entry is accomplished using a ScramblePad. If this is a DS37L ScramblePad, an MRIB is located in the reader housing. If this is a DS47L, the ScramblePad includes the MRIB circuitry.

Once an authorized code is entered, the gate rises and the vehicle drives over the safety and close loops. The safety and close loops keep the gate open until the car is safely past the arm.

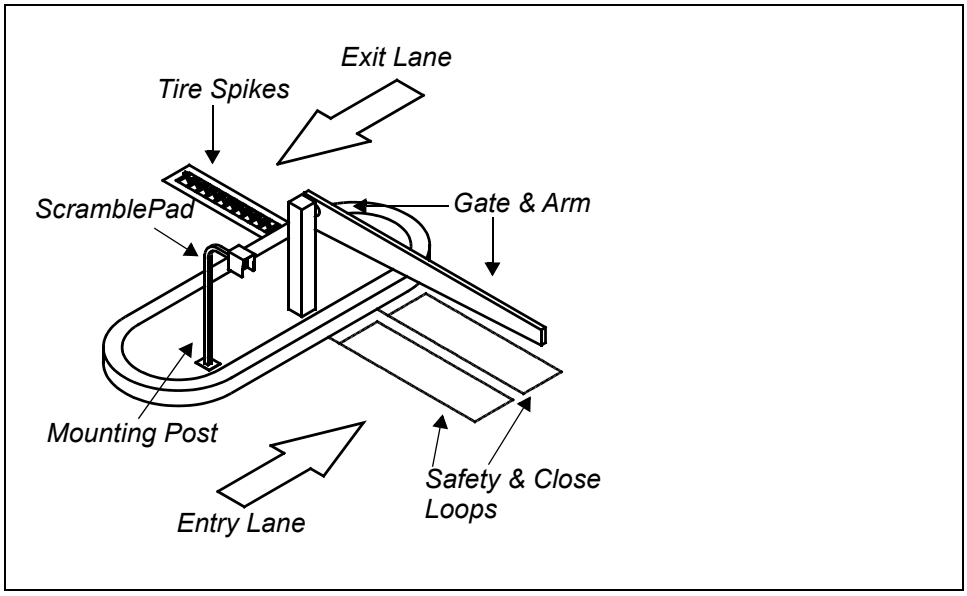


Figure 6-28: Parking Gate (Top View)

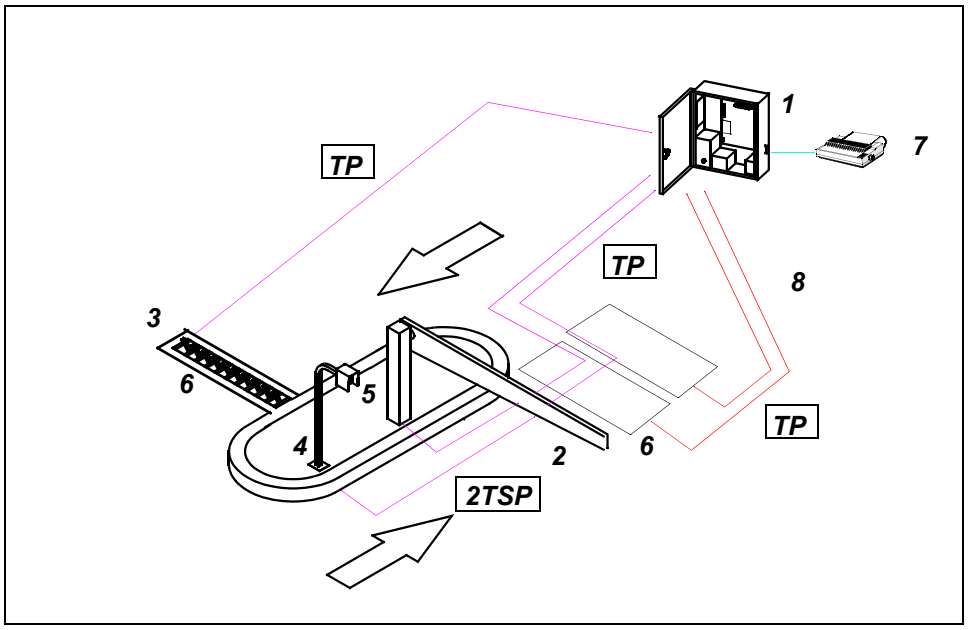


Figure 6-29: Parking Gate (Controller View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M2 or M8
2	Entry Device	Parking Gate Operator
3	Exit Device	Parking Gate Operator
4	Mounting Hardware	MB5 and MP41
5	Identification Device, Keypad	DS37L-HI ScramblePad. DS47L-HI includes MRIB circuitry
6	Vehicle Present sensor (loops & tire spike trough)	Parking Gate Operator
7	Printer	PR1 Parallel printer

Software Programming Commands

Command	Meaning
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
45	Define control zone
03	Define Entry-Exit reader
46	Select passback mode
304	Define master control zone
305	Select time zone for master control zone
235	Define occupancy limit
236	Occupancy count trigger control zone
310	Add access card user
34	List users inside

Example 11:

Card Reader Entry, Dual Technology Exit: Man Trap - Interlocking, Who's Inside

Objectives:

- ❑ Limit access to secured area to authorized personnel only.
- ❑ Require presentation of valid card to enter portal.
- ❑ Require presentation of valid card and code to exit portal.
- ❑ Unauthorized individuals are detained in portal until removed by guard.
- ❑ Prevent simultaneous opening of both doors. (Doors to be interlocked.)
- ❑ Log all entry and exit transactions.
- ❑ Initiate an alarm signal when door is either forced open or is held open.
- ❑ Generate a list of all users currently inside the secured space.

Solution:

This example demonstrates the use of an interlocking portal, otherwise called a man trap. This serves as a very secure entrance and exit control, requiring use of a card to enter the portal and a card and code to exit. There is also an enrollment station located on the secure side of Door 2 which enables programming of the man trap. In addition, the controller is programmed so that only one door can be opened at a time. The mantrap is used for many high-security operations including prisons and drug dispensaries.

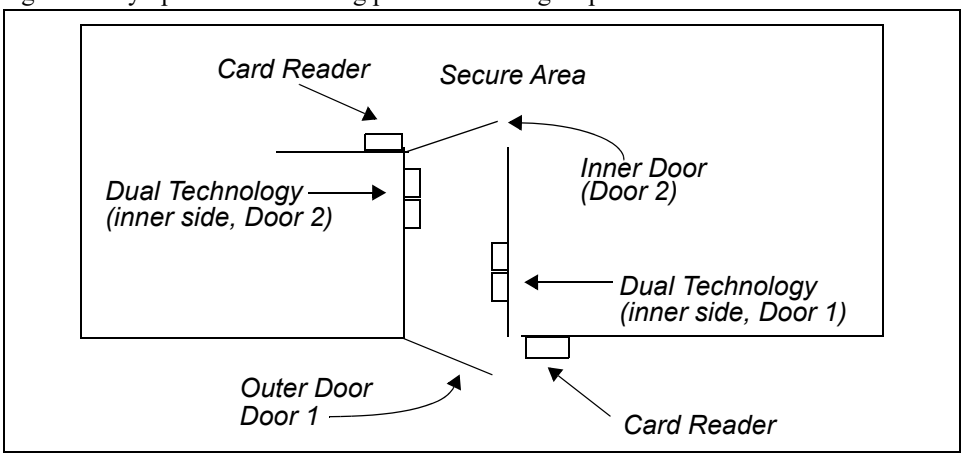


Figure 6-30: Interlocking Access Portal (Top View)

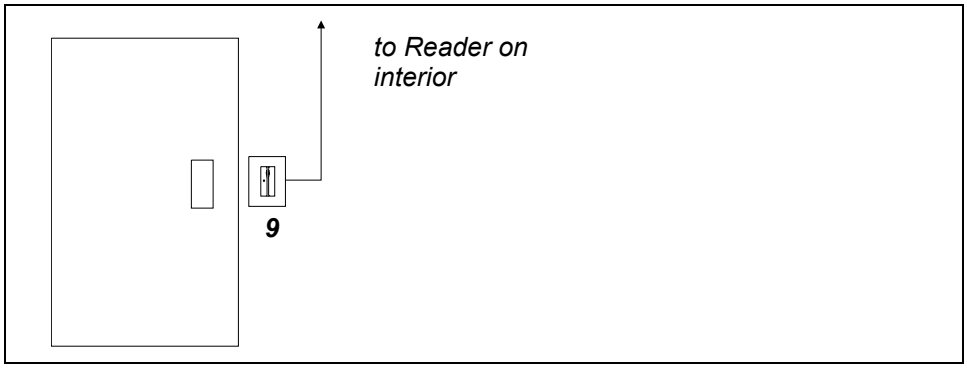


Figure 6-31: Mantrap (Inner Door 2 View)

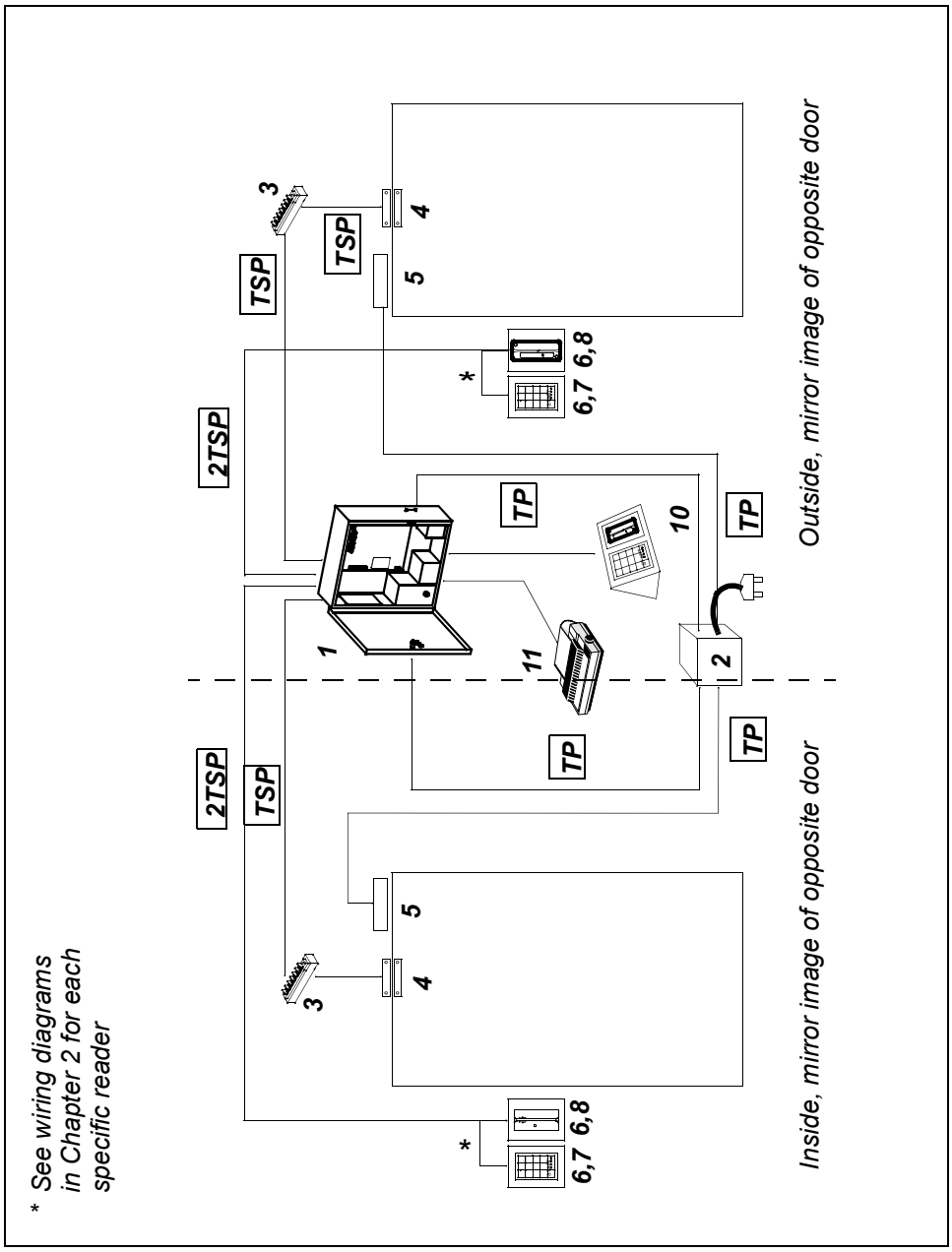


Figure 6-32: Mantrap (Interior Portal View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M8 or M2
2	Door Lock Power Supply	PS2
3	Line Module	DTLM3
4	Door Contact	Magnetic Switch
5	Electric Door Lock	Magnetic lock
6	Mounting Hardware	MB1 or MB2, each side of each door
7	Identification Device, Key-pad	DS37L ScramblePad, inside portal, each door
8	Identification Device, Reader	MR11LA mag stripe card reader, inside portal, each door
9	Identification Device, Reader	CR11LA mag stripe card reader, exterior side, each door
10	Enrollment Station	DMES-M (DS37L + MR11L in ES2)
11	Printer	PR1 parallel printer
	Identification Cards	IDC10 Magnetic stripe cards

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry/exit ScramblePad, inner door
45	Define control zone
84	Line module input triggers control zone
87	Relay trigger control zone
84	Line module input retrigger control zone
304	Define master control zones
305	Define time zone for master control zone
381	Set control delay for expansion relay
312	Add access user - card and card + code
41	Add top priority reset user
34	List all users inside
46	Set passback mode for report, forgive

Example 12:

ScramblePad Entry and Exit: Sally Port - Interlocking, Who's Inside

Objective:

- ❑ Limit pedestrian and vehicular access to secured area at all times for all employees.
- ❑ Allow 24 hour access to management.
- ❑ Log all entry and exit transactions.
- ❑ Lock one gate while the other gate is open.
- ❑ Prohibit both gates from being open at the same time.
- ❑ Initiate an alarm signal when gate is open too long or is propped open.
- ❑ Generate a list of all users currently inside the secured space.

Solutions:

The sally port is a variation of the man trap. While a mantrap uses doors to control entry and exit, sally ports use gates. For this reason, many variations of sally ports are used in high-security operations, including prisons and high-security military installations.

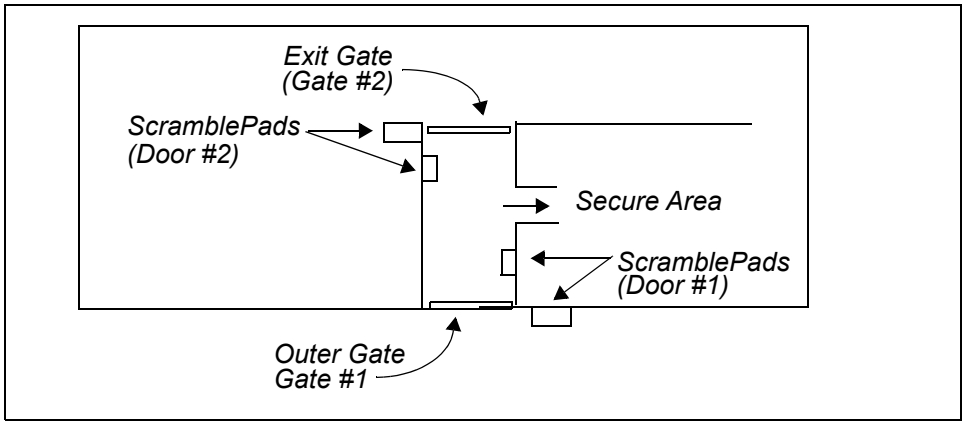


Figure 6-33: Sally Port (Top View)

The example shown here is for a ScramblePad for both entry and exit gates on both inner and outer sides.

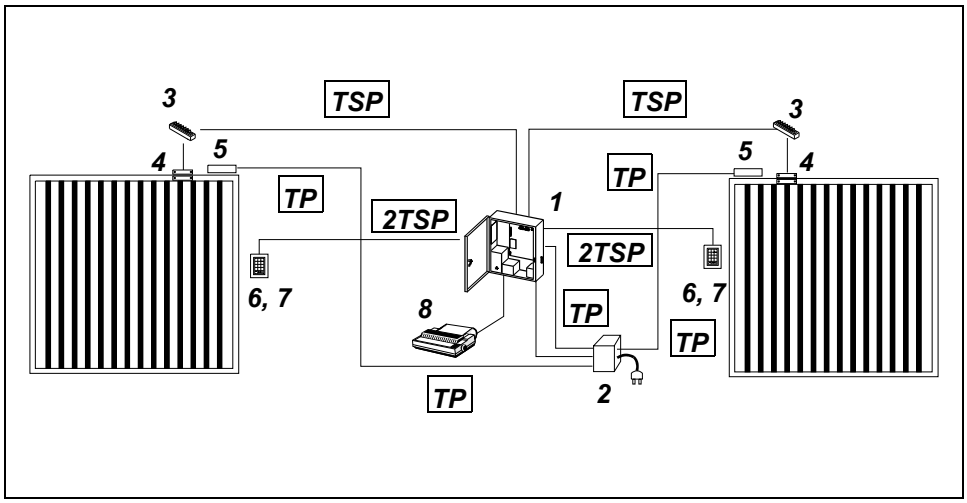


Figure 6-34: Sally Port Entry (Inner and Outer Gates)

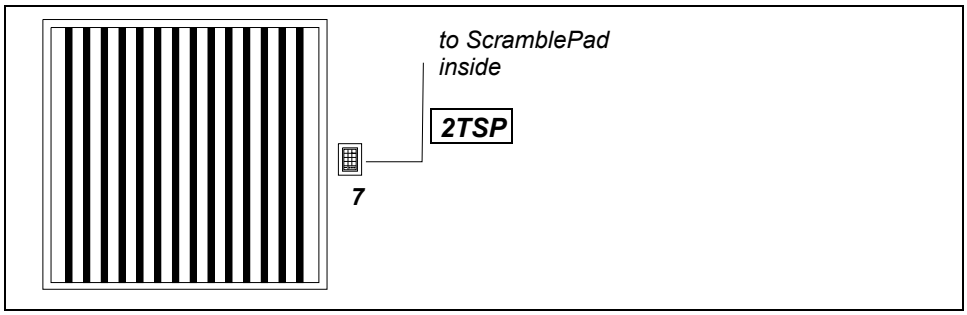


Figure 6-35: Sally Port Exit (Inner and Outer Gates)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M2 or M8
2	Door Lock Power Supply	PS2
3	Line Module	DTLM3/MELM3
4	Door Contact	Magnetic switch
5	Electric Door Lock	Electric dead bolt
6	Mounting Hardware	MB5 for entry, as required for exit
7	Identification Device	DS37L-HI ScramblePad, entry side of doors DS37L ScramblePad, exit side of doors
8	Printer	PR1 Parallel printer

Software Programming Commands

Command	Meaning
73	Define exit device function
80	Define door unlock time (1 - 8100 seconds)
74	Define door-open-too-long interval (1 - 8100 seconds)
85	Define relock function
52	Define time zone
17	Define access zone
03	Define entry/exit ScramblePad
45	Define control zone
84	Line module input triggers control zone
87	Relay trigger control zone
84	Line module input retrigger control zone
304	Define master control zones
305	Define time zone for master control zone
381	Set control delay for expansion relay
312	Add access user - card and card + code
41	Add top priority reset user
34	List all users inside

Example 13:

ScramblePad Floor Selection: Elevator Control - Floor Control

Objective:

- ❑ Limit after-hour elevator use to authorized employees.
- ❑ Allow floor access to authorized floor only.
- ❑ Require all users to enter code when using elevator after business hours.
- ❑ Log all after hours access transactions.

Solutions:

This example demonstrates the use of elevator/floor access control. This restricts the access to certain floors in a building. Only those people entering the right codes or presenting the correct cards can access certain floors. For example, a chief executive punches in his code inside the elevator cab and is then allowed to reach the top floor where his office is. Another worker, however, without executive clearance, enters his code, then punches the button for the top floor and is denied access.

This is done through a series of programmed relay outputs. A code or card triggers relays inside a Model SP Controller located in the elevator equipment room. Each relay is wired to an input on the elevator control panel that enables a specified floor button. Using this scheme, any combination of floors can be included or excluded for a specific code or card.

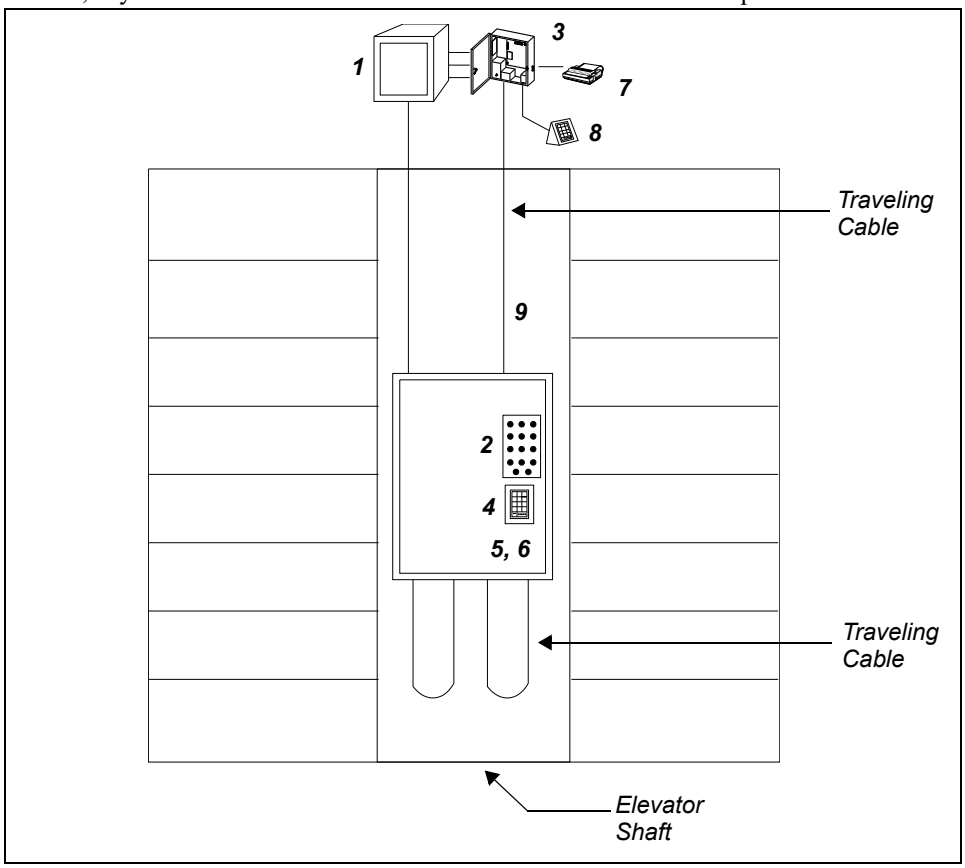


Figure 6-36: Elevator/Floor Access Control (Shaft View)

A view of the elevator cab is shown here.

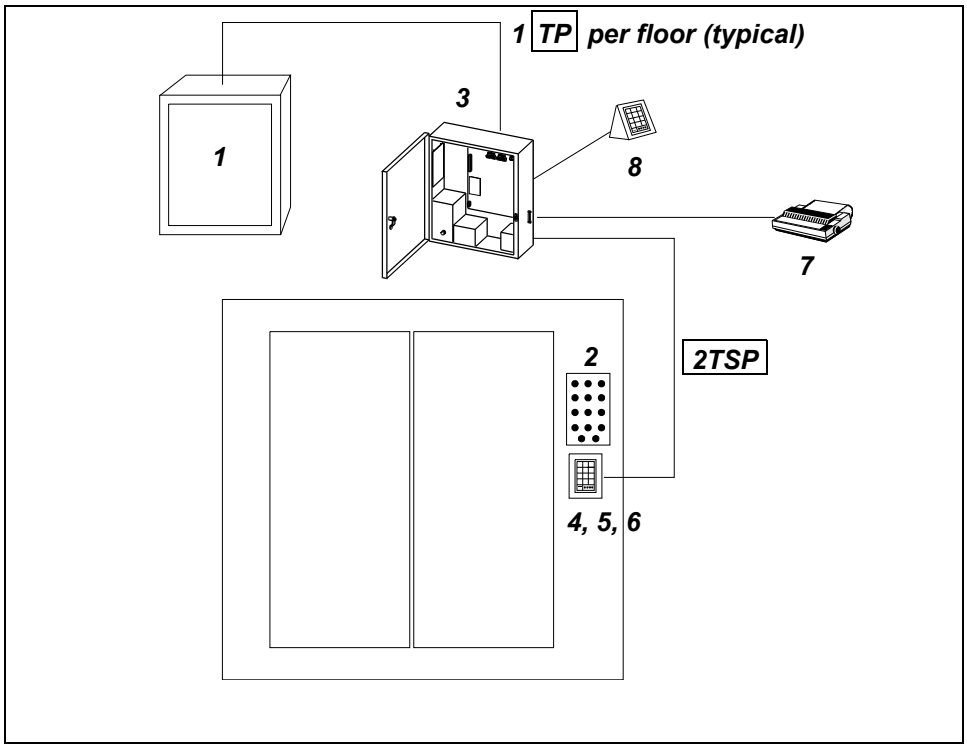


Figure 6-37: Elevator/Floor Access Control (Equipment View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch/3rd Party Product
1	Elevator control panel	Elevator company equipment
2	Elevator floor button panel	Elevator company equipment
3	Controller	MSP-8R or M64
4	Identification device	DS37L ScramblePad, inside cab
5	Mounting hardware	MB2 back box
6	Mounting hardware	UMK Universal Mounting Kit
7	Printer	PR1 parallel printer
8	Programming station	DS37L in ES1 stand
9	Cabling	All cabling sourced and installed by elevator company

Software Programming Commands

Command	Meaning
52	Define time zone
45	Define control zone
301	Add expansion relays to control zone
181	Set control time for expansion relay
40	Add control code user to specific control zone

Example 14:

ScramblePad Disarming: Medical Cabinets - Multi-Door Access Monitoring

Objectives:

- ❑ Limit access to cabinets for all medical personnel.
- ❑ Allow 24-hour access to physicians and management.
- ❑ Log all transactions.
- ❑ Initiate an alarm signal when unauthorized cabinet is opened, or if an authorized cabinet is opened too long or is propped open.
- ❑ Generate a list of all users currently authorized to open cabinets and create an audit trail.
- ❑ Create audit trail detailing who opened which cabinets.

Solution:

Access to specific medical cabinets is restricted to those entering the proper codes. While cabinets can be locked, in this example cabinets are alarmed so that if a cabinet is opened by an unauthorized person, the alarm sounds. This configuration uses a Model 16 Controller to monitor door contacts which are mounted on each cabinet.

Personnel entering proper codes may temporarily mask an alarm that would otherwise occur when a cabinet door is opened. Opening a door without a mask code sounds an alarm. All authorized activity is printed and logged for an audit trail. The ScramblePad is also used for programming.

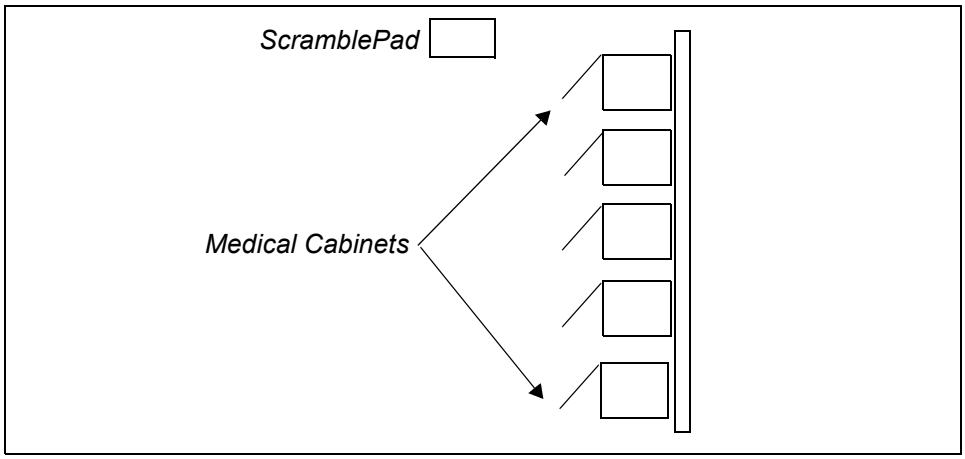


Figure 6-38: Medical Cabinets (Top View)

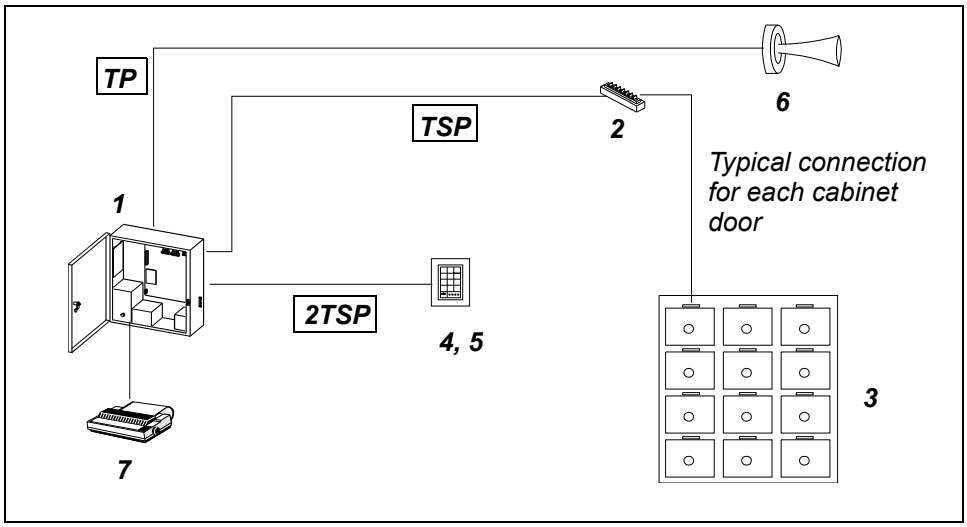


Figure 6-39: Medical Cabinets (Inside Cab View)

Hardware (match number to diagrams)

No.	Device Type	Hirsch Product
1	Controller	M16
2	Line Module	MELM1
3	Door Contact	Magnetic Switch
4	Mounting Hardware	MB2, UMK
5	Identification Device	DS37L ScramblePad
6	Alarm Annunciator	
7	Printer	PR1 Parallel Printer

Software Programming Commands

Command	Meaning
52	Define time zone
45	Define control zone
301	Add expansion inputs to control zone
174	Change expansion door open too long time
42	Add users to selected masked/unmasked inputs
184	Expansion input trigger control zone
34	List all users of inputs

Setup & Installation

7

Overview

This section provides detailed instructions on how to set up and install each Hirsch security device.

This chapter does not cover installation instructions for any devices not manufactured by Hirsch. For installation instructions on non-Hirsch devices, refer to the installation manual for that specific product.

General Connection Rules and Procedures

When installing or working with DIGI*TRAC controllers, line modules, or input/output devices, follow these rules:

- ❑ Locate the Controller in a safe and secure area. They are often installed in electrical rooms, telephone equipment rooms, or closets. An environmentally managed room is not required as long as the temperature ranges don't exceed the Controller's specifications.
- ❑ Make sure the power is off at the main circuit breaker before installing or connecting any part of the DIGI*TRAC system.
- ❑ Make sure the building's electrical system is properly grounded. This means the building wiring should be connected to ground via a pipe embedded in the earth – not grounded to a conduit or left completely ungrounded.
- ❑ Connect power last (primary AC input lines) after all other devices have been installed, wired, and connected.
- ❑ Don't block access to a DIGI*TRAC Controller's parallel printer port on the cabinet's right side because a local printer may be required for standalone programming or troubleshooting.
- ❑ Follow cable specifications for the controller, reader, line module, and lock installation exactly. This will minimize any related cabling problems. Major cable manufacturers make cable that meets Hirsch's specs of common, low voltage, noise resistant cable.
- ❑ Cable splices can cause trouble. Fortunately, most installations should have cable runs that are short enough, or straightforward enough, to allow unspliced runs. Make sure you measure your runs and order sufficient cable for unspliced runs. If splicing is required, solder the splices together, rejoin the shielding the best you can, and restore (heat shrink) the cable insulation. Make all terminations accurately and neatly to prevent any 'whiskers' from shorting between lines at terminal blocks and connectors.
- ❑ Label each cable run and each individual wire. Make sure you don't cross cables at splices or junctions. Color coded cable makes life easier and assures straight through connections.
- ❑ Carefully lay, tie, and dress cables when they enter the controller, power systems, and reader mounting boxes. There are a number of different types of cable ties and holders with self-adhesive backing that can make your installation neat and professional.
- ❑ Always allow for service loops, especially in the reader boxes. Don't make service loops too long in the controller cabinet, because too much cabling can get in the way when closing the door.
- ❑ Wherever possible and available, install the controllers on the building emergency power circuits.

Tools and Equipment

No special tools and equipment are required for installing Hirsch Systems. However, installing electric locks or strikes can require unique cutters, jigs, and fixtures for steel frames or doors. If the door and frame condition on any specific job are difficult, consider subcontracting the lock work to a qualified industrial locksmith who has experience in similar situations.

Connecting the Power Supply

Locate the Controller near a dedicated AC power source. A 15-Amp circuit with isolated ground is required. Make sure the building(s) and corresponding electrical system(s) are properly grounded.

The Controller's internal power supply is a dual range, auto sensing, switching power supply, which means it senses whether the power source is 110V or 230V AC and adjusts accordingly; however they do require different harnesses, as indicated in Table 7-1. To protect the DIGI*TRAC controller, a dedicated circuit breaker is recommended.

Note: Do not power other equipment from the system's power supply or standby battery pack. Doing so may cause intermittent operation, product damage, and void the manufacturer's warranty. Also, do not tap any power source for other than its intended use.

To Connect the Power Supply:

1. Remove the protective cover next to the power supply, by removing two hex screws and washers. The terminal block is revealed.

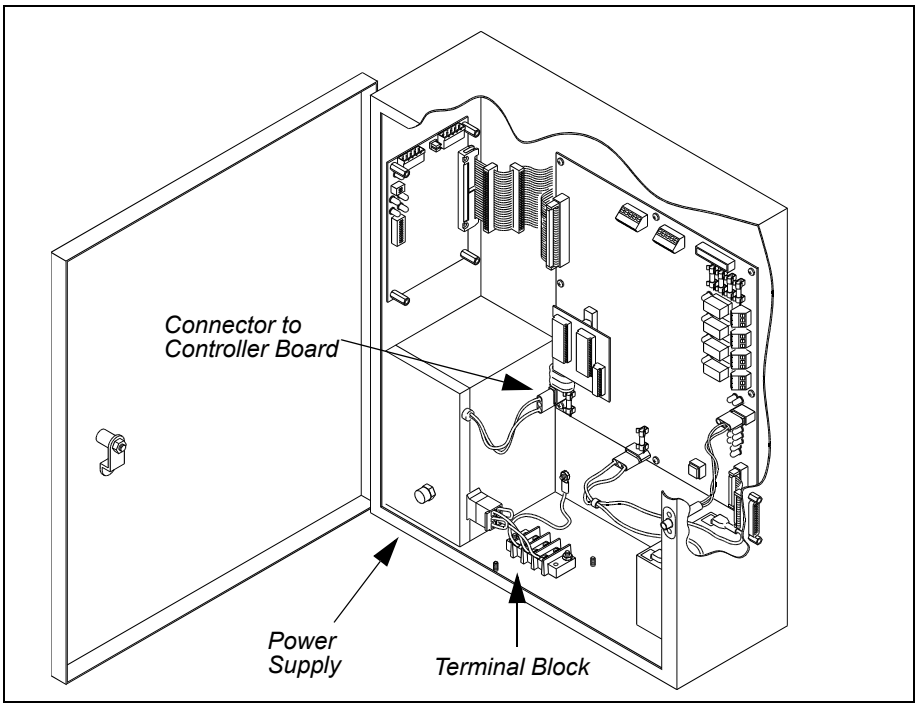


Figure 7-1: Power Supply Connection

2. Remove the lower center knock-out from the back or bottom (as required) of the controller enclosure, and install the power conduit to it. Examine the connector leading from the terminal block into the power supply. The color of the connector indicates the voltage range for which this controller is configured.

AC Power	Description
90 – 130 V, 50/60 Hz	Black connector and harness
180 – 260 V, 50/60 Hz	White connector and harness

Table 7-1: Internal Controller Power Supply

Figure 7-2 shows connections that will already be made when you open the protective cover.

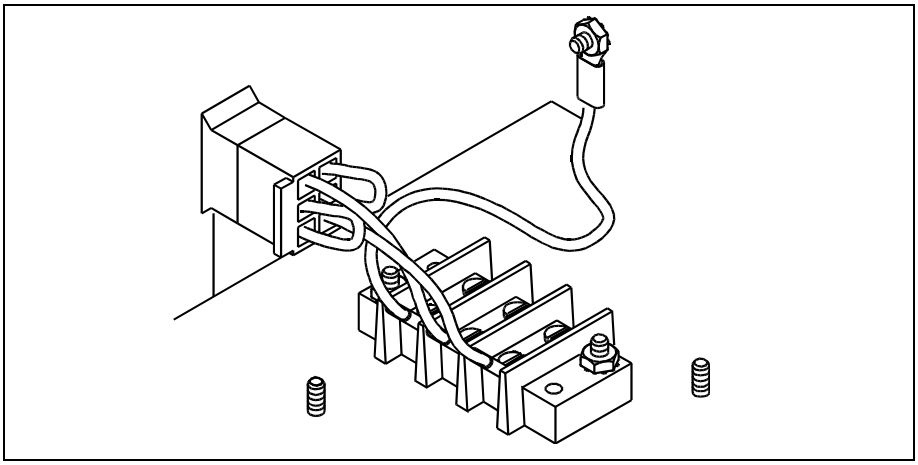


Figure 7-2: Connections to the Power Block

3. Pull the power cable through the knock-out hole, and strip the wires.
4. Attach the power wiring to the appropriate connector, and tighten the screws until secure. Spade lugs or ring tongues are recommended.

   Attach the ground wire to the left terminal, the white or blue wire (neutral) to the middle terminal, and the black or brown wire (hot) to the right terminal.

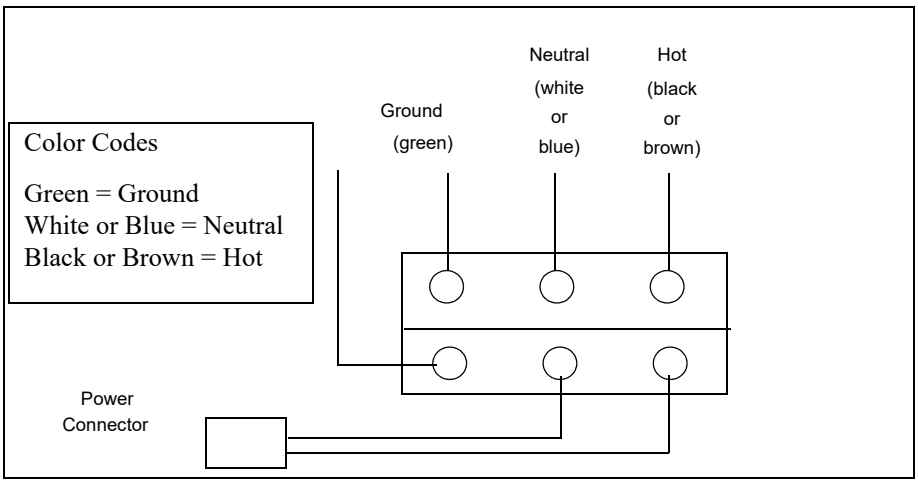


Figure 7-3: Power Cable Orientation

5. Replace the protective cover.

Connecting Wires to the Controller Boards

Connecting wires to a controller board is accomplished by attaching the appropriate wires to the correct terminal blocks. Terminal blocks located on expansion boards, ScramblePads, and MATCHs are removable, while those located on the Controller Board itself are not. For instructions on wiring a specific controller, refer to “Controller Installation” on page 7-17.

To Connect Wires to Terminal Blocks on the Controller Board:

1. Punch out the knockout(s) through which you plan to route the wires. Primary AC power cables are typically brought in through the bottom or lower back of the enclosure; all other cables (including low voltage power runs) are brought in from the top or sides. Those other cables must be separated from the AC power input wires and the standby battery pack's wires by at least 0.25 inches.
2. Route the wires in their conduit or sleeve through the knockout hole. The wire/cable should always be protected; don't route a bare cable through the knockout hole.
3. Loosen the screws on each terminal block you plan to use.
4. Remove insulation from the end of the wire and insert the specified wires into the green connectors, as shown in Figure 7-4.
   - If this is a ScramblePad or MATCH terminal, connect four wires and the shield. ScramblePad/MATCH input connectors have five slots available: G (Ground), + (Plus Voltage), A (Data A), B (Data B), and S (Shield). Always observe polarity.
   - If this is a line module terminal, connect two wires and the shield. Input connectors, such as from the DTLM, have three possible slots available marked HI, LO, and S. Always observe polarity: HI must go to HI; LO must go to LO. The shield connects to the S terminal of the controller but floats at the line module.
   - If this is an output line, connect two wires. Output relays, which control electric strikes, magnetic locks, or audible alarms, have three possible slots available marked NO (Normally Open), C (common), and NC (Normally Closed). Connect one wire to the common slot and the other to either the NO or NC slot, depending on whether the device's state is normally open or normally closed.

   For more information about which wires to connect, refer to the installation instructions for the specific device later in this chapter.

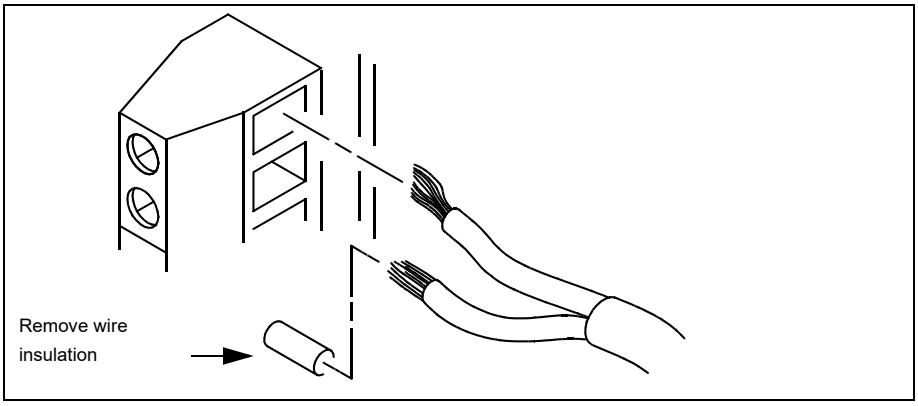


Figure 7-4: Connecting Wires to the Connector Slots

5. Tighten the screws until the wire is securely fastened in the slot.
6. Repeat this process for each wire you need to connect.

Connecting Expansion Boards

The capabilities of any DIGI*TRAC controller can be expanded using the many expansion boards designed for use with them.

All expansion boards are mounted on the left side of the controller enclosure. If more than one board is installed, use the supplied standoffs to stack them. You may stack up to five

expansion boards in each enclosure (except for the M64 which only holds 4 boards).

To install the board, you must perform these steps:

1. Configure the expansion board by setting jumpers and DIP switches.
2. Remove the power from the controller.
3. Mount the board in the controller's enclosure.
4. If this is an AEB8, REB8, SCIB, or SNIB board, connect the board to its assigned inputs/outputs. If a SNIB board is included, make sure it is mounted on top.
5. Restore power to the controller.

Mounting and Connecting Expansion Boards to the Controller

Because of the space limitation, make sure you connect an expansion board to the EBIC5 cable *before* you mount the board in the box.

To mount and connect an expansion board:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Configure the board by setting jumpers and DIP switches.
3. Connect the first (bottom) expansion board to one end of the EBIC cable, as shown in Figure 7-6. The first expansion board is the one that mounts to the left inside enclosure wall. Each board is shipped with its own EBIC5 Expansion Board Interface Cable. The EBIC5 connects up to five boards. If an acceptable cable is already in your system, save the new cable as a spare.
4. Mount the bottom board to the left inside of the Controller's enclosure wall. Use standoffs to secure the board to the studs mounted on the enclosure, as shown here:

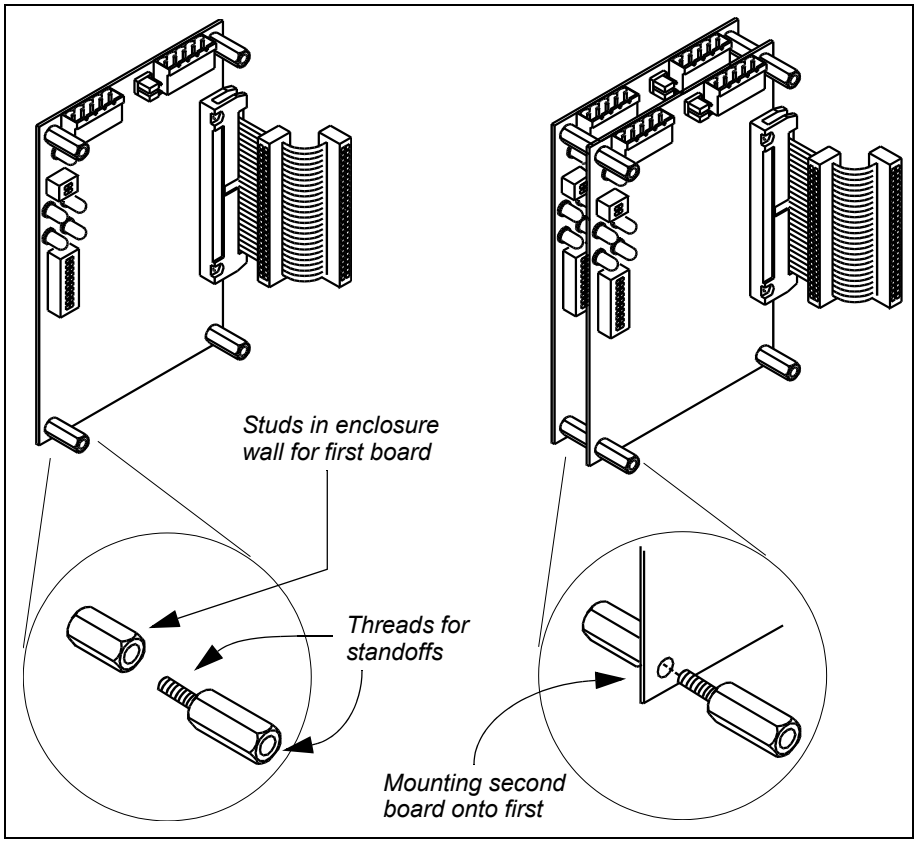


Figure 7-5: Securing a Board Using Studs and Standoffs

5. Connect the second board to the second EBIC5 cable connector.
6. Use the standoffs to connect the second expansion board to the first board, as shown in Figure 7-5.
7. Follow the procedure in the preceding steps until all the expansion boards are mounted. The topmost (last) board is mounted to the controller with screws rather than standoffs.
8. Connect the other end of the cable into the connector on the upper left side of the controller board, as shown in Figure 7-6.

Note: When adding expansion boards to a controller with an MEB/CE or MEB/BE board already installed, do not disconnect the EBIC5 cable from either these boards or the controller; otherwise, the controller will have to be reprogrammed.

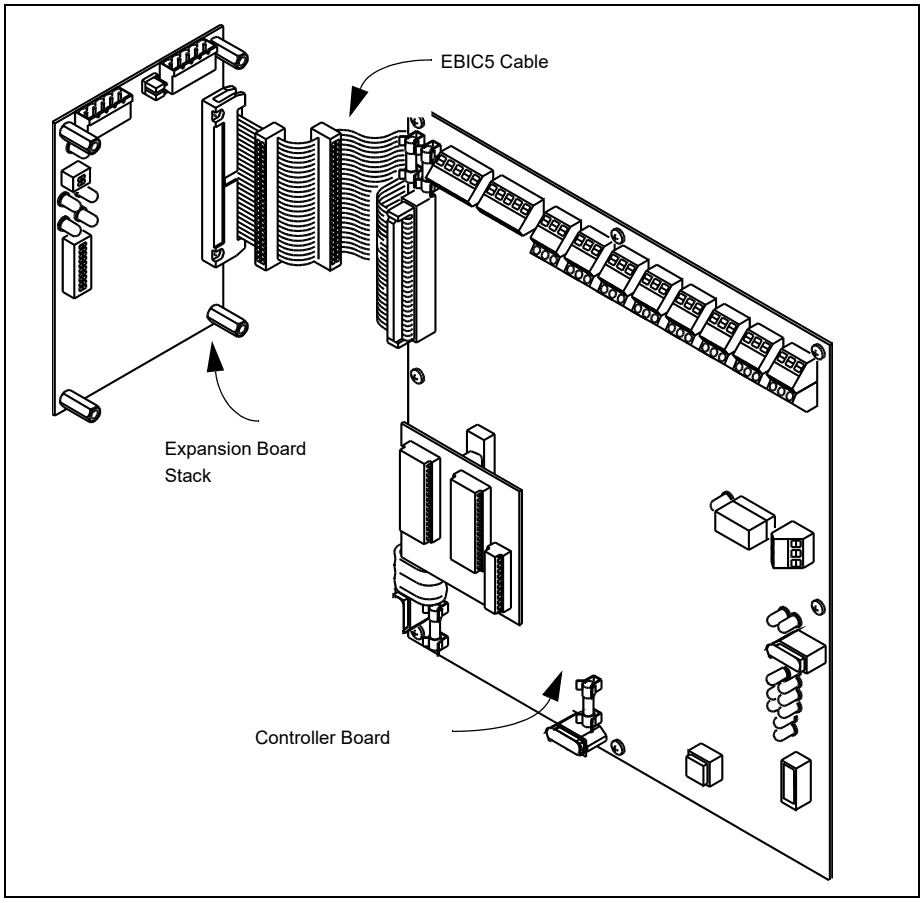


Figure 7-6: Connecting Between Expansion Boards and a Controller Board

If a SNIB expansion board is included in the stack, this should be the last (topmost) board installed.

For detailed expansion board setup instructions, refer to the specific expansion board later in this chapter.

Connecting Wires to Expansion Boards

If you are installing an AEB8, REB8, SCIB, or SNIB, you must also connect the board to its assigned input/output wires. Unlike the controller board, expansion boards use terminal blocks that detach from the board; otherwise, these are similar to the controller board's terminal blocks as to how wires are connected.

To Connect Wires to the Expansion Board Connector Blocks:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Punch out the knockout in the controller enclosure where you plan to route the wires. Either route these wires through the same opening used for controller board connections, or knock out a new opening for wires going to the expansion boards.
3. Route the wires through the opening.

Note: Don't run through a knockout without a sleeve or conduit.

4. Loosen the screws on each connector plug you will be using.
5. Remove (strip) insulation from the wire and connect the specified wires into the green connectors at the required slots, as described in Step 4 on page 7-13.
6. Tighten the screws until the wire is securely fastened in the slot.
7. Push the green connector into the appropriate socket until it locks into place. The connector and socket are keyed, so there is only be one way to plug it in.

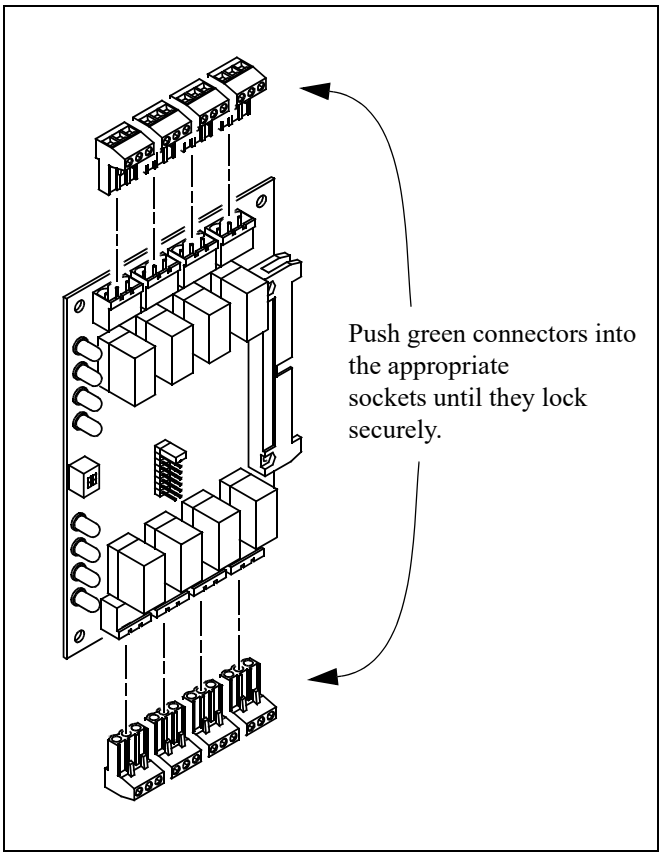


Figure 7-7: Plugging in Terminal Blocks on an Expansion Board

8. Repeat this procedure for each wire you need to connect.

Controller Installation

While DIGI*TRAC Controllers vary in design and function, they share many common elements, including the way in which they are configured, mounted, and connected to input and output cables. Where there are differences between the controllers, these are noted.

Controller Set Up

There are no DIP switches or jumpers to be configured before installing the M2 or M8 controller.

The M1N has an integrated SNIB with associated DIP switches that must be configured before installation. For more about setting these DIP switches, refer to “SNIB Setup” on page 7-43. Mx controllers have integrated SNIB2 capability, with associated DIP switches that must be configured before installation. For more about setting these DIP switches, refer to “Configuring the Integrated SNIB2” on page 8-26.

Mounting the Controller

To Mount the Controller:

1. If it makes the job easier, remove the controller door by lifting it straight up off its hinges.

   The M64’s door has six cables tied to it. For this reason, it isn’t recommended that you remove this door unless you absolutely have to. If, for some reason, you have to remove the door, disconnect the cable plugs from the SP controller board.
2. Punch out the knockouts needed for the conduits and cables. In most installations the top entry knockouts are used for conduit and cable installation. Side entry knockouts may be more convenient for expansion boards. Bottom or back knockouts are recommended for power cabling. For an illustration of this principle, see Figure 8-3, “Cable Inlets of the Mx Controller’s Enclosure”, on page 8-14.
3. If this is an M2, M16, or MSP-8R, use the three keyhole mounting holes along the top of the controller cabinet to hang the controller. Holes are 4¾ inches (12cm) apart.

   If this is an M8 or M64, use the two keyhole mounting holes along the top of the cabinet to hang the Controller. Holes are 16 inches (40.6cm) apart. Use the two bottom mounting holes for additional security.

Note: For best results, mount the Controller to a ¾-inch plywood backboard.

4. Because most controller cabinets (except for the M8 and M64) are too narrow to mount on a pair of wall studs, use the center keyhole to catch a stud. Use molly bolts or similar hardware in the other two keyholes to secure the cabinet to the wall. Use the bottom mounting holes for further mounting security.
5. If you’re installing a local printer at this site, make sure the printer connector on the right side of the cabinet has room to connect to the printer cable. The parallel printer cable can only be 12 feet long. Also, the printer requires a power outlet.
6. If you’re installing a ScramblePad for programming at the controller site – this is not normally required for networked system installations – consider using a portable ScramblePad and a flexible cable. This enables the programmer or operator to hold the ScramblePad (or sit with it) during command entry, which is more comfortable than programming on a wall-mounted ScramblePad.

Wiring to the Controller

DIGI*TRAC Controllers include these components:

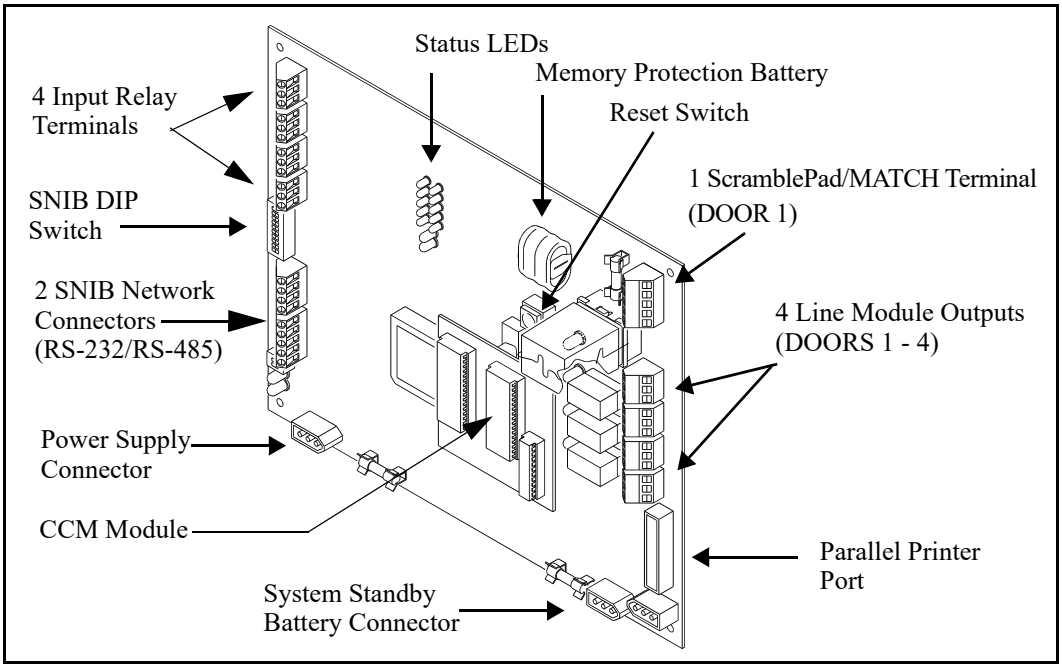


Figure 7-8: M1N Controller Board

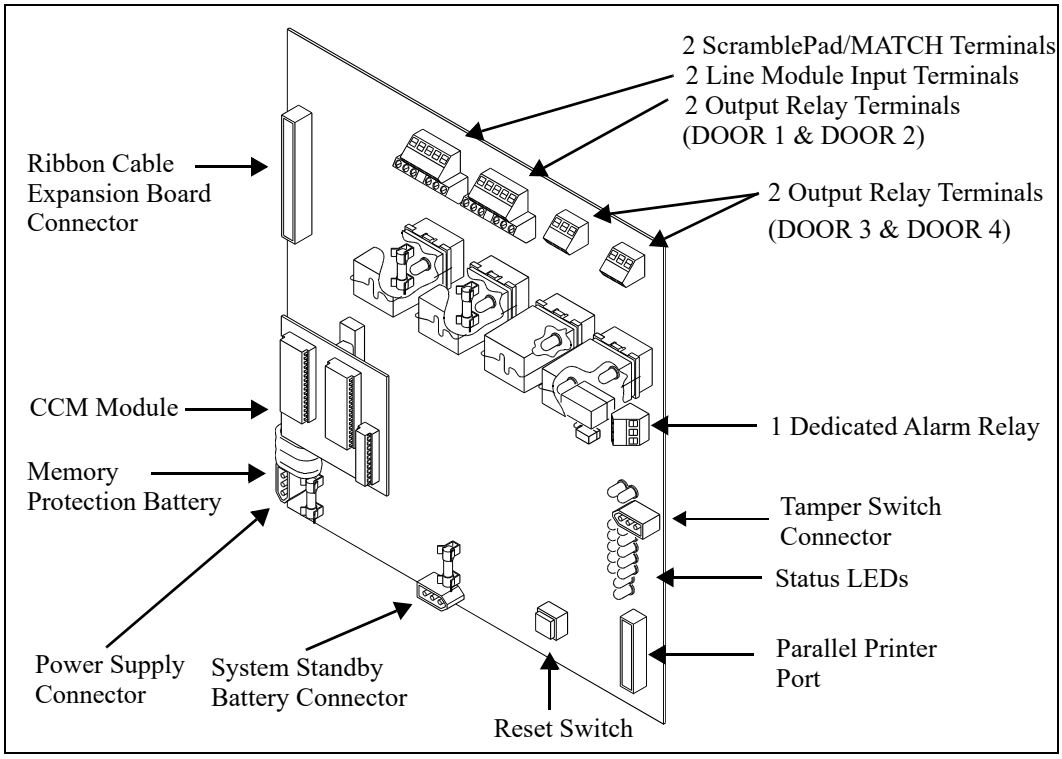


Figure 7-9: M2 Controller Board

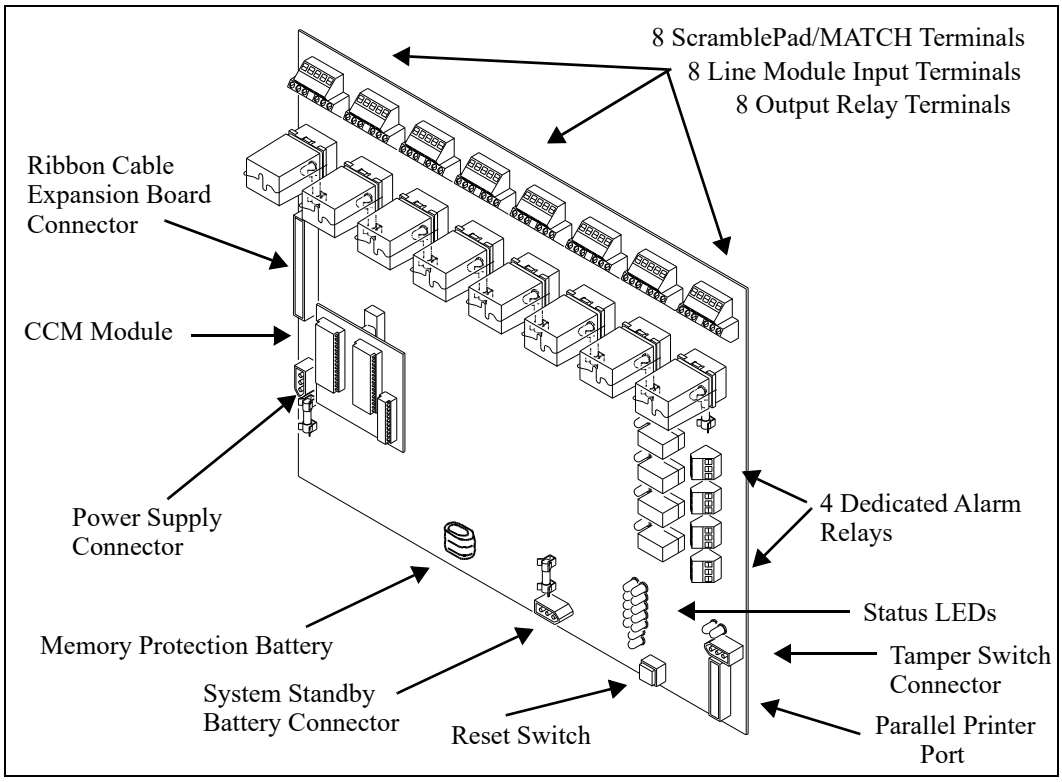


Figure 7-10: M8 Controller Board

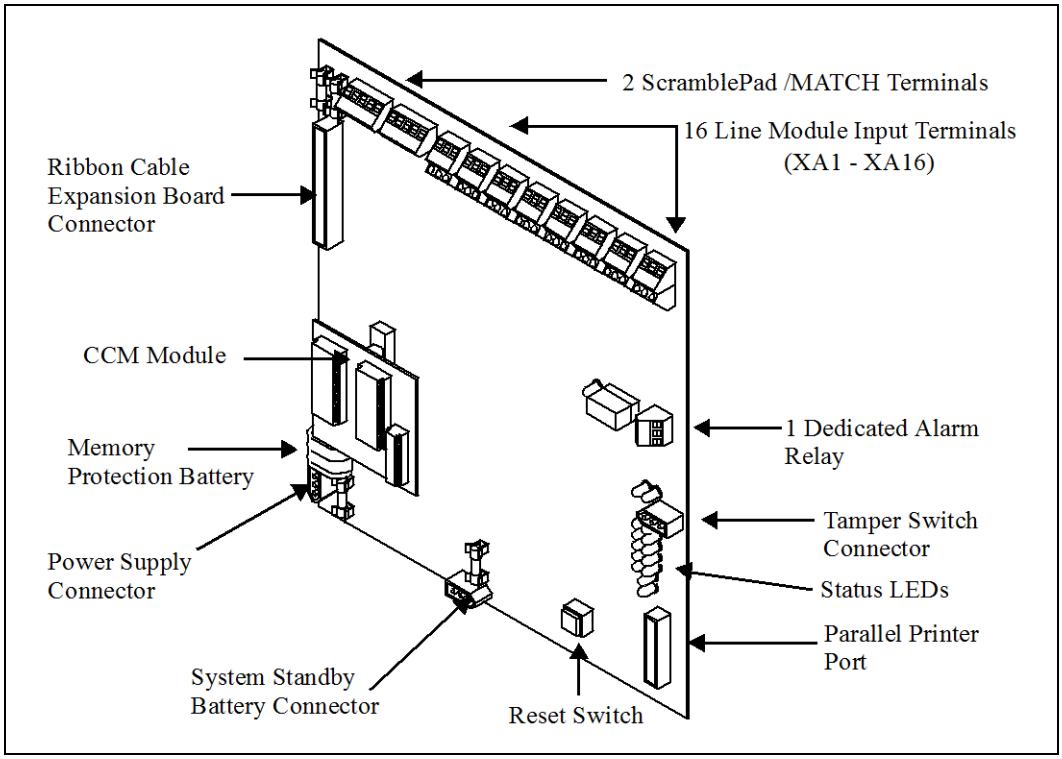


Figure 7-11: M16 Controller Board

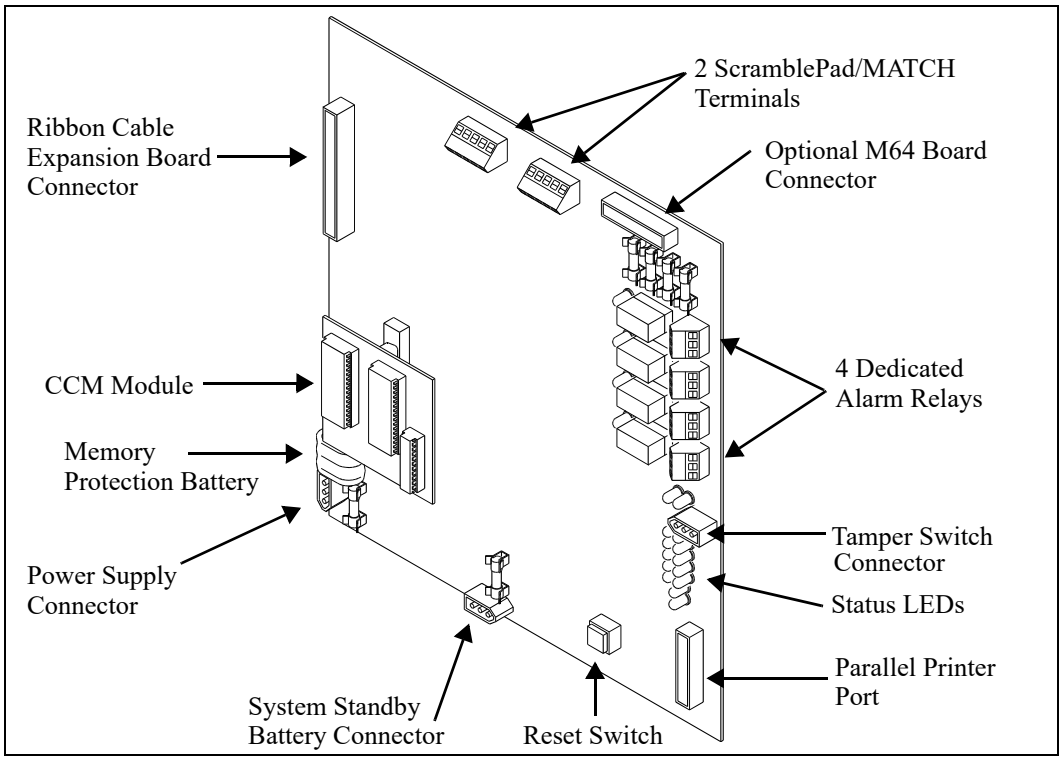


Figure 7-12: MSP Controller Board Connectors

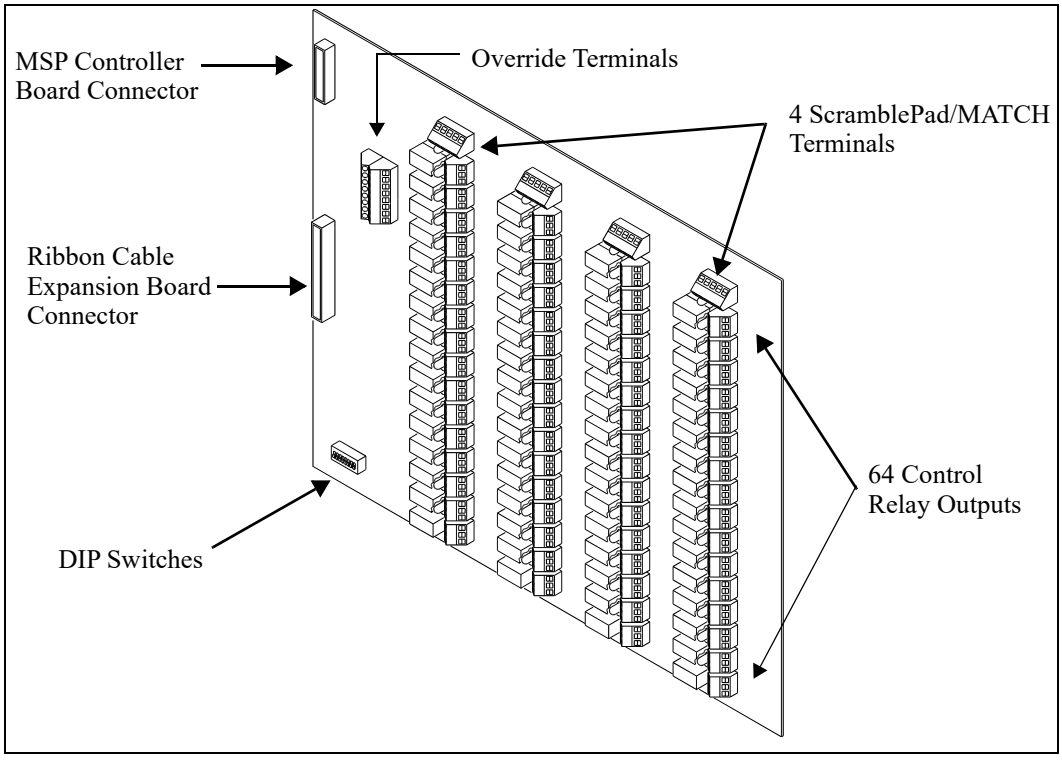


Figure 7-13: M64 Relay Board

Although the M64 Relay Board resides in the position within the M64 Controller cabinet usually reserved for the controller board, it can be best thought of as a large expansion relay board. The MSP controller board is actually mounted on the door and is connected to the relay board by ribbon cables. The M64 contains several override terminal blocks. These blocks enable an external shunt to force off all M64 relays. There is an override on the M64 for each bank of 8 relays.

During operation, the Status LEDs that reside on the M1N, M2, M8, M16, and MSP controller boards can prove useful in diagnosing problems that may occur. For more about troubleshooting the controller using the onboard LEDs, see “Troubleshooting the Controller Using Status LEDs” on page 7-382.

Connecting Line Module Inputs

The typical line module input features a connection between a Door Contact or Alarm Sensor, an RQE button, a line tamper, and the Controller. The DIGI*TRAC Controller uses a line supervision module device called a *line module* to supervise the input circuit. It should be located as close to the door contact or alarm sensor as possible. The DIGI*TRAC Line Module (DTLM) uses terminal blocks for connections. The Miniature Embedded Line Module (MELM) uses flying leads. The MELM is normally small enough to fit inside the monitored device.

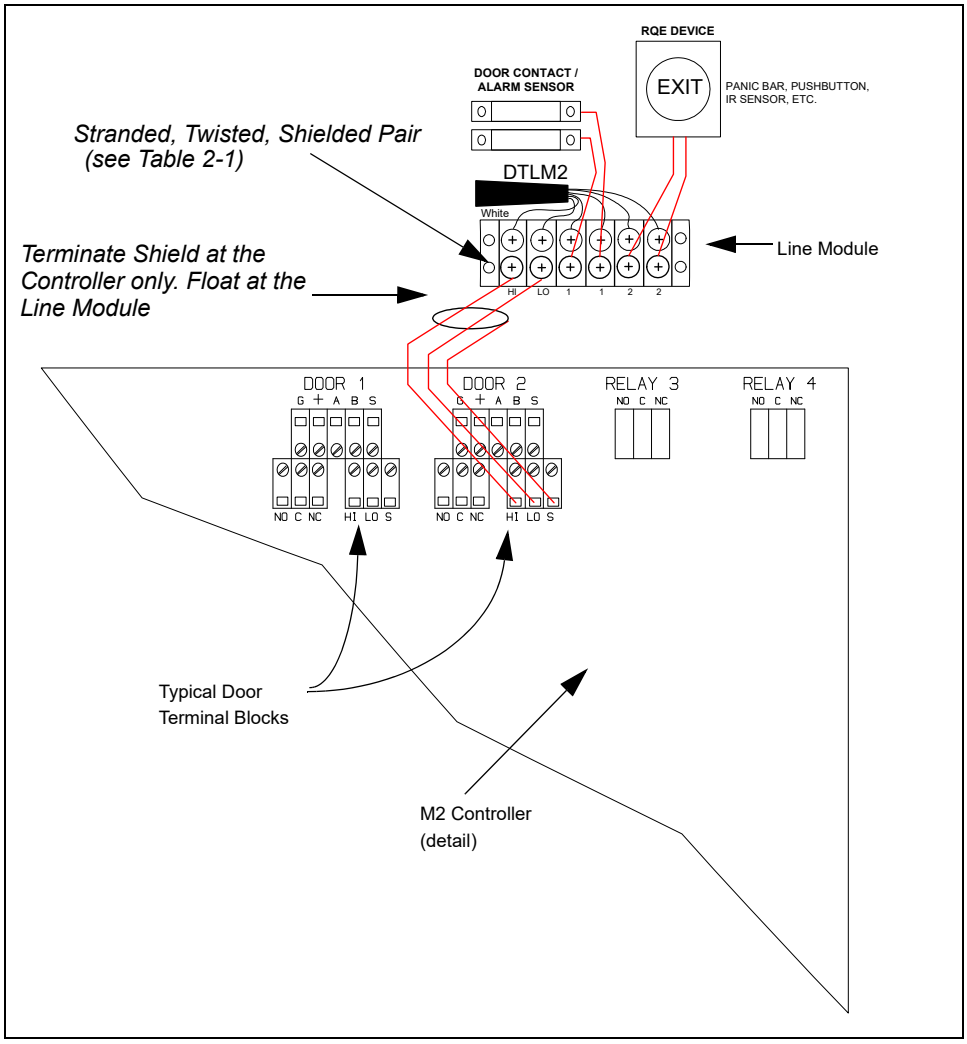


Figure 7-14: Typical Line Module Input Connection

To Connect Line Module Inputs to the Controller's Line Module Input Terminals:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Run the HI, LO, and Shield wire from the Line Module to the Controller.
3. Punch out the knockout(s) in the enclosure through which you plan to route the wires. Typically cables are brought in from the top.
4. Route the wires through the knockout hole.

Note: Don't run a wire through a knockout without a sleeve or conduit.

5. Loosen the screws on each connector block you plan to use.
6. Remove excess insulation from the wire and insert the specified wires into the green connectors at the required slots, as shown in Figure 7-4 on page 7-13.
7. Connect the HI, LO, and shield wires at the controller.
8. Connect the HI and LO wires at the line module. Make sure you observe polarity: HI must go to HI; LO must go to LO.

Note: Only connect the shield wire at the controller; float it at the line module.

The line module connected to an input terminal block on the Controller is automatically assigned the door ID to which it is connected. For example, if a line module is connected to the DOOR 1 terminal block, it is associated with the ScramblePad/MATCH assigned an ID of 1 or 9; a line module connected to DOOR 2 is associated with the ScramblePad/MATCH assigned ID 2 or 10.

The ID of a ScramblePad/MATCH is not associated with the terminal block to which it's connected; IDs for ScramblePads/MATCHs are assigned by their DIP switches, and are independent of their physical connection to the Controller board. For example, a ScramblePad assigned an ID of 3 on an M2 Controller can be connected to the DOOR 2 terminal block and still control the relay for DOOR 3. However, connecting the proper ScramblePad/MATCH to the same group of Door Terminals as the associated line module input makes troubleshooting much easier.

For more about installing and wiring Line Modules, refer to "Line Module Installation" on page 7-313.

Note: It is necessary for ScramblePads and MATCH Interfaces to have the same address as the relays they control for door access control.

Connecting Outputs

The typical output requires a connection between an output device (such as a door lock/strike) and an output relay on the controller board. An example of such a connection is shown in this figure.

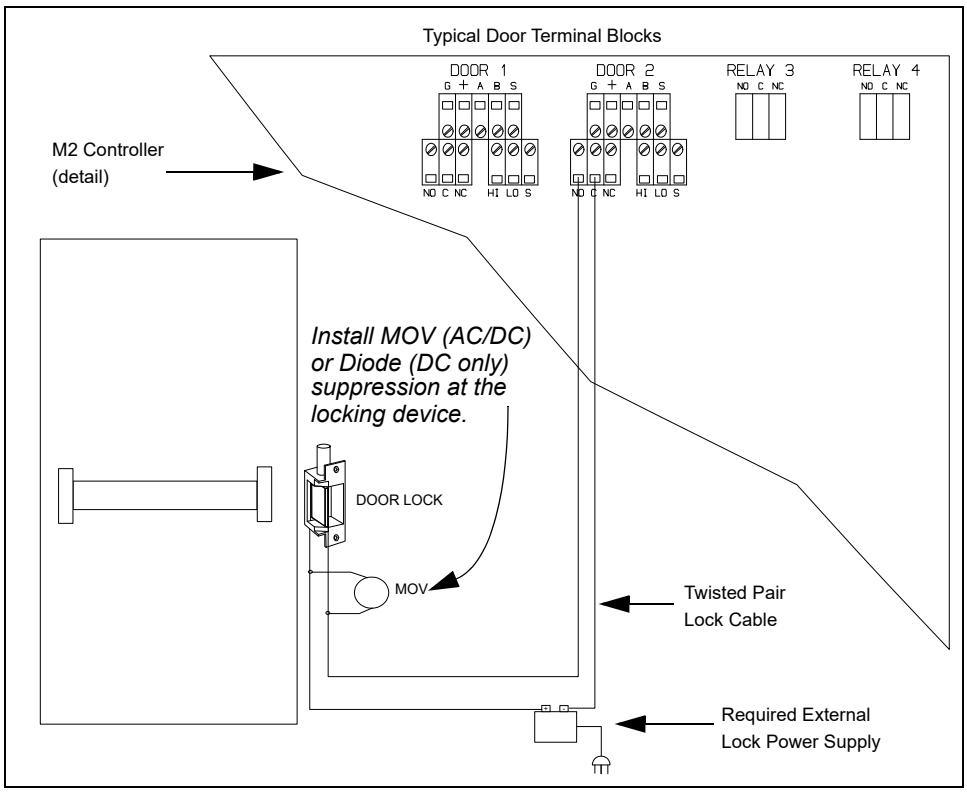


Figure 7-15: Typical Output Connection

To Connect Outputs to the Controller:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Run the control wires (N.O. or N.C. and Common) from the Output device to the Controller.
3. Punch out the appropriate knockout(s) in the enclosure to route the wires. Typically, output cables are brought in from the top.
4. Route the wires through the knockout hole.

Note: Don't run a wire through a knockout without a sleeve or conduit.

5. Loosen the screws on each terminal block to be used.
6. Remove excess insulation from the wire and insert the specified wires into the green connectors at the required slots, as shown in Figure 7-4 on page 7-13.
7. Connect the two wires. N.O. connects to N.O., N.C. to N.C., and C to C. Never connect to both NO and NC. An output device is either Normally Open or Normally Closed, but not both.

   To determine which set of contacts to connect to (N.O. or N.C.), refer to the device's installation manual. The choice is usually determined by the type of lock it is.

8. Install MOV suppression at the lock end. Use Hirsch Part# MOV35, Thomson VE09M00250K, GE #V39ZA1, or equivalent. If this is a DC lock, you can use a diode instead. Use a 1A, 400V diode (available as Hirsch Part # DIODE).

   Many locks come with suppression included. Make sure your lock does not have built-in suppression before adding an MOV or diode to the circuit.

Note: Don't attempt to run lock or strike cable within 6 inches (15cm) of ScramblePad/ MATCH cables or line module cables unless the lock cable is a twisted pair. Zip cord is not acceptable. When connecting to an electric strike/lock or other output device requiring more than the relay's contact ratings, an intermediate relay is required. Remember: Hirsch relays do not output voltage; separate power is required for output devices.

The terminal block to which the device is connected determines the device's ID assignment. For example, if an electric strike is connected to DOOR 2, it is associated with ID 2. If connected to DOOR 1, it is associated with ID 1.

Connecting ScramblePad and MATCH Interfaces

The typical ScramblePad/MATCH input features a connection between a ScramblePad keypad or MATCH Interface and the Controller. An example is shown in Figure 7-16.

Note: Card Readers communicate with the controller through the MATCH Interface Board.

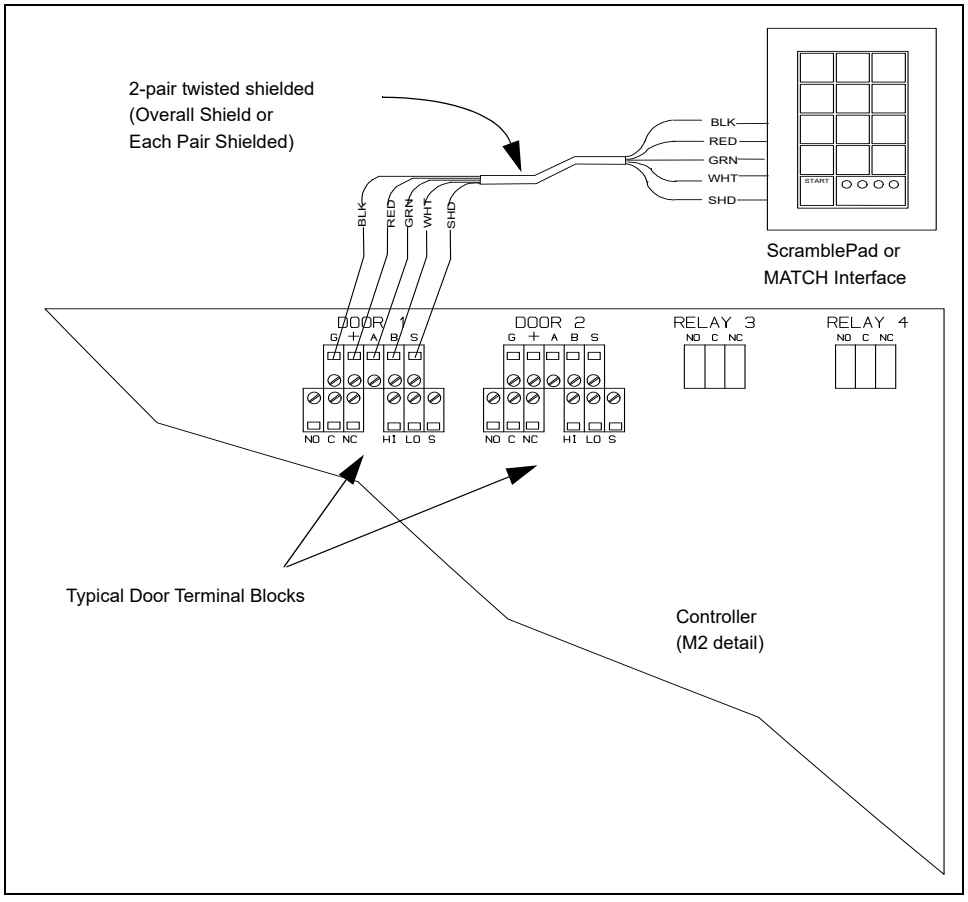


Figure 7-16: Typical ScramblePad/MATCH Input Connection

To Connect ScramblePad/MATCH Interfaces to the Controller:

1. Turn all system power off, remove connectors to the standby battery, and then remove connectors to the AC power.
2. Run the black, red, green, white, and shielded wires from the DIGI*TRAC connectors on the back of the ScramblePad or MATCH (MRIA or MRIB) to the corresponding terminals on the Controller's ScramblePad/MATCH terminal blocks.

   Terminals are color-coded as shown in Table 7-2:

Wire Color	Terminal Designation
Black	G
Red	+
Green	A
White	B
Shield	S

Table 7-2: ScramblePad/MATCH Wire Color to Terminal Designation

3. Punch out the knockout(s) in the Controller enclosure to route the wires. Typically ScramblePad/MATCH cables are pulled in from the top.
4. Route the wires through the knockout hole.
5. Loosen the screws on each connector block to be used.
6. Remove excess insulation from the wire and insert the specified wires into the green connectors at the required slots, as shown in Figure 7-4 on page 7-13.
7. Connect the five wires to the appropriate ScramblePad/MATCH terminal blocks: G (Ground), + (Plus Voltage), A (Data A), B (Data B), and S (Shield). Always observe polarity.

   For more about connecting to the ScramblePad, refer to "ScramblePad Installation" on page 7-97. For more about connecting to the MATCH, refer to "MATCH Interface Installation" on page 7-134.

The ID of a ScramblePad/MATCH is not associated with the terminal block to which it's connected; IDs for ScramblePads/MATCHs are assigned by their DIP switches and are independent of their physical connection to the Controller board. For example, a ScramblePad assigned an ID of 3 on an M2 Controller can be connected to the DOOR 2 terminal block and still control the relay for DOOR 3. However, connecting the appropriate ScramblePad/MATCH to its associated line module input makes troubleshooting much easier.

If two ScramblePads are installed at the same door – one for entry and the other for exit – they can share the same terminal block connection; however, the ScramblePads must have different IDs. The Controller's firmware recognizes that IDs 1-8 are for entry, and IDs 9-16 are for exit.

Resetting the Controller

In addition to the connectors and LEDs on the controller board, there is also a reset button at the lower right corner of the board. This button performs three types of reset, depending on how long you hold down the button, as shown in Table 7-3 below.

1 second	Resets any active alarm relay. Clears the alarm buffer.
5 seconds	Resets System Code to 123. Resets ScramblePads to original programming parameters.
30 seconds	Resets System. Clears all memory and returns all values to factory default.

Table 7-3: Reset Switch Functions

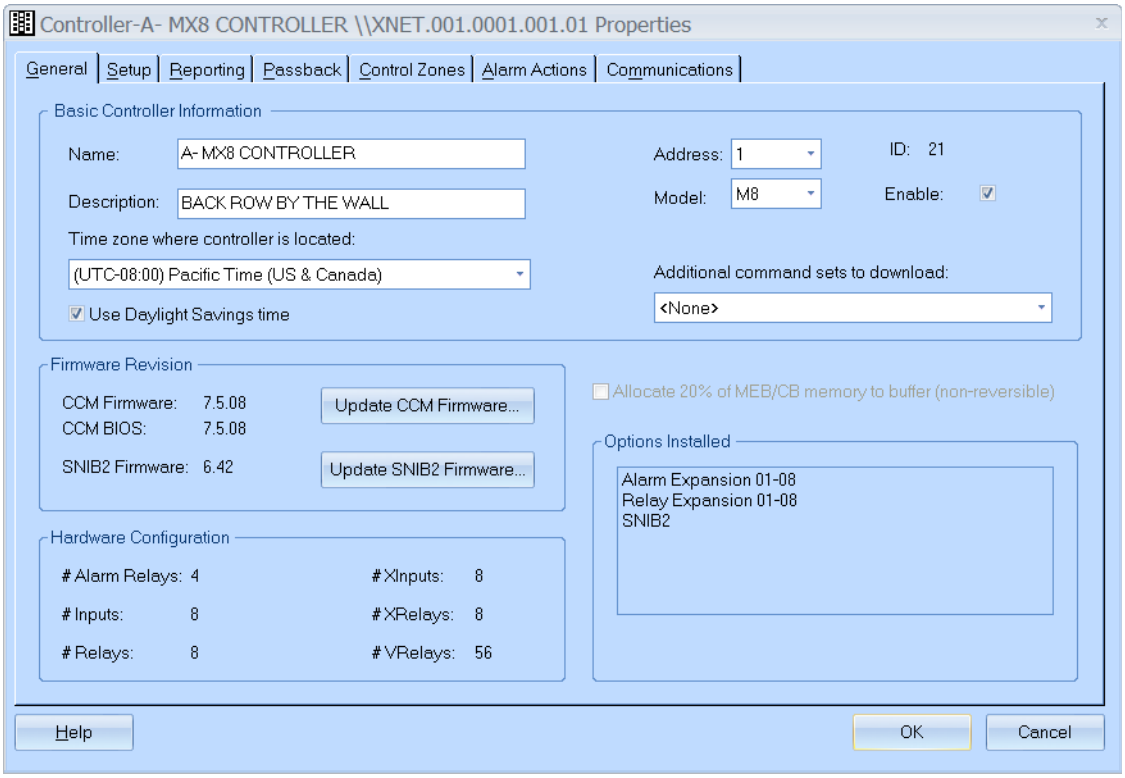
The normal procedure for using the reset button is:

- ❑ Press the button for 1 second if you have a problem that won't clear within a few minutes. All alarm conditions in the alarm buffers will be deleted and any alarm relays that are currently active will be turned off and reset.
- ❑ Press the button for 5 seconds to reset the system code to the factory default of 123.
- ❑ Press the button for 30 seconds if a major and persistent problem occurs. This resets the entire controller, clears all Controller memory, and returns all settings to the original factory default values. Only do this as a last resort.
- ❑ You can also use this option on a new system. Many installers will perform a cold start before they begin programming a new system. For more about controller cold starts, refer to "Hardware Cold Start Procedure" on page 7-385.

Upgrading the CCM

The Command and Control Module (CCM) is easily removed and replaced. The upgrade procedure required for a CCM varies according to its version number. To determine the version number of the current CCM on this controller:

❑ If there is a firmware version label on the CCM, it can only show the version that was originally installed. (To locate the CCM, see Figure 1-4 on page 1-8.) To determine the currently installed version of the CCM firmware on a controller, right-click on that controller in the system tree of the Administration module in Velocity's main window, and select Properties from the pop-up menu. The CCM Firmware version is displayed in the Firmware Revision section on the General tab of the resulting Controller Properties dialog:



❑ Specify the Date, Time, Version Number printout by specifying Command 88*1.

Make sure you perform this operation during a period of low activity, because several of the steps in the procedure incapacitate the controller.

Note: If you are updating from a CCM version before 6.3.0, you must first perform a system cold start. See "Hardware Cold Start Procedure" on page 7-385.

Preparing For Update

Before removing and replacing the CCM, you must first print out all setups, ACBs, and Codes so that you'll have a complete blueprint of the controller's configuration. To do this:

1. If you don't have a printer attached to the controller, obtain an 80-column dot-matrix parallel printer and plug it into the printer parallel connector on the side of the cabinet.

2. Enter programming mode at a ScramblePad connected to this controller. Enter these commands:

To print out:	Type:
All users with Codes	
for versions 6.3.0 – 6.3.11	`38 * 1 #`

for versions 6.4.0 – 6.4.3
without expansion boards
with MEB/CE4
with MEB/CE16
	
	`38 * 1 * 0 * 999 #`
	`38 * 1 * 0 * 4094 #`
	`38 * 1 * 0 * 16382 #`

for versions 6.5.0 – 6.6.27	`36 * 1 * 999 #`
	`36 * 1 * 4095 #`
	`36 * 1 * 163834 #`

All setups	`88 * 0 #`
All commands programmed in	
for version 6.5.0 – 6.6.27	`188 * 0 #`
All ACBs	`260 * 0 #`

After the update, you should request the same printouts so you can compare the two. Because of electrical charges and computer chips, it's always possible that your configuration will change unexpectedly. These printouts are your template, enabling you to reconfigure the controller, if required, and restore it.

Removing and Replacing the CCM

After you've documented the configuration, it's time to change the CCM. Most of you will have to replace the old CCMs (V6.x) on your Hirsch controller boards with the new V7.0 CCMs.

Note: CCM Version 5.x and older are not upgradable.

To upgrade your CCM to V7.0:

1. Ground yourself by touching the controller enclosure or power supply to remove any potential static electricity.
2. Turn all controller system power off by removing connectors for both AC power and the standby battery.
   a. Disconnect the DC battery. To locate the DC battery, see Figure 1-3 on page 1-7.
   b. Disconnect the main power to the controller.
   c. Remove the AC fuse located on the power supply in the lower left corner of the enclosure.
3. Locate the CCM.

The CCM is a separate daughter board like the two shown in these M1N and M2 examples:

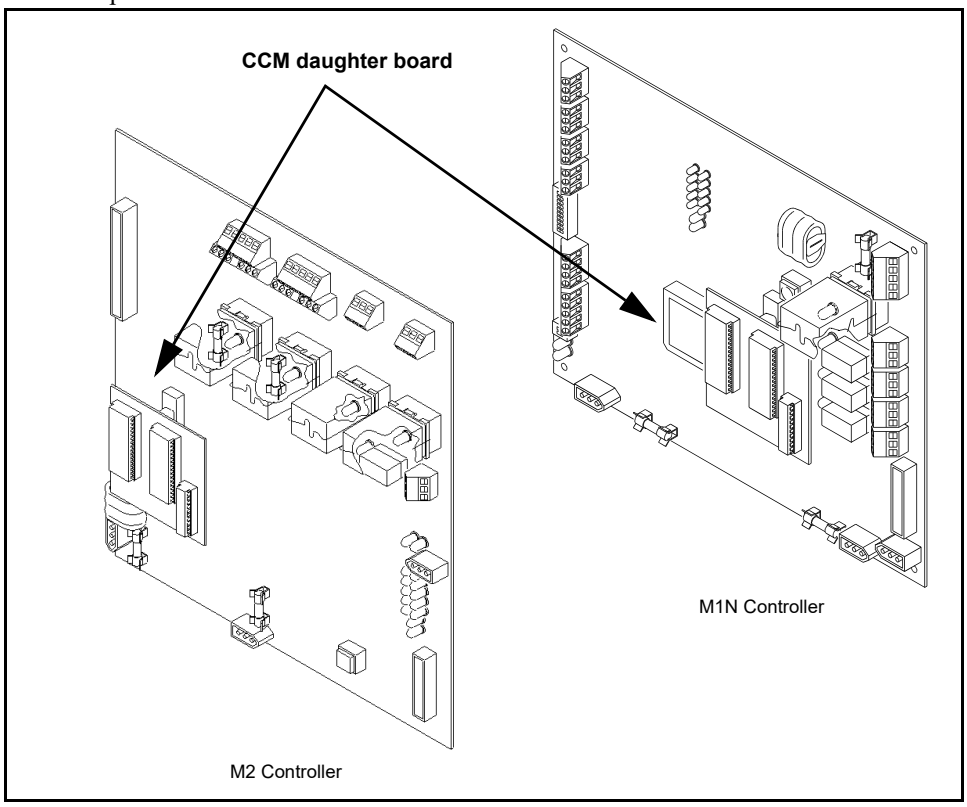


Figure 7-17: CCM Upgrade

4. Carefully remove the old CCM.
   a. Remove the screws anchoring the CCM circuit board.
   b. Grab the CCM circuit board by the edges. Pull it up and away from the controller board.

   Normally you should be able to perform this operation with your fingers.
5. Find the RAM memory chips which are located, in most cases, just to the right of the CCM socket on the controller board.
   - If the memory chip is soldered, continue with step 6. The new memory chips onboard the new CCM will assume the duties of the old chips.
   - If the memory chip is not soldered, remove it.

Note: From the second quarter of 1998 on, most controllers Hirsch sold contained the unsoldered (socketed) RAM memory; if you have this memory type, you MUST remove the memory before installing the new CCM. The new CCM contains replacement memory chips.

6. Install the new CCM daughter board.
   a. Grab the new CCM circuit board by the edges and align the CCM connector with the mating connector on the controller board. The CCM has a male D connector and can only be installed in one orientation.

b. Press the CCM down until it is firmly seated.

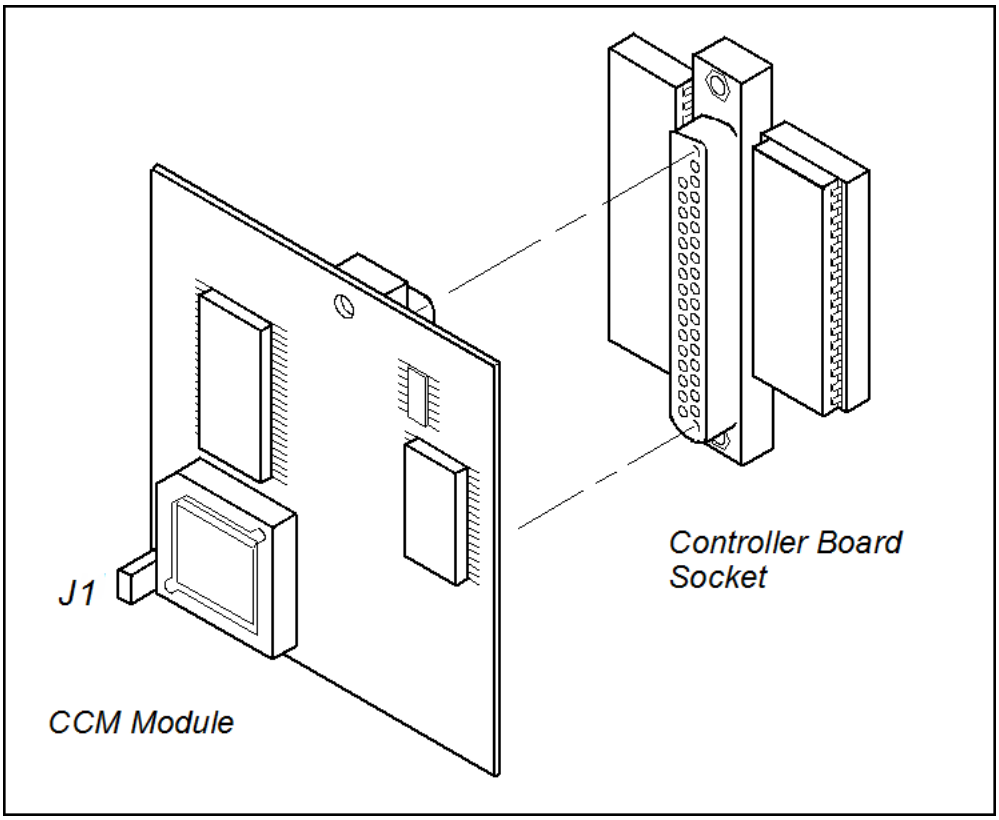


Figure 7-18: CCM Module and Controller Board Socket

7. Reconnect the AC power then the standby DC battery.

   The LEDs on the controller board alternate ON and OFF in different patterns while the controller performs a startup and self-test procedure. After the startup has finished, the lights should appear in their normal pattern. Refer to “Troubleshooting” on page 7-377 for more information.

   The line printer will print out some information including a header block showing the new CCM’s version number.

8. Print out a new list of configuration values and compare them to the old values. Reprogram any functions that require it.

9. You’re now finished. For information about troubleshooting potential problems with CCM updating, refer to “DIGI*TRAC Troubleshooting Guide” on page 7-379.

NOTE: The CCM module is shipped with a jumper across the J1 pins, which enables you to upgrade the CCM’s firmware. (To prevent anyone from changing the CCM’s firmware, you can remove that jumper.) For more information, see the **Firmware Updates > Updating CCM Firmware** topic in Velocity’s main help system.

Expansion Board Installation

Set up and installation for each of the expansion boards is explained on the following pages.

Memory Expansion Boards Installation

The MEB/CE4, MEB/CE16, MEB/BE, MEB/CB64, and MEB/CB128 boards provide a DIGI*TRAC Controller with enhanced ability to store events and codes.

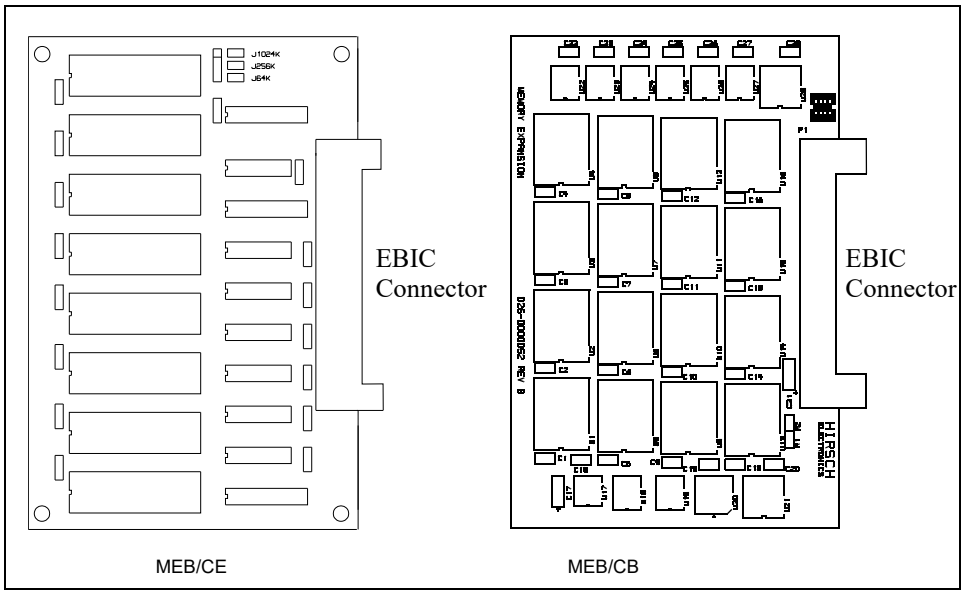


Figure 7-19: Sample Memory Expansion Board

Warning: Once installed, removing a memory expansion board from the controller will lose all codes.

Memory Board Setups

The MEB/CE4, MEB/CE16, MEB/CB64, MEB/CB128, and MEB/BE boards require no setup before installing.

Note: MEB/CB64 or MEB/CB128 are only supported by CCM 7.0 or higher.

Memory Board Mounting & Wiring

To install any of the expansion boards:

1. Turn all system power off and remove connectors for both AC power and the standby battery.
2. Install the board on the supplied standoffs and connect the EBIC cable, as described in “Connecting Expansion Boards” on page 7-13.

Note: Only one MEB/CE code expansion board may be installed in a controller at a time. If you have an MEB/CB64 or MEB/CB128 installed, there is no need for an additional buffer board because this board expands both code and buffer memory.

Warning: Once installed, removing a memory expansion board from the controller will lose all codes.

Because a memory board only communicates with the controller board, it has no inputs or outputs other than the EBIC cable. After a Memory Expansion Board (MEB) has been installed, removing it will instantly delete all codes or logged history records. Furthermore, a cold restart will be required, which will erase all additional information in memory and require complete system reprogramming or restoration from a backup.

Hirsch can provide a preconfigured system containing an EBIC5 cable together with the SNIB and MEB/BE boards. Other factory-preconfigured systems are also available on special request.

Testing the Memory Boards

After installing the board, you can test it by following this procedure:

1. Attach a printer to the Controller or make sure the Controller is attached to a Host PC.
2. Power up the controller by first connecting AC then standby battery.

   The system goes through its self-test. See this information printed out at a local printer.

   If this is an MEB/CE4:

   ```
   Max Users = 4,095
   ```

   If this is an MEB/CE16:

   ```
   Max Users = 16,383
   ```

   and under the Options section, this line appears:

   ```
   CODE Expansion
   ```

   If this is an MEB/BE, see this line in the Options section:

   ```
   Buffer Expansion
   ```

   If this is an MEB/CB64:

   ```
   Max Users = 65,536
   ```

   and under the Options section, these lines appear:

   ```
   CODE Expansion
   Buffer Expansion
   ```

   If this is an MEB/CB128:

   ```
   Max Users = 131,072
   ```

   and under the Options section, these lines appear:

   ```
   CODE Expansion
   Buffer Expansion
   ```
3. If this is a networked system, view maximum user information using the Host PC software.
4. If the correct information doesn't appear on the printouts, power down the Controller and recheck the EBIC-5 connections, then retry the test procedure. If it still doesn't work, contact Hirsch.

Warning: Once installed, removing a memory expansion board from the controller will lose all codes.

Alarm Expansion Board (AEB8) Installation

The AEB8 is an 8-input Alarm Expansion board where each input is supervised like the inputs on the Controller Board.

A Line Module is required for each input. For more about the Line Modules, refer to “Line Module Installation” on page 7-313.

Note: In the older version of the board, no more than 2 AEB8s can be installed in the M2, M8, M64, MSP-8R, or M64. In the newer version, no more than 4 AEBs can be installed. The M16 cannot accommodate an AEB8.

AEB8 Setup

The AEB8 has four jumper positions in the middle of the board which control board addressing:

J1	Addresses 1 - 8 (factory default for first AEB8)
J2	Addresses 9 - 16 (for second AEB8)
J3	Addresses 17 - 24 (for third AEB8)
J4	Addresses 25 - 32 (for fourth AEB8)

AEB8 Mounting

To install the AEB8 expansion board(s):

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Install the board on the supplied standoffs and connect the EBIC5 cable as described in “Connecting Expansion Boards” on page 7-13.
3. If you are installing two or more AEB8s, it is recommended that you install the AEB8 set to J1 on top of the AEB8 set to J2 and so on.
4. After each board is installed, connect the appropriate EBIC5 connector.

Note: If a SNIB is included in the expansion stack, make sure it is installed as the topmost board.

AEB8 Wiring

To connect inputs to this board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Punch out the knockout in the enclosure where you plan to route the wires. Either route these wires through the same opening you’re using for controller board connections, or knock out a new opening for wires going to the expansion boards.
3. Route the wires through the opening or knockout.
4. If it makes wiring easier, detach each green connector from the board as you need it.
5. Loosen the screws on each connector plug you will be using.
6. Remove insulation from the wire and connect the alarm wire to the designated pin on the green connector. If the device goes low to signal an alarm, connect the wire to the LO pin on the green connector. If the device goes high to signal an alarm, connect the wire to the HI pin on the green connector. For more about this, refer to the discussion on page 7-12.

If you need to, connect the shielded wire to the S pin on the green connector.

7. Tighten the screws until the wire is securely fastened in the slot.
8. Push the green connector into the appropriate socket until it locks into place. The connector and socket are keyed, so there is only one way to plug it in.

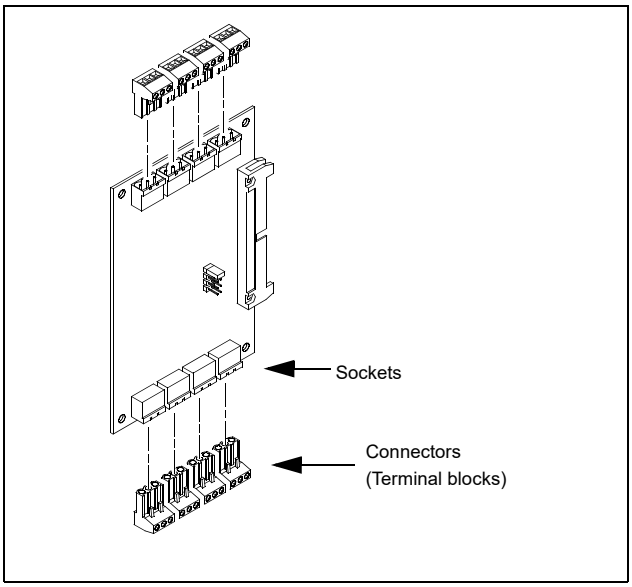


Figure 7-20: Connecting the AEB8

9. Repeat this procedure for each wire you need to connect.

Note: If a SNIB is included in the expansion stack, make sure it is installed as the topmost board.

Testing the AEB8

After installing the board, you can test it by following this procedure:

1. Attach a printer to the Controller or make sure the Controller is attached to a Host PC.
2. Power the system up by first connecting the AC power, then the standby battery.

   The system goes through its self-test. You should see this information printed out at the local printer under the Configurations section:

   `Expansion Inputs = 8` if one AEB8 is installed, or

   `Expansion Inputs = 16` if two AEB8s are installed, or

   `Expansion Inputs = 24` if three AEB8s are installed, or

   `Expansion Inputs = 32` if four AEB8s are installed.

   For CCM V.6.x, the controller can recognize up to 16 expansion inputs. For CCM V.7.x, the controller can recognize up to 32 expansion inputs.
3. Under the Options section, you should see this line:

   `AEB8-N` where N is the number of AEB8s installed (maximum of 4).
4. Use Command **88*2** from the ScramblePad to request the Max Users and Options information, or use Host PC software.

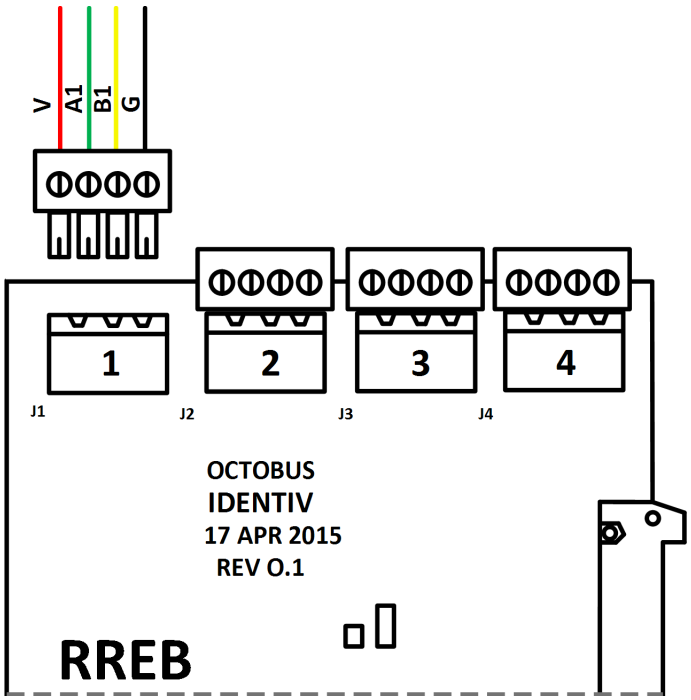
If the correct information doesn't appear on the printouts, power down the Controller and recheck the EBIC connections, then retry the test procedure. If it still doesn't work, contact Identiv.

RS-485 Readers Expansion Board (RREB) Installation

When installing an RREB, you will typically also be installing a SNIB3 (unless one was previously installed in your controller) as part of upgrading your traditional Velocity system to a FICAM-capable solution. Here is the general procedure for installing an RREB and a SNIB3.

1. Power down the controller.
   a. Disconnect the battery backup power from the controller.
   b. Disconnect the AC power cables to the controller.
2. If this is an existing controller which still has a SNIB or SNIB2 board installed, remove it.

   NOTE: If this is an Mx controller (which provides SNIB2 functionality using a daughterboard attached to the main board), see "Preparing an Mx Controller to Use a SNIB3" on page 7-75 for detailed instructions.
3. If this is an existing controller which is wired to traditional readers that are being upgraded, disconnect the wires from the MATCH and/or Wiegand terminals (on the controller's main board).
4. If you are upgrading an existing system, there might be enough slack in the wire runs that you can reuse the existing wires. Otherwise, run the necessary wires from the new readers to the controller.
5. Connect the appropriate wires to the male end of the RS-485 connectors, as shown in "Example Wiring Diagram for an RREB" on page 2-29. Here is a close-up diagram of an RS-485 connector:

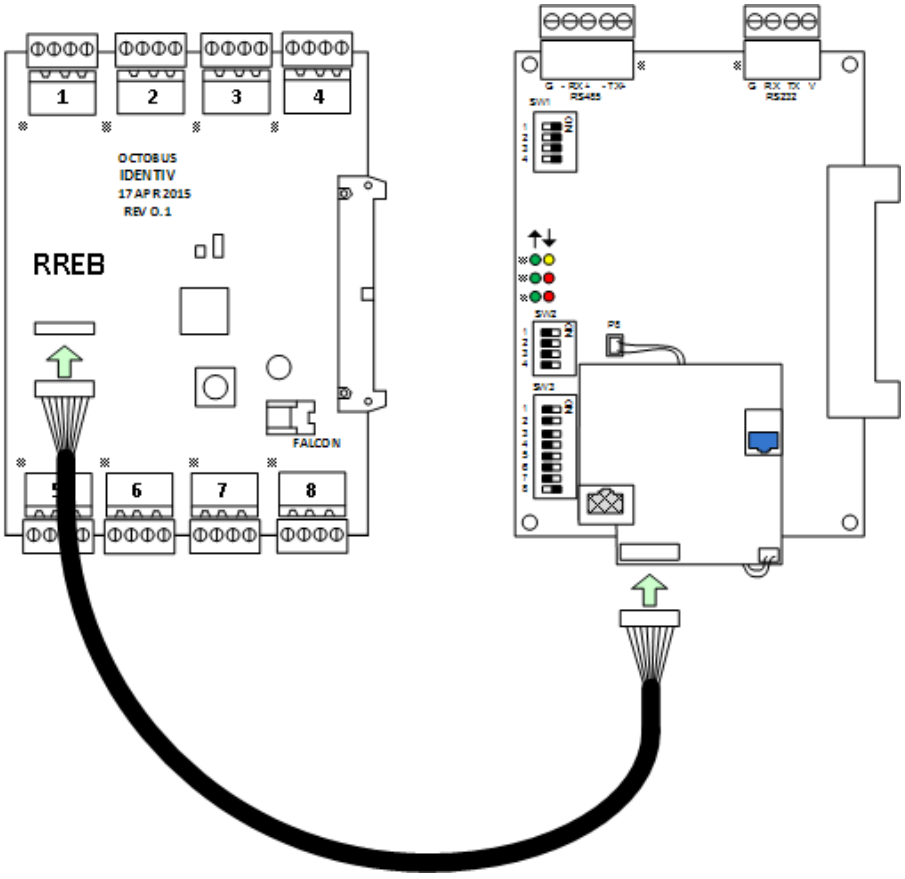


6. Install the RREB on the supplied standoffs, and attach it to the next-to-last connector on the EBIC5 ribbon cable. If you need more details, see "Connecting Expansion Boards" starting on page 7-13.
7. Plug the wired male end of each RS-485 connector that is used into the female end of the correct door's port on the RREB.

8. Check whether your SNIB3 is a current version which includes surge protection, or whether it is the initial version (sold only to a few US federal government agencies) which did not include surge protection.

   When using the initial version of the SNIB3 board (which has a serial number of the form SNIB3-S-nnnnn), surge protection must be provided for the master SNIB3 in each chain of connected controllers, using the Sankosha Guardian Net LAN-CAT5e-P+ surge protection device. For details, see "Providing Surge Protection for a Master SNIB3" starting on page 7-72.

9. Connect the 8-wire data cable between the RREB and the SNIB3, as shown in the following diagram.



10. Install the SNIB3 on the supplied standoffs, and attach it to the last connector on the EBIC5 ribbon cable, so it is the topmost board on this controller's stack of expansion boards.
11. Route the incoming Cat5 Ethernet cable through a knockout hole in the controller's cabinet and connect it to the Ethernet connector 1 RJ-45 jack on the SNIB3 board (which is colored blue on the previous diagram).
12. Restore power to the controller.
    a. Reconnect the AC power cables to the controller.
    b. Reconnect the battery backup power to the controller.
13. At the Velocity host, use Velocity to configure the SNIB3, as explained in"Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.

Relay Expansion Board (REB8) Installation

In order to expand the output relay capacity of the controller, install the Relay Expansion Board (REB8). This provides 8 additional 2-Amp (at 24VDC) Form C relay outputs.

REB8 Setup

The REB8 provides a set of jumpers (J1 through J8) to configure the address range assigned to these additional relays. The jumper is configured in this way:

J1	Addresses 1 - 8 (factory default)
J2	Addresses 9 - 16 (for second REB8)
J3	Addresses 17 - 24 (for third REB8)
J4	Addresses 25 - 32 (for fourth REB8)
J5	Addresses 33 - 40 (for fifth REB8)
J6	Addresses 41 - 48 (for virtual sixth REB8)
J7	Addresses 49 - 56 (for virtual seventh REB8)
J8	Addresses 57 - 64 (for virtual eighth REB8)

Amongst other things, these jumpers can be used for elevator control—where each address corresponds to an individual floor. Jumpers J6 through J8 specify virtual relays.

The REB8 is also equipped with a master relay override DIP Switch. This switch can override all relays to either the ON or OFF positions.

SW1	OFF	Normal operating position.
	ON	Forces all 8 relays OFF so no system function can actuate the controller until the master override is OFF.
SW2	OFF	Normal operating position.
	ON	Forces all 8 relays ON so no system function will actuate the relays until the master override is OFF.

Note: Only use the Master Override function for testing or troubleshooting.

REB8 Mounting

To install the REB8 expansion board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Install the board on the supplied standoffs and connect the EBIC5 cable as described in “Connecting Expansion Boards” starting on page 7-13.
3. Test the board as described in “Testing the REB8” starting on page 7-38.

REB8 Wiring

To connect outputs to this board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.

2. Punch out the knockout in the enclosure where you plan to route the wires. Either route these wires through the same opening you're using for controller board connections, or knock out a new opening for wires going to the expansion boards.
3. Route the wires through the opening or knockout. If it makes wiring easier, detach each green connector from the board as you need it.
4. Loosen the screws on each connector plug you will be using.
5. Remove insulation from the wire and connect the specified wires into the green connectors at the required slots as described on page 7-12.
6. Tighten the screws until the wire is securely fastened in the slot.
7. If you detached the green connectors from the board in Step 3, push the connector into the appropriate socket until it locks into place, as shown in Figure 7-21. The connector and socket are keyed, so there is only one way to plug it in.

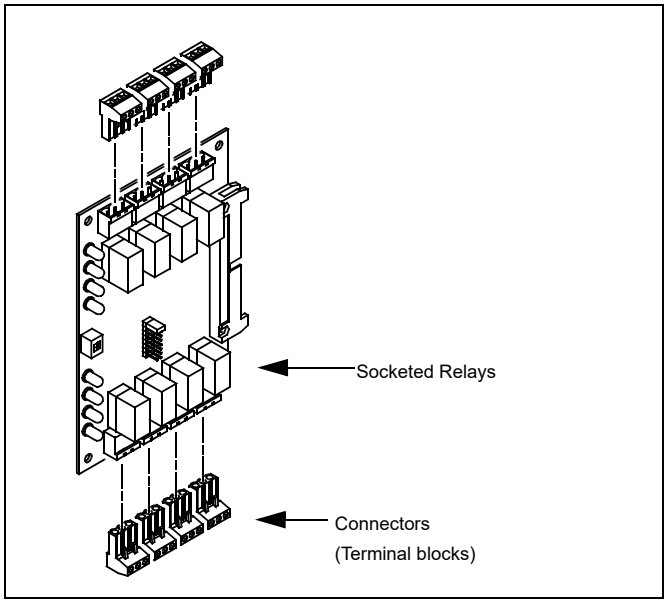


Figure 7-21: Connecting the REB8

8. Repeat this procedure for each wire you need to connect.

Note: If a SNIB is included in the expansion stack, make sure it is installed as the top board.

Testing the REB8

After installing the board, you can test it by following this procedure:

1. Attach a printer to the Controller or make sure the Controller is attached to a host PC.
2. Power the system up by first connecting AC then standby battery.

   The system goes through its self-test. You should see this information printed out at the printer or displayed on the screen. Under the Configurations section, you should see this:

   ```
   Expansion Relays = 8
   ```

   if one REB8 is installed and

   ```
   Expansion Relays = 16
   ```

if two REB8s are installed, and so on up to 5 boards. Under the Options section, you should see this line:

```
REB8-1
```

if one REB8 is installed and

```
REB8-2
```

if two REB8s are installed, and so on.

3. Use Command 88*2 from the ScramblePad to request configurations and options information, or use Host PC software.
4. If the correct information doesn't appear on the printouts, power down the Controller and recheck the EBIC connections, then retry the test procedure. If it still doesn't work, contact Hirsch.

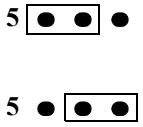
Serial Communications Interface Board (SCIB) Installation

The SCIB provides both RS-232 and RS-485 hardware interfaces to a printer.

SCIB Setup

The SCIB possesses one jumper at MD1 and a DIP switch bank of 8 switches at S1.

The MD1 jumper configures the RS-232 port as either 5VDC or 9VDC. Leave it at the factory default.



Provides 5V DC from the V terminal on the RS-232 port. (factory default)

Reserved for future use.

The SW1 switch bank provides only one function:

SW1-7		Not used.
SW8	OFF	Port will connect a serial printer. (factory default)
	ON	Port will connect a serial terminal.

SCIB Mounting

To install the SCIB expansion board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Install the board on the supplied standoffs and connect the EBIC5 cable as described in "Connecting Expansion Boards" on page 7-13.

Note: The SNIB should always be the topmost board in the expansion board stack, if present.

SCIB Wiring

The power and data lines should be fully isolated from the controller, providing immunity from transients and common-mode ground voltages between the controller and the remote terminal or printer.

To connect outputs to SCIB board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Remove the green terminal plug you need (either P1 or P2) from the appropriate SCIB port. P1 is RS-232 and P2 is RS-485.
3. Fabricate the printer or terminal cable to the required length using the following components:

RS-232 Serial Printer	One 3-conductor cable, 1 DB-25M (25-pin male RS-232 connector with cover and strain relief)
RS-485 Serial Printer	One 5-conductor cable, 1 SPA (RS-232-to-RS-485 Serial Printer Adaptor)

Table 7-4: Serial Cable and Connector Requirements

For more on cabling and pinout specifications, see “Serial Cabling and Pinouts” starting on page 7-40.

4. Either route these wires through the same opening you’re using for controller board connections, or knock out a new opening for wires going to the expansion boards.
5. Loosen the screws on each connector plug you will be using.
6. Remove insulation from the wire and connect the specified wires into the green connectors at the required slots as described on page 7-12.
7. Tighten the screws until the wire is securely fastened in the slot.
8. Push the green connector into the appropriate P1 or P2 socket until it locks into place. The connector and socket are keyed, so there is only one way to plug it in.

   Make sure the wires you connect to the terminal block are appropriate to the serial cable assembly.

Note: You can only connect to the P1 or the P2 port, not both at the same time.

9. Make sure the wires going into the other end of the serial cable are correctly aligned. The RS-232 connection (P1) wires must be soldered to a DB-25M or DB-25F connector. The RS-485 connection (P2) must connect to either a SPA or NET*ADAPT. For instructions on correct cabling for these connectors, refer to “Serial Cabling and Pinouts” starting on page 7-40.
10. Connect the other end of the cable into the appropriate printer:
    - If this is an RS-232 printer connection, connect the DB-25M connector into the serial printer.
    - If this is an RS-485 printer connection, connect the SPA terminal block (available from Hirsch) into the network printer.

Serial Cabling and Pinouts

This section describes how you should wire the serial cable to the appropriate plug and/or terminal block for your particular printer requirement.

RS-232 Cable Assembly to Printer

First, you must fabricate the required connector and 3-conductor cable assembly to the required length. The cable should be 22-gauge, stranded and twisted with a cable length not to exceed 50 feet (15.2 meters).

Follow this wiring and pinout diagram:

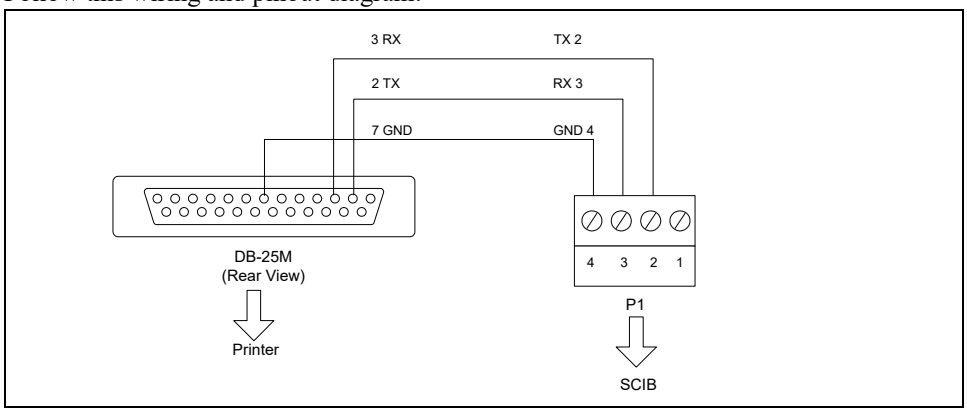


Figure 7-22: RS-232 Cabling and Pinout Diagram

Install the P1 and DB-25 connectors as shown in Figure 7-22. The P1 connector provides terminal screws to secure each wire. The DB-25 requires soldered connections.

RS-485 Cable Assembly to Printer

First, you must purchase the required connectors and one 5-conductor cable of the required length (see Table 7-4 on page 7-40).

The cable should be 2-twisted and shielded pairs such as Belden #8723 or equivalent. The cable length should not exceed 4,000 feet (1220 m).

Follow this wiring and pinout diagram to assemble the necessary cable:

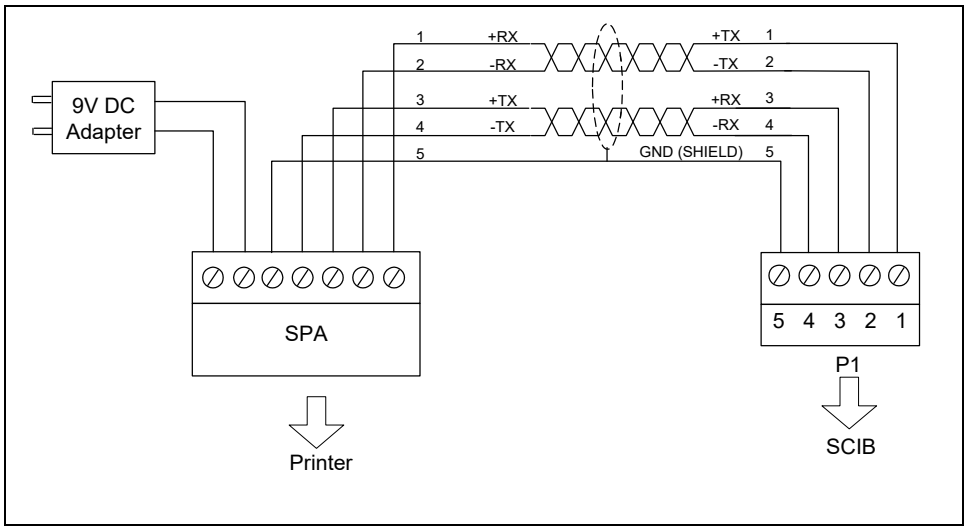


Figure 7-23: RS-485 Cabling and Pinout Diagram

Secure Network Interface Board (SNIB, SNIB2, or SNIB3) Installation

RS-232 is best for modems or local PCs. (It is not available on the SNIB3.)

When installed, the SNIB, SNIB2, or SNIB3 expansion board enables a DIGI*TRAC or Mx controller to be programmed, monitored, and controlled from a properly-configured IBM-compatible host PC running the Velocity software. Communication is secured by Hirsch's proprietary Hirsch Encrypted Standard (HES) protocol SCRAMBLE*NET network.

- An optically isolated RS-232 port is provided on the original SNIB and the SNIB2.
- An optically isolated RS-485 port (required for multi-drop or long hardwired connections) is provided on the SNIB, the SNIB2, and the SNIB3.
- An RJ-45 Ethernet port (which requires a host-to-master controller TCP/IP connection) is provided on the SNIB2 and the SNIB3.

NOTE: The SNIB3 is compatible with the SNIB2, but not with the original SNIB.

The M1N controller does not require the addition of a SNIB or SNIB2 because it already has SNIB circuitry integrated into its main board. The Mx controller's main board includes SNIB2 functionality on a daughterboard, which can be removed to enable using a SNIB3.

The following subsections provide installation instructions for the SNIB (page 7-43), the SNIB2 (page 7-49), and the SNIB3 (page 7-72).

Installing the SNIB

This section includes installation instructions for the original SNIB.

SNIB Setup

The wiring and settings of the SNIB are shown in Figure 7-24.

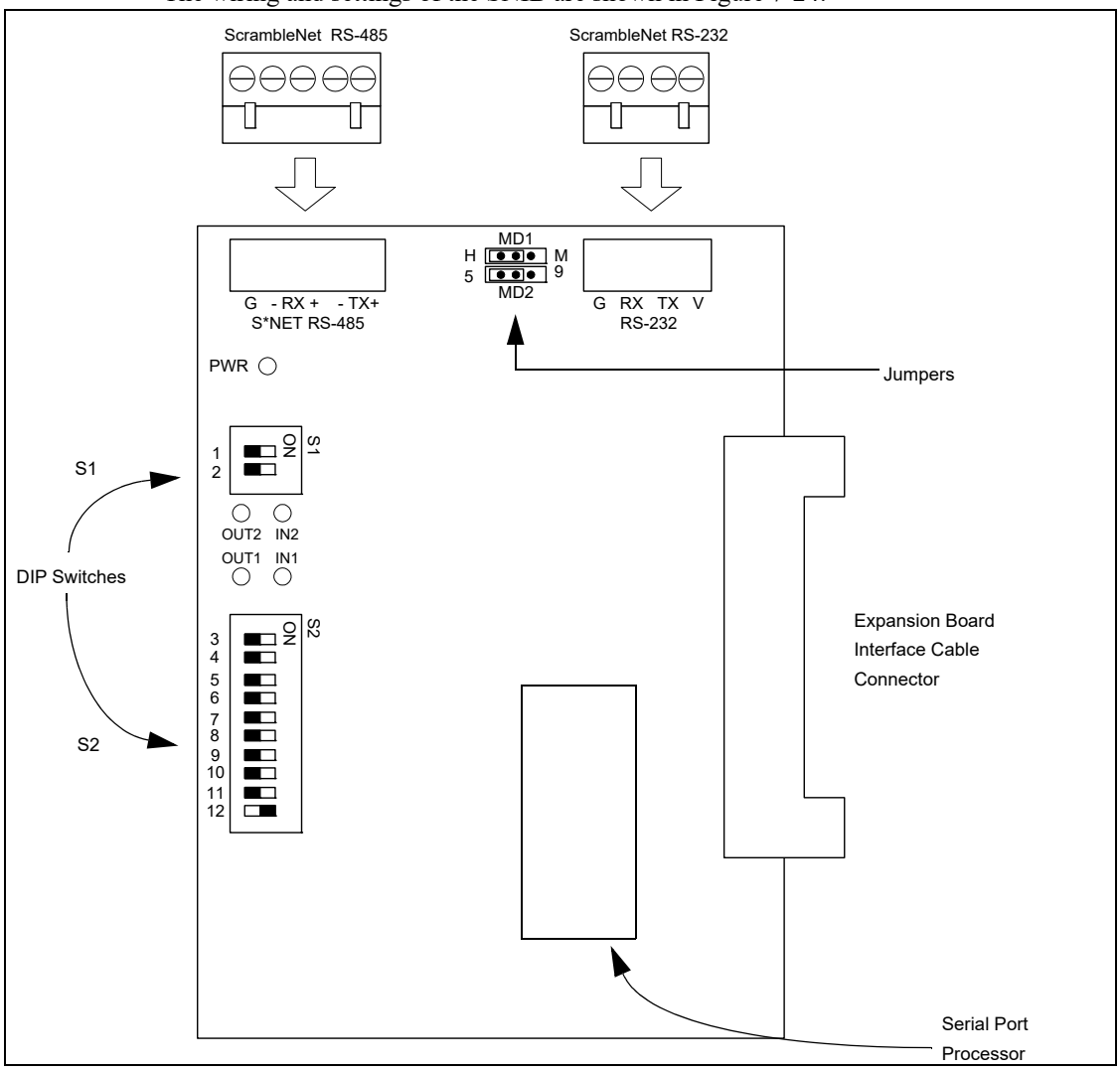


Figure 7-24: Secure Network Interface Board (SNIB)

MD1 - 2

Because the M1N has integrated SNIB circuitry, the DIP switches are located on the controller itself, to either side of the network connections. (Refer to Figure 2-1 on page 2-4.) Set these switches as you would a normal SNIB. There are no SNIB jumpers on the M1N.

The board has two jumpers, MD1 and MD2. Both are explained here:

In reality, changing the MD1 jumpers does not appear to affect the operation of the SNIB. The factory default works well for both modes.

MD1	
H ● ● ●	Host Connection via RS-485 port for hardwired (H) connections. (factory default)
● ● ● **M**	Host Connection via RS-232 port for modem (M) or short connections less than 50 feet hardwired.

MD2	
5 ● ● ●	Provides 5V DC from the V terminal on the RS-232 port. (factory default)
5 ● ● ●	Reserved for future use.

There are also a number of DIP switches on the SNIB which can configure the board.

SW1/SW2

The last controller on any network cable run, or any single controller connected to a modem through the RS-232 port, must have its terminating resistors set to ON. To do this, set both SW1 and SW2 on switch bank S1 to ON.

SW1 SW2	OFF	This SNIB is not the last one on the network cable. (Default)
	ON	This SNIB is the last one on the network cable.

SW3/SW4

The switch bank at S2 has 9 switches which configure a number of properties for the SNIB. SW3 determines the Modem Mode.

For M1N Rev. B controllers only: to enable modem mode, **SW3-4** must both be **ON**.

SW3	OFF	Disable Modem Mode. There is no dial-up modem connected to this SNIB. (Default)
	ON	Enable Modem Mode. There is a dial-up modem connected to this SNIB and you are using it as part of a Remote Site Management Network.The controller then supervises the modem and provides auto-answer.
SW4		Not Used.

SW5/SW6

SW5-6 determines the SNIB's baud rate. The rates you can select depend on the SNIB version you have.

Older (pre-1998) SNIBs have a '16450' or '16C450' serial port. Look for '16450' or '16C450' on the big rectangular chip. This works with 2400 and 9600 bps and may work with 19200 bps as well (depending on the SNIB date). DIP switch settings for this are:

SW5	ON	OFF (default)	OFF	ON	ON
SW6	OFF	OFF (default)	ON	OFF	ON
Baud Rate	19,200	9600	2400	1200 (old)	300 (old)

Current production SNIBs have a '16550' or '16C550' serial port processor. Look for '16550' or '16C550' on the big rectangular chip. This configuration should work on all three baud rates.

SW5	ON	OFF (default)	OFF	ON
SW6	OFF	OFF (default)	ON	ON
Baud Rate	19,200	9600	2400	300

DIGI*TRAC 7.0 supports 19,200 bps SCRAMBLE*NET. This means that while 9600 and 2400 are supported by both the 1200 and 300 baud rates are supported by the older SNIB.

To do this, set the SNIB DIP switch 5 (the third one on the second set of dip switches) to ON, and set the Test Tool or equivalent host software (or Xbox) to 19200 bps

Note: All Controllers on the network must have the same baud rate setting.

If you're using an Xbox with your controllers, the SNIB baud rate on all controllers must match the XBox's 'Net Speed' baud rate. Current production XBoxes only allow 2400 or 9600 bps baud rates. When changing baud rates, you must stop and restart all controllers on the network as well as all XBoxes.

SW7 - SW12 SW7-12 are used to set the Network Address. Each switch represents a binary value in this way:

Switch	7	8	9	10	11	12
Value	32	16	8	4	2	1

The only exception to this scheme is Network Address 64 where SW7-12 are all OFF. (This is currently not supported by SAM.) Table 7-5 provides a complete list of all network addresses and their corresponding switch setup:

Address	SW7	SW8	SW9	SW10	SW11	SW12
1	OFF	OFF	OFF	OFF	OFF	ON
2	OFF	OFF	OFF	OFF	ON	OFF
3	OFF	OFF	OFF	OFF	ON	ON
4	OFF	OFF	OFF	ON	OFF	OFF
5	OFF	OFF	OFF	ON	OFF	ON
6	OFF	OFF	OFF	ON	ON	OFF
7	OFF	OFF	OFF	ON	ON	ON
8	OFF	OFF	ON	OFF	OFF	OFF
9	OFF	OFF	ON	OFF	OFF	ON
10	OFF	OFF	ON	OFF	ON	OFF
11	OFF	OFF	ON	OFF	ON	ON
12	OFF	OFF	ON	ON	OFF	OFF
13	OFF	OFF	ON	ON	OFF	ON

Table 7-5: SNIB DIP Switch Network Address Settings

Address	SW7	SW8	SW9	SW10	SW11	SW12
14	OFF	OFF	ON	ON	ON	OFF
15	OFF	OFF	ON	ON	ON	ON
16	OFF	ON	OFF	OFF	OFF	OFF
17	OFF	ON	OFF	OFF	OFF	ON
18	OFF	ON	OFF	OFF	ON	OFF
19	OFF	ON	OFF	OFF	ON	ON
20	OFF	ON	OFF	ON	OFF	OFF
21	OFF	ON	OFF	ON	OFF	ON
22	OFF	ON	OFF	ON	ON	OFF
23	OFF	ON	OFF	ON	ON	ON
24	OFF	ON	ON	OFF	OFF	OFF
25	OFF	ON	ON	OFF	OFF	ON
26	OFF	ON	ON	OFF	ON	OFF
27	OFF	ON	ON	OFF	ON	ON
28	OFF	ON	ON	ON	OFF	OFF
29	OFF	ON	ON	ON	OFF	ON
30	OFF	ON	ON	ON	ON	OFF
31	OFF	ON	ON	ON	ON	ON
32	ON	OFF	OFF	OFF	OFF	OFF
33	ON	OFF	OFF	OFF	OFF	ON
34	ON	OFF	OFF	OFF	ON	OFF
35	ON	OFF	OFF	OFF	ON	ON
36	ON	OFF	OFF	ON	OFF	OFF
37	ON	OFF	OFF	ON	OFF	ON
38	ON	OFF	OFF	ON	ON	OFF
39	ON	OFF	OFF	ON	ON	ON
40	ON	OFF	ON	OFF	OFF	OFF
41	ON	OFF	ON	OFF	OFF	ON
42	ON	OFF	ON	OFF	ON	OFF
43	ON	OFF	ON	OFF	ON	ON
44	ON	OFF	ON	ON	OFF	OFF
45	ON	OFF	ON	ON	OFF	ON
46	ON	OFF	ON	ON	ON	OFF
47	ON	OFF	ON	ON	ON	ON
48	ON	ON	OFF	OFF	OFF	OFF
49	ON	ON	OFF	OFF	OFF	ON

Table 7-5: SNIB DIP Switch Network Address Settings (Continued)

Address	SW7	SW8	SW9	SW10	SW11	SW12
50	ON	ON	OFF	OFF	ON	OFF
51	ON	ON	OFF	OFF	ON	ON
52	ON	ON	OFF	ON	OFF	OFF
53	ON	ON	OFF	ON	OFF	ON
54	ON	ON	OFF	ON	ON	OFF
55	ON	ON	OFF	ON	ON	ON
56	ON	ON	ON	OFF	OFF	OFF
57	ON	ON	ON	OFF	OFF	ON
58	ON	ON	ON	OFF	ON	OFF
59	ON	ON	ON	OFF	ON	ON
60	ON	ON	ON	ON	OFF	OFF
61	ON	ON	ON	ON	OFF	ON
62	ON	ON	ON	ON	ON	OFF
63	ON	ON	ON	ON	ON	ON
64[a]	OFF	OFF	OFF	OFF	OFF	OFF

Table 7-5: SNIB DIP Switch Network Address Settings (Continued)

a. Velocity software does not recognize Address 64.

SNIB Mounting

The SNIB should always be the top board installed on the standoffs. Install all other boards first (underneath the SNIB), then the SNIB.

To install the SNIB expansion board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Install the board on the supplied standoffs and connect the EBIC5 cable as described in “Connecting Expansion Boards” on page 7-13.

SNIB Wiring

To connect SCRAMBLE*NET to this board:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Connect the wires on one end of the cable to the terminal block you require – either the RS-232 or S*NET (RS-485) port. Both RS-232 and RS-485 use SCRAMBLE*NET protocol. If necessary, you can remove the terminal blocks and replace them after you’ve wired them.

The wires are connected in this way:

*For RS-485 S*NET Cabling*:

Terminal	5	4	3	2	1
Wire	G	-RX	+RX	-TX	+TX

For RS-232 Cabling:

Terminal	4	3	2	1
Wire	G	RX	TX	V

3. Connect the other end of the cable to the RS-485 of a NET*ADAPT, NET*MUX4, or to the serial port of the PC (with NAPC installed).

SNIB Pinout Information

The following tables provide pinout information on connections between the SNIB and a number of devices and connectors.

NAPC to First SNIB		**NA1 to First SNIB**	
Pin on NAPC	**Pin On SNIB**	**Pin on NA1**	**Pin on SNIB**
1 RX+	1 TX+	1 RX+	1 TX+
2 RX–	2 TX–	2 RX–	2 TX–
3 TX+	3 RX+	3 TX+	3 RX+
4 TX–	4 RX–	4 TX–	4 RX–
5 G	5 G	5 G	5 G

XBox to First SNIB (RS-485)		**XBox to First SNIB (RS-232)**	
Pin on XBox	**Pin On SNIB**	**Pin on XBox**	**Pin on SNIB**
1 RX+	1 TX+	Unused	1 V
2 RX–	2 TX–	1 RX	2 TX
3 TX+	3 RX+	2 TX	3 RX
4 TX–	4 RX–	3 G	5 G
5 G	5 G		

NET*MUX4 to SNIB (RS-485)		**NET*MUX4 to SNIB (RS-232)**	
Pin on NET*MUX4	**Pin On SNIB**	**Pin on NET*MUX4**	**Pin on SNIB**
1 RX+	1 TX+	Unused	1 V
2 RX–	2 TX–	2 RX	2 TX
3 TX+	3 RX+	3 TX	3 RX
4 TX–	4 RX–	4 G	4 G
5 G	5 G		

COM Port (DB25F) to First SNIB		COM Port (DB9F) to First SNIB	
Pin on DB25F	**Pin On SNIB**	**Pin on DB9F**	**Pin on SNIB**
Unused	1 V	Unused	1 V
2 RX	2 TX	2 RX	2 TX
3 TX	3 RX	3 TX	3 RX
7 G	4 G	5 G	4 G

Modem (DB9M) to SNIB		Modem (DB25M) to SNIB	
Pin on DB9M	**Pin On SNIB**	**Pin on DB25M**	**Pin on SNIB**
Unused	1 V	Unused	1 V
2 RX	2 TX	3 RX	2 TX
3 TX	3 RX	2 TX	3 RX
5 G	4 G	7 G	4 G

Wiring Between SNIB	
Pin on SNIB	**Pin On SNIB**
1 TX+	1 TX+
2 TX-	2 TX-
3 RX+	3 RX+
4 RX-	4 RX-
5 G	5 G

SNIB Testing

After installing the board and connecting to a PC, you can test the SNIB using Host PC software.

Installing the SNIB2

This section includes setup and installation instructions for the SNIB2.

Note: The first three steps of the following procedure only apply if you are replacing original SNIB boards with newer SNIB2 boards.

To install the SNIB2:

1. If necessary, download CCM 7.3.08 or later firmware to the required controllers.

   For instructions about doing this, refer to “Firmware Updates > Updating CCM Firmware” in the main Velocity help.

2. Make sure each controller in the sequence shows the CCM version as 7.3.08 or later, and the BIOS as Version 7.2.19 or later.

   If these version numbers do not appear, replace the controller’s CCM.

3. Pull the original SNIBs from each required controller.

Hint We recommend removing the SNIBs controller-by-controller to ensure that each SNIB2 comes online successfully.

4. Run the required network cable to the controller(s) with the master SNIB2s.

   The Ethernet cable you are connecting to each master SNIB2 should be connected to the Velocity host through a hub or switch.

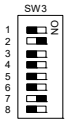
5. Run RS-485 cable downstream from the master SNIB2.

   The run between the master SNIB2 and the second SNIB2 should be wired according to the instructions in "SNIB2 Cabling" starting on page 7-53.

6. Set the DIP switches on each SNIB2, which vary depending on whether it is the master, one in the middle, or the last one.

   In general, use the settings shown in the following tables.

Bank	Switch	Setting	Comments
Master SNIB2:			
SW1	S1-S4	all **ON**	Indicates this is the first/master SNIB2 (or the last one) in the run
SW2	S1	OFF	The SNIB2 communicates with the Velocity host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. Because this is the master SNIB2, you must also 'Reset Encryption' on the Velocity Port settings. All downstream units must have their encryption keys reset as well.
	S2-S3	OFF	Normal operation. (These switches should only be ON when resetting this SNIB2 to the factory default settings; see "Resetting the SNIB2 to its Factory Default Values" on page 7-68.)
	S4	ON	This SNIB2 is first in the sequence (the master) and is connected to the host via Ethernet or direct RS-232 connection (not dial-up). This SNIB2 controls polling.
SW3	S1 S2	OFF ON	Set downstream RS-485 speed (38400 in this example)
	S3-S8	—	Address as required (Address 1 shown)



Bank	Switch	Setting	Comments
SNIB2s in the middle:			
SW1	S1-S4	all OFF	Indicates this SNIB2 is in the middle of the run
SW2	S1	OFF	The SNIB2 communicates with the Velocity host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. All downstream units must have their encryption keys reset as well. Because this is a downstream unit, the master SNIB2 automatically detects that the keys have been reset.
	S2-S3	OFF	Normal operation. (These switches should only be ON when resetting this SNIB2 to the factory default settings; see “Resetting the SNIB2 to its Factory Default Values” on page 7-68.)
	S4	OFF	This SNIB2 is not the first/master (or you only have one controller)
SW3	S1 S2	OFF ON	Set downstream RS-485 speed (38400 in this example)
	S3-S8	—	Address as required (Address 2 shown)

Bank	Switch	Setting	Comments
Last SNIB2 in run:			
SW1	S1-S4	all ON	Indicates this is the last SNIB2 (or the first/master) in the run
SW2	S1	OFF	The SNIB2 communicates with the Velocity host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. All downstream units must have their encryption keys reset as well. Because this is a downstream unit, the master SNIB2 automatically detects that the keys have been reset.
	S2-S3	OFF	Normal operation. (These switches should only be ON when resetting this SNIB2 to the factory default settings; see "Resetting the SNIB2 to its Factory Default Values" on page 7-68.)
	S4	OFF	This SNIB2 is not the first/master (or you only have one controller)
SW3	S1 S2	OFF ON	Set downstream RS-485 speed (38400 in this example)
	S3-S8	—	Address as required (Address 3 shown)

Refer to "Setting Up the SNIB2" on page 7-54 for more configuration options.

7. Install the new SNIB2s into their controllers. For detailed instructions, see "SNIB2 Mounting" starting on page 7-53.

Warning: Handle the SNIB2 with care. The board is very sensitive to static discharges. Observe the normal anti-static precautions by using grounded wrist straps and anti-static devices when installing the board.

8. Plug the RJ-45 connector from the cable into the Ethernet connector on the SNIB2.
9. Connect the RS-485 cables to their respective SNIB2.
10. Reconnect and power up the controllers.
11. At the host, open Velocity and configure the new SNIB2s.

    For more about this, refer to your Velocity documentation.

SNIB2 Mounting

To mount the SNIB2 expansion board:

1. Turn all system power off: remove the connector for the standby battery, and then disconnect the AC power connector or the power supply fuse.
2. Install the new SNIB2 board into the upper left corner of the enclosure using the supplied screws. If there are additional expansion boards to install, install them first using the supplied standoffs. Install the SNIB2 board last so that it is at the top of the stack, as shown in Figure 7-25. (This enables you to wire the board, configure its DIP switches, view the status LEDs, and more easily access the Ethernet connector.)

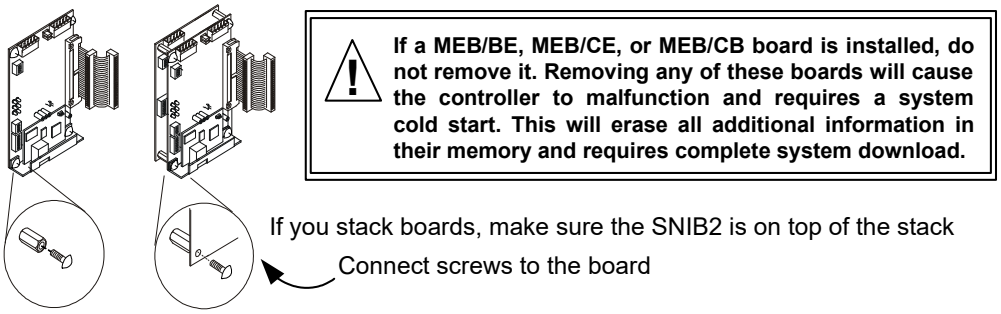


Figure 7-25: Putting the SNIB2 on top of the expansion boards stack

3. Connect the EBIC5 connector, as described in "Connecting Expansion Boards" starting on page 7-13.
4. Reconnect the AC power connector (or power supply fuse), then reconnect the standby battery connector. The controller board's yellow test LED should light; the other lights go through a start up sequence. When the sequence is complete, the yellow test LED goes out and the other lights stabilize.
5. If required, connect an RJ-45 network cable to the SNIB2 Ethernet connector.

SNIB2 Cabling

The cable linking the first controller (master) to the second (subordinate) in a multi-dropped RS-485 series must crossover the RX± and TX± wires in this manner:

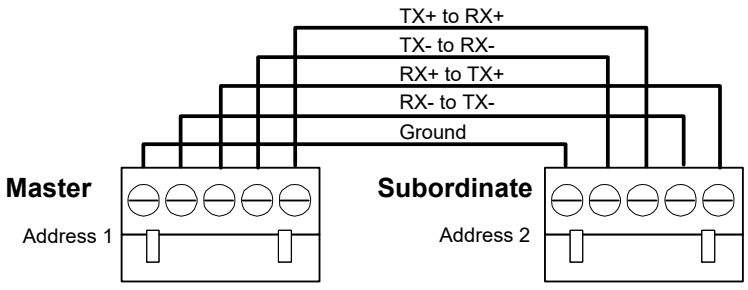


Figure 7-26: Master-to-Subordinate SNIB2 Wiring in Simple Array

If more than two controllers are connected in the series, the wiring would look like this:

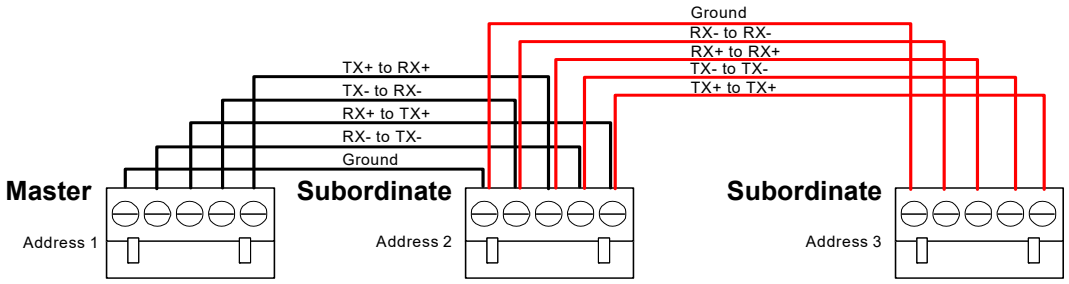


Figure 7-27: Master-to-Subordinate SNIB2 Wiring in Multiple Array

At 9600 baud, the maximum allowed cable run between controllers is shown in the following table:

Connection	Maximum Distance
Total Max. Run from Master to Last Downstream SNIB2	4000 feet (1,220 m.)

In general, communications become less robust as baud rates increase, wire gauge decreases, and distances increase. For this reason, it may not be possible to implement the higher baud rates supported by the SNIB2 if you have long wire runs or small wire gauges.

Higher baud rates are also more dependent on the number of twists per foot, so capacitance specifications must be strictly adhered to: total wire run per port is not to exceed acceptable capacitance of 11-17 p*f* and a total of 100,000 p*f*.

Hint We recommend using Cat5/Cat6 cable for your cable runs. Use 1 pair for the RX pair, 1 pair for the TX pair, and 1 conductor or pair for the ground connection.

Setting Up the SNIB2

The SNIB2 includes three DIP switch banks. The first bank (SW1) and second bank (SW2) have four DIP switches each. The third bank (SW3) possesses eight DIP switches.

Switch Bank 1 (SW1)

SNIB2s can be used throughout a multidrop run; however, you must specify whether a specific SNIB2 is connected to a controller that is in the beginning, middle, or at the end of a run.

To do this, set S1-S4 on switch bank SW1 to all ON or all OFF in this way:

S1-S4	OFF	This SNIB2 is in the middle of a multidrop sequence.
	ON	This SNIB2 is either the first (master) or last (termination) one in the multidrop sequence.

Switch Bank 2 (SW2)

The second switch bank at SW2 has 4 switches which configure such properties as the type of XNET protocol you are using, and the SNIB2's location in the multidrop run.

S1	OFF	The SNIB2 communicates with the host PC in XNET 2, using the encryption keys stored in memory.
	ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. If this is the master SNIB2, you must also 'Reset Encryption' on the Velocity Port settings. All downstream units must have their encryption keys reset as well. If this is a downstream unit, the master SNIB2 automatically detects that the keys have been reset.
S2-S3	OFF	Normal operation.
	ON	These switches should only be ON when resetting this SNIB2 to the factory default settings; see "Resetting the SNIB2 to its Factory Default Values" on page 7-68.
S4	OFF	Indicates this SNIB2 is NOT first in the multidrop sequence, or you only have one controller.
	ON	Indicates this SNIB2 is first in the sequence (master), and is connected to the host via Ethernet or direct RS-232 connection (not dial-up). This SNIB2 controls polling.

Switch Bank 3 (SW3)

Switch bank SW3 is used to specify the SNIB2 speed (S1-S2) and the SNIB2 address (S3-S8). DIP switch settings for this are:

S1	OFF	OFF	ON	ON
S2	OFF	ON	OFF	ON
Baud Rate	9,600	38,400	57,600	115,200

This controls the baud rate for the RS-485 multi-drop line and the RS-232 connection. 57,600 and 115,200 bps are only available if your RS-485 cables are made from Cat5/Cat6 data grade wire. These speeds are not recommended for installations using:

- ❑ RS-232 connections to host
- ❑ 18-gauge to 22-gauge shielded twisted-pair cable
- ❑ NET*MUX4s
- ❑ Mixed SNIBs/SNIB2s

Baud rates only apply to the SNIB2's RS-485 and RS-232 ports. The SNIB2's Ethernet port is used for host-to-controller connections and runs at 10/100 BaseT speeds. All SNIBs/SNIB2s in an RS-485 multi-drop sequence must be set to the same speed, and if connected to a host PC using RS-232 direct connection, the same speed must also be used. For example, if one SNIB2 in the sequence is set to 9600, all other SNIBs and SNIB2s (and the RS-232 host connection, if used) must be set to the same baud rate.

The remaining DIP switches on SW3 set the SNIB2's address:

Address	SW3	SW4	SW5	SW6	SW7	SW8
1	OFF	OFF	OFF	OFF	OFF	**ON**
2	OFF	OFF	OFF	OFF	**ON**	OFF
3	OFF	OFF	OFF	OFF	**ON**	**ON**
4	OFF	OFF	OFF	**ON**	OFF	OFF
5	OFF	OFF	OFF	**ON**	OFF	**ON**
6	OFF	OFF	OFF	**ON**	**ON**	OFF
7	OFF	OFF	OFF	**ON**	**ON**	**ON**
8	OFF	OFF	**ON**	OFF	OFF	OFF
9	OFF	OFF	**ON**	OFF	OFF	**ON**
10	OFF	OFF	**ON**	OFF	**ON**	OFF
11	OFF	OFF	**ON**	OFF	**ON**	**ON**
12	OFF	OFF	**ON**	**ON**	OFF	OFF
13	OFF	OFF	**ON**	**ON**	OFF	**ON**
14	OFF	OFF	**ON**	**ON**	**ON**	OFF
15	OFF	OFF	**ON**	**ON**	**ON**	**ON**
16	OFF	**ON**	OFF	OFF	OFF	OFF
17	OFF	**ON**	OFF	OFF	OFF	**ON**
18	OFF	**ON**	OFF	OFF	**ON**	OFF
19	OFF	**ON**	OFF	OFF	**ON**	**ON**
20	OFF	**ON**	OFF	**ON**	OFF	OFF
21	OFF	**ON**	OFF	**ON**	OFF	**ON**
22	OFF	**ON**	OFF	**ON**	**ON**	OFF
23	OFF	**ON**	OFF	**ON**	**ON**	**ON**
24	OFF	**ON**	**ON**	OFF	OFF	OFF
25	OFF	**ON**	**ON**	OFF	OFF	**ON**
26	OFF	**ON**	**ON**	OFF	**ON**	OFF
27	OFF	**ON**	**ON**	OFF	**ON**	**ON**
28	OFF	**ON**	**ON**	ON	OFF	OFF
29	OFF	**ON**	**ON**	**ON**	OFF	**ON**
30	OFF	**ON**	**ON**	**ON**	**ON**	OFF
31	OFF	**ON**	**ON**	**ON**	**ON**	**ON**
32	**ON**	OFF	OFF	OFF	OFF	OFF
33	**ON**	OFF	OFF	OFF	OFF	**ON**
34	**ON**	OFF	OFF	OFF	**ON**	OFF
35	**ON**	OFF	OFF	OFF	**ON**	**ON**

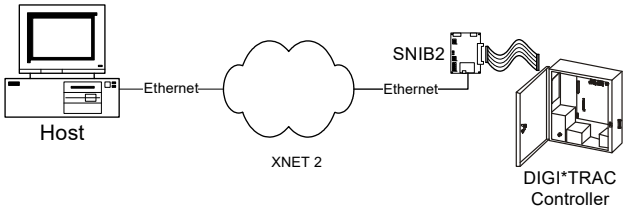
Table 7-6: SNIB2 DIP Switch Address Settings

Address	SW3	SW4	SW5	SW6	SW7	SW8
36	**ON**	OFF	OFF	**ON**	OFF	OFF
37	**ON**	OFF	OFF	**ON**	OFF	**ON**
38	**ON**	OFF	OFF	**ON**	**ON**	OFF
39	**ON**	OFF	OFF	**ON**	**ON**	**ON**
40	**ON**	OFF	**ON**	OFF	OFF	OFF
41	**ON**	OFF	**ON**	OFF	OFF	**ON**
42	**ON**	OFF	**ON**	OFF	**ON**	OFF
43	**ON**	OFF	**ON**	OFF	**ON**	**ON**
44	**ON**	OFF	**ON**	**ON**	OFF	OFF
45	**ON**	OFF	**ON**	**ON**	OFF	**ON**
46	**ON**	OFF	**ON**	**ON**	**ON**	OFF
47	**ON**	OFF	**ON**	**ON**	**ON**	**ON**
48	**ON**	**ON**	OFF	OFF	OFF	OFF
49	**ON**	**ON**	OFF	OFF	OFF	**ON**
50	**ON**	**ON**	OFF	OFF	**ON**	OFF
51	**ON**	**ON**	OFF	OFF	**ON**	**ON**
52	**ON**	**ON**	OFF	**ON**	OFF	OFF
53	**ON**	**ON**	OFF	**ON**	OFF	**ON**
54	**ON**	**ON**	OFF	**ON**	**ON**	OFF
55	**ON**	**ON**	OFF	**ON**	**ON**	**ON**
56	**ON**	**ON**	**ON**	OFF	OFF	OFF
57	**ON**	**ON**	**ON**	OFF	OFF	**ON**
58	**ON**	**ON**	**ON**	OFF	**ON**	OFF
59	**ON**	**ON**	**ON**	OFF	**ON**	**ON**
60	**ON**	**ON**	**ON**	**ON**	OFF	OFF
61	**ON**	**ON**	**ON**	**ON**	OFF	**ON**
62	**ON**	**ON**	**ON**	**ON**	**ON**	OFF
63	**ON**	**ON**	**ON**	**ON**	**ON**	**ON**

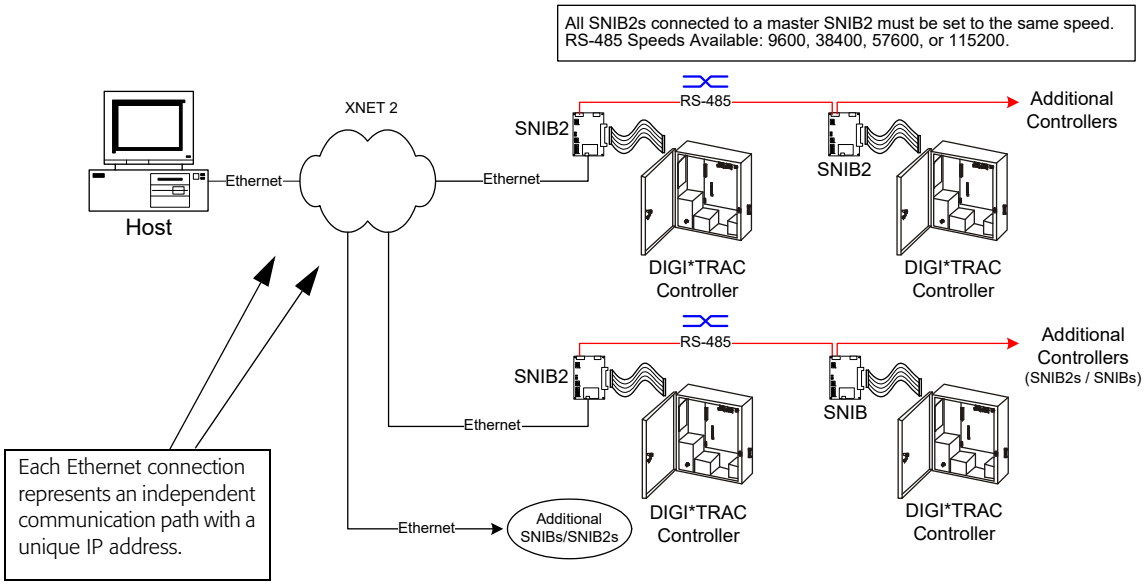
Table 7-6: SNIB2 DIP Switch Address Settings (Continued)

SNIB2 Network Configuration Options

The SNIB2's Ethernet port provides high-speed TCP/IP communication over an Ethernet network between the host computer and the controller.



In a multiple controller sequence, the configuration can look like this example:



= this cable segment swaps the RX± and TX± wires.; see "SNIB2 Cabling" on page 7-53.

This enables communication between the controller with the master SNIB2 and host PC at 10/100BaseT. Speeds between the master SNIB2 and other connected downstream SNIB2s range up to 115200 bps when using Cat5/Cat6 cable. Speeds between a master SNIB2 and downstream SNIBs are limited by the top speed of the older SNIBs (38400 bps).

Higher baud rates are also more dependent on the number of twists per foot, so capacitance specifications must be strictly followed: total wire run per port is not to exceed acceptable capacitance of 11-17 p*f* and a total of 100,000 p*f*.

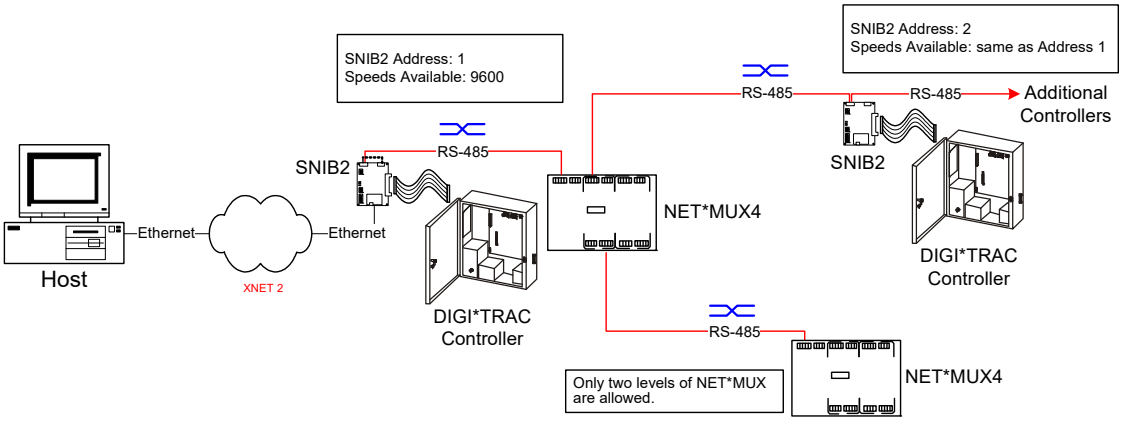
Before the Velocity server can communicate over Ethernet with a SNIB2, you must first configure the SNIB2 through Velocity. For more about this, refer to "Configuring a Master SNIB2 on the Same Subnet" starting on page 7-61.

Whenever an Ethernet connection is employed between the host and the SNIB2, Velocity views the SNIB2 as an XNET port because the SNIB2 includes XBox functionality. The host communicates with the Ethernet-connected SNIB2 using AES-encrypted XNET 2.

Controller-to-controller speeds range from 9600 to 115200 bps. For each string of controllers, the first (master) SNIB2 with the Ethernet connection must be assigned the same address as the XBox port.

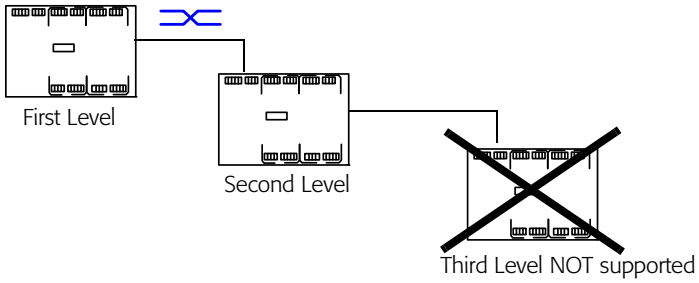
When the host is connected to a SNIB2 using Ethernet, Velocity views the first (master) SNIB2 as both a DIGI*TRAC controller and an XBox residing on an XNET port. Subsequent multidropped controllers in the sequence do not appear as XBox controllers.

You can also use the SNIB2 with the NET*MUX4. The NET*MUX4 consists of a single input for either RS-232 or RS-485 and four outputs to which a series of controllers or additional NET*MUX4s can be wired, as shown in the following illustration:



= this cable segment swaps the RX± and TX± wires.; see "SNIB2 Cabling" on page 7-53.

If required, you can add a second level of NET*MUX4s to create additional controller runs; however, Hirsch does not support more than two levels of NET*MUX4s.



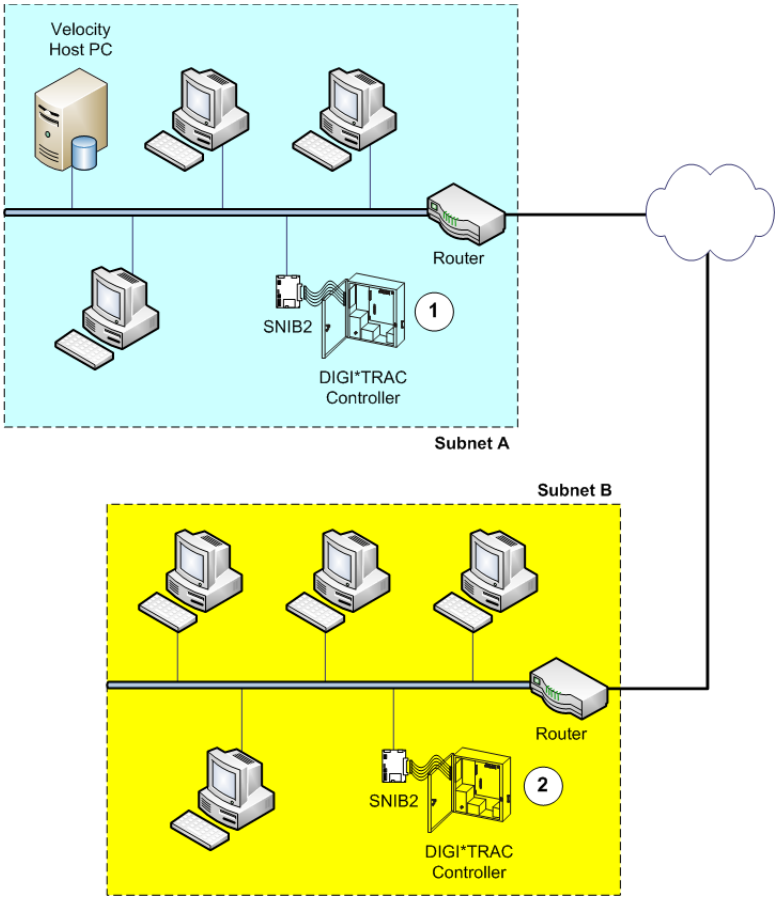
NET*MUX4 speeds are dictated by wire gauge and distance. We recommend using Cat5/Cat6 cable.

Deploying the SNIB2

Each master SNIB2 (Velocity port) must be assigned a unique IP address so it can communicate with Velocity on the host PC. Depending on the network location of the master SNIB2, this is accomplished in one of two ways:

- ❑ If the SNIB2 is located within the same subnet as the host PC, then you can use Velocity to assign the IP address. For more about this, refer to "Configuring a Master SNIB2 on the Same Subnet" on page 7-61.
- ❑ If the master SNIB2 is located outside the host PC's subnet, you must use the SNIB2 Configuration Utility. For more about this, refer to "Configuring a Master SNIB2 in a Different Subnet" on page 7-64.

What is a subnet? Put simply, a subnet is any group of PCs and other devices, such as printers and scanners, connected by network cable to a network router. Anything behind the router is considered part of the subnet. Anything beyond this router is not part of the subnet.



In the preceding illustration, the master SNIB2 and controller labeled 1 is located in the same subnet as the host PC (Subnet A). This SNIB2 can therefore be configured using Velocity; however, the master SNIB2 and controller labeled 2 is located behind a different router, in a different subnet (Subnet B), and must be configured using the SNIB2 Configuration Utility.

Any number of computers and devices can be behind a single router, but for reasons of security and speed, a company network often incorporates many routers. It isn't uncommon to find that each department within a company has its own router. Routers not only find the quickest way to ferry packets of information between two points, but also could serve as a rudimentary firewall against potential intrusion.

Configuring a Master SNIB2 on the Same Subnet

When a master SNIB2 is connected via Ethernet to the host PC sharing the same subnet, configure and assign a new IP address through the Velocity port properties dialog.

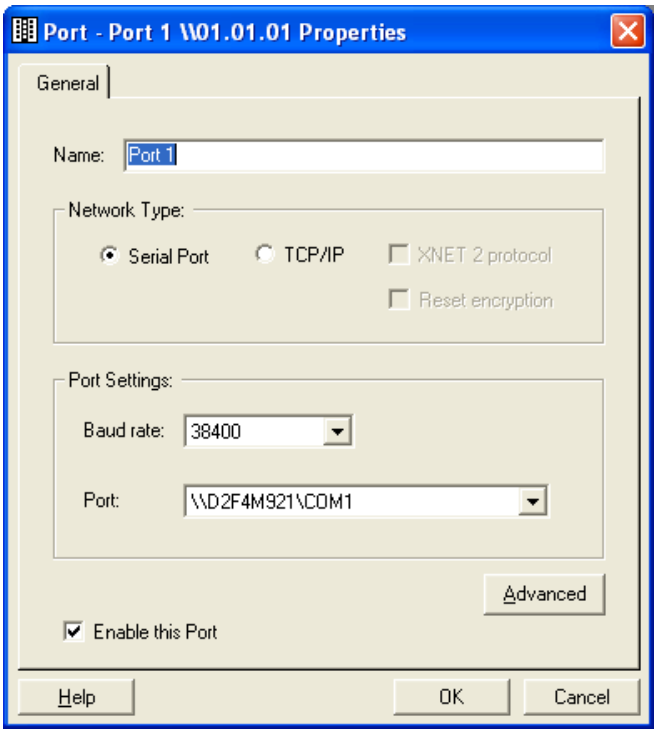
To do this:

1. Open Velocity.
2. In the System Tree pane, click and expand the DIGI*TRAC Configuration system folder, .

   Three port folders are currently available: SNET, XNET, or Dial-Up.
3. Expand the XNET Port folder.

   When the Velocity host is connected to a SNIB2 via Ethernet, it treats it as an XNET port.
4. Double-click **Add New XNET Port** in the Components pane.

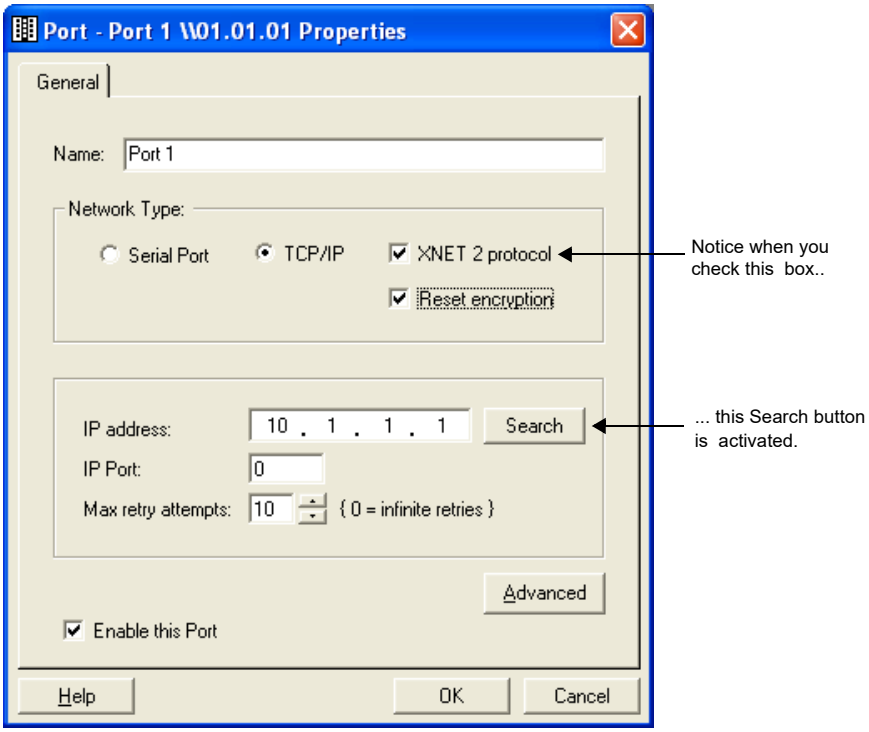
   The Port Properties dialog appears:



5. Click to select the **TCP/IP** radio button.

   The dialog changes to show the ‘IP Address’, ‘Port’, and ‘Max Attempts’ fields.

6. Check the **XNET 2 Protocol** checkbox, to indicate this port is using encrypted XNET 2 protocol.

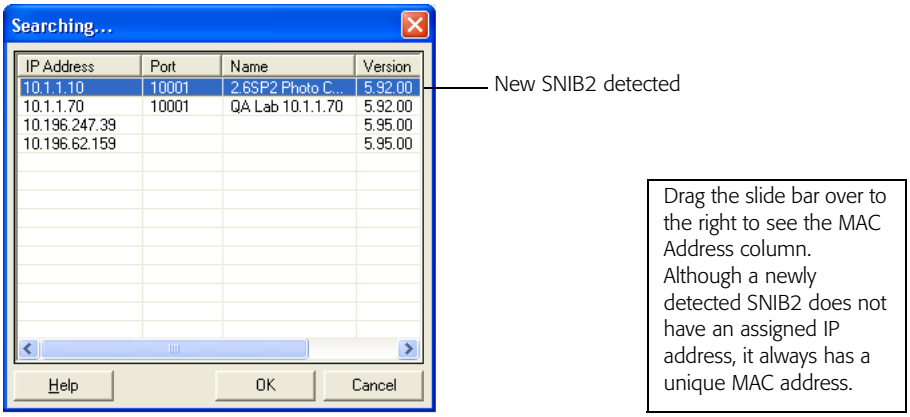


7. Click the **Search** button.

   Velocity searches on the subnet for all SNIB2s that Velocity is not using.

Note: If a SNIB2 is currently logged on, the search feature will not detect it.

A dialog listing all new SNIB2s appears:



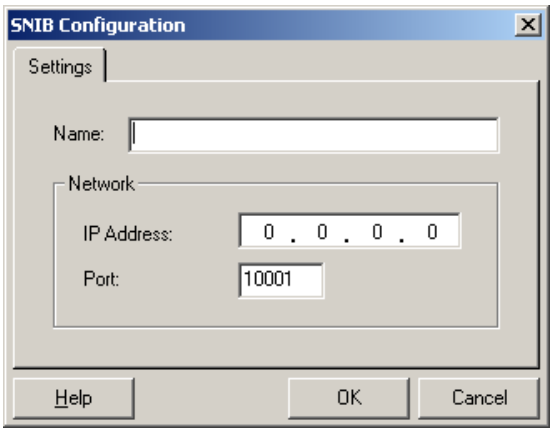
Drag the slide bar over to the right to see the MAC Address column. Although a newly detected SNIB2 does not have an assigned IP address, it always has a unique MAC address.

Because all SNIB2 MAC addresses start with the same six digits (00:90:C2), the label on the SNIB2 only lists the last six digits.

Although a newly-detected SNIB2 does not possess an IP address, port number, or name, it should have a unique MAC address. To see this MAC address, drag the slide bar at the bottom of the dialog to the right. The MAC address for each SNIB2 is printed on a white label located on the left side of the SNIB2's daughterboard. This label contains both a barcode and a six-digit number. This number is the last six digits of the MAC address.

8. From this list, double-click the SNIB2 entry you want to configure.

   The SNIB Configuration dialog appears:



9. In the ‘Name’ field, enter the name you want to assign to the SNIB2.
10. In the ‘IP Address’ field, enter the IP address for the SNIB2 connected to this Velocity PC.

    In version 5.95 and later, all SNIB2s have a factory default IP address in the format 10.*x.y.z* where the variables are supplied from a hash of the MAC address. For versions earlier than that, you must enter the required IP address.
11. In the ‘Port’ field, enter the correct port number.

    All network ports possess an address used to identify the SNIB2’s physical port address. The default Velocity port is **10001**.

Note: Consult your system administrator for the correct values for both the IP and port address.

12. Click **OK**. The Searching screen reappears.
13. Click **OK**.

    The Port Properties screen reappears with the Name, IP Address, and IP Port fields populated.
14. In the ‘Max retry attempts’ field, specify the maximum number of retries this PC will attempt. Increment or decrement the value using the counter buttons.

    If you get port errors, increase this number.
15. Check the ‘Enable this Port’ box if this port is currently active. Clear this box if the port is not currently active.
16. If required, click the **Advanced** button to access the Advanced Settings dialog to specify additional options for this port.
17. When you’re finished, click **OK**.

The new SNIB2 port appears in the Components pane.

Note: If you ever need to reassign an IP address, repeat this procedure.

Configuring a Master SNIB2 in a Different Subnet

To connect a master SNIB2 via Ethernet to a host PC residing outside the host PC's subnet, configure and assign a new IP address for the master SNIB2 on its own subnet using the SNIB2 Configuration Utility.

To configure a master SNIB2 using the SNIB2 Configuration Utility:

1. If you haven't already done so, install the SNIB2 Configuration Utility on a PC in the same subnet as the master SNIB2 you want to configure. To do this:
   a. Insert the Velocity CD or DVD in your PC's optical drive, or go to the *\Velocity* folder.
   b. Using Windows Explorer, navigate to the *\SNIB2* folder. The file SNIB2CONFIG.EXE should be located here.
2. Double-click **SNIB2CONFIG.EXE**.

   The SNIB2 Configuration Utility appears:

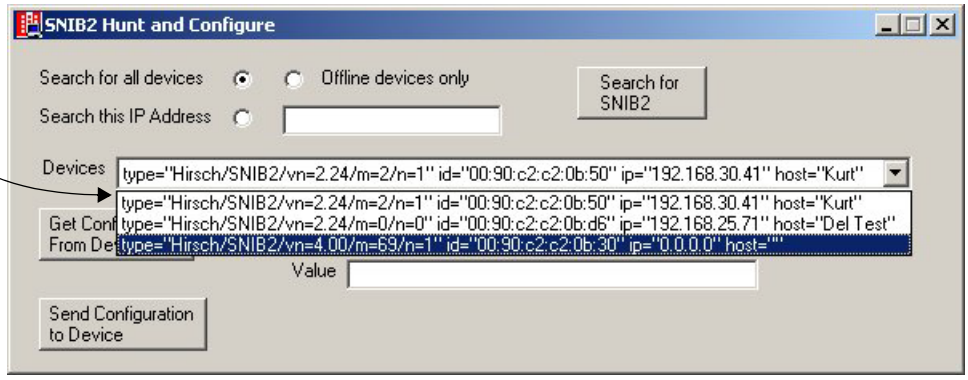
3. Select one of these radio buttons:

Search for all devices	Select this option to search for all SNIB2s on this subnet. *Note: If a SNIB2 is currently logged on, the utility will not detect it.*
Offline devices only	Select this option to search only for SNIB2s that are currently offline. It automatically eliminates all SNIB2s that are already configured for this subnet. This is the default selection.
Search this IP Address	Select this option if you know the address of the SNIB2 you are programming, then enter the SNIB2's current IP address in the field to the right of this radio button. Use this option to change the IP or port address of a previously-configured SNIB2.

4. Click the **Search for SNIB2** button.

   The utility scans the network within the current subnet, and returns a list of all devices meeting the criterion specified by the radio button.

5. Click the ‘Devices’ pick list to display all devices currently detected by the utility, like the following example:



Because all SNIB2 MAC addresses start with the same six digits (00:90:C2), the label on the SNIB2 only lists the last six digits.

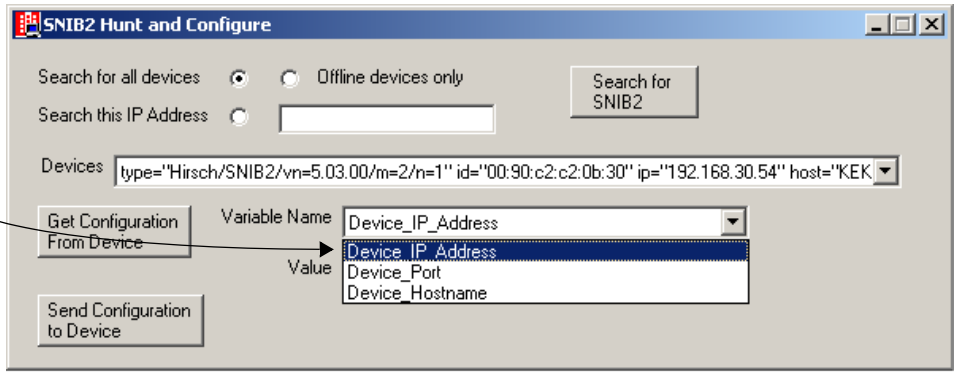
6. Select the correct SNIB2.

   You can identify which SNIB2 you need by its MAC address (id=). The MAC address for each SNIB2 is printed on a white label located on the left side of the SNIB2’s daughterboard. This label contains both a barcode and a six-digit number. This number is the second half of the MAC address.

7. Select the **Get Configuration From Device** button.

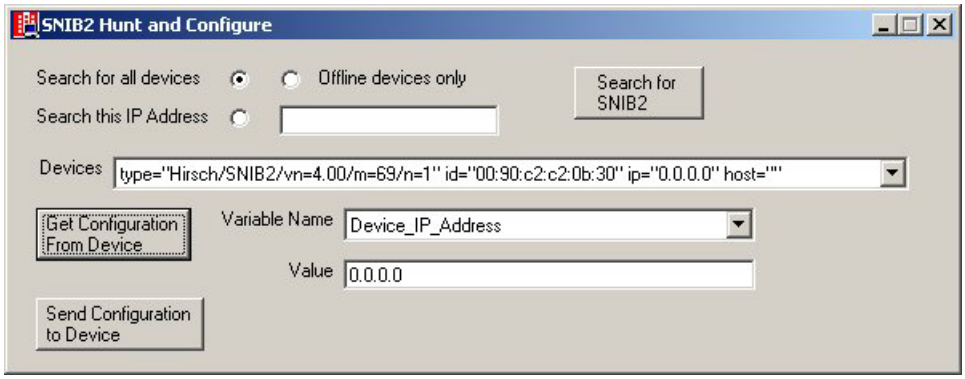
   A list of variables specific to this SNIB2 appear in the ‘Variable Name’ window.

   The three options used for SNIB2 configuration are: **Device_IP_Address**, **Device_Port**, and **Device_Hostname**, as shown in the following example:



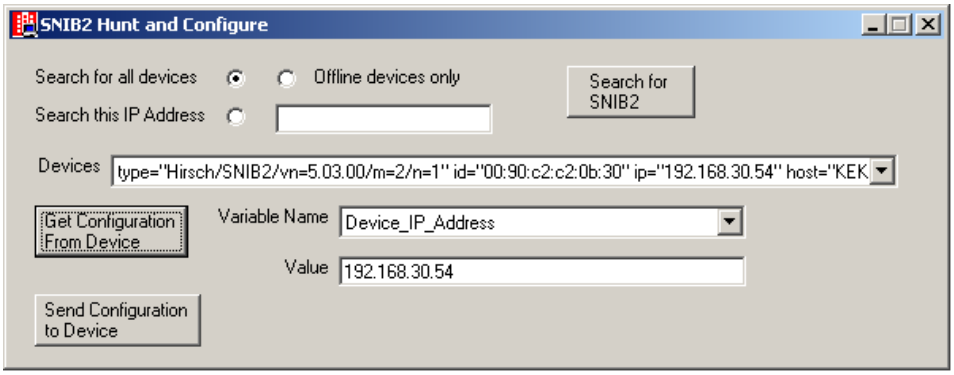
8. From the ‘Variable Name’ pick list, select **Device_IP_Address**.

   A screen like this appears:



9. In the 'Value' field, enter the IP address you require for this SNIB2.

   A screen like this appears:



   Consult your IT or Security Administrator for the proper address.

10. From the 'Variable Name' pick list, select **Device_Port**.
11. In the 'Value' field, enter a port address for this SNIB2.

    All network ports possess an address used to identify the SNIB2's physical port address. The default Velocity port is **10001**.

12. From the 'Variable Name' pick list, select **Device_Hostname**.
13. In the 'Value' field, enter a name for this SNIB2.
14. Click the **Send Configuration to Device** button to send the information to the SNIB2.
15. Click the **Search for SNIB2** button again to verify that the SNIB2 has correctly received the information.

Make sure to write down the address, port, and host name you assigned for each SNIB2. These values are required when you configure the SNIB2 in Velocity.

Hint If there are a lot of master SNIB2s to configure remotely, we recommend using a dedicated portable computer with SNIB2CONF already installed. This should enable the installer to do the job more rapidly. But be careful: make sure you are on-site when you do this. A SNIB2 does not retain its IP address for more than 5 minutes after being unplugged from a controller. If you are planning to program several SNIB2s from a controller then move them to a remote site, you probably won't have time before the IP address in each SNIB2 is irrevocably lost.

After the installer has assigned the remote master SNIB2 an IP address and port, use Velocity on the host PC to identify it to the system. To do this:

1. Create a new XNET port, as specified in Steps 1–5 of "Configuring a Master SNIB2 in a Different Subnet" on page 7-64.

Note: Do not use the Search button. This only works for finding SNIB2s that are currently residing on the host PC's subnet.

2. In the 'Name' field, enter the name you assigned to the SNIB2 using the SNIB2 Configuration Utility (Device_Hostname).
3. In the 'IP Address' field, enter the IP address you assigned to this device using the SNIB2 Configuration Utility (Device_IP_Address).

4. In the 'Port' field, enter the port number you assigned to this device using the utility (Device_Port). The default value is **10001**.
5. Make sure the 'Enable this Port' box is checked.
6. Click **OK**.

This enables Velocity to find and monitor the remote SNIB2.

Resetting SNIB2 Encryption Keys

After Velocity creates the encryption keys required for secure Host-to-SNIB2 communication, it continues to use those keys. If for some reason you need to change these keys, there are several ways to do it.

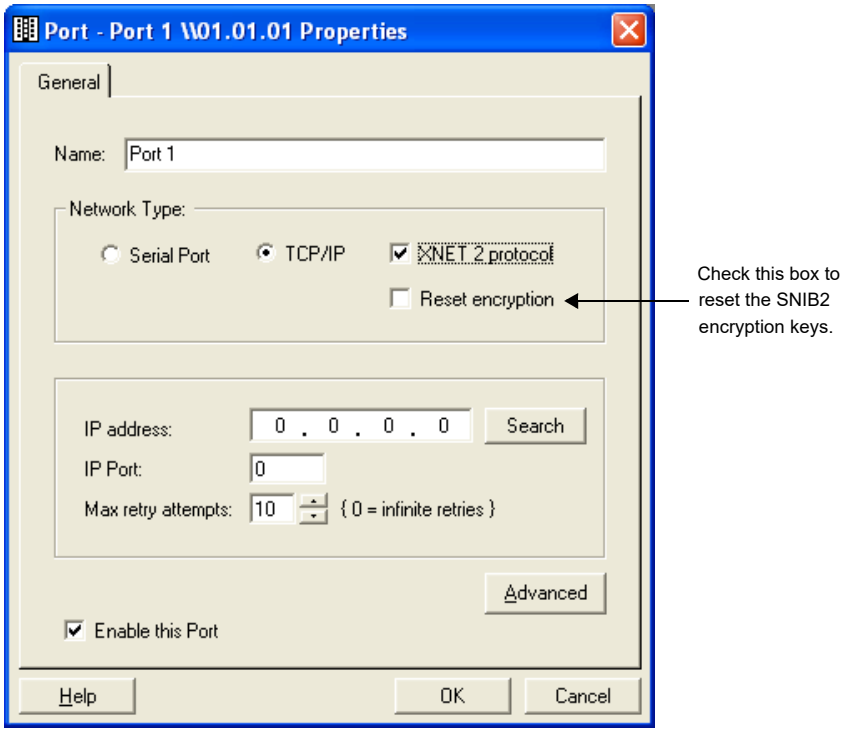
Note: Several of these techniques reset not only the SNIB2 encryption keys but also the controller.

Set SW2-1 to:	Procedures/Results
 **OFF**	• Cycle power on controller. SNIB2 retains encryption keys. Controller retains setups. • Press the blue Reset button on the controller until it resets. SNIB2 retains encryption keys. Controller loses setups. • Download SNIB2 firmware through Velocity. SNIB2 retains encryption keys. Controller retains setups.
 **ON**	• Cycle power on controller. SNIB2 resets encryption keys. Controller retains setups. • Press the blue Reset button on the controller until it resets. SNIB2 resets encryption keys. Controller loses setups. • Download SNIB2 firmware through Velocity. SNIB2 resets encryption keys. Controller retains setups.
OFF or **ON**	Download CCM firmware through Velocity. SNIB2 retains encryption keys. Controller retains setups.

After you have reset the encryption key to its default value (set SW2-1 to ON, recycle controller power, then reset SW2-1 to OFF), you must assign a new key so that Velocity and the master SNIB2 can talk to each other. To do this:

1. From the Velocity Administrator system tree, click and expand the DIGI*TRAC Configuration system folder until the master SNIB2 port you require appears.
2. Right-click on the SNIB2 port and select **Properties**.

The Port Properties dialog appears. The master SNIB2 Properties should look like this:



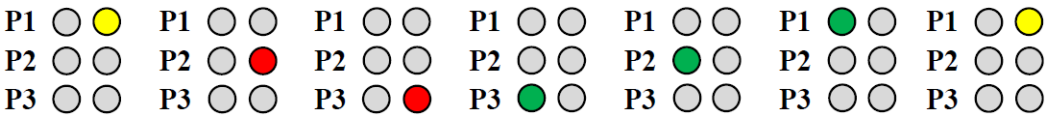
3. Check the 'Reset encryption' box, and click **OK**.

This resets and syncs the encryption key at host SNIB2.

Resetting the SNIB2 to its Factory Default Values

Starting with version 6.42 of the SNIB2 firmware, a SNIB2 board can be reset to the factory default values for its encryption keys and network settings. To reset a SNIB2 board to have an IP address based on its unique MAC address, perform the following steps:

1. Set all four DIP switches in Switch Bank 2 to ON, and set all eight DIP switches in Switch Bank 3 to OFF.
2. Cycle power to the controller containing this SNIB2 board.
3. Watch the status LEDs on the SNIB2 board, to ensure that they display the Lamp Test start up pattern, and then display the following SNIB2/CCM Synchronization pattern:

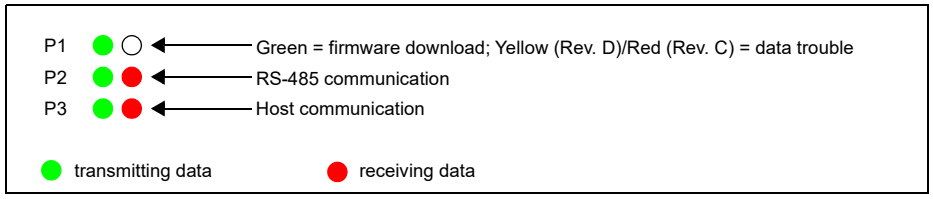


4. Turn off power to the controller.

You can then reconfigure the SNIB2 board as needed, using its DIP switches and Velocity.

Controller and SNIB2 LED Diagnostics

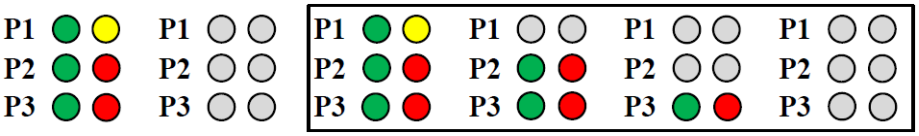
The SNIB2 has three pairs of LEDs that show you how the SNIB2 is communicating with the Velocity Server.



Special Light Patterns: Start Up

This consists of the following light patterns during start up.

First comes the **Lamp Test**.



Power-up might include the first two patterns. If you've just reflashed the SNIB2, the sequence starts with the ones in the box.

This pattern is followed by:

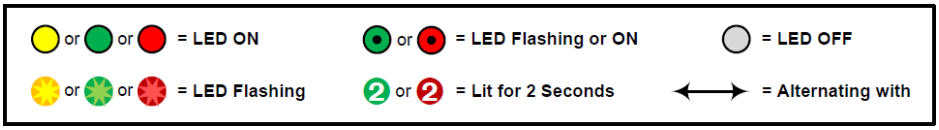
This is the **SNIB2/CCM Synchronization**. This pattern repeats until the CCM and SNIB2 are synchronized. This light pattern should not persist longer than four minutes if there are no memory expansion boards on the controller.

Normal Operation

This table illustrates the various light patterns displayed during normal operation for both the master and subordinate SNIB2s:

Master or Subordinate	
P1 P2	Ordinary communication between master and subordinates. Lights may blink or stay lit during heavy data transfers. They will go out every 4 seconds during idle or low-traffic periods; this is normal, indicating the master is hunting for new addresses, such as newly-added controllers, or controllers that went offline and are expected back online.

Legend:



Master	
P1 ○ ○ P2 ● ● P3 ● ●	This could be programming activity (downloads) or events, or both.
P1 ○ ○ P2 ● ✹ P3 ● ●	P2's red LED flashes while P2 green and P3 red and green stay lit. This normally means that the Velocity server is in the process of downloading CCM or SNIB2 firmware to one or more controllers.
P3 ✹ ✹	Heartbeat. If the P3 LED flashes appear to be about 5 seconds apart, it means the host is keeping the communication link open.
Subordinate	
P1 ○ ○ P2 ○ ✹ P3 ○ ○	The master is polling a different SNIB2. This SNIB2 ignores those polls.
P1 ○ ○ P2 ○ ● P3 ○ ○	If this stays lit and doesn't go out every 4 seconds, that means there's a lot of data going to or coming from some other controller(s). If you don't see any green flashes at all, this unit won't come online until the data traffic decreases. This pattern may also alternate with occasional red or green P3 flashes.
P1 ○ ○ P2 ✹ ● P3 ○ ○	If these stay flashing and lit, it means there is a lot of data going to or coming from several controllers. This occurs particularly when you have many controllers.
P1 ○ ○ P2 ● ● P3 ○ ○	If these stay lit, it means there is a lot of data going to or coming from this particular controller.
Legend:	
● or ● or ● = LED ON ◉ or ◉ = LED Flashing or ON ○ = LED OFF ✹ or ✹ or ✹ = LED Flashing ② or ② = Lit for 2 Seconds ⟷ = Alternating with	

For more about the status LEDs, especially for the patterns displayed during a firmware reflash or during data trouble, refer to the **SNIB2 Troubleshooting Guide** included with the SNIB2.

The SNIB2 also causes certain changes to the way the controller LEDs display as shown below:

LED Configuration	Meaning
● ○ **AC** ○ ○ **BAT** ● ○ **SYS** ○ ○ **KPD** ● ○ **NET**	The NET green LED is on; the NET red LED blinks intermittently depending on the amount of data being received from the host. This indicates the SNIB2 is working properly. *Note: The exact NET LED behavior depends on the controller version.*
● ○ **AC** ○ ○ **BAT** ● ○ **SYS** ○ ○ **KPD** ○ ○ **NET**	Neither NET LED is blinking or only the NET green LED is on. In either case, the master SNIB2 is not communicating with the host. Check both your Ethernet connection and your Velocity port configuration.

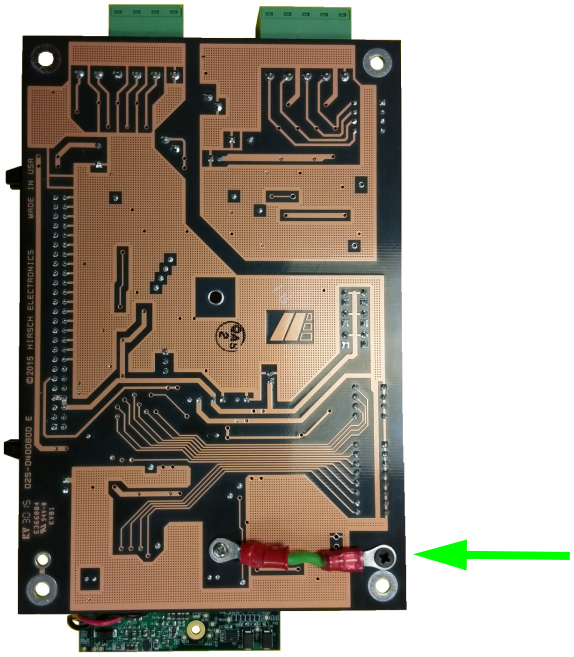
Installing and Configuring the SNIB3

This section includes installation and configuration instructions for the SNIB3.

Because the SNIB3 board is sensitive to discharges of static electricity, you must observe the normal anti-static precautions (of using grounded wrist straps and anti-static devices) when handling the board.

Providing Surge Protection for a Master SNIB3

The current version of the SNIB3 board (which has a serial number of the form SNIB3-nnnnn) includes protection against extreme power surges, such as those caused by nearby lightning strikes, which might damage the Ethernet port. This surge protection is provided on a small printed circuit board which is mounted on the underside of the communications daughterboard. The presence of the surge protection is indicated by a jumper wire on the lower back of the SNIB3's main board:



If a SNIB3 board does not have this jumper wire, then it is the initial version (sold only to a few US federal government agencies) which did not include surge protection. When using the initial version of the SNIB3 board (which has a serial number of the form SNIB3-**S**-nnnnn), surge protection must be provided for the master SNIB3 in each chain of connected controllers, using the Sankosha Guardian Net LAN-CAT5e-P+ surge protection device.

The specifications for this device are shown in the following table:

Specifications for the Guardian Net SPD			
Model			LAN-CAT5e-P+ II
Connector Type			RJ-45
Ethernet Data Rate			1000Base-T 100Base-TX 10Base-T
POE	IEEE802.3af		Yes Alternative A & B
POE Plus	IEEE802.3at		Yes Alternative A & B
Maximum Continuous Operating Voltage (Uc)			L-E 60VDC
DC Breakdown Voltage		100V/s	180-300 VDC
Voltage Protection Level (Up) 1.2/50µs 10kV			≤ 500V
Impulse Durability	Cat. C2 (8/20µs)		5kA 10 Times
	Cat. D1 (10/350µs)		2.5kA 2 Times

To be effective, this surge protection device (hereafter referred to as the "Guardian Net SPD") must be properly installed so it is securely grounded to the controller's metal enclosure. If this was not already done by Identiv, you can do it by performing the following steps.

1. Make sure the controller shows its CCM firmware version as 7.5.37 or later. (This information can be found in the controller's Properties dialog within Velocity.)

   If necessary, update the CCM firmware. For details, see the "Firmware Updates > Updating CCM Firmware" topic in the Velocity help system.

2. Power down the controller.

   a. Disconnect the battery backup power from the controller.

   b. Disconnect the AC power cables to the controller.

3. If this controller still has a SNIB or SNIB2 board installed, remove it.

   NOTE: If this is an Mx controller (which provides SNIB2 functionality using a daughterboard attached to the main board), see "Preparing an Mx Controller to Use a SNIB3" on page 7-75 for detailed instructions.

4. Install the SNIB3 board using the last connection on the EBIC5 ribbon cable, so it is the topmost board on this controller's stack of expansion boards.

5. Connect one end of the green ground wire to the underside of the Guardian Net SPD (using its ground screw), and connect the other end of the green ground wire to one of the controller's mounting screws.
   - For a small controller cabinet (used for an M2, M16, MSP, Mx-2, Mx-4, or Mx-8), see Figure 7-28.
   - For a large controller cabinet (used for an M8 or M64), see Figure 7-29.

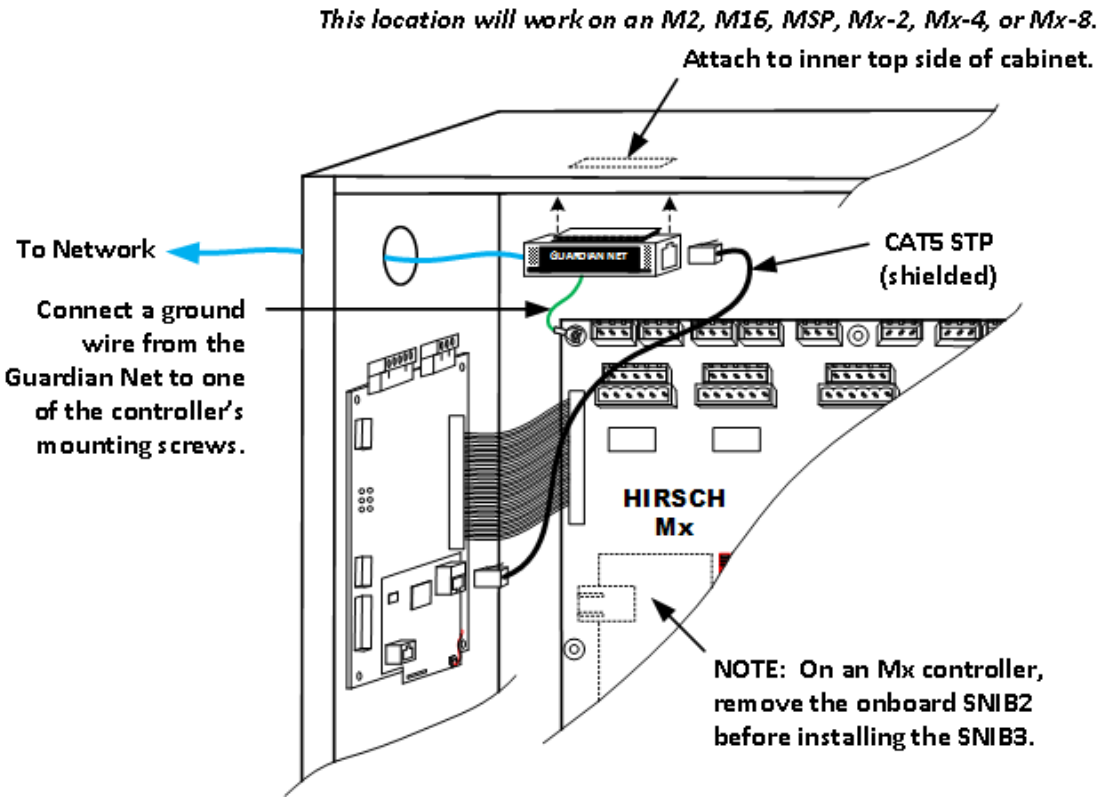


Figure 7-28: Installing a Guardian Net SPD for a SNIB3 in a Small Controller Cabinet

6. Connect one end of the included Cat5 STP Ethernet cable to the **Ethernet connector 1** RJ-45 jack on the SNIB3 board, and connect the other end of the cable to the RJ-45 jack marked **EQUIP** of the Guardian Net SPD.
7. Peel the protective covering off one side of the adhesive-backed Velcro strip, and press the exposed adhesive firmly against the appropriate side of the Guardian Net SPD, as shown in either Figure 7-28 or Figure 7-29.
8. Peel the protective covering off the other side of the adhesive-backed Velcro strip, and press the exposed adhesive firmly against either the:
   - inner **top** side of a **small** controller cabinet, or the
   - inner **left** side of a **large** controller cabinet.
9. Route the incoming Cat5 Ethernet cable through a knockout hole in the controller's cabinet and connect it to the RJ-45 jack marked **LINE** of the Guardian Net SPD.

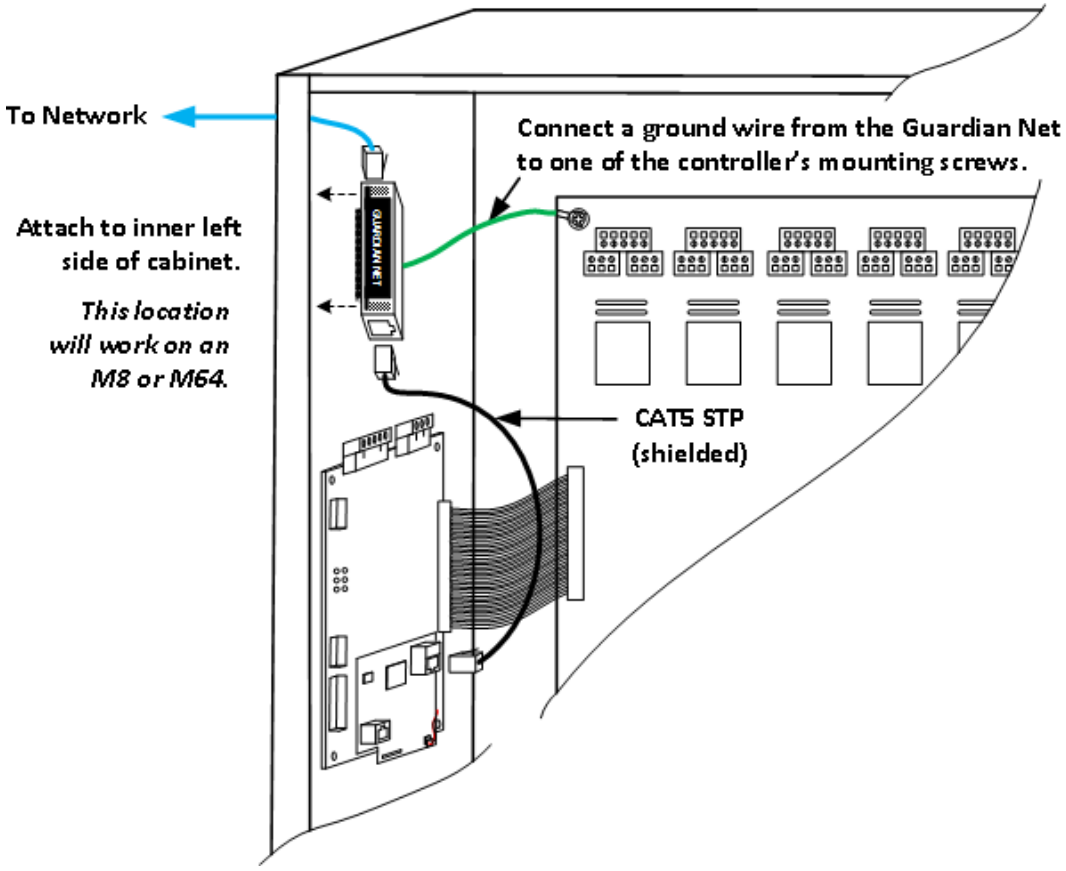


Figure 7-29: Installing a Guardian Net SPD for a SNIB3 in a Large Controller Cabinet

10. Restore power to the controller.
    a. Reconnect the AC power cables to the controller.
    b. Reconnect the battery backup power to the controller.
11. At the Velocity host, use Velocity to configure the SNIB3 as explained in "Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.

Preparing an Mx Controller to Use a SNIB3

Before the SNIB3 board was available, every Mx controller provided SNIB2 functionality using a daughterboard (with an Ethernet connector) attached to the main board, as shown in Figure 8-2 on page 8-6. Now when you order a new Mx controller, you have the option to instead have a SNIB3 board installed in an expansion slot.

But if you want to use the SNIB3 with an existing Mx controller that has a SNIB2 daughterboard, you must first remove that daughterboard from the Mx controller's main board. To do so, perform the following steps:

1. Make sure the controller shows its CCM firmware version as 7.5.37 or later. (This information can be found in the controller's Properties dialog within Velocity.)

   If necessary, update the CCM firmware. For details, see the "Firmware Updates > Updating CCM Firmware" topic in the Velocity help system.

2. Power down the Mx controller.
   a. Disconnect the battery backup power from the controller.
   b. Disconnect the AC power cables to the controller.
3. Remove the screw in the middle of the SNIB2 daughterboard.

   The SNIB2 daughterboard is mounted on the Mx controller's main board above the Mx logo, and it includes one RJ-45 Ethernet connector.
4. Carefully unplug the daughterboard from the Mx controller's main board.

   This usually requires holding opposite corners or ends of the daughterboard, and carefully rocking it out of its socket.
5. After the daughterboard has been removed, see "Providing Surge Protection for a Master SNIB3" on page 7-72 to determine whether you have an initial version of the SNIB3 (sold only to a few US federal government agencies) which did not include surge protection.
   - If so, follow the procedure in that topic.
   - Otherwise, install the SNIB3 expansion board in the normal way, as explained next in "Installing the SNIB3 in a Controller without a SNIB or a SNIB2" on page 7-76.

Installing the SNIB3 in a Controller without a SNIB or a SNIB2

The SNIB3 can be used with most DIGI*TRAC controllers, except for the M1N (which does not support any expansion boards). If you want to use a SNIB3 with an existing Mx controller, be sure to see "Preparing an Mx Controller to Use a SNIB3" on page 7-75.

Hint When installing SNIB3s in multiple controllers, you should install and test each SNIB3 before proceeding to the next one. This provides a means to troubleshoot any problems that might arise with a particular board or controller.

To install the SNIB3 in a controller which does not already have a SNIB or a SNIB2, perform the following steps:

1. Make sure each controller in the sequence shows its CCM firmware version as 7.5.37 or later. (This information can be found in the controller's Properties dialog within Velocity.)

   If necessary, update the CCM firmware. For details, see the "Firmware Updates > Updating CCM Firmware" topic in the Velocity help system.
2. Power down the controller.
   a. Disconnect the battery backup power from the controller.
   b. Disconnect the AC power cables to the controller.
3. Run a network cable to the controller. Make sure that:
   - The network cable is in good condition and is Cat 5 at a minimum; otherwise, run new cable.
   - The network cable is properly connected to the Velocity host through a hub or switch.
4. Set the DIP switches on the SNIB3 to its appropriate address and other parameters.

   For details, see "Setting the DIP Switches on a SNIB3" starting on page 7-81.

5. If necessary, run RS-485 cable downstream from the master or slave SNIB3.

   For details, see "RS-485 Cabling for SNIB3s" on page 7-80.

6. Connect the necessary cables and wires to the controller and the SNIB3, including:
   - the EBIC5 ribbon cable between the SNIB3 and the controller
   - the network cable into the SNIB3's RJ-45 Ethernet 1 port
   - any RS-485 wires connecting to a downstream controller

7. Mount the SNIB3 on the expansion board standoffs and secure the screws.

   For details, see "Mounting and Connecting Expansion Boards to the Controller" on page 7-14.

8. Restore power to the controller.
   a. Reconnect the AC power cables to the controller.
   b. Reconnect the battery backup power to the controller.

9. At the Velocity host, use Velocity to configure the SNIB3 as explained in "Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.

Replacing a Controller's SNIB or SNIB2 by a SNIB3

SNIB3s can communicate with SNIB2s, but they cannot communicate with original SNIBs. Any SNIBs existing on your security system must be replaced with SNIB2s or SNIB3s in order to use the faster speeds and greater encryption available with SNIB3s. If you have an M1N controller (which has built-in SNIB functionality and does not support any expansion boards), you must replace it with a different model of controller.

If you want to use a SNIB3 with an existing Mx controller, be sure to see "Preparing an Mx Controller to Use a SNIB3" on page 7-75.

Hint When installing SNIB3s in multiple controllers, you should install and test each SNIB3 before proceeding to the next one. This provides a means to troubleshoot any problems that might arise with a particular board or controller.

To replace a controller's existing SNIB or SNIB2 board by a SNIB3, perform the following steps:

1. Make sure the controller shows its CCM firmware version as 7.5.37 or later. (This information can be found in the controller's Properties dialog within Velocity.)

   If necessary, update the CCM firmware. For details, see the "Firmware Updates > Updating CCM Firmware" topic in the Velocity help system.

2. Power down the controller.
   a. Disconnect the battery backup power from the controller.
   b. Disconnect the AC power cables to the controller.

3. Disconnect the cables and wires attached to the existing SNIB or SNIB2 board, including:
   - the EBIC5 ribbon cable between the controller and the SNIB or SNIB2
   - the network cable into the SNIB2's RJ-45 Ethernet port
   - any RS-485 wires connecting to a downstream controller

4. Unscrew the expansion board standoff screws, and remove the existing SNIB or SNIB2 board.
5. If necessary, run a network cable to the controller. Make sure that:
   - The network cable is in good condition and is Cat 5 at a minimum; otherwise, run new cable.
   - The network cable is properly connected to the Velocity host through a hub or switch.
6. If necessary, run RS-485 cable downstream from the master or slave SNIB3.

   For details, see "RS-485 Cabling for SNIB3s" on page 7-80. Note that in an RS-485 array that includes a SNIB3, the master must be a SNIB3.
7. Set the DIP switches on the SNIB3 to its appropriate address and other parameters.

   For details, see "Setting the DIP Switches on a SNIB3" starting on page 7-81.
8. Connect the necessary cables and wires to the controller and the SNIB3, including:
   - the EBIC5 ribbon cable between the SNIB3 and the controller
   - the network cable into the SNIB3's RJ-45 Ethernet 1 port
   - any RS-485 wires connecting to a downstream controller
9. Mount the SNIB3 on the expansion board standoffs and secure the screws.

   For details, see "Mounting and Connecting Expansion Boards to the Controller" on page 7-14.
10. Restore power to the controller.
    a. Reconnect the AC power cables to the controller.
    b. Reconnect the battery backup power to the controller.
11. At the Velocity host, use Velocity to configure the SNIB3 as explained in "Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.

SNIB3 Network Configuration Options

Be aware that the SNIB3 is backwards compatible with the SNIB2, but not with the original SNIB. Each connected DIGI*TRAC or Mx controller must have its own SNIB2 or SNIB3 board installed.

The SNIB3 provides both an RS-485 port and a 10/100/1000BaseT RJ-45 Ethernet port, which enables you to choose the security network configuration that is most appropriate for your situation:

- If you are using only SNIB3 boards in all of your controllers, you can use either the XNET2 or the XNET3 protocol, and the downstream controllers in your security network can either be connected directly using the RJ-45 Ethernet port, or be connected to a master SNIB3 using the RS-485 port. (These options are shown in Figure 2-31, "Example Network Configurations Using Only SNIB3 Boards", on page 2-42.)
- If you are using SNIB2 boards in some of your controllers, you cannot use the XNET3 protocol, and those controllers must be downstream slaves to a master SNIB3, connected using the RS-485 port. (This option is shown in Figure 2-32, "Example Network Configuration Using SNIB2 and SNIB3 Boards", on page 2-42.)
- The SNIB3 also supports connections to the NET*MUX4, as explained in "Using NET*MUX4s with SNIB3s" on page 7-81.

Using Ethernet

The SNIB3's RJ-45 Ethernet port provides high-speed TCP/IP communication over an Ethernet network between the Velocity host computer and the controller, using either IPv4 or IPv6. With multiple controllers, each one can have an independent communication path with a unique IP address, as shown in Figure 7-30:

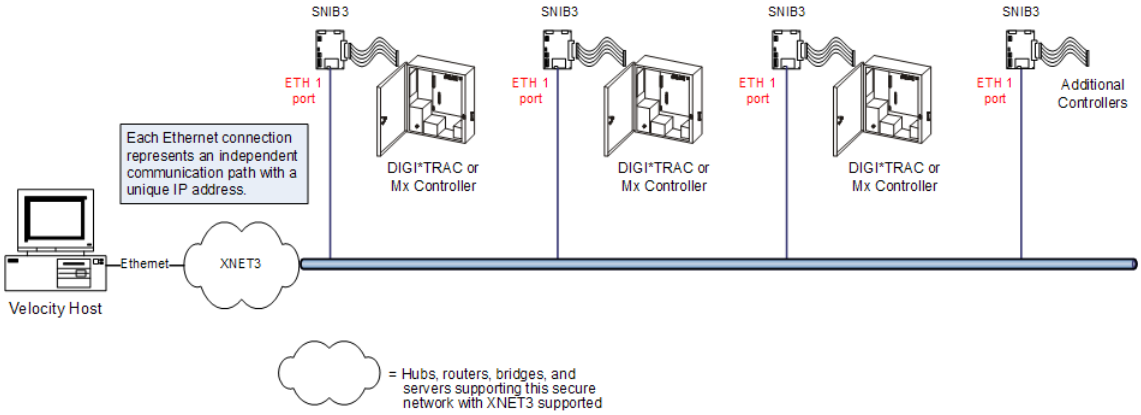


Figure 7-30: Multiple Controllers Connected Directly to an Ethernet Network

After an Ethernet connection has been established between the Velocity host and the SNIB3, Velocity views the SNIB3 as an XNET3 port. By default, the host communicates with the Ethernet-connected SNIB3 using AES 256-bit encrypted XNET3. However, before the Velocity server can communicate over Ethernet with a SNIB3, the SNIB3 must be configured through Velocity, as explained in "Configuring a SNIB3" on page 7-85.

Using Serial RS-485

The SNIB3's RS-485 port provides support for downstream serial connectivity, where the master of each chain must be a SNIB3 which is connected to the Velocity host using Ethernet. This master SNIB3 must be assigned the same address as the XBox port.

Velocity views the master SNIB3 as both a DIGI*TRAC or Mx controller and an XBox residing on an XNET port. (Subsequent multidropped controllers in the sequence do not appear as XBox controllers.)

- If every controller has a SNIB3, the XNET3 protocol can be used.
- If any downstream controller has a SNIB2, the XNET2 protocol must be used, and the top speed is limited to 38,400 bps.

The SNIB3's RS-485 connector enables wire runs of up to 4000 feet (1220 meters). Higher baud rates are more dependent on the number of twists per foot, so capacitance specifications must be strictly followed: total wire run per port is not to exceed acceptable capacitance of 11-17 p*f* and a total of 100,000 p*f*.

An example of connecting downstream slave controllers using serial RS-485 is shown in

Figure 7-31:

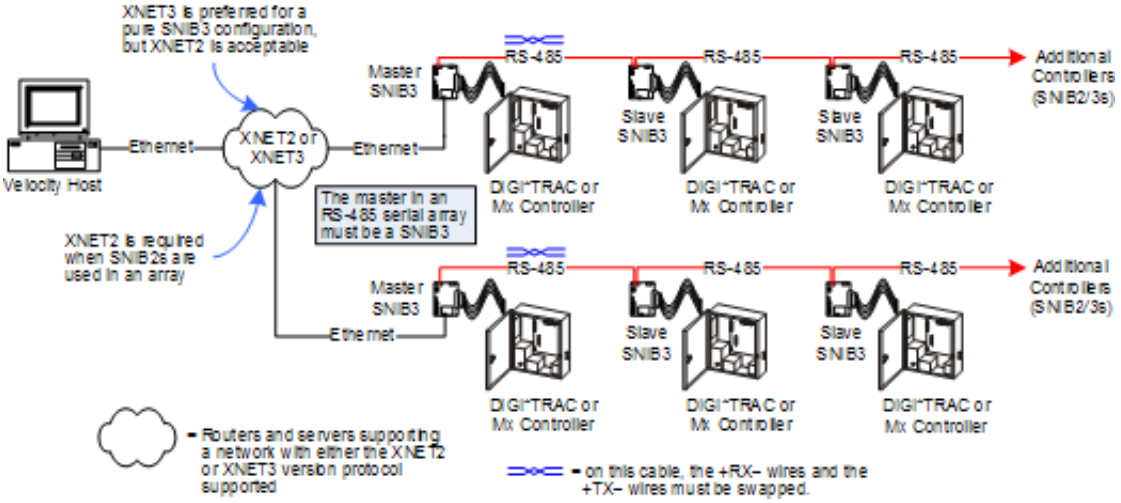


Figure 7-31: Downstream Slave Controllers Connected Using Serial RS-485

RS-485 Cabling for SNIB3s

As noted in Figure 7-31, the RS-485 cable linking the first (master) controller to the second (slave) controller in a multidropped RS-485 series must cross over the RX± and TX± wires. The cable for each subsequent slave controller is wired straight through. The details of this wiring is shown in Figure 7-32:

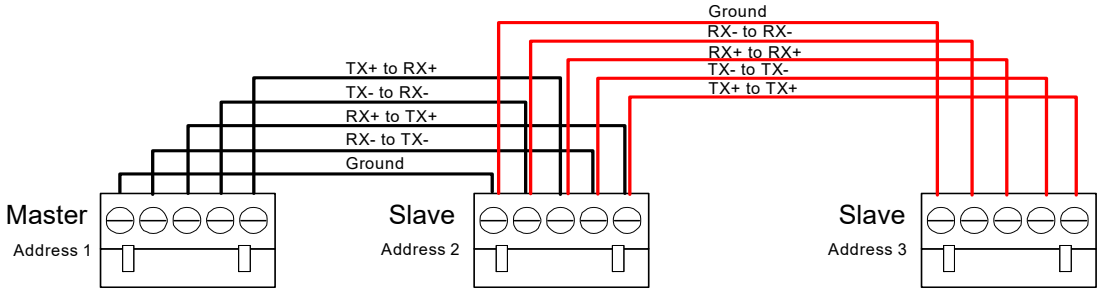


Figure 7-32: Wiring for RS-485 Chains

For an RS-485 chain, the maximum total cable run (from the master SNIB3 to the last downstream SNIB2 or SNIB3) is 4,000 feet (1,220 m). Higher baud rates are more dependent on the number of twists per foot, so capacitance specifications must be strictly followed: total wire run per port is not to exceed acceptable capacitance of 11-17 p*f* and a total of 100,000 p*f*.

In general, communications become less robust as baud rates increase, wire gauge decreases, and distances increase. For this reason, it may not be possible to implement the higher baud rates supported by the SNIB3 if you have long wire runs or small wire gauges.

Hint We recommend using Cat5 or Cat6 cable for your cable runs, with one pair for the RX pair, one pair for the TX pair, and one conductor or pair for the ground connection.

Using NET*MUX4s with SNIB3s

Like the SNIB2, the SNIB3 can be used with NET*MUX4s to enable a host PC running Velocity to program, monitor, and control up to 63 controllers on a port. This type of network configuration is shown in Figure 7-33:

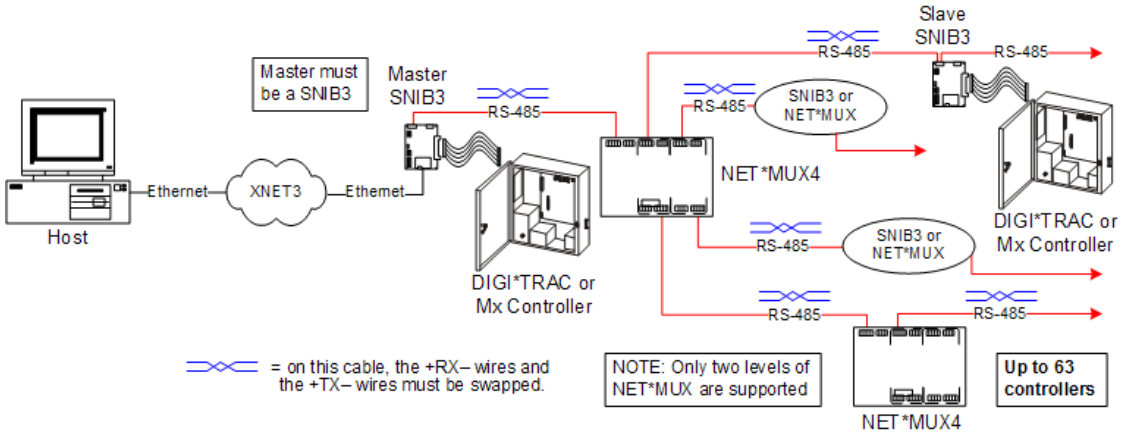


*Figure 7-33: Example Network Using NET*MUX4s with SNIB3s*

Note that:

- The master SNIB3 is connected to the Velocity host using Ethernet.
- All of the cables leading into and out of a NET*MUX4 are crossovers, where the RX± and TX± wires must be swapped.
- Only two levels of NET*MUX4s are supported.
- Each connected controller must have its own SNIB3 board installed.

The NET*MUX4 has a single RS-485 input and four RS-485 outputs to which a series of controllers or additional NET*MUX4s can be wired. However, the baud rate is limited to only 9600 bps.

Setting the DIP Switches on a SNIB3

The SNIB3 includes three DIP switch banks. The first bank (SW1) and second bank (SW2) have four DIP switches each. The third bank (SW3) has eight DIP switches.

Switch Bank 1 (SW1)

SNIB3s can be used throughout an RS-485 multidrop run; however, you must specify whether a specific SNIB3 is connected to a controller that is at the beginning, middle, or end of a run.

To do this, set S1-S4 on switch bank SW1 to either all ON or all OFF in this way:

S1-S4	OFF	This SNIB3 is in the middle of a multidrop sequence.
	ON	This SNIB3 is either the first (master) or last (termination) one in the multidrop sequence.

Switch Bank 2 (SW2)

The second switch bank at SW2 has four switches, where S1 configures encryption properties and S4 configures the SNIB3's location in the multidrop run. (S2 and S3 are used to reset a SNIB3 to its factory default settings.)

S1	**OFF**	The SNIB3 communicates with the host PC using the encryption keys stored in memory.
	ON	Return the encryption keys to their default settings. If this switch is set when the SNIB3 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. You must also check the 'Reset Encryption' option on the Velocity Port settings.
S2-S3	**OFF**	Normal operation.
	ON	These switches should only be ON when resetting this SNIB3 to the factory default settings; see "Resetting a SNIB3 to its Factory Default Values" on page 7-93.
S4	OFF	Indicates this SNIB3 is NOT first in the multidrop sequence.
	ON	Indicates this SNIB3 is first in the sequence (master), and is connected to the host via Ethernet. This SNIB3 controls polling.

Switch Bank 3 (SW3)

Switch bank SW3 is used to specify the SNIB3 speed (S1-S2) and the SNIB3 address (S3-S8). The DIP switch settings for the speed are:

S1	OFF	OFF	**ON**	**ON**
S2	OFF	**ON**	OFF	**ON**
Baud Rate	9,600	38,400	57,600	115,200

This controls the baud rate for the RS-485 multi-drop line. 57,600 and 115,200 bps are only available if your RS-485 cables are made from Cat5/Cat6 data grade wire. These speeds are not recommended for installations using:

- 18-gauge to 22-gauge shielded twisted-pair cable
- NET*MUX4s

Baud rates only apply to the RS-485 ports for SNIB2s and SNIB3s. The SNIB3's Ethernet port is used for host-to-controller connections and runs at 10/100/1G BaseT speeds. All SNIB2s and SNIB3s in an RS-485 multi-drop sequence must be set to the same speed.

The remaining DIP switches (S3-S8) on SW3 set the SNIB3's address, just like for the

SNIB2:

Address	SW3	SW4	SW5	SW6	SW7	SW8
1	OFF	OFF	OFF	OFF	OFF	**ON**
2	OFF	OFF	OFF	OFF	**ON**	OFF
3	OFF	OFF	OFF	OFF	**ON**	**ON**
4	OFF	OFF	OFF	**ON**	OFF	OFF
5	OFF	OFF	OFF	**ON**	OFF	**ON**
6	OFF	OFF	OFF	**ON**	**ON**	OFF
7	OFF	OFF	OFF	**ON**	**ON**	**ON**
8	OFF	OFF	**ON**	OFF	OFF	OFF
9	OFF	OFF	**ON**	OFF	OFF	**ON**
10	OFF	OFF	**ON**	OFF	**ON**	OFF
11	OFF	OFF	**ON**	OFF	**ON**	**ON**
12	OFF	OFF	**ON**	**ON**	OFF	OFF
13	OFF	OFF	**ON**	**ON**	OFF	**ON**
14	OFF	OFF	**ON**	**ON**	**ON**	OFF
15	OFF	OFF	**ON**	**ON**	**ON**	**ON**
16	OFF	**ON**	OFF	OFF	OFF	OFF
17	OFF	**ON**	OFF	OFF	OFF	**ON**
18	OFF	**ON**	OFF	OFF	**ON**	OFF
19	OFF	**ON**	OFF	OFF	**ON**	**ON**
20	OFF	**ON**	OFF	**ON**	OFF	OFF
21	OFF	**ON**	OFF	**ON**	OFF	**ON**
22	OFF	**ON**	OFF	**ON**	**ON**	OFF
23	OFF	**ON**	OFF	**ON**	**ON**	**ON**
24	OFF	**ON**	**ON**	OFF	OFF	OFF
25	OFF	**ON**	**ON**	OFF	OFF	**ON**
26	OFF	**ON**	**ON**	OFF	**ON**	OFF
27	OFF	**ON**	**ON**	OFF	**ON**	**ON**
28	OFF	**ON**	**ON**	ON	OFF	OFF
29	OFF	**ON**	**ON**	**ON**	OFF	**ON**
30	OFF	**ON**	**ON**	**ON**	**ON**	OFF
31	OFF	**ON**	**ON**	**ON**	**ON**	**ON**
32	**ON**	OFF	OFF	OFF	OFF	OFF
33	**ON**	OFF	OFF	OFF	OFF	**ON**
34	**ON**	OFF	OFF	OFF	**ON**	OFF
35	**ON**	OFF	OFF	OFF	**ON**	**ON**

Table 7-7: SNIB3 DIP Switch Address Settings

Address	SW3	SW4	SW5	SW6	SW7	SW8
36	**ON**	OFF	OFF	**ON**	OFF	OFF
37	**ON**	OFF	OFF	**ON**	OFF	**ON**
38	**ON**	OFF	OFF	**ON**	**ON**	OFF
39	**ON**	OFF	OFF	**ON**	**ON**	**ON**
40	**ON**	OFF	**ON**	OFF	OFF	OFF
41	**ON**	OFF	**ON**	OFF	OFF	**ON**
42	**ON**	OFF	**ON**	OFF	**ON**	OFF
43	**ON**	OFF	**ON**	OFF	**ON**	**ON**
44	**ON**	OFF	**ON**	**ON**	OFF	OFF
45	**ON**	OFF	**ON**	**ON**	OFF	**ON**
46	**ON**	OFF	**ON**	**ON**	**ON**	OFF
47	**ON**	OFF	**ON**	**ON**	**ON**	**ON**
48	**ON**	**ON**	OFF	OFF	OFF	OFF
49	**ON**	**ON**	OFF	OFF	OFF	**ON**
50	**ON**	**ON**	OFF	OFF	**ON**	OFF
51	**ON**	**ON**	OFF	OFF	**ON**	**ON**
52	**ON**	**ON**	OFF	**ON**	OFF	OFF
53	**ON**	**ON**	OFF	**ON**	OFF	**ON**
54	**ON**	**ON**	OFF	**ON**	**ON**	OFF
55	**ON**	**ON**	OFF	**ON**	**ON**	**ON**
56	**ON**	**ON**	**ON**	OFF	OFF	OFF
57	**ON**	**ON**	**ON**	OFF	OFF	**ON**
58	**ON**	**ON**	**ON**	OFF	**ON**	OFF
59	**ON**	**ON**	**ON**	OFF	**ON**	**ON**
60	**ON**	**ON**	**ON**	**ON**	OFF	OFF
61	**ON**	**ON**	**ON**	**ON**	OFF	**ON**
62	**ON**	**ON**	**ON**	**ON**	**ON**	OFF
63	**ON**	**ON**	**ON**	**ON**	**ON**	**ON**

Table 7-7: SNIB3 DIP Switch Address Settings (Continued)

Configuring a SNIB3

The location of a SNIB3 on your network relative to the Velocity host will determine the method you must use for configuring that SNIB3:

- If the SNIB3 is on the same subnet, then you will configure it using Velocity. See "Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.
- If the SNIB3 is on a different subnet, then you will configure it using the SNIB Configuration Tool. See "Configuring a SNIB3 on a Different Subnet" starting on page 7-89.

Overview of Network Subnets

Each SNIB3 that is connected to the network using Ethernet (instead of being a down-stream controller in a serial RS-485 chain) must be assigned a unique IP address so it can communicate with the Velocity host. The method for doing that depends on the location of that SNIB3 on your network relative to the Velocity host. The determining factor is whether they are both on the same subnet.

What is a subnet? Put simply, a subnet is any group of PCs and other devices, such as printers and scanners, connected by network cable to a network server, router, or hub. Anything behind the router/hub is considered part of the subnet. Anything beyond this router/hub is not part of the subnet. This concept is illustrated in Figure 7-34.

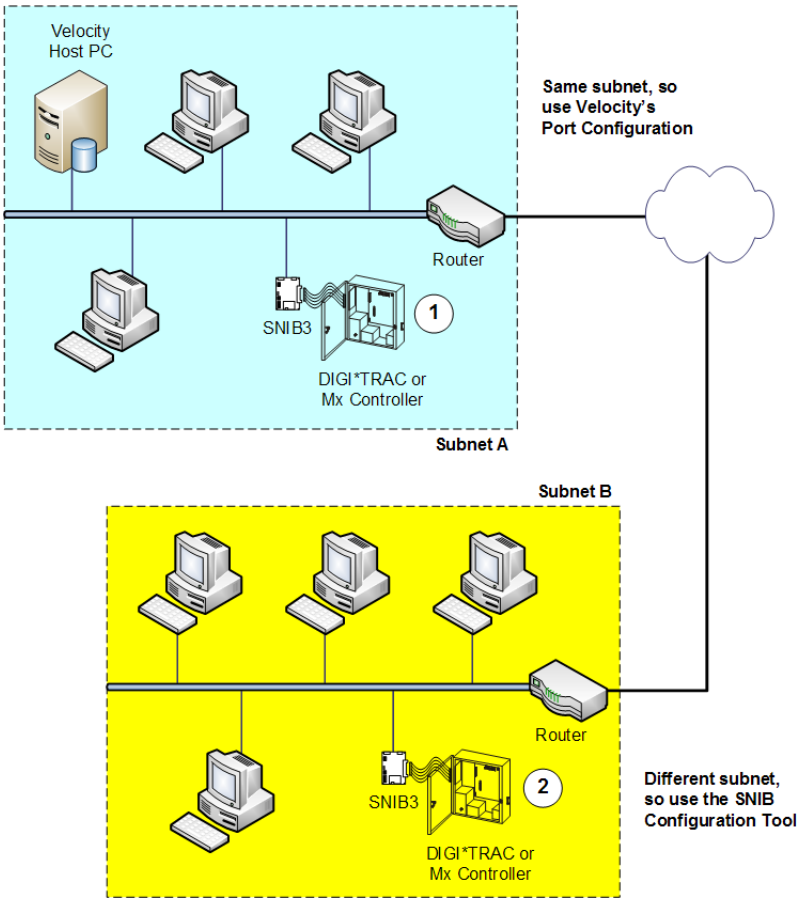


Figure 7-34: Example of Network Subnets

In Figure 7-34, the SNIB3 and its attached controller labeled 1 are located in the same

subnet as the host PC (Subnet A). This SNIB3 can therefore be configured using Velocity; however, the SNIB3 and controller labeled 2 are located behind a different router, in a different subnet (Subnet B), and must be configured using the SNIB Configuration Tool.

Any number of computers and devices can be behind a hub or router, but for reasons of security and speed, a company network often incorporates many network servers, hubs, and routers. It is fairly common to find that each department within a company has its own server connected to its own hub and/or router. Routers and hubs not only find the quickest way to ferry packets of information between two points, but also can serve as a rudimentary firewall against potential intrusion.

Hint Port monitoring tools (such as Norton Antivirus and Windows firewall) may obstruct the discovery of network devices. To avoid this issue, you should temporarily disable this type of tool while trying to discover SNIB3s using either Velocity or the SNIB Configuration Tool.

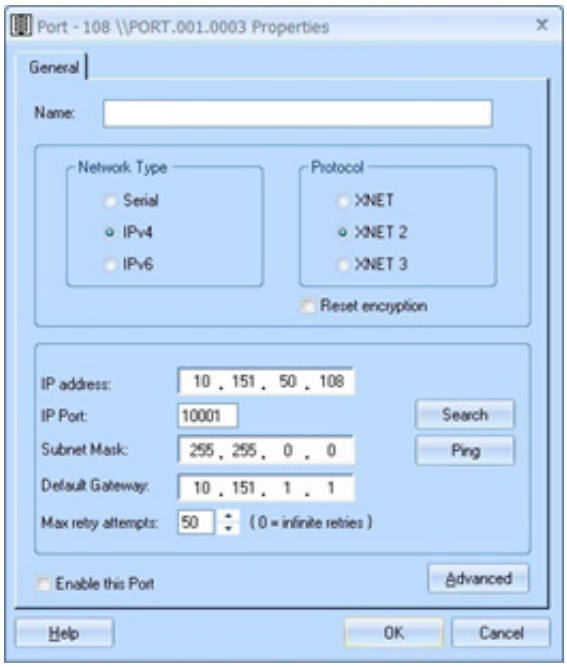
Using Velocity to Configure a SNIB3 on the Same Subnet

If a SNIB3 is on the same subnet as the Velocity host, then you will configure it using Velocity. (If the SNIB3 is on a different subnet, then you will configure it using the SNIB Configuration Tool, as explained in "Configuring a SNIB3 on a Different Subnet" starting on page 7-89.)

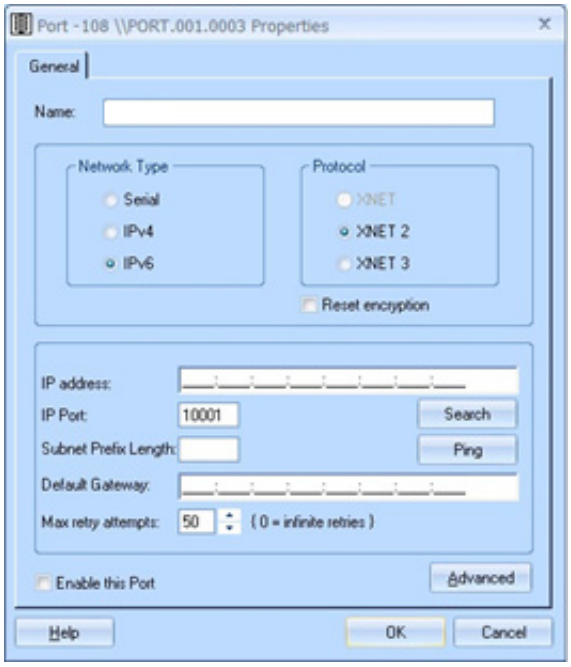
To configure a SNIB3 which is on the same network subnet as the Velocity host:

1. If you have not yet done so, install the SNIB3 board in the controller. For details, see either:
   - "Installing the SNIB3 in a Controller without a SNIB or a SNIB2" on page 7-76, or
   - "Replacing a Controller's SNIB or SNIB2 by a SNIB3" on page 7-77.
2. If you have not yet done so, connect the controller to the network. For guidance, see "SNIB3 Network Configuration Options" on page 7-78.
3. In Velocity's Administration window, double-click the **Add New XNET Port** item.

The resulting Port Properties dialog varies according to whether your network is using IPv4 or IPv6 addressing. For IPv4 addressing:

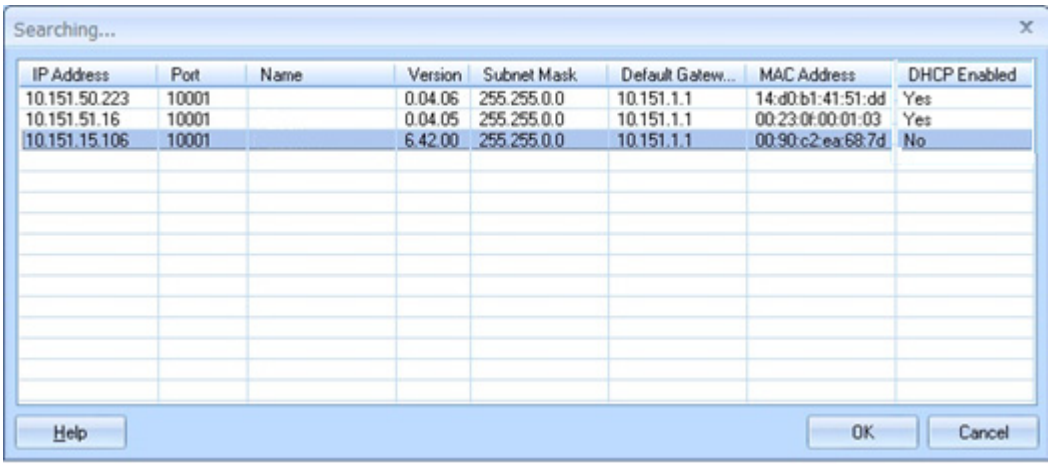


For IPv6 addressing:

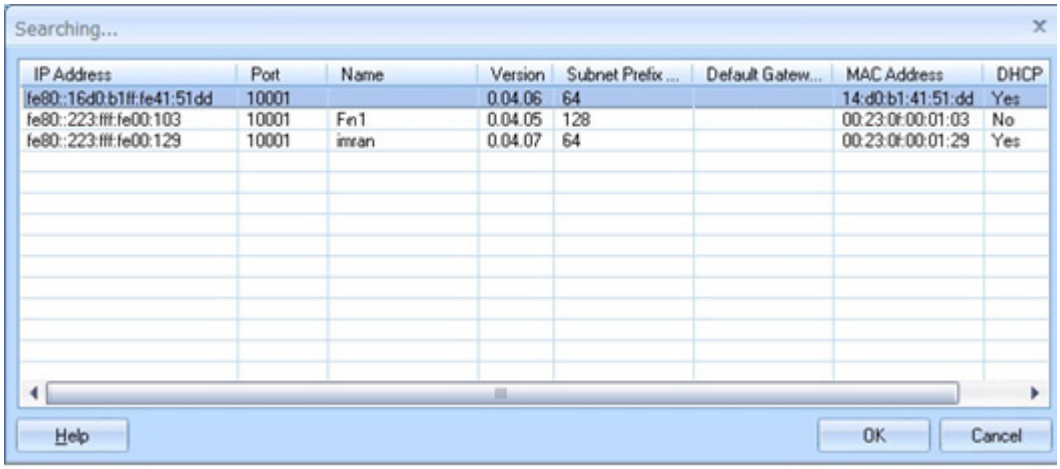


4. On the **Port Properties** dialog:
   a. If necessary, for the 'Network Type' select either the IPv4 or the IPv6 option.
   b. For the 'Protocol', select either the XNET2 or XNET3 option.
   c. Click the **Search** button.

The results depend on the options you specified for the Network Type and the Protocol. Here is an example for an IPv4 network using the XNET2 protocol:



Here is an example for an IPv6 network using the XNET3 protocol:

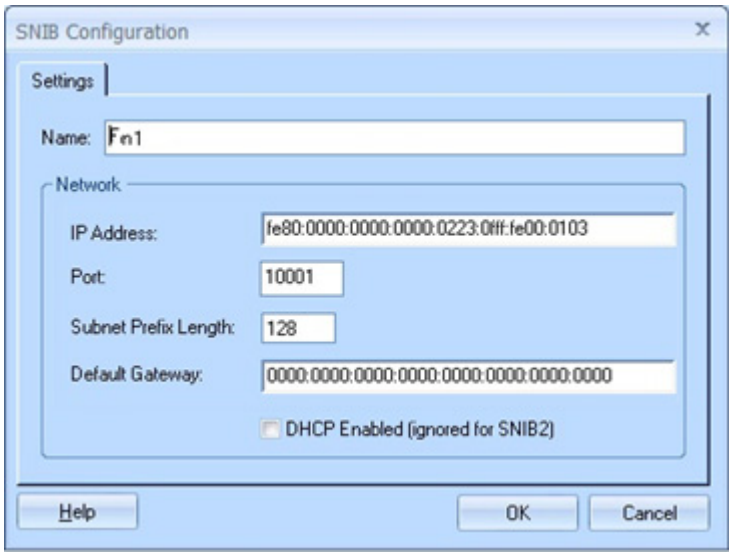


Note that although the SNIB2 and the SNIB3 support dynamic IP addressing using the Dynamic Host Configuration Protocol (DHCP) for both IPv4 and IPv6, Identiv strongly recommends using static or reserved IP addresses. For this reason, all SNIB2s and SNIB3s that have the value of Yes in the **DHCP Enabled** column should be changed to have assigned fixed IP addresses before they are added to the Velocity network.

5. To change the settings for one of the displayed ports, perform these steps:

   a. Double-click on an entry in the **Searching** dialog's results table.

b. In the resulting **SNIB Configuration** dialog, make the necessary changes.



For example:

- If you need to change the Port number from the default value of 10001, then make sure to stay within the range from 1024 to 32767. Outside of this range, SNIB3 cannot communicate with the Velocity host.
- If you plan to assign a fixed address to this port, then clear the check box for the 'DHCP Enabled (ignored for SNIB2)' option.

c. When you are finished, click **OK** to close this dialog.

6. Back in the **Searching** dialog, click on the appropriate row to select the desired SNIB3 board, and click **OK**.

Velocity starts communicating with the specified SNIB3, and its port appears in the Ports folder within the Administration window.

Configuring a SNIB3 on a Different Subnet

If a SNIB3 is on a different subnet than the Velocity host, you will configure it using the SNIB Configuration Tool. (If the SNIB3 is on the same subnet, then you will configure it using Velocity, as explained in "Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.)

Hint You should work with your IT administrator to determine which IP addresses to assign to your new SNIB3s. Otherwise, for each SNIB3 you must record the configuration information assigned using the SNIB Configuration Tool, so you can later finish configuring the SNIB3 in Velocity.

To configure a SNIB3 which is on a different network subnet than the Velocity host:

1. If you have not yet done so, install the SNIB3 board in the controller. For details, see either:
   - "Installing the SNIB3 in a Controller without a SNIB or a SNIB2" on page 7-76, or
   - "Replacing a Controller's SNIB or SNIB2 by a SNIB3" on page 7-77.
2. If you have not yet done so, connect the controller to the network. For guidance, see "SNIB3 Network Configuration Options" on page 7-78.

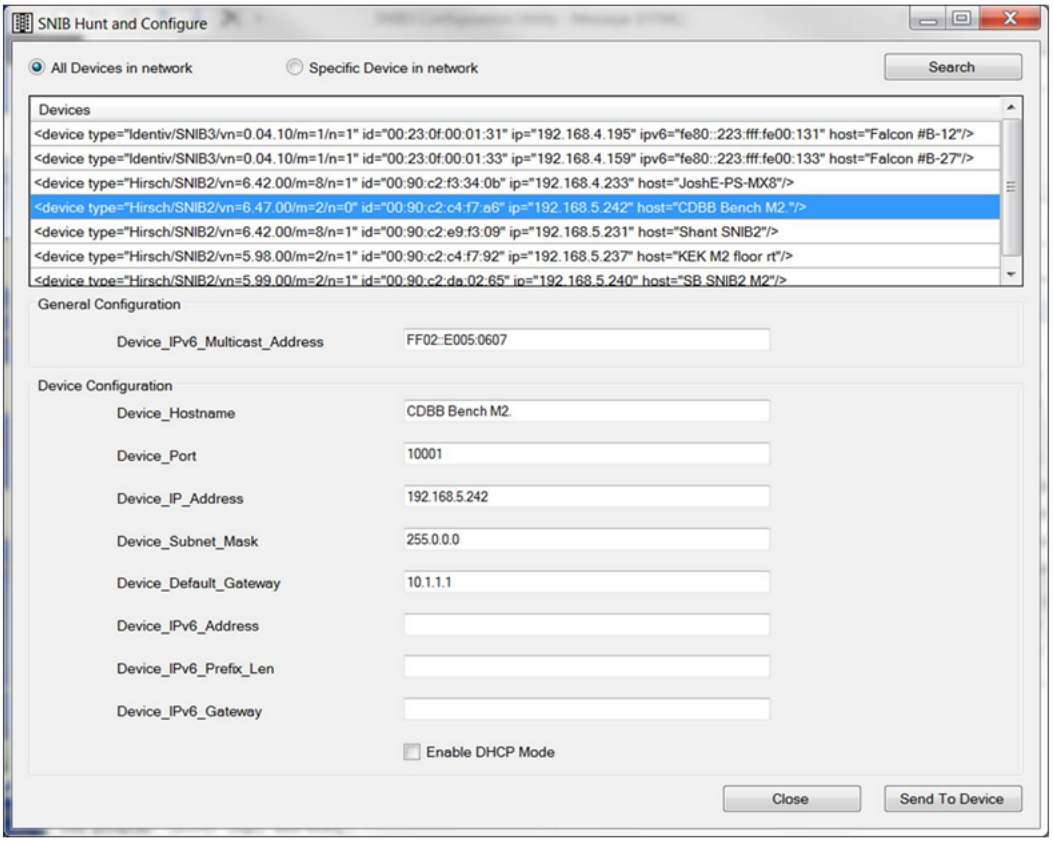
3. If you have not yet done so, download the SNIB Configuration Tool to a PC which you will use to configure the SNIB3:

   On that PC, download the **SNIBConfigTool.exe** file from the Identiv website. (Use your Web browser to go to the **identiv.com/support** page, click the **Support: Hirsch Products** link, click the **SNIB3 - Documents and Downloads** link, and click on the link to download the SNIB Configuration Tool.)

4. Connect that PC to the same network subnet as the SNIB3 being configured.

5. Locate and double-click the **SNIBConfigTool.exe** file.

6. On the resulting **SNIB Hunt and Configure** window:



   a. Select one of these options:

      - **All Devices in network**, to search for all SNIB2s or SNIB3s on this network subnet. (If a SNIB2 or SNIB3 is currently logged on, this utility will not detect it.)
      - **Specific Device in network**, to search for a specific SNIB2 or SNIB3 on this network subnet. If you select this option, enter a search term such as an IP address in the text field which appears after this option. (This option works for both IPv4 and IPv6.)

   b. Click the **Search** button.

   c. From the resulting list of previously-undetected SNIB2s or SNIB3s displayed in the **Devices** list, double-click on the entry for the desired SNIB3, so its information appears in the subsequent fields on this window.

Note that the Device_IP_Address, Device_Subnet_Mask, and Device_Default_Gateway fields are specific to IPv4. The Device_IPv6_Multicast_Address, Device_IPv6_Address, Device_IPv6_Prefix_Len, and Device_IPv6_Gateway fields are specific to IPv6.

Hint You can identify a SNIB3 by its MAC address (id=), which is printed on a white label attached to its RJ45 Ethernet connector. This label includes both a barcode (in QR code format) and the full MAC address (in small print).

d. Enter the values required for this SNIB3 in the relevant fields. For example:
   - In the **Device_Hostname** field, enter the SNIB3 name that the Velocity host will use to identify this SNIB3.
   - In the **Device_Port** field, enter the network port number for this SNIB3. If you need to change this from the default value of 10001, then make sure to stay within the range from 1024 to 32767. Outside of this range, SNIB3 cannot communicate with the Velocity host.
   - Enter the necessary IP address in either the Device_IP_Address field (for IPv4) or in the **Device_IPv6_Address** field (for IPv6).
   - If you follow our recommendation to use static or reserved IP addresses, then clear the check box for the **Enable DHCP Mode** option.

e. Click the **Send to Device** button, to send the updated values to this SNIB3.

f. Click the **Search** button again, to verify that the SNIB3 has correctly received the updated information.

g. Record this SNIB3's device hostname, port number, and IP address.

   You will need this information to finish configuring the SNIB3 in Velocity.

h. When you are finished, click the **Close** button.

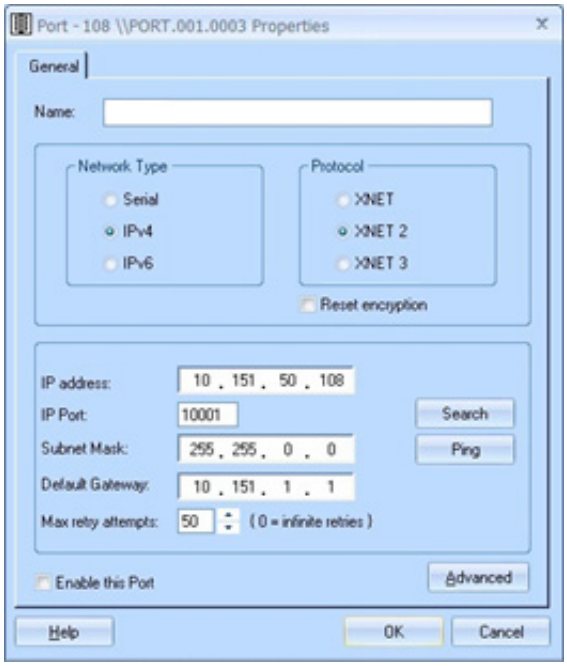
Hint If you have a lot of SNIB3s to configure remotely, you should use a portable computer which has the SNIB Configuration Tool installed. This should enable the installer to do the job more rapidly. But make sure you are on-site when you do this, because a SNIB3 does not retain its IP address for more than 5 minutes after being unplugged from a controller. (If you were planning to program several SNIB3s using one controller then move them to other controllers at a remote site, you probably won't have time before the IP address in each SNIB3 is lost.)

After you have used the SNIB Configuration Tool to assign the device hostname, port number, and IP address to a remote SNIB3, you must use Velocity to assign that SNIB3 to a new port.

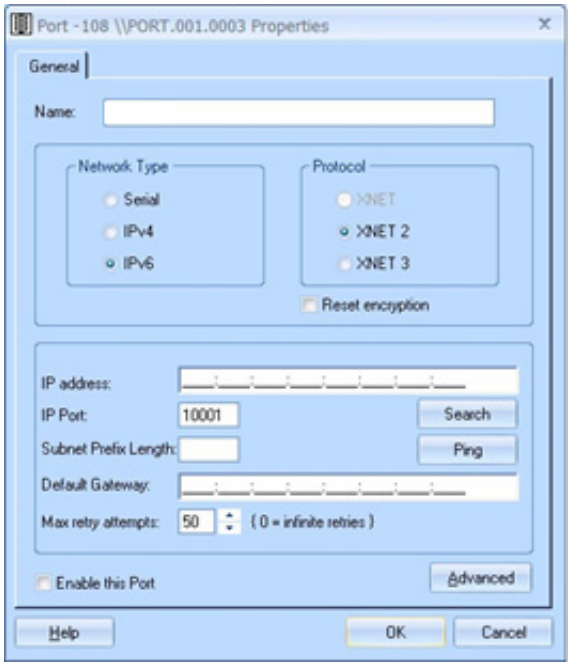
To assign a remote SNIB3 to a new port on Velocity:

1. In Velocity's Administration window, double-click the **Add New XNET Port** item.

The resulting Port Properties dialog varies according to whether your network is using IPv4 or IPv6 addressing. For IPv4 addressing:



For IPv6 addressing:



2. On the **Port Properties** dialog:
   a. If necessary, for the '**Network Type**' select either the IPv4 or the IPv6 option.
   b. For the '**Protocol**', select either the XNET2 or XNET3 option.
   c. In the '**Name**' field, enter the value you assigned as the Device_Hostname (when using the SNIB Configuration Tool).

d. In the '**IP address**' field, enter the value you assigned as either the Device_IP_Address or the Device_IPv6_Address (when using the SNIB Configuration Tool).

e. In the '**IP Port**' field, enter the value you assigned as the Device_Port (when using the SNIB Configuration Tool).

f. Make sure the '**Enable this Port**' option is checked.

g. Click **OK**.

Velocity should then be able to find and monitor this remote SNIB3.

Resetting SNIB3 Encryption Keys

After Velocity creates the encryption keys required for secure Host-to-SNIB3 communication, it continues to use those keys. If for some reason you need to change these keys, there are several ways to do it.

Set SW2-1 to:	Procedures/Results
 **OFF**	• Cycle power on controller. SNIB3 retains encryption keys. Controller retains setups. • Press the blue Reset button on the controller until it resets. SNIB3 retains encryption keys. Controller **loses** setups. • Download SNIB3 firmware through Velocity. SNIB3 retains encryption keys. Controller retains setups.
 **ON**	• Cycle power on controller. SNIB3 **resets** encryption keys. Controller retains setups. • Press the blue Reset button on the controller until it resets. SNIB3 **resets** encryption keys. Controller **loses** setups. • Download SNIB3 firmware through Velocity. SNIB3 **resets** encryption keys. Controller retains setups.

After you have reset the SNIB3's encryption key to its default value (by setting SW2-1 to ON, recycling controller power, then resetting SW2-1 to OFF), you must perform the following steps to assign a new key:

1. In the Velocity Administration system tree, expand the **DIGI*TRAC Configuration** system folder until the master SNIB3 port you require appears.
2. Right-click on that SNIB3 port, and select **Properties** from the pop-up menu.
3. On the resulting **Port Properties** dialog, check the box for the '**Reset encryption**' option, and then click **OK**.

This resets the encryption key at the Velocity host.

Resetting a SNIB3 to its Factory Default Values

A SNIB3 board can be reset to the factory default values for its encryption keys and network settings. To reset a SNIB3 board to have an IP address based on its unique MAC address, perform the following steps:

1. Set all four DIP switches in Switch Bank 2 to ON, and set all eight DIP switches in Switch Bank 3 to OFF.

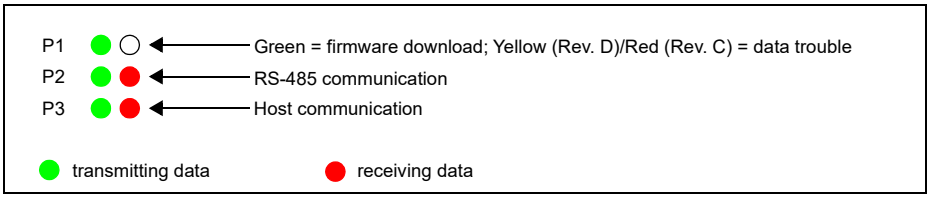
2. Cycle power to the controller containing this SNIB3 board.
3. Watch the status LEDs on the SNIB3 board, to ensure that they display the Lamp Test start up pattern, and then display the following SNIB2/CCM Synchronization pattern:

4. Turn off power to the controller.

You can then reconfigure the SNIB3 board as needed, using its DIP switches and Velocity.

Controller and SNIB3 LED Diagnostics

The SNIB3 has three pairs of LEDs that show you how the SNIB3 is communicating with the Velocity Server.



Special Light Patterns at Startup

At startup, the following pattern may be observed:

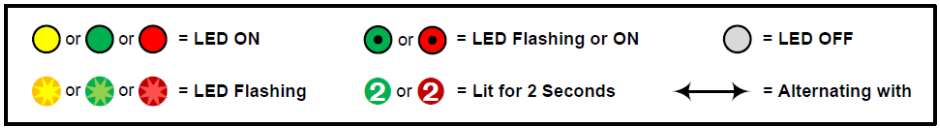
This indicates the **SNIB3/CCM Synchronization**. This pattern repeats until the CCM and SNIB3 are synchronized. This light pattern should not persist longer than four minutes if there are no memory expansion boards on the controller.

Light Patterns for Normal Operations

This table illustrates the various light patterns displayed during normal operation for SNIB3s:

Master or Slave SNIB3 Communications	
P1 P2	Ordinary communication between the SNIB3 and its host is observed. Lights may blink or stay lit during heavy data transfers. They will go out every 4 seconds during idle or low-traffic periods; this is normal, indicating the master is hunting for new addresses, such as newly-added controllers, or controllers that went offline and are expected back online.

Legend:



Master SNIB3 Communications	
P1 ○ ○ P2 ● ● P3 ● ●	This could be programming activity (downloads) or events, or both.
P1 ○ ○ P2 ● ✹ P3 ● ●	P2's red LED flashes while P2 green and P3 red and green stay lit. This normally means that the Velocity server is in the process of downloading CCM or SNIB3 firmware to one or more controllers.
P3 ✹ ✹	Heartbeat. If the P3 LED flashes appear to be about 5 seconds apart, it means the host is keeping the communication link open.
Slave SNIB3 Communications	
P1 ○ ○ P2 ○ ✹ P3 ○ ○	The master is polling a different SNIB3. This SNIB3 ignores those polls.
P1 ○ ○ P2 ○ ● P3 ○ ○	If this stays lit and doesn't go out every 4 seconds, that means there's a lot of data going to or coming from some other controller(s). If you don't see any green flashes at all, this unit won't come online until the data traffic decreases. This pattern may also alternate with occasional red or green P3 flashes.
P1 ○ ○ P2 ✹ ● P3 ○ ○	If these stay flashing and lit, it means there is a lot of data going to or coming from several controllers. This occurs particularly when you have many controllers.
P1 ○ ○ P2 ● ● P3 ○ ○	If these stay lit, it means there is a lot of data going to or coming from this particular controller.

Legend:

○ or ● or ● = LED ON	◉ or ◉ = LED Flashing or ON	○ = LED OFF
✹ or ✹ or ✹ = LED Flashing	② or ② = Lit for 2 Seconds	⟷ = Alternating with

Like the SNIB2, the SNIB3 also causes certain changes to the way the controller LEDs display, as shown below:

LED Configuration	Meaning
● ○ AC ○ ○ BAT ● ○ SYS ○ ○ KPD ● ○ NET	The NET green LED is on; the NET red LED blinks intermittently depending on the amount of data being received from the host. This indicates the SNIB3 is working properly. *Note: The exact NET LED behavior depends on the controller version.*
● ○ AC ○ ○ BAT ● ○ SYS ○ ○ KPD ○ ○ NET	Neither NET LED is blinking, or only the NET green LED is on. In either case, the master SNIB3 is not communicating with the host. Check both your Ethernet connection and your Velocity port configuration.

For more information, see “Troubleshooting the Controller Using Status LEDs” on page 7-382.

ScramblePad Installation

In order to install the ScramblePad, you must:

- ❑ Install the Mounting Box – instructions on how to install the correct mounting boxes, determine the correct mounting height for each device, and the dimensions of each ScramblePad box.
- ❑ Set up the ScramblePad – instructions on how to set ScramblePad DIP switches to assign each an ID.
- ❑ Wire the ScramblePad – detailed instructions on how to wire the ScramblePad to the controller.

Each of these tasks is discussed in this section.

Installing the Mounting Box

Each ScramblePad must be installed in a mounting box. The available mounting boxes are shown in Figure 7-35.

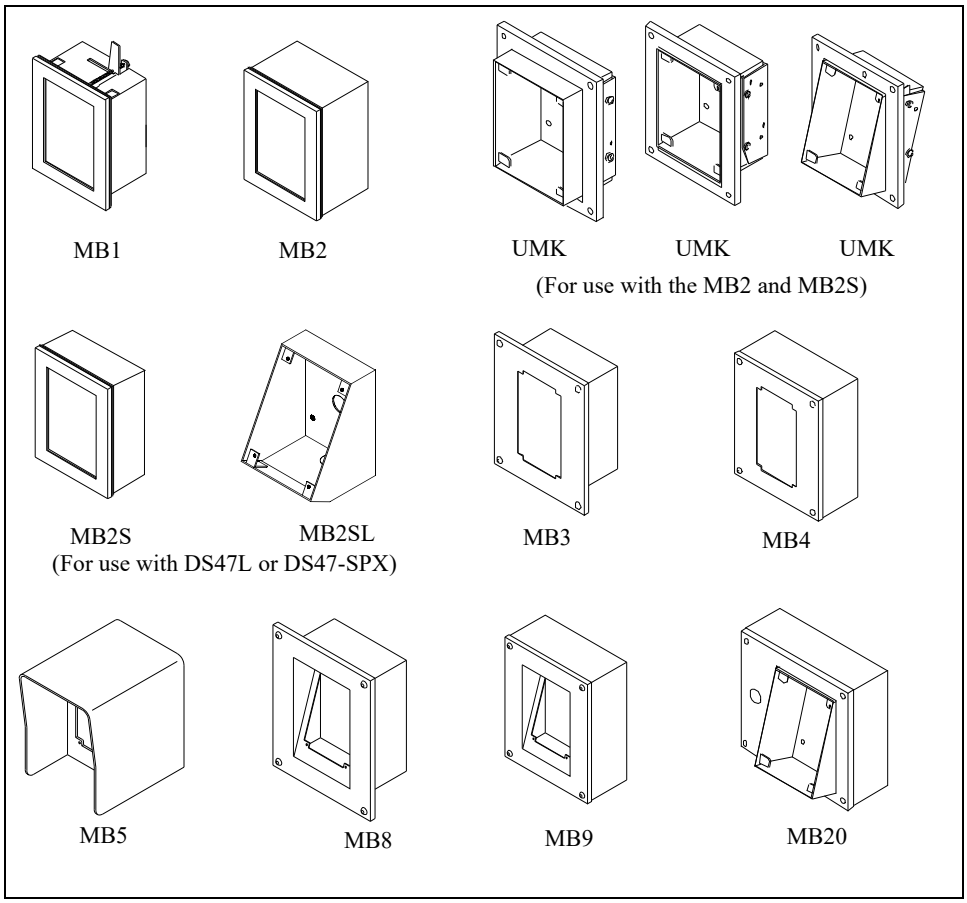


Figure 7-35: ScramblePad Mounting Boxes

Note: The Universal Mounting Kit (UMK) is designed for use with the MB2. The UMKS is designed for use with the MB2S.

Some of the mounting boxes—like the MB1, MB3, and MB8—are designed for flush

mounting, meaning the box is embedded in the wall. Other boxes—like the MB2, MB2S, MB4, MB9, and MB20—are designed for surface mounting, which means the box is attached to and juts from the wall. However, when used with the UMK, the MB2 becomes flush, semi-flush, or handicap mountable.

The MB2S is designed specifically for the DS47LScramblePad and DS47L-SPX ScrambleProx. When used with the UMK or UMKS, the MB2S becomes flush or handicap mountable.

The MB20 is used for mounting a keypad and magstripe reader side-by-side (dual technology). This box also enables you to install both a magstripe and prox reader at the same door, if you so choose. This entails installation of the ScrambleProx in the keypad position.

The MB5 is used for parking and other outdoor operations. It can be surface-mounted on a wall or, for parking applications, can use either the MP35 or MP41 mounting post.

To determine how much space you'll need for the mounting box, study the dimensions for each box as shown on the following pages.

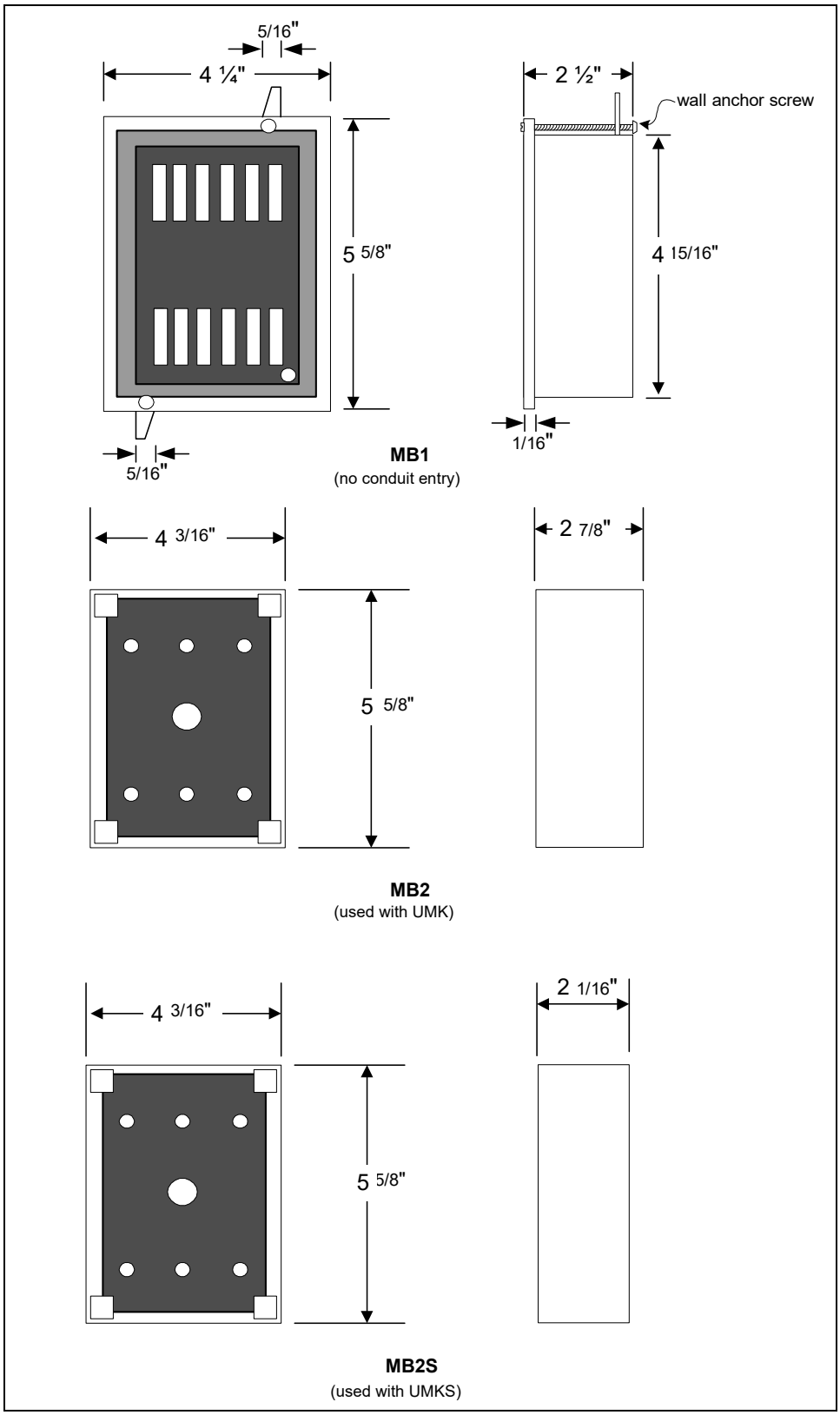


Figure 7-36: ScramblePad Mounting Boxes Dimensions - MB1, MB2, & MB2S

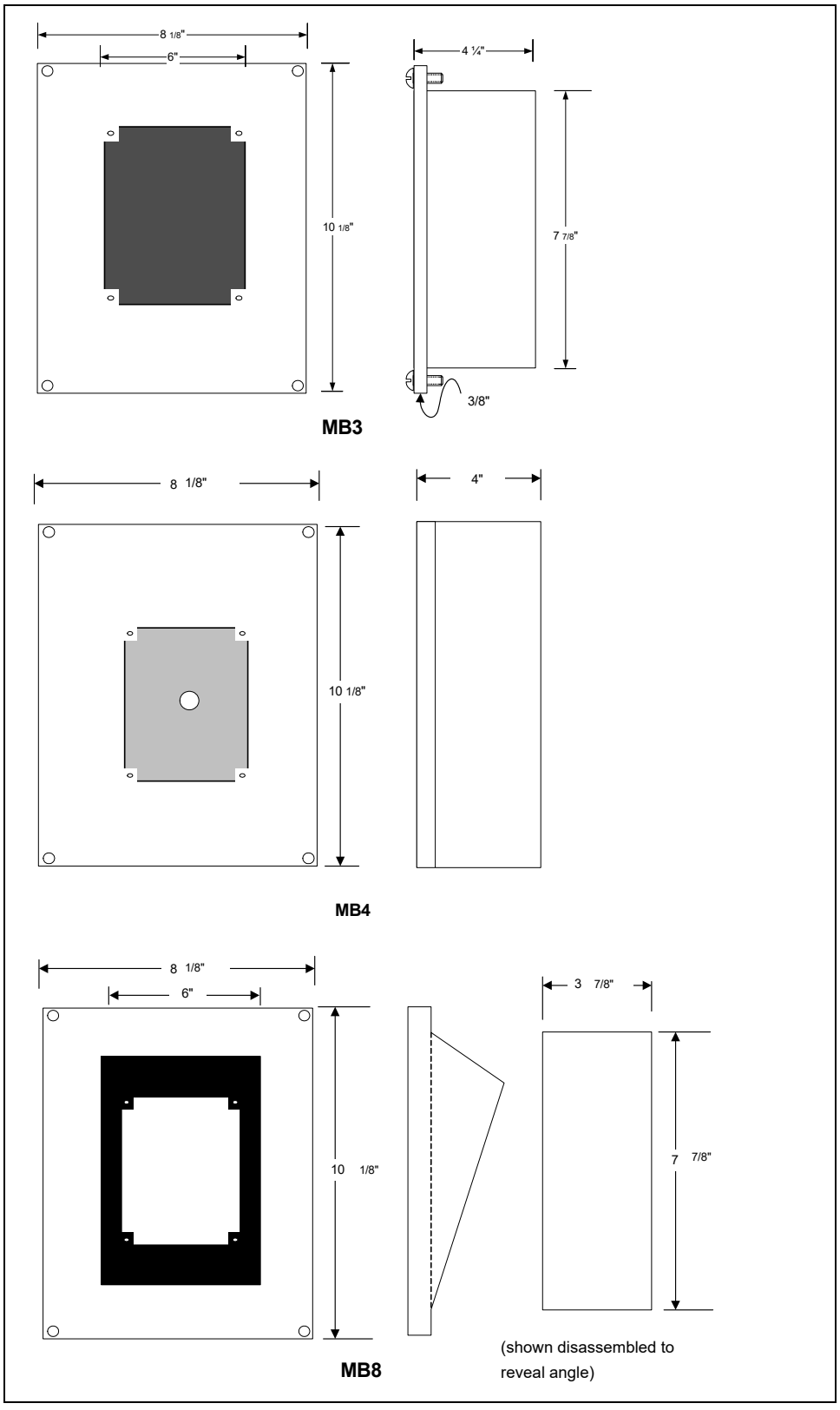


Figure 7-37: ScramblePad Mounting Boxes Dimensions - MB3, MB4 & MB8

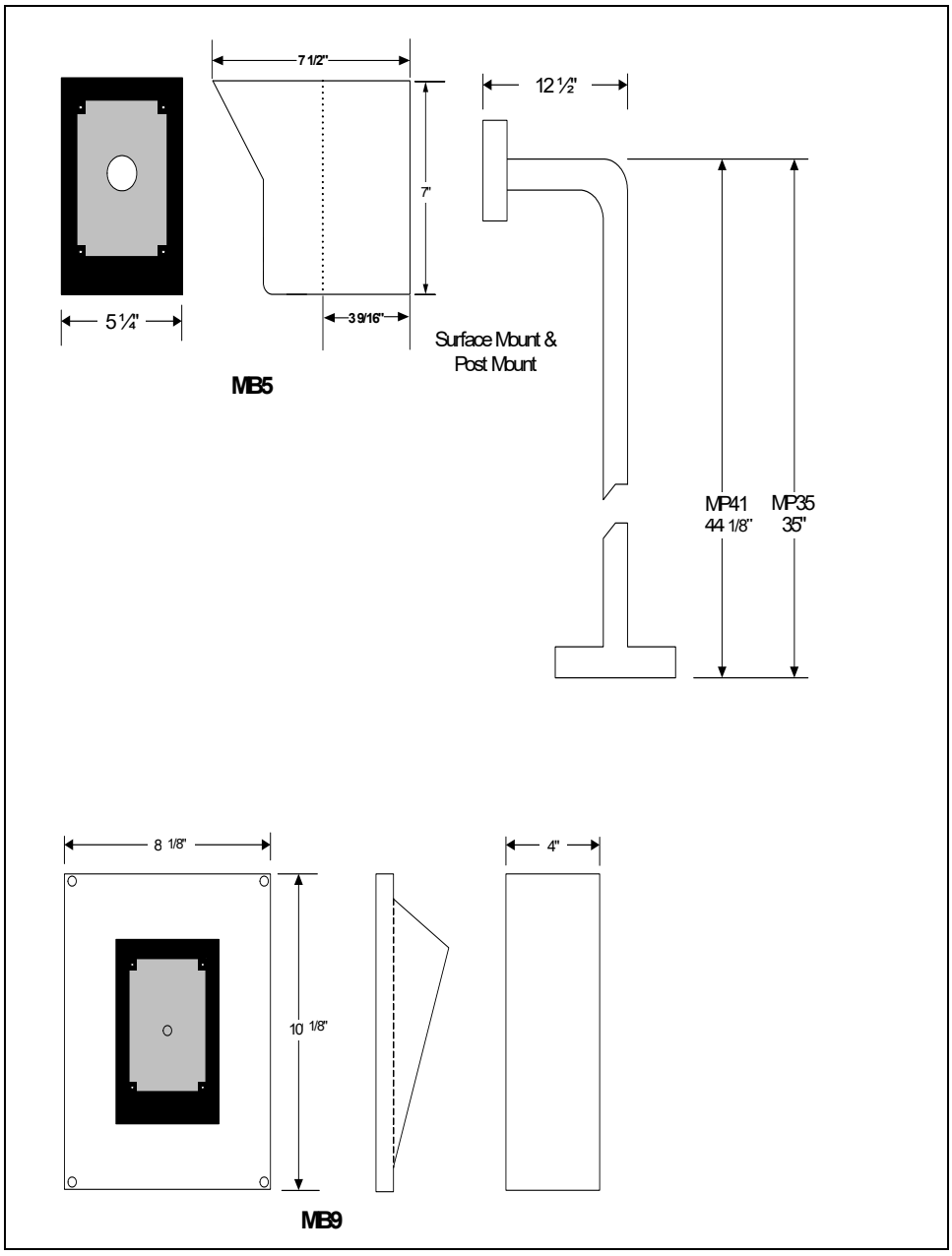


Figure 7-38: ScramblePad Mounting Boxes/Posts Dimensions - MB5, MB9, MP35, and MP41

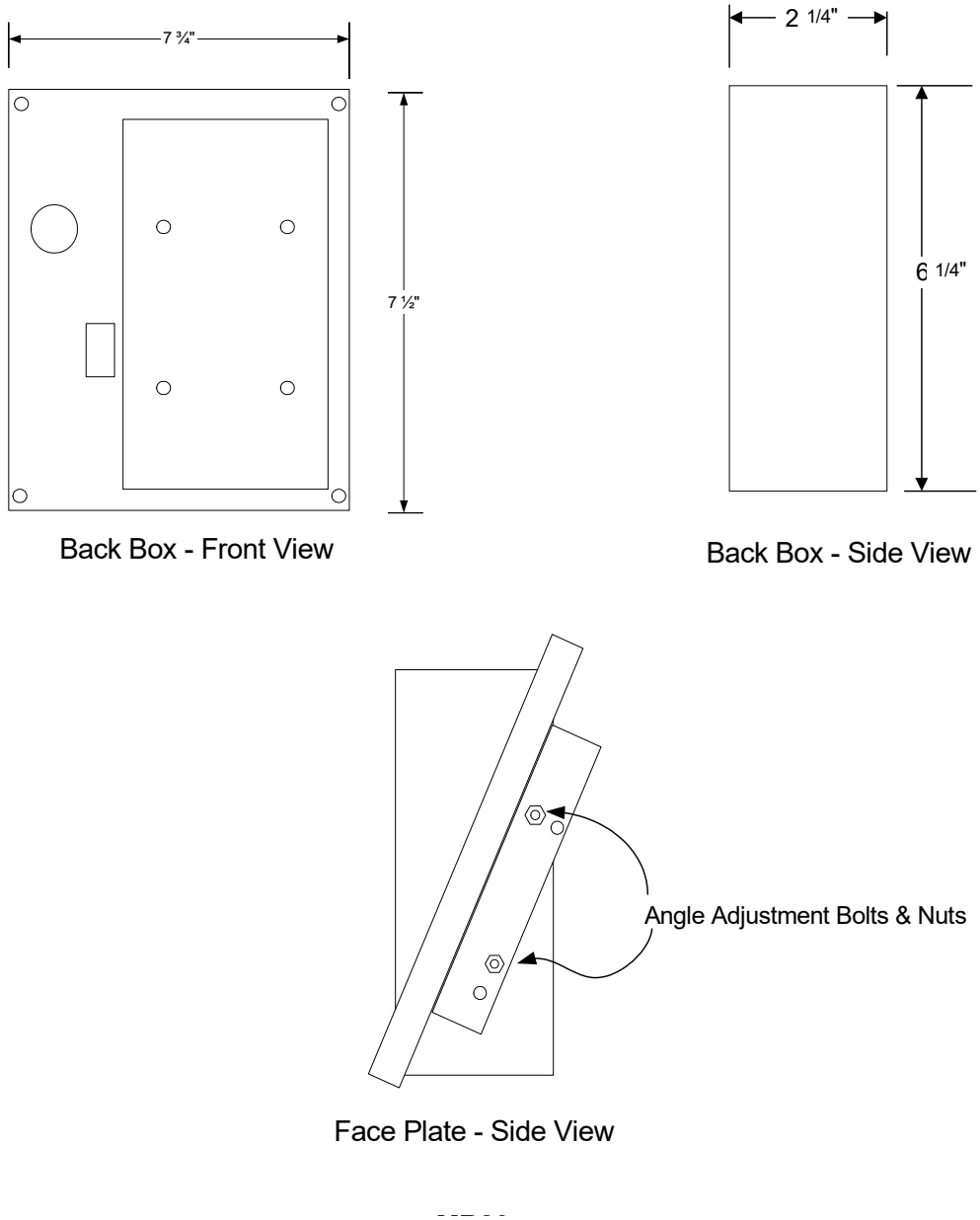


Figure 7-39: ScramblePad and Reader Mounting for MB20

Selecting a Mounting Height

Select the correct mounting height for the construction conditions at each door. If it isn't right, the ScramblePad will be difficult to use properly.

Figure 7-40 shows how the ScramblePad mounting height differs according to the angle of

viewing.

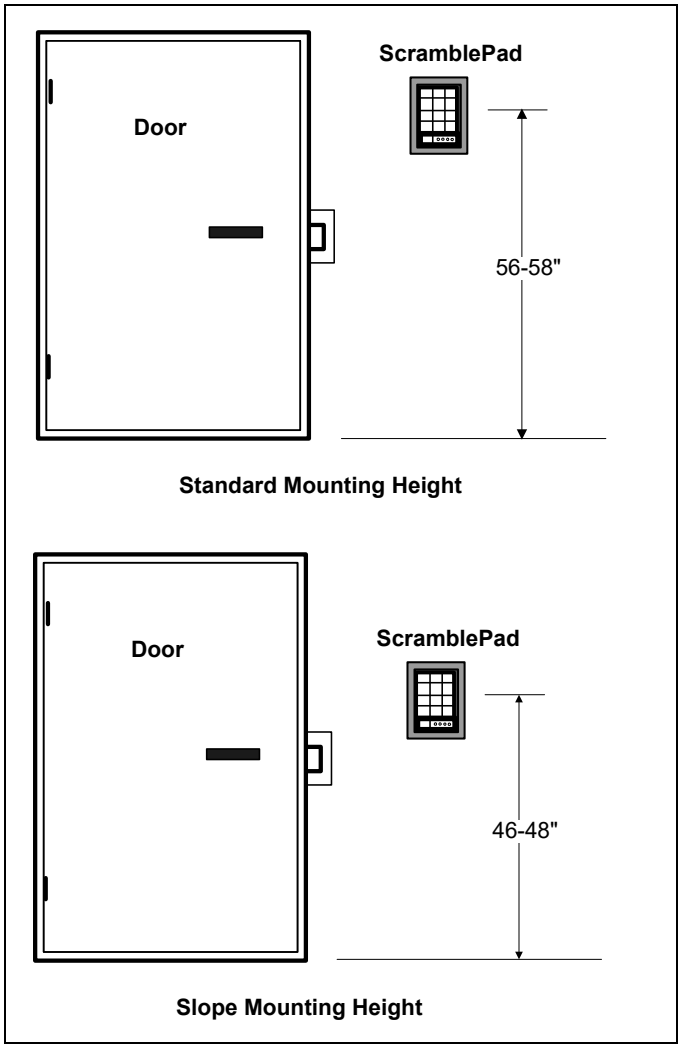


Figure 7-40: ScramblePad Height Adjustment

If users of the ScramblePad or MATCH are handicapped, pay particular attention to the height of the box. Most states require strict compliance with conditions of the ADA (Americans with Disabilities Act) in addition to many local and regional code requirements. Consult the local codes for exact height requirements.

Each box requires slightly different instructions for mounting.

Installation instructions for each box and kit are provided on the following pages.

Installing the MB1

To Mount the MB1:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Use the template included with the MB1 to locate the best possible position for the box. You can also use the template to trace an outline on the wall.

3. Cut a hole in the wall matching the dimensions provided for the MB1 in Figure 7-36 on page 7-99.
4. Locate and pull the cable up to the hole.
5. Thread the cable through one of the holes in the MB1.
6. Insert the MB1 into the hole until it is flush with the wall. Make sure that the wall anchors on top and bottom of the box fit inside the wall.

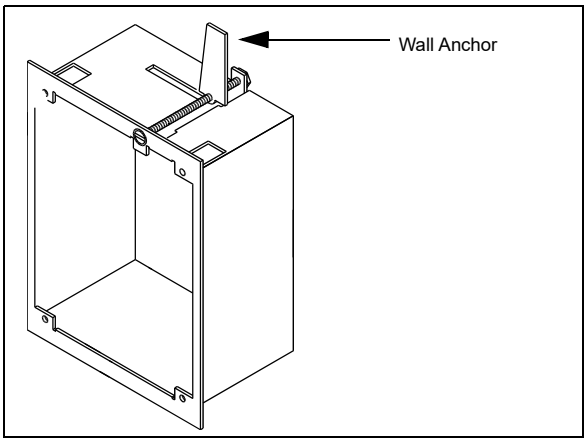


Figure 7-41: Installing the MB1

7. Turn the wall anchor screws (located at the upper right and lower left) until the box is firmly secured.
8. Install the ScramblePad. Refer to “Setting Up ScramblePad” on page 7-114.

Installing the MB2

To Surface Mount the MB2:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Use the conduit hole at the back of the MB2.
3. Hold the back box up to the wall at the intended location and outline the holes at the back of the mounting box on the wall surface. There are six screw holes and one conduit hole.
4. Drill as many of the screw holes in the wall as are required to secure the box. Insert screw anchors, if desired.
5. Pull the conduit through the conduit wall hole, then thread to the MB2 conduit hole.
6. Put the MB2 in position and screw it to the wall.
7. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

Installing the MB2S

To Surface Mount the MB2S:

1. Determine the height which is correct for this location.

   Refer to “Selecting a Mounting Height” on page 7-102.
2. Hold the back box up to the wall at the intended location and outline the holes at the back of the mounting box. There are six screw holes and one conduit hole.

3. Drill out as many of the screw holes as required. Insert screw anchors, if desired.
4. Pull the cable through the larger hole then thread through MB2S conduit nut.
5. Put the MB2S in position and screw it to the wall.
6. Continue with the ScramblePad installation.

Refer to “Setting Up ScramblePad” on page 7-114.

Installing the MB2SL

To Mount the MB2SL:

1. Determine the height which is correct for this location.

   Keep in mind that a sloped box is intended to be viewed from an angle either above or below the reader/keypad position.

   Refer to “Selecting a Mounting Height” on page 7-102.
2. Hold the back box up to the wall at the intended location and outline the holes at the back of the mounting box. There are six screw holes and one conduit hole.

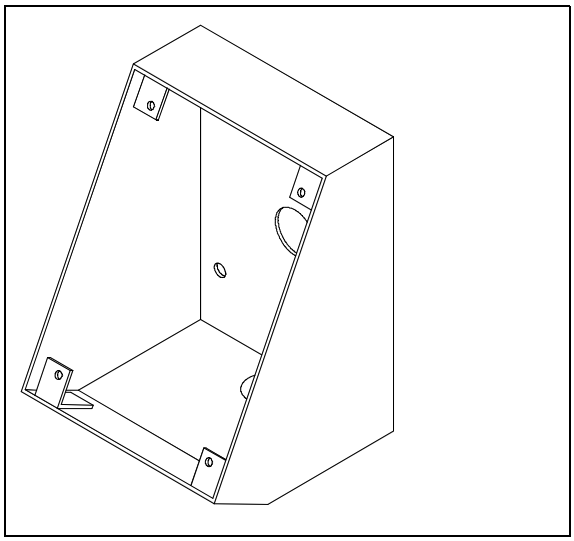


Figure 7-42: MB2SL Box

3. Drill out as many of the screw holes as required. Insert screw anchors, if desired.
4. Pull the cable through the larger hole then thread through MB2SL conduit nut.
5. Put the MB2SL in position and screw it to the wall.
6. Continue with the ScramblePad installation.

Refer to “Setting Up ScramblePad” on page 7-114.

Installing the Universal Mounting Kits

The Universal Mounting Kit (UMK) works with the MB2 to provide three different configurations:

- ❑ Flush
- ❑ Semi-Flush
- ❑ Sloped (Handicap)

The Universal Mounting Kit Shallow (UMKS) works with the MB2S to provide two different configurations:

- ❑ Flush
- ❑ Sloped (Handicap)

The MB2S and UMKS are only suitable for the DS47L-series ScramblePad and ScrambleProx. The DS37L-series ScramblePad is too deep for the MB2S. Each configuration is shown in Figure 7-43:

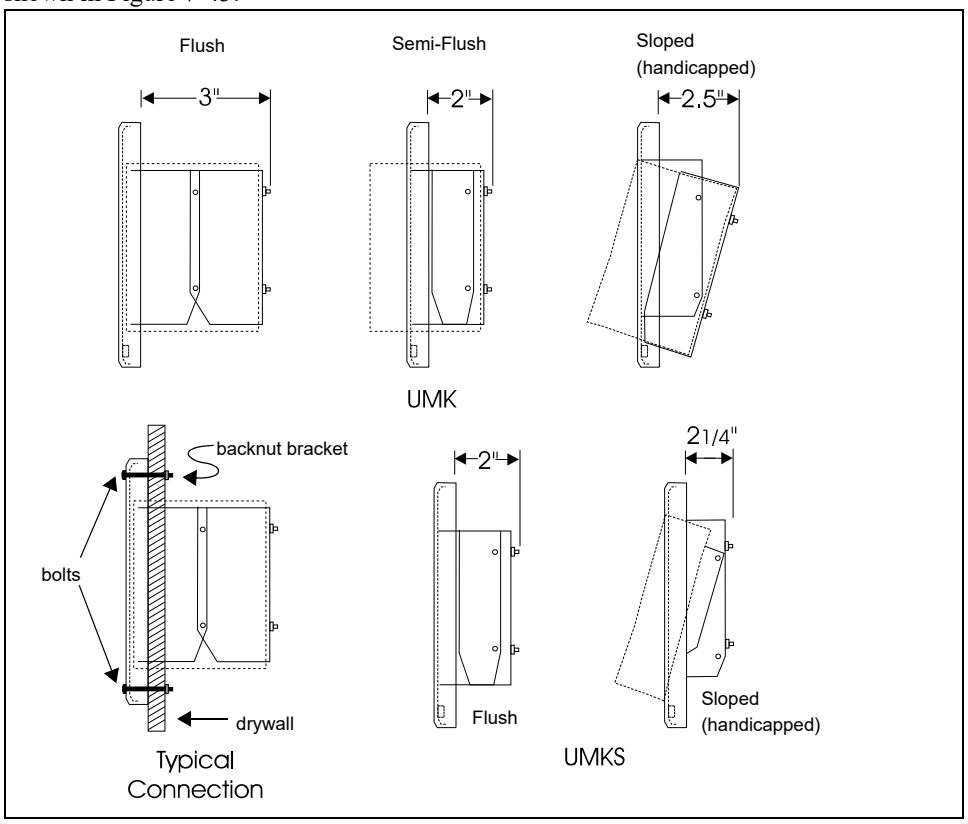


Figure 7-43: UMK/UMKS Configurations

To Mount the MB2 and UMK:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Use the template in Figure 7-44 to cut the wall hole for the UMK/UMKS.

   For the Flush or Semi-Flush UMK/UMKS adaptor, use the solid lower line. For handicap mounting using the tilted UMK/UMKS adaptor, select the dotted lower line.

Note: The UMKS does not use the Semi-Flush configuration.

3. Attach the left and right brackets to the faceplate flanges for flush, semi-flush, or handicap mounts using the 6/32 nuts as shown in Figure 7-45 on page 7-109.
4. For flush and semi-flush face plates only, use the ¼” faceplate insert below the MB2/MB2S for a proper fit.
5. Mount the faceplate-bracket assembly to the wall as shown in Figure 7-43.

   Use the wall backnut brackets and the tamper-proof screws.

6. Route the ScramblePad cable from the controller or MATCH Reader Interface Board through the MB2/MB2S backbox.

   The MATCH Reader Interface Board is included in the DS47L or DS47L-SPX package, so there is no need for an MRIB cable; however, there may be a cable to a reader.

7. Mount the MB2 or MB2S into the faceplate using the 8/32 screws.

8. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

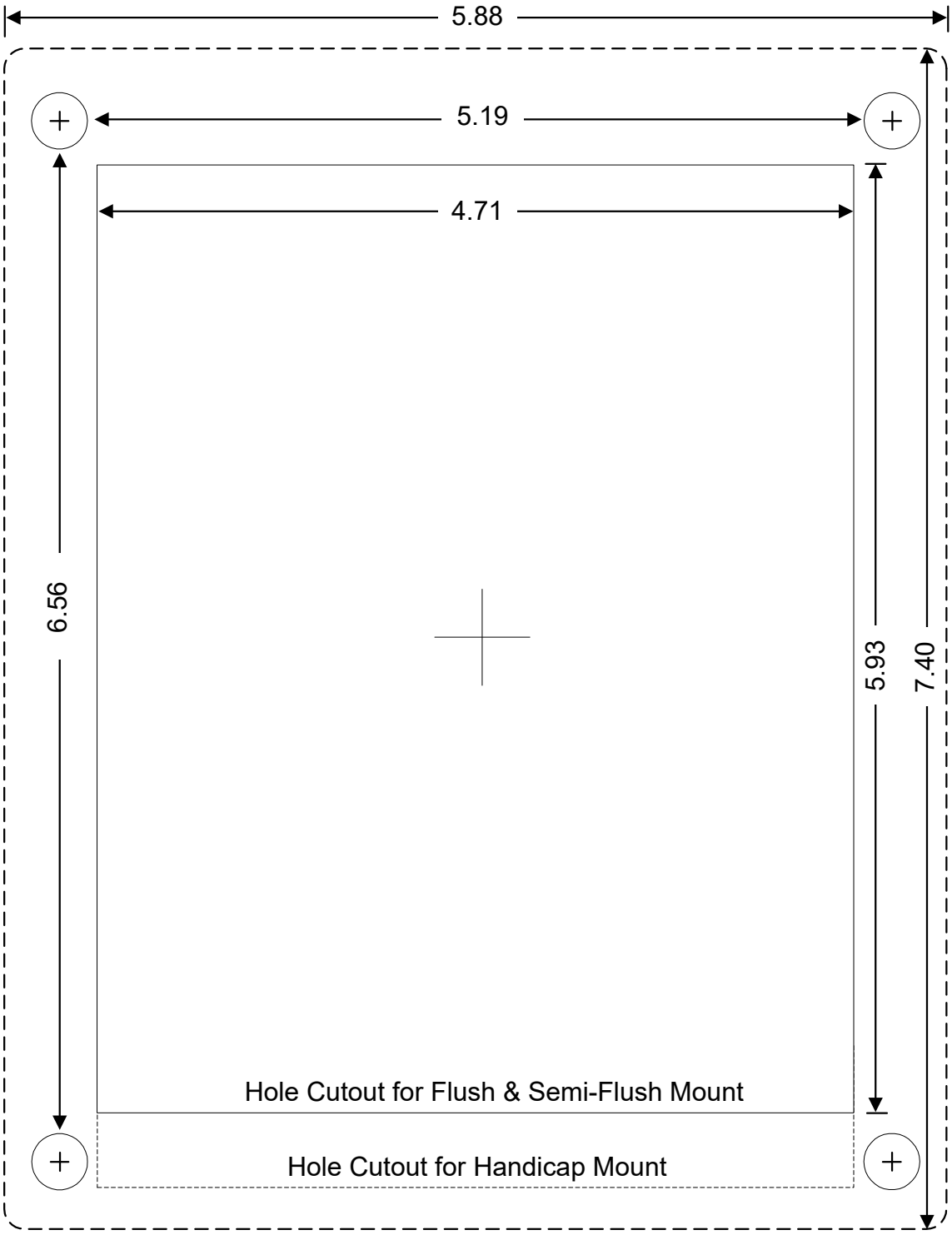


Figure 7-44: UMK/UMKS Template (dimension in inches)

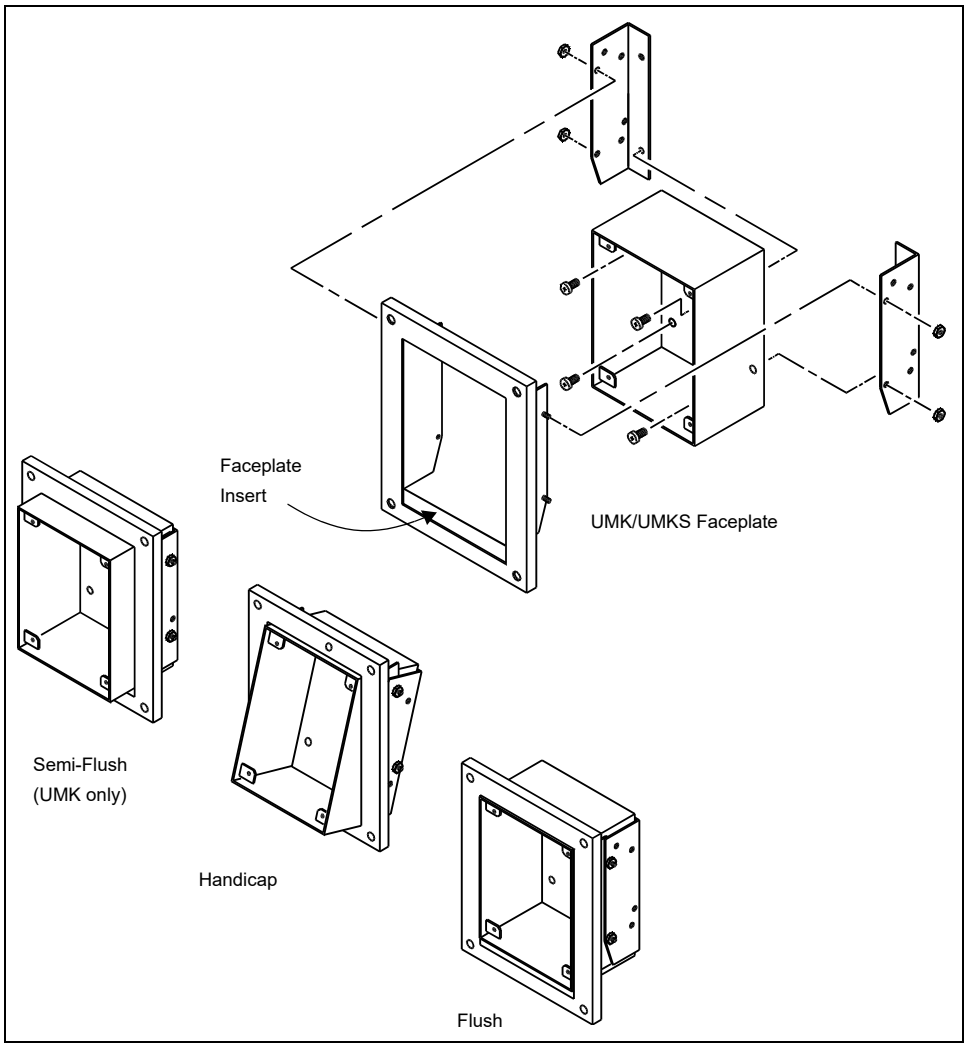


Figure 7-45: Installing an MB2 in a UMK/UMKS Faceplate

Installing the MB3

To Mount the MB3:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Drill or knock out a hole in the MB3 back box for the conduit.
3. Place the MB3 backbox against the wall in the selected location and outline the device.
4. Using the outline, cut a hole in the wall.
5. Pull the appropriate cable up and out of the wall.
6. Attach the spacer plate to the back box with 4 screws as shown in Figure 7-46.
7. Attach face plate to spacer plate as shown in Figure 7-46.
8. Pull cable through knockout and insert assembled MB3 into the wall hole.
9. Secure to the wall with 4 bolts.

10. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

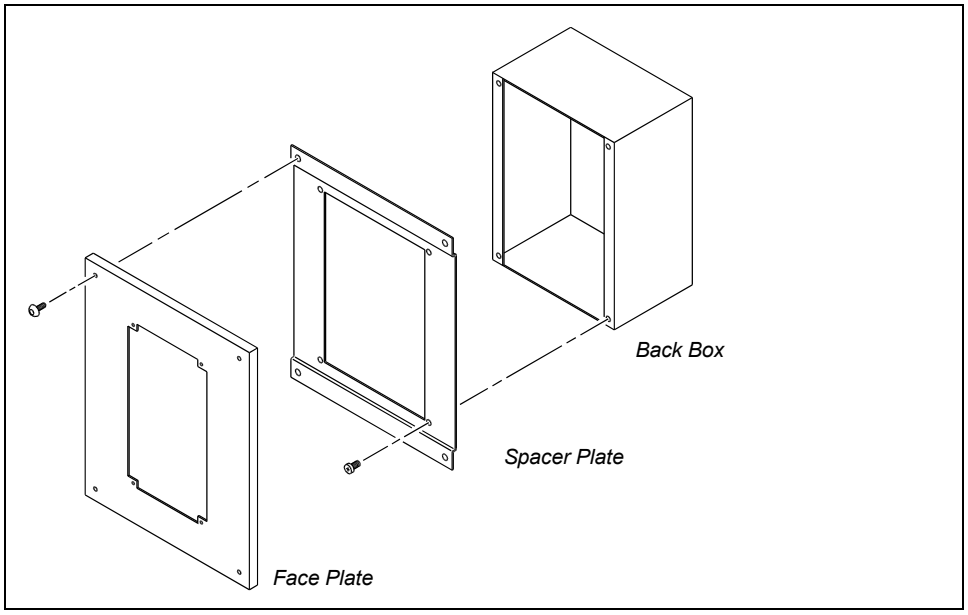


Figure 7-46: Installing the MB3

Installing the MB4

To Mount the MB4:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Knock out the hole in the back of the MB4 back box for the conduit.
3. Place the MB4 backbox against the wall in the selected location and outline the four bolt holes at the back of the box and the knockout.
4. Using the outlined holes, drill five holes in the wall. If required, insert screw anchors into bolt holes.
5. Pull the appropriate cable out of the wall and thread through knockout in back box.
6. Attach the back box to the wall with 4 bolts.
7. Attach face plate to the back box with 4 screws as shown in Figure 7-47.
8. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

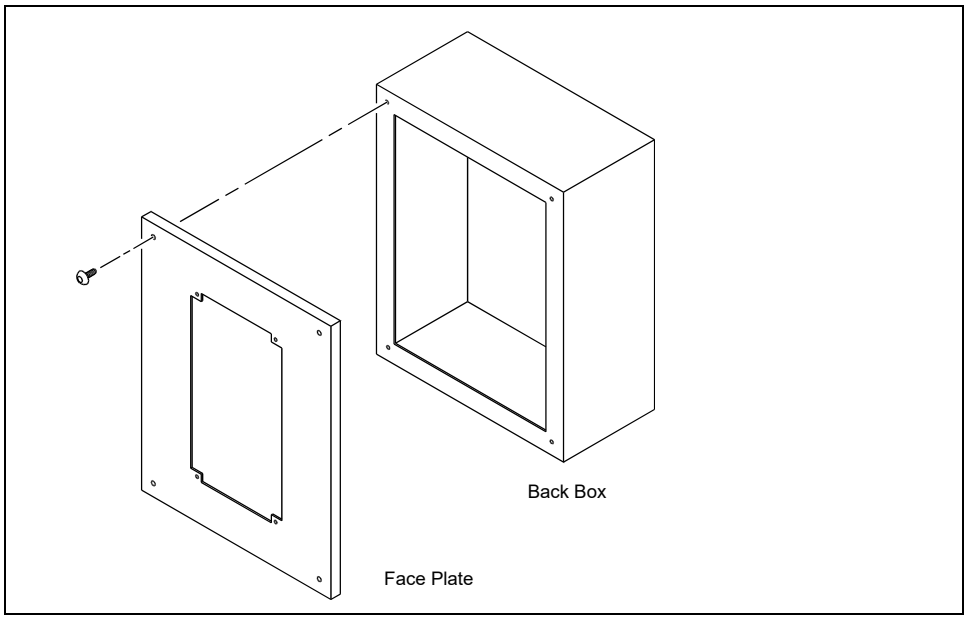


Figure 7-47: Installing the MB4

Installing the MB5 and MP35/MP41 Mounting Posts

The MB5 can either be surface-mounted or post-mounted. Both installations are discussed here.

To Mount the MB5 on a Wall:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Place the MB5 backbox against the wall in the selected location and outline the four bolt holes and the conduit hole at the back of the box.
3. Using the outlined holes, drill five holes in the wall. If required, insert screw anchors into bolt holes.
4. Pull the appropriate cable out of the wall and thread through knockout in back box.
5. Attach the back box to the wall with 4 bolts.
6. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

To Mount the MB5 and MP35/MP41 Mounting Post:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102. The MP35 is 35 inches high while the MP41 is 41 inches. Both mounting posts are 12½ inches deep. Both bases are 5 inches x 6 inches.
2. Place the mounting post in the position required. Outline the post base bolt holes on the ground.
3. Drill the bolt holes into the ground. Since this is usually concrete, asphalt, or some other hard material, be sure to use the appropriate drill. If required, use bolt anchors.
4. Pull the cable to the appropriate location. This can require laying down conduit beneath the surface (before the concrete is poured) or cutting existing concrete/ asphalt and laying down a new cable.

Alternatively, lay metal pipe and conduit across the surface; however, this is not as secure or weather-resistant.

5. Thread cable up through mounting pipe.
6. Bolt the mounting post into place.
7. Pull cable through hole in back of the MB5.
8. Join MB5 to the mounting post with four bolts.
9. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

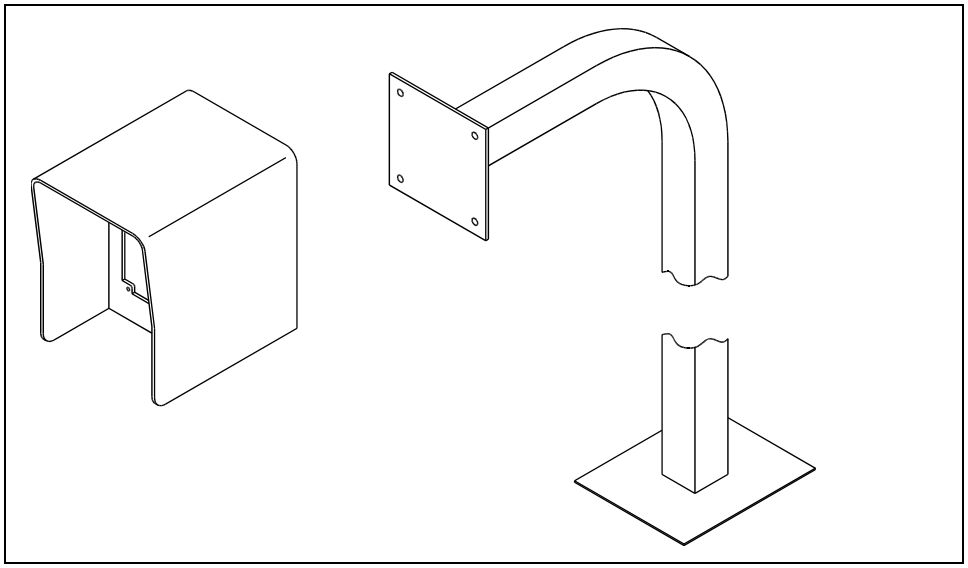


Figure 7-48: Mounting the MB5 and Mounting Post

Installing the MB8

To Mount the MB8:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Drill or knock out a hole in the MB8 back box for the conduit.
3. Place the MB8 backbox against the wall in the in the selected location and outline the device.
4. Using the outline, cut a hole in the wall.
5. Pull the appropriate cable out of the wall.
6. Attach the spacer plate to the back box with 4 screws as shown in Figure 7-49.
7. Attach face plate to spacer plate as shown in Figure 7-49.
8. Pull cable through knockout and insert assembled MB8 into the wall hole until it is flush against wall.
9. Secure to the wall with 4 bolts.
10. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

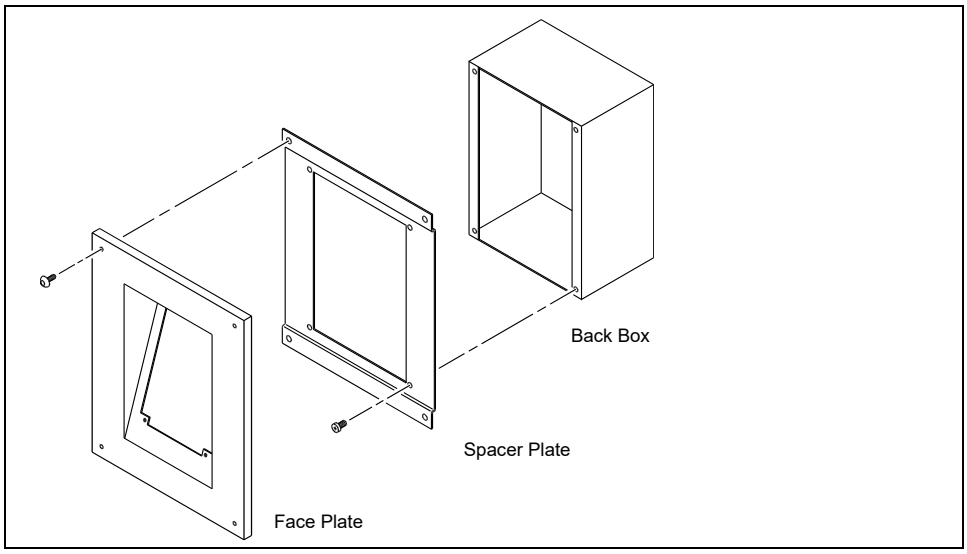


Figure 7-49: Installing the MB8

Installing the MB9

To Mount the MB9:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Knock out the hole in the back of the MB9 back box for the conduit.
3. Place the MB4 backbox against the wall in the in the selected location and outline the four bolt holes at the back of the box and the knockout.
4. Using the outlined holes, drill five holes in the wall. If required, insert screw anchors into bolt holes.
5. Pull the appropriate cable out of the wall and thread through knockout in back box.
6. Attach the back box to the wall with 4 bolts.
7. Attach face plate to the back box with 4 screws as shown in Figure 7-50.
8. Continue with the ScramblePad installation. Refer to “Setting Up ScramblePad” on page 7-114.

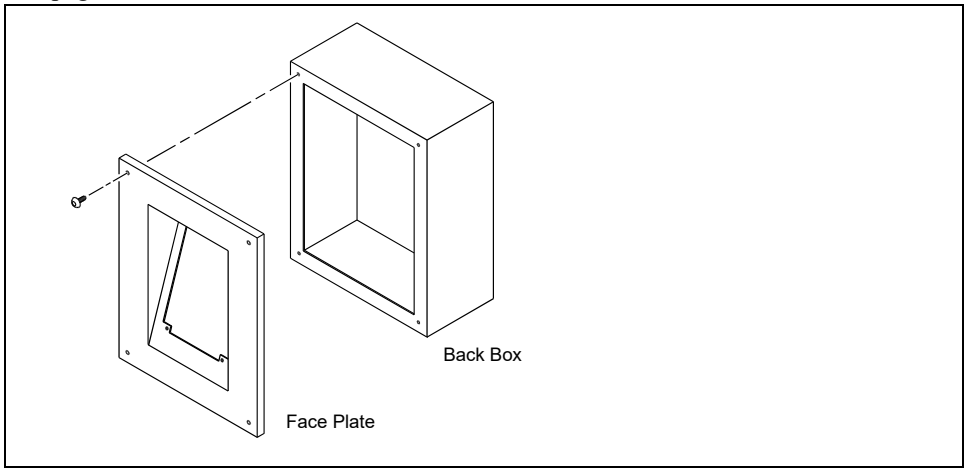


Figure 7-50: Installing the MB9

To continue with the ScramblePad installation, go to the next section: “Setting Up ScramblePad” starting on page 7-114.

Installing the MB20

To Mount the MB20:

1. Determine the height which is correct for this location. Refer to “Selecting a Mounting Height” on page 7-102.
2. Place the MB20 backbox against the wall in the selected location and outline the four bolt holes at the back of the box as well as the central conduit hole in the middle.
3. Using the outlined holes, drill five holes in the wall.

   If required, insert screw anchors into bolt holes.
4. Pull the appropriate cables out of the wall through the large central conduit hole, then thread the cable through the large hole at the back of the box. These cables should service both the keypad and the reader.
5. Attach the back box to the wall with 4 bolts.
6. Before attaching the face plate, adjust the angle of the plate to your requirements. This is done by unscrewing and repositioning the four bolts and nuts that secure the adjustable box to the face plate.
7. Run the required reader cable through the large hole on the front plate.
8. Attach the face plate to the back box with 4 screws.
9. Install the ScramblePad as described in “Setting Up ScramblePad” starting on page 7-114.
10. Attach a reader to the right of the ScramblePad as described in your reader’s documentation.

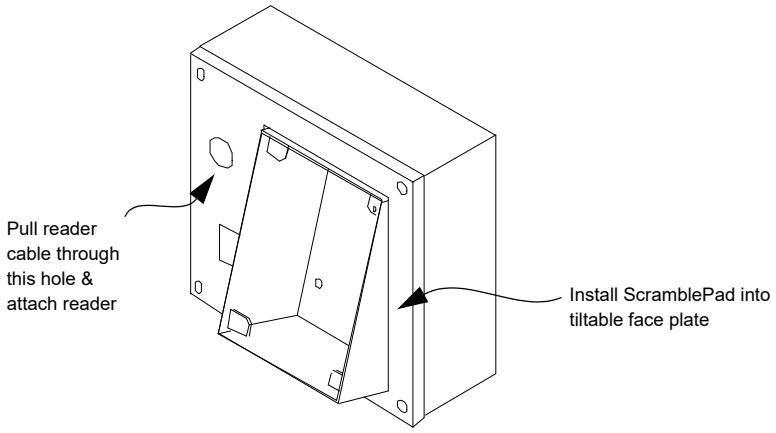


Figure 7-51: Installing MB20

To continue with the ScramblePad installation, go to the next section: “Setting Up ScramblePad” starting on page 7-114.

Setting Up ScramblePad

After you install the mounting boxes, but before you connect the ScramblePad to the cable, you must first configure the ScramblePad.

There are eight DIP switches on the back of the DS37L-series ScramblePads (see Figure 7-52 on page 7-118) and ten on the back of the DS47L-series ScramblePads.

These switches:

- ❑ assign the Address
- ❑ change the Mean Response Time (on the DS37L)
- ❑ enable/disable the Tamper Alarm Function
- ❑ test the unit

DS37L ScramblePad Setup

To setup the DS37L-series ScramblePad:

1. Assign an address to the ScramblePad. Use the chart on the back of the unit to help you determine the correct ID setting.

SW1	SW2	SW3	SW4	ID (Address)	Door
OFF	OFF	OFF	ON	1 (default)	1 entry
OFF	OFF	ON	OFF	2	2 entry
OFF	OFF	ON	ON	3	3 entry
OFF	ON	OFF	OFF	4	4 entry
OFF	ON	OFF	ON	5	5 entry
OFF	ON	ON	OFF	6	6 entry
OFF	ON	ON	ON	7	7 entry
ON	OFF	OFF	OFF	8	8 entry
ON	OFF	OFF	ON	9	1 exit
ON	OFF	ON	OFF	10	2 exit
ON	OFF	ON	ON	11	3 exit
ON	ON	OFF	OFF	12	4 exit
ON	ON	OFF	ON	13	5 exit
ON	ON	ON	OFF	14	6 exit
ON	ON	ON	ON	15	7 exit
OFF	OFF	OFF	OFF	16	8 exit

Table 7-8: ScramblePad Door Assignment Settings

In this binary addressing scheme, SW1 = 8, SW2 = 4, SW3 = 2, and SW4 = 1.

Assign up to a maximum of 16 IDs per controller. IDs do not translate into Doors. The maximum number of doors handled by a Hirsch controller (Model 8) is still eight, but the controller interprets 1 - 8 as entries and 9 - 16 as exits. In this way, you can assign two ScramblePads/MATCHs for each door. For example, assign ID 1 to the entry ScramblePad on Door 1; assign ID 9 to the exit ScramblePad at Door 1.

The controller to which the ScramblePad is connected must read the ID (address) from the ScramblePad before it can act, so it is important that this is set correctly.

Note: If two ScramblePads have the same ID, the system will not operate properly. A flashing red LED on the front of the ScramblePad indicates duplicate ScramblePad IDs.

2. To change the Mean Response Time (MRT) between keystrokes, set SW5 to ON. When ON, the ScramblePad allows 15 seconds between keystrokes; when OFF, it allows 10 seconds between keystrokes.

   If a keystroke is not received in the requisite time, the ScramblePad resets.

3. To enable the ScramblePad Tamper Alarm, set SW6 to ON. When ON, the ScramblePad can detect attempts to tamper with it. If tampering is detected, all LEDs on the face flash red and the ScramblePad is disabled and an alarm is generated in the controller.

4. Set SW7 and SW8 to enable two different test procedures.

   SW7 = ON initiates the switch test. All keys are tested by pressing each key. The LEDs at the bottom will give the key number in binary. (The # key is identified as 10, the * key is 11, and the START key is 12.)

   SW8 = ON causes the LEDs to blink in sequence and all segments of each LED displays an 8.

DS47L ScramblePad/ScrambleProx Setup

To setup the DS47L-series ScramblePad/ScrambleProx:

1. Assign an address to the ScramblePad using SW1 – SW4. Refer to Table 7-8 on page 7-115.

   Assign up to a maximum of 16 IDs per controller. IDs do not translate into Doors. The maximum number of doors handled by a Hirsch controller (Model 8) is still eight, but the controller interprets 1 - 8 as entries and 9 - 16 as exits. In this way, you can assign two ScramblePads/MATCHs for each door. For example, assign ID 1 to the entry ScramblePad on Door 1; assign ID 9 to the exit ScramblePad at Door 1.

   The controller to which the ScramblePad is connected must read the ID (address) from the ScramblePad before it can act, so it is important that this is set correctly.

Note: If two ScramblePads have the same ID, the system will not operate properly. A flashing red LED on the front of the ScramblePad indicates duplicate ScramblePad IDs.

2. If required, enable dual readers by setting SW5 to ON. This enables the DS47L or DS47L-SPX to connect to a second reader for entry and exit applications.

Note: For dual entry, dual exit applications with a DS47L ScramblePad, use two ScramblePads, each with a single reader, and SW5 set to OFF (disabled).

3. Specify whether the readers attached to Reader 1 and Reader 2 ports are Wiegand or ABA Track 2 Mag Stripe by setting SW6:

   OFF = ABA Track 2 Mag Stripe
   ON = Wiegand

Note: If two readers are attached, then both readers must be either Wiegand or Track 2 Mag Stripe.

4. Specify whether the readers attached to the reader ports are Insert or Swipe by setting SW7:

   OFF = Swipe
   ON = Insert

Note: If two readers are attached, both readers must be either Swipe or Insert.

5. Enable the Physical Tamper Alarm by setting SW8 to 1 (ON). When ON, the ScramblePad/ScrambleProx can detect attempts to tamper with it. If tampering is detected, all LEDs on the face flash red and the ScramblePad is disabled.
6. Set SW9 and SW10 to enable two different test procedures.

   OFF causes the LEDs to blink in sequence. All segments of each LED displays an 8. ON initiates the switch test. All keys are tested.
7. Set SW10 = ON to enable test modes.

   SW10 must be enabled before SW9 can run either test.

Wiring the ScramblePad

After you've set up the ScramblePad/ScrambleProx, it's time to route and connect the cable linking the ScramblePad to the controller.

For more about powering a ScramblePad locally, refer to "Powering the ScramblePad Locally" on page 7-125. For more about powering a MATCH locally, refer to "Powering the MATCH Locally" on page 7-143.

To wire the ScramblePad to the Controller:

1. Connect cable runs from the controller to the access control points for each ScramblePad at each door (as shown in Figure 7-55).

   Recommended cable for both DS37L- and DS47L-series ScramblePads is 2-pair, stranded, twisted, shielded cable, either 22 AWG or 18 AWG. Overall shield or individual shielded pairs are acceptable. Color coded cable – black, red, green, and white – is recommended. Pair 1, black and red, provide power to the ScramblePad; pair 2, green and white, provide data communications between the ScramblePad and the Controller. Digital signals are sent to the controller from the ScramblePad over the cabling—cable must be protected from surges, spikes and noise normally found on electric lock cables.

   For information on wiring distances and connecting entry/exit or dual technology ScramblePads, refer to Table 2-5 and Table 2-6 starting on page 2-16.

Note: Use conduit where required by law.

   Two ScramblePads at the same door can share the same cable.

Note: Do not run ScramblePad cable with lock cables unless you are using shielded, twisted pair cable for the lock cable.

2. Remove the green plastic connector from the back of the ScramblePad and loosen screws on all connector slots.
3. Insert each wire into the ScramblePad connector as shown in Table 7-9, Figure 7-52, and Figure 7-53:

Connector	Wire Color/Type	Connects to this Controller Slot:
1	Black	G
2	Red	+
3	Green	A

Table 7-9: ScramblePad Connector Orientation

Connector	Wire Color/Type	Connects to this Controller Slot:
4	White	B
5	Shield	S

Table 7-9: ScramblePad Connector Orientation (Continued)

Use Figure 7-52 to aid you with the cabling the DS37L-series ScramblePads.

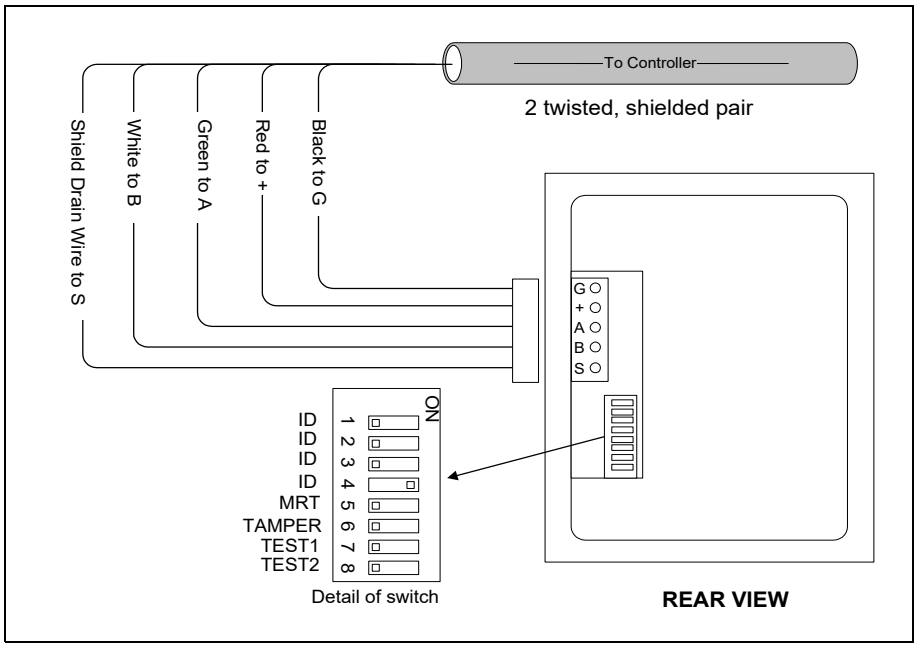


Figure 7-52: DS37L-Series ScramblePad Setup and Wiring

Use Figure 7-53 to aid you with the cabling the DS47L-series ScramblePads.

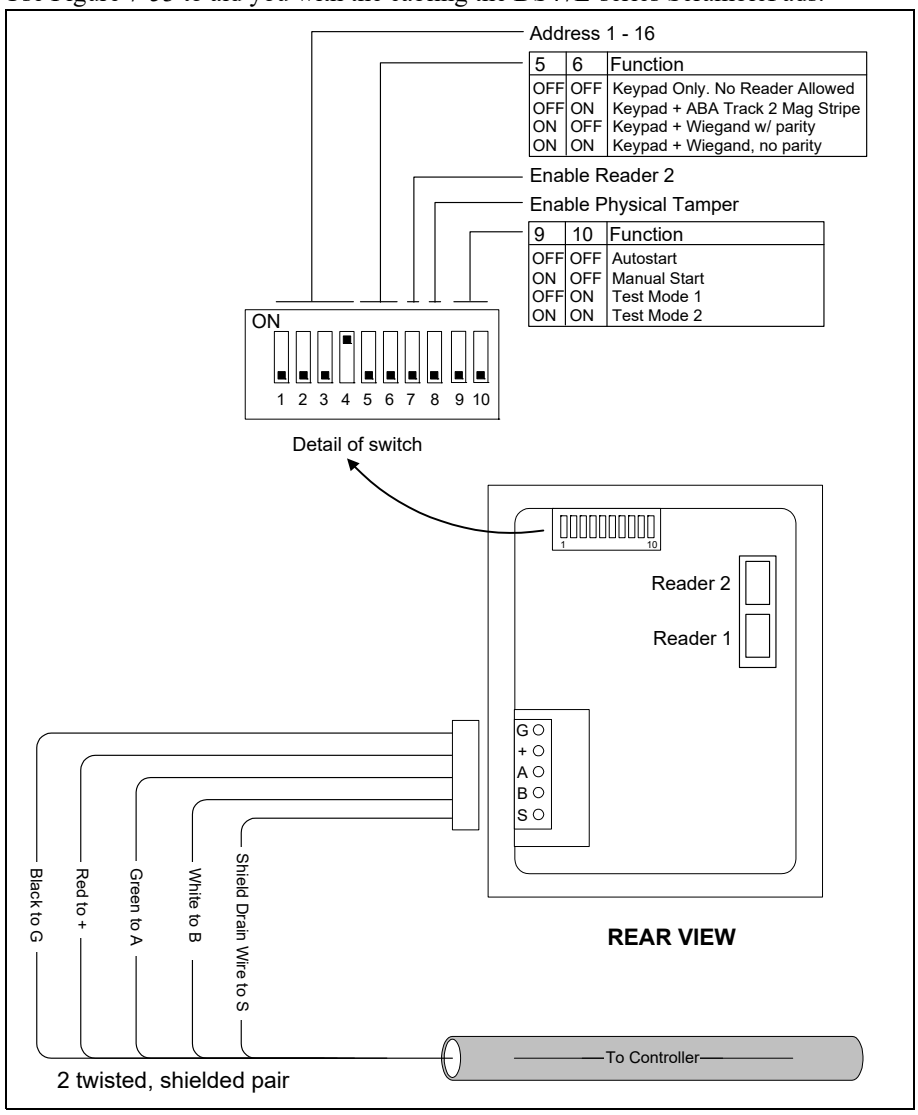


Figure 7-53: DS47L-Series ScramblePad Setup and Wiring

SW5 - SW10 settings for the DS47 differ depending on the generation being used.

*Note: To determine which firmware version you are using, press the * and # keys on the ScramblePad.*

The most recent DS47 ScramblePad generation (firmware versions 980313, 980103, and 971102) is displayed in Figure 7-53 and also in Table 7-10:

Switch	Meaning		
5-6	SW5	SW6	Reader Data Format
	OFF	OFF	MATCH disabled. No readers can be attached.
	OFF	ON	ABA Track 2 Mag Stripe
	ON	OFF	Wiegand, 25-55 bit with parity. For prox card readers
	ON	ON	Wiegand, 25-55 bit, without parity
7	OFF (default) = 1 card reader, ON = Reader 2 enabled (support 2 card readers)		
8	OFF = No physical tamper, ON = Physical tamper enabled		
9-10	SW9	SW10	Start State
	OFF	OFF	Auto-Start. SW5-6 must be set to support MATCH function when card reader plugged into the first connector. For more, refer to “Auto-Start” on page 7-124.
	ON	OFF	Manual Start.
	OFF	ON	Test Functions.

Table 7-10: MATCH SW5 - SW8 Settings (Versions 980313, 980103, and 971102)

The previous DS47L ScramblePad (firmware version 971023 and 971024) settings are shown in Table 7-11:

Switch	Meaning		
5-6	SW5	SW6	Reader Data Format
	OFF	OFF	MATCH disabled.
	OFF	ON	Mag Stripe (ABA format)
	ON	OFF	Wiegand Swipe. For prox card readers
	ON	ON	Wiegand Insert/Reverse
7	OFF (default) = 1 card reader, ON = Reader 2 enabled (support 2 card readers)		
8	OFF = No physical tamper, ON = Physical tamper enabled		
9-10	SW9	SW10	Start State
	OFF	OFF	Auto-Start. SW5-6 must be set to support MATCH function when card reader is plugged into first connector. For more, refer to “Auto-Start” on page 7-124.
	ON	OFF	Manual Start.
	OFF	ON	Test Functions.

Table 7-11: MATCH SW5 - SW10 Settings (Version 971023 and 971024)

The original release of the DS47 (firmware version before 970923) settings are shown in Table 7-12:

Switch	Meaning		
5	OFF (default) = 1 card reader, ON = Reader 2 enabled (support 2 card readers)		
6-7	SW6	SW7	Reader Data Format
	OFF	OFF	MATCH disabled.
	OFF	ON	Mag Stripe (ABA format)
	ON	OFF	Wiegand Swipe. For prox card readers
	ON	ON	Wiegand Insert/Reverse
8	OFF = No physical tamper, ON = Physical tamper enabled		
9-10	SW9	SW10	Mode
	OFF	OFF	Normal operation.
	ON	ON	Test mode

Table 7-12: MATCH SW5 - SW10 Settings (Prior to Version 971023)

The insertion technique is shown in Figure 7-54:

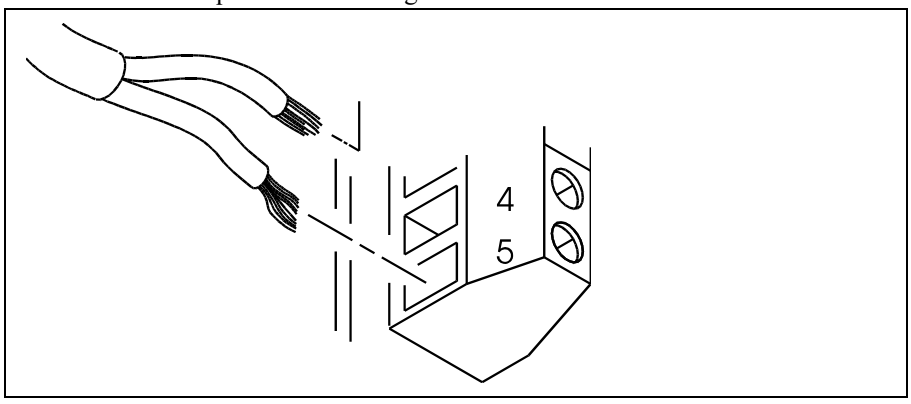


Figure 7-54: Inserting Wires into the Terminal Block Connector Slots

4. Tighten the screws on each connector until the wires are securely fastened.

5. Plug the green connector into the keyed ScramblePad connector socket as shown in Figure 7-55.

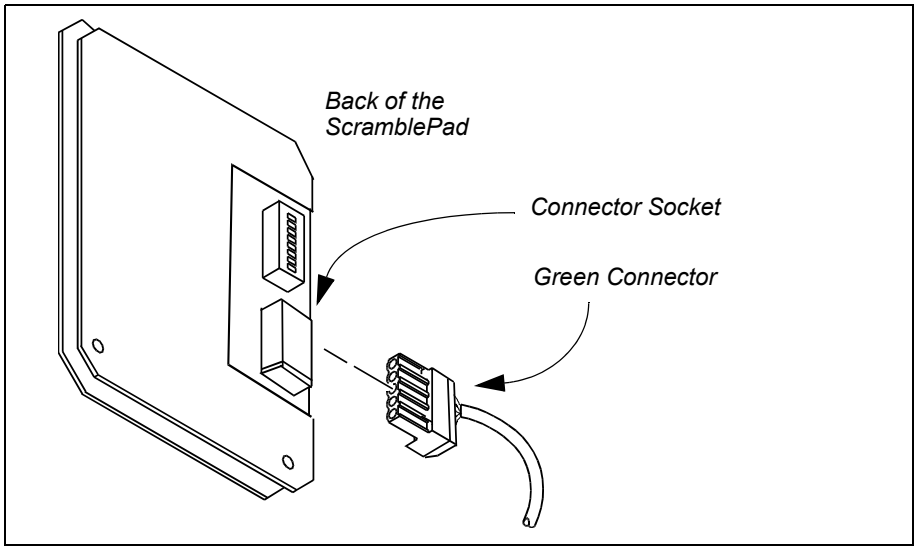


Figure 7-55: Plugging the Terminal Block Connector into the ScramblePad

6. If this is a DS47L, connect one or two card readers to the Reader 1 and Reader 2 ports as described in "Readers Setup" starting on page 7-145. Because the DS47L-series ScramblePads have integrated MATCH Reader Interfaces, connect each reader cable to the back of the DS47L just as you would to the back of an MRIB.
7. If this is a DS47L-SPX, the Reader 1 port is already connected to the integrated proximity reader. Connect a second reader to the Reader 2 port.
8. Use the supplied screws to mount the scramblepad into the mounting box as shown in Figure 7-56.

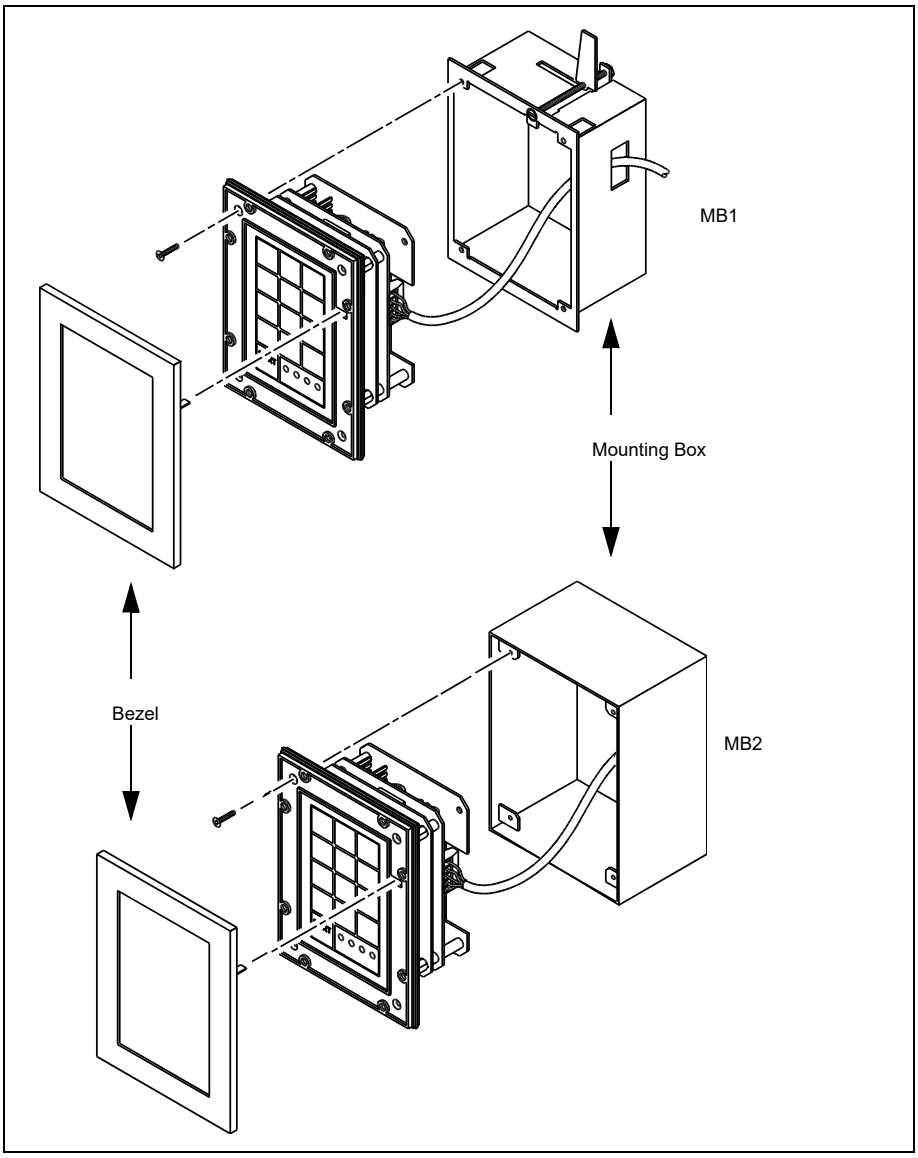


Figure 7-56: Mounting the ScramblePad Examples (MB1 and MB2)

If this is an MB3, MB4, MB5, MB8 or MB9 for outdoor use, insert a heavy-duty weather gasket (Hirsch # HB-HDG) between the Scramblepad and the box as shown in Figure 7-57.

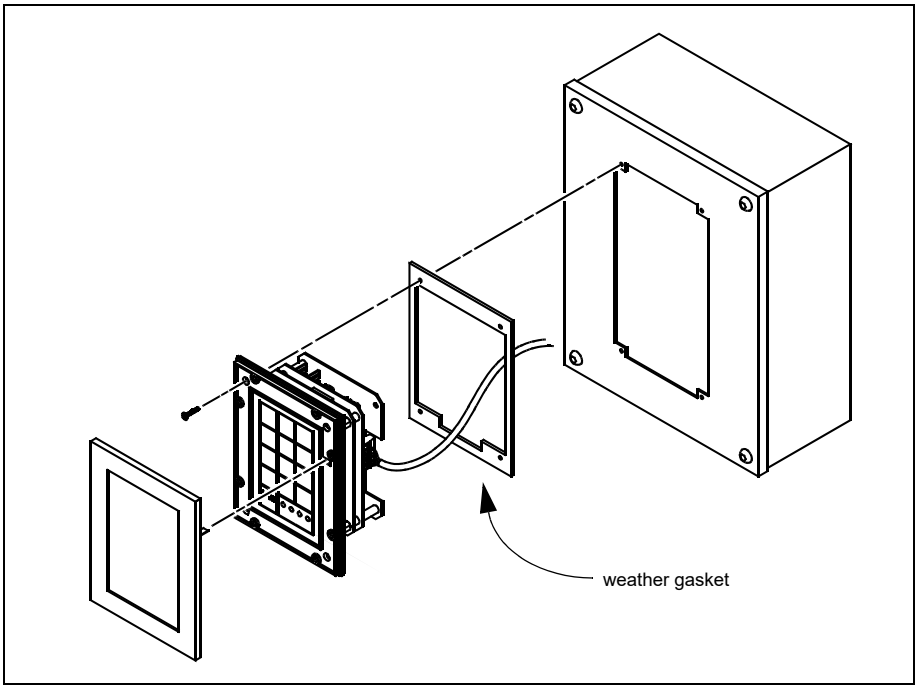


Figure 7-57: Mounting the ScramblePad with Weather Gasket

9. Secure the bezel to the ScramblePad as shown in Figure 7-57.

Auto-Start

The Auto-Start function only works if the DS47's MATCH functionality is enabled, using SW5-6. If SW5-6 are set to OFF-OFF—that is, if the DS47 is configured to act like a DS37—the ScramblePad will not auto-start. The auto-start feature works with any type of reader plugged into the MATCH connector.

When using CCM version 6.5.xx, the new DS47 with auto-start enabled doesn't change the way DIGI*TRAC firmware handles dual codes. Under normal dual operation, both the MATCH and DS47 keypad accepts a card code, then waits for the send (#) key to be pressed. Under CCOTZ operation, the MATCH or DS47 sends the card code immediately to validate the code. In this situation, the DS47 does not auto-start.

When using CCM version 6.6, the ScramblePad provides "Smart Auto-Start" capability. When you present a card, the firmware immediately tries to validate it. If the code is valid, it grants access. If the card's code is present in the code record database, it processes it appropriately. If the card's code is invalid, the firmware blinks the yellow LED once and automatically starts up the ScramblePad. When a ScramblePad code is entered, the firmware attempts to process the card code and the ScramblePad code as a dual code, granting or denying access based on that combination.

Powering the ScramblePad Locally

Most of the time, the Controller provides sufficient power to run an attached ScramblePad. However, there are conditions which require more power than the Controller can supply. This can occur when more than the supported number of ScramblePads are connected to the Controller; or if the cable connecting the Controller to the ScramblePad exceeds the distance limitations specified in Table 2-5 on page 2-16.

When this happens, you should connect a local 24VDC power supply with battery backup into the ScramblePad's connector. To do this:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Locate a 12VDC - 27VDC (for normal ScramblePad) or 18VDC - 27VDC (for high-intensity ScramblePad) power supply (1 Amp) near the ScramblePad.
3. Run a pair of wires (usually twisted, shielded pair) from the power supply to the ScramblePad.
4. Connect the GND and + connectors at the power supply end.
5. Remove the ScramblePad terminal block from the ScramblePad's.
6. If the Controller is already connected to the ScramblePad, disconnect the + (Red) wire. It will not be used.
7. Rewire the block in this way:
   - Attach a GND wire from the auxiliary power supply to the G terminal on the ScramblePad terminal block, along with the G (black) wire from the Controller.
   - Attach a red wire from the power supply to the + terminal on the ScramblePad.
8. Power up the system. Figure 7-58 provides a view of this arrangement:

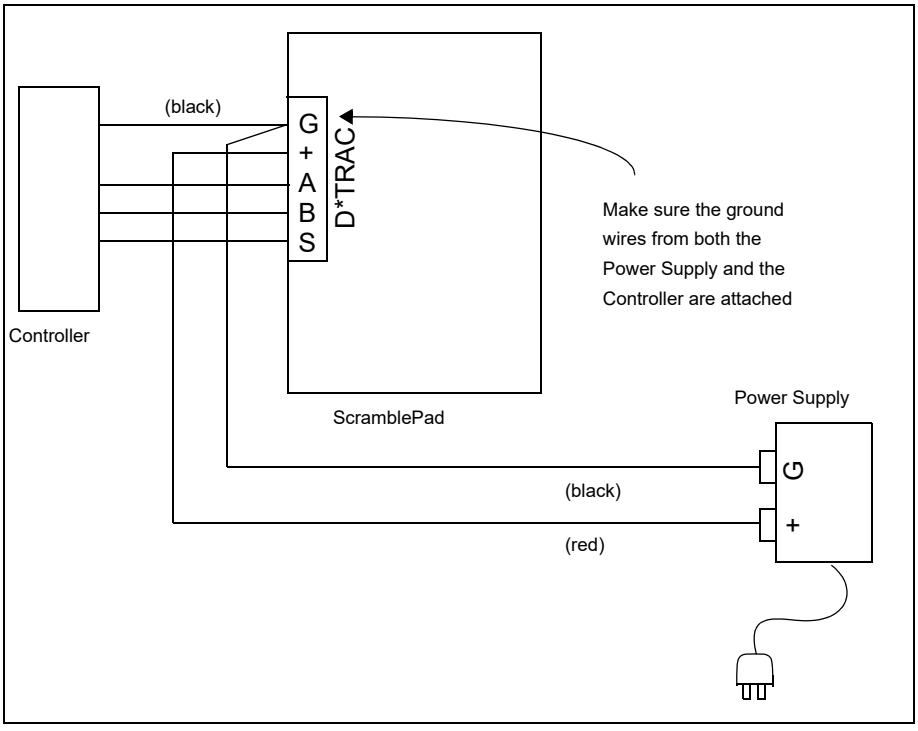


Figure 7-58: Powering the ScramblePad Locally

Testing the ScramblePad

Use the ScramblePad to request a status check. To request status, press:

```
START * #
```

This displays the status of the relay and line module input associated with the ScramblePad ID from which the request was entered.

To request the status of any specific relay and line module input connected to the controller, press:

```
START * door relay/line module input (1 - 8) #
```

For example, to display the status of Relay 8 and Alarm 8 from any ScramblePad, press:

```
START * 8 #
```

This displays the status of Relay 8 and Alarm 8.

ScramblePad status reports are returned to and can be read from the ScramblePad LEDs as shown in Table 7-13:

LED Condition	Meaning
Red LED ON Steady	Line Module Input Unmasked (armed)
Red LED Flashing, Tone ON	Alarm is Active
Red LED OFF	Alarm is Masked (disarmed)
1st Yellow LED ON	Line Module Input is Disabled
2nd Yellow LED ON	Line Module Input is Unsecure (door open, sensor active)
2nd Yellow LED OFF	Line Module Input is Secure (door closed, sensor inactive)
Green LED ON	Relay Active
Green LED OFF	Relay Inactive

Table 7-13: ScramblePad Status LEDs

Figure 7-59 shows the ScramblePad LEDs:

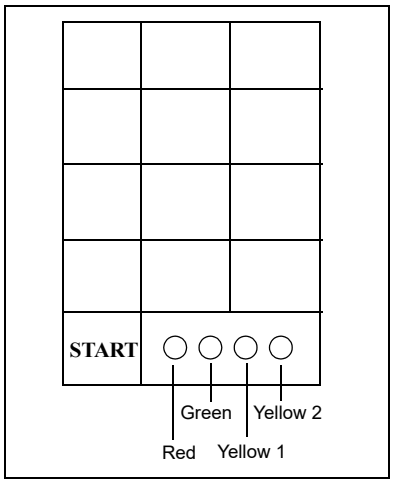


Figure 7-59: ScramblePad LEDs

For more about troubleshooting ScramblePads, refer to “Troubleshooting the Controller Using Status LEDs” on page 7-382.

ScramblePad Maintenance

The only required maintenance for ScramblePads is a regular cleaning of the key face. Over time the key face can become dirty from a mixture of finger oil and acids along with normal dust and dirt. If regular cleaning is not performed, the key face will eventually require replacement. Clean with a non-abrasive cleaner, such as Simple Green.

Also, key faces on exterior ScramblePads in bright sunlit installations will eventually discolor from the sun’s UV rays. Once discolored, the key face should be replaced.

Verification Station Installation

The RUU-201 Verification Station can be connected to your security system in several different ways:

- ❑ Station to DIGI*TRAC controller via MATCH 2 card using Wiegand wiring
- ❑ Station to Velocity Host using Ethernet cable
- ❑ Station to Velocity Host using RS-485 serial wiring

Note: Most configurators will connect the Verification Station to their security system either through Wiegand wiring or Ethernet cabling.

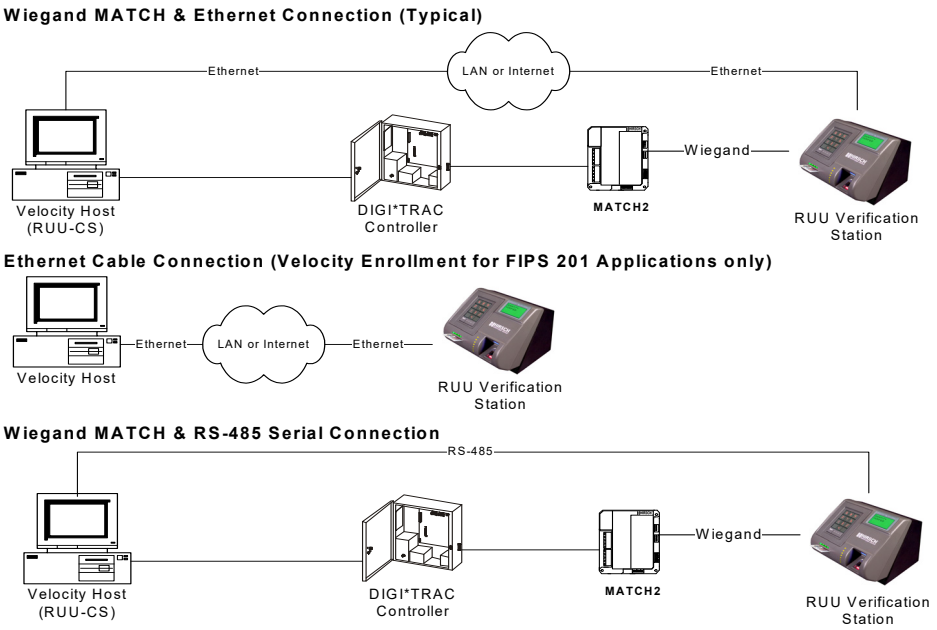


Figure 7-60: Typical Verification Station Systems

Each of these approaches is explained on the following pages.

Wiring for Wiegand MATCH Connection

Many Hirsch DIGI*TRAC security system users will choose to connect the Verification Station to their system by wiring the station to the nearest DIGI*TRAC™ controller via a MATCH™ 2 board, using established Wiegand technology.

Before you can use this connection scheme, you must have:

- ❑ a fully installed, connected, and configured DIGI*TRAC controller (such as an M1N, M2, or M8)
- ❑ a MATCH 2 board that has been previously connected to the controller
- ❑ a Velocity host that is connected to the security system that includes the specified controller

Once these requirements are met, you can connect the station in this manner:

1. Set MATCH 2 DIP switches as shown below:

Bank 1	SW4, 7, 8 ON, all others OFF
Bank 2	As required: 18 for GSA + MATCH code 20 for GSA + Pass-through (no parity) 22 for GSA + Pass-through (with parity)

2. Customize a cable and connect the MATCH 2 block terminal to the Verification Station as shown below.

Connect MATCH wire:	**To Station connector:**
1 DATA 1 (white)	Wieg Out 1 (J7_2)
2 STRAP (black w/ white) and 6 GND (black)	Wieg GND (J7_3)
3 DATA 0 (green)	Wieg Out 0 (J7_1)

3. Connect power to the Verification Station in one of two ways:
   - Plug the included DC power block into the nearest electrical outlet and the other end into the station's power connector.
   - Wire a previously installed 12 VDC power supply to the back of the station in this way:

Connect Wire:	**To Station Connector:**
GND (black)	GND (J6_2)
+ (red)	Power In (J6_1)

An illustration of this process is shown in Figure 7-61.

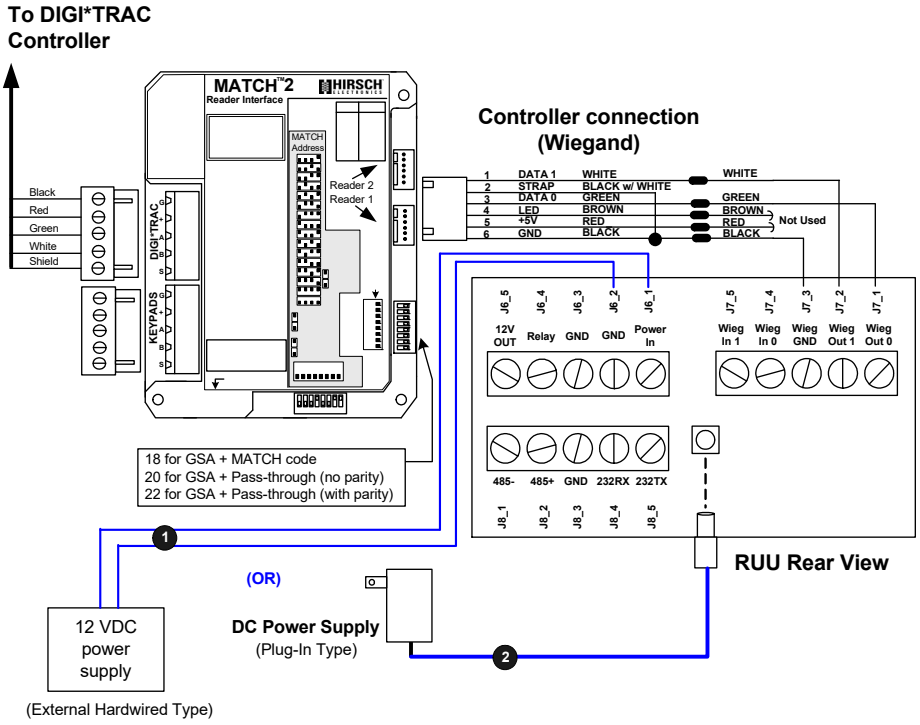


Figure 7-61: Wiegand MATCH to Verification Station Connection

Cabling for Ethernet Connection

Many configurators will elect to connect the Verification Station to the security system via a high-speed network. This network can be either a dedicated LAN or an encrypted internet connection.

Before you can use this connection type, you must have:

- ❑ a configured network (either intranet, such as a dedicated LAN, or internet) that includes the required switcher/hubs and routers
- ❑ a Velocity host that is connected to the security system that includes the network

Once these components are in place, you can connect the station in this way:

1. Connect one end of a CAT5 or CAT6 cable to your network.

   This can be through a direct connessscction to the network or through a hub or switch.
2. Connect the other end of the cable to the RJ-45 connector on the back of the Verification Station.

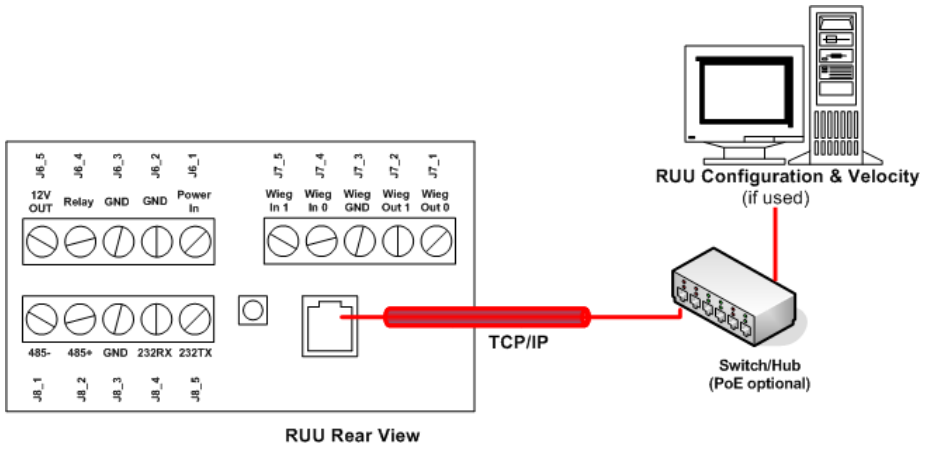


Figure 7-62: Ethernet to Verification Station Connection

3. To power the Verification, do one of these:
   - If you are connecting to a powered hub or switch, you can use the power from one of the hub/switch PoE ports to power the station. (Standard Ethernet ports are not powered.)
   - Plug the included DC power block into the nearest electrical outlet and the other end into the station's power connector.
   - Wire a previously installed 12 VDC power supply to the back of the station in this way:

Connect Wire:	To Station Connector:
GND (black)	GND (J6_2)
+ (red)	Power In (J6_1)

An illustration of this process is shown in Figure 7-63.

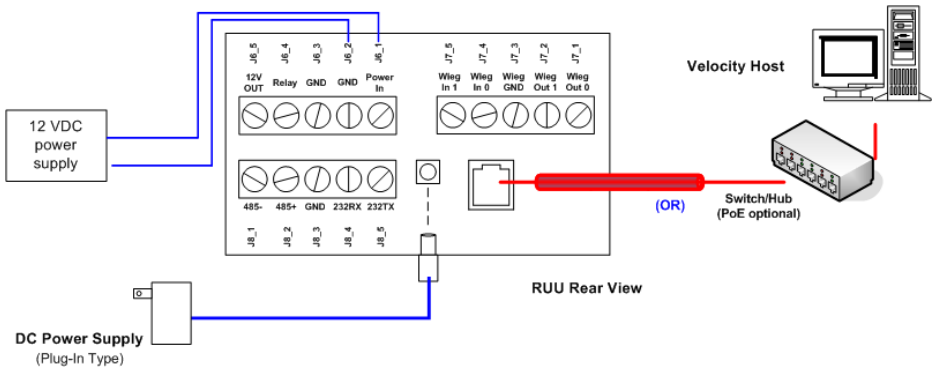


Figure 7-63: Ethernet to Verification Station Power Cabling

Configuring the Ethernet Connection

If you connect to the Verification Station using an Ethernet connection, you must make sure that you set up the TCP/IP settings on the connected host appropriately.

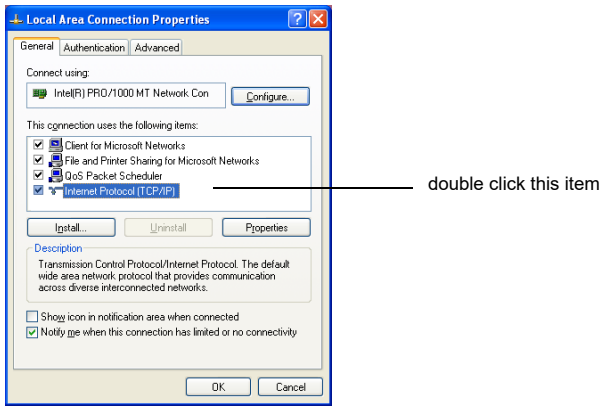
In particular, you must configure the host with a static IP address. A computer that depends on a network router to generate an address on-the-fly using DHCP will not work with a connected station.

At least initially, you should set up your host PC using the following instructions:

1. From the desktop of your host computer, select **Start > Control Panel**.
2. Double click **Network Connections**.
3. Right click on the **Local Area Connection**.

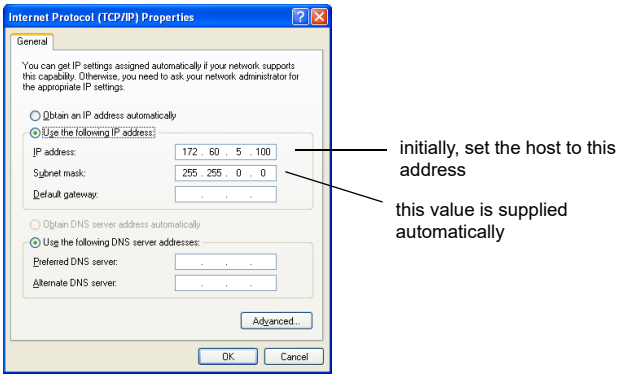
   If you don't have a Local Area Connection already defined, use the **Create a new connection** wizard to set one up.
4. Select **Properties** from the pop-up list.

   The Local Area Connection Properties list appears like this example.



5. Double click on the Internet Protocol (TCP/IP) item in the window.

The Internet Protocol (TCP/IP) properties sheet appears like this example:



6. Click the **Use the following IP address** radio button.
7. At the 'IP address' field, enter this value:

   `172.60.5.100`

   This is the default IP address the Verification Station assumes it will see from the connected host when it is powered up for the first time.

   Once you have entered this value in the 'IP address' field, the program automatically populates the Subnet Address field.
8. Leave all other fields blank and **OK**.
9. Go to the Configuration Program and set up the station IP address using the default value:

   `172.60.5.103`

For more on this, refer to the appropriate section in the *Verification Station Configuration Guide*.

Once you set up the Verification Station, you should go back and change the IP addresses for both the station and its connected host. Remember, however, that whatever IP addresses you select, the two settings must have the same gateway network address: the first three groups of numbers in the address must be the same.

Wiring for RS-485 Serial Connection

Daisy-chained DIGI*TRAC controllers employ a proprietary encrypted RS-485 serial network called ScrambleNet to communicate. This connection is both fast and encrypted, assuring the configurator of a hardwired solution to communicating between the Verification Station and the Velocity-controlled security system.

Before you can implement this method, you must a Velocity host that is connected to the security system and has an installed RS-485 port.

Once this requirement is met, you can connect the station in this manner:

1. Customize a cable with one end connected to a DB-9 plug.

   This DB-9 plug must be wired to the Verification Station in the following way:

DB9 connector:	Station connector:
1 & 2 strapped	485 + (J8_2)
6 & 7 strapped	485 – (J8_1)

An example of this connection is shown in Figure 7-64.

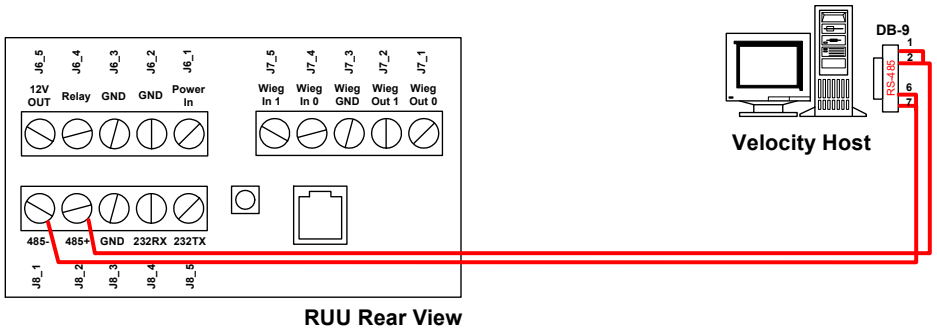


Figure 7-64: RS-485 Verification Station Connection

2. Plug the DB-9 connector into the designated RS-485 port on the back of the Velocity host.
3. Connect the 1/2 and 6/7 wires to the required 485 connectors on the back of the Verification Station.
4. Connect power to the Verification Station in one of two ways:
   - Plug the included DC power block into the nearest electrical outlet and the other end into the station's power connector.
   - Wire a previously installed 12 VDC power supply to the back of the station in this way:

Connect Wire:	To Station Connector:
GND (black)	GND (J6_2)
+ (red)	Power In (J6_1)

An illustration of this process is shown in Figure 7-65.

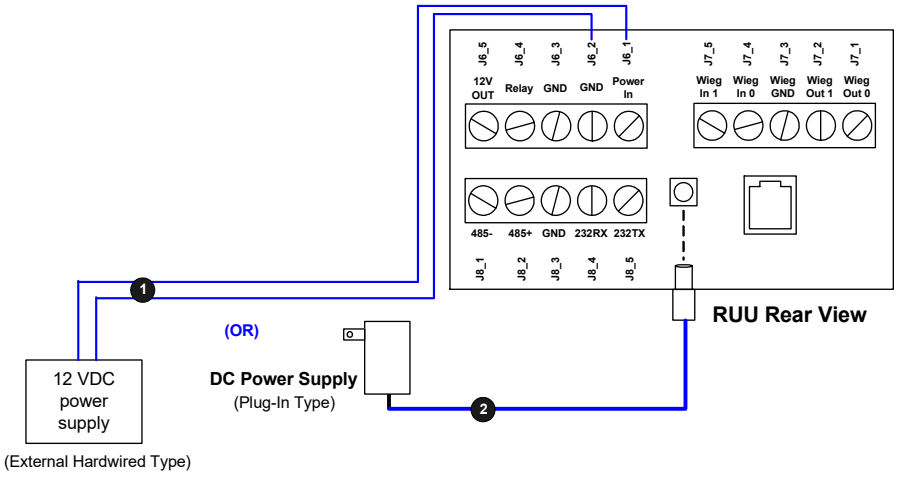


Figure 7-65: RS-485 Verification Station Powering Connection

For more information on configuring the RUU-201 for use with Velocity refer to the *RUU-201 Verification Station Configuration Guide*.

MATCH Interface Installation

This is a three-step process:

- ❑ Setting up the MATCH
- ❑ Mounting the MATCH
- ❑ Wiring the MATCH Each process is detailed in this section.

Note: If you are using one of the DS47L family of ScramblePads, you will find it provides an integrated MATCH. If you are using another type of ScramblePad (such as the DS37L) or readers without ScramblePads, you must install a MATCH.

Setting Up the MATCH

The MATCH Reader Interface Board (MRIB) contains two connectors for linking both a ScramblePad and DIGI*TRAC controller. On the other side are two ports for connecting two reader cables.

There is also a 3-pin connector (P1) on the bottom of the MATCH enabling it to connect directly to a host PC for enrollment station applications as well as another 3-pin connector (P2) used for connecting the MATCH to a DIGI*TRAC Annunciator (DTA).

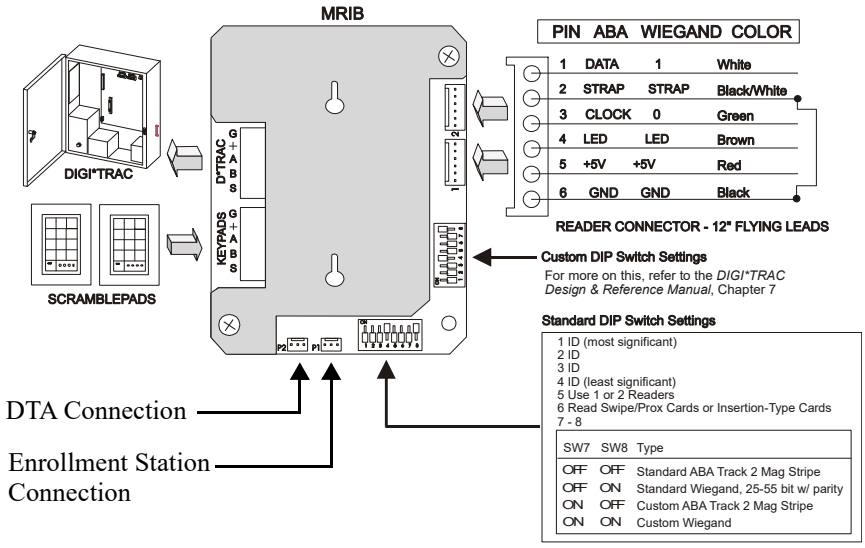


Figure 7-66: Layout View of MRIB

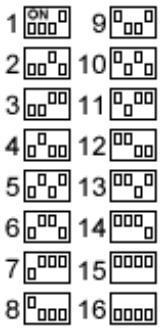
S1 Bank

The MATCH2 pictured above possesses the same number of connectors as the previous MATCH but has two, rather than one, DIP switch banks.

The S1 bank configures all standard settings for the MATCH – such as address, direction, and number of readers – as shown in Figure 7-60. For detailed settings, refer to Table 7-13 and Table 7-14. Use the S2 bank for specifying custom settings. These settings are pre-programmed into the MATCH2's ROM and are implemented by setting the appropriate switches. For more on this, see Table 7-15. The Channel 1 input is dedicated to readers located on the entry side of the door. Channel 2 input is restricted to readers located on the exit side of the door.

S1 bank's SW1 - SW4 settings are shown in Table 7-14 with a graphic of the switch con-

figuration possibilities to the left.



SW1	SW2	SW3	SW4	ID (Address)	Door
OFF	OFF	OFF	**ON**	1 (default)	1 entry
OFF	OFF	**ON**	OFF	2	2 entry
OFF	OFF	**ON**	**ON**	3	3 entry
OFF	**ON**	OFF	OFF	4	4 entry
OFF	**ON**	OFF	**ON**	5	5 entry
OFF	**ON**	**ON**	OFF	6	6 entry
OFF	**ON**	**ON**	**ON**	7	7 entry
ON	OFF	OFF	OFF	8	8 entry
ON	OFF	OFF	**ON**	9	1 exit
ON	OFF	**ON**	OFF	10	2 exit
ON	OFF	**ON**	**ON**	11	3 exit
ON	**ON**	OFF	OFF	12	4 exit
ON	**ON**	OFF	**ON**	13	5 exit
ON	**ON**	**ON**	OFF	14	6 exit
ON	**ON**	**ON**	**ON**	15	7 exit
OFF	OFF	OFF	OFF	16	8 exit

Table 7-14: MATCH S1 Bank SW1 - SW4 Settings

For more information about addressing, refer to “ScramblePad/MATCH Addressing Conventions” on page 7-139.

S1 bank’s SW5-8 settings are shown in Table 7-15:

Switch	Meaning		
5	OFF (default) = 1 card reader, ON = 2 card readers		
6	OFF (default) = read swipe and proximity cards ON = read insertion-type cards		
7-8	SW7	SW8	Reader Data Format
	OFF	OFF	Standard ABA/ISO Track 2 Mag Stripe
	OFF	**ON**	Standard 25-55 Bit Wiegand (with parity)
	ON	OFF	Custom ABA Track 2 Mag Stripe
	ON	**ON**	Custom Wiegand

Table 7-15: MATCH S1 Bank SW5 - SW8 Settings

The standard mag stripe is ISO track 2 (ABA). The 8-digit MATCH code is a hash sum of all data on the card.

Note: For preexisting cards, there is a possibility of duplicate MATCH codes (2 different cards hashing to the same MATCH code).

The standard Wiegand is 25-55 bits, with even parity as the most significant bit, and odd parity as the least significant bit. The MATCH code is built from the 26 least significant data bits, excluding the odd parity bit. All other bits are discarded. The 26 bits are shuffled before conversion to the 8-digit MATCH code.

S2 Bank

Note: Use the Wiegand with parity for prox card readers.

If SW7 on the S1 bank is ON (indicating custom mag stripe) or both SW7 and SW8 on the S1 bank are ON (indicating custom Wiegand), the switches on the second switch bank (S2) enable you to specify which custom setting is required.

The currently available custom reader settings, requiring SW4 – SW8 on the S2 bank, are shown in Table 7-16.

Custom Type	Vn	Date Code	S2 Bank				
			4	5	6	7	8
Custom Mag Stripe – S1 bank: SW7 = ON, SW8 = OFF							
Standard Track 2 pass-thru, max 37 digits. *Requires Vn. 7.0.0 or later DIGI*TRAC*	38	010327	OFF	OFF	OFF	OFF	OFF
West Virginia Vet.Adm. Track 1 Custom	Proprietary format: contact Hirsch factory for details						
Japan JIS 210 bpi Track 2	Proprietary format: contact Hirsch factory for details						
Japan JIS SPECIAL	Proprietary format: contact Hirsch factory for details						
Dept of the Treasury (Track 1)	Proprietary format: contact Hirsch factory for details						
MAGTEK MT-215 Insert Reader	38	010327	OFF	OFF	**ON**	OFF	**ON**
ABA First 8	Proprietary format: contact Hirsch factory for details						
Rocky Flats	Proprietary format: contact Hirsch factory for details						
UC Riverside / Ohio Wesleyan University	Proprietary format: contact Hirsch factory for details						
Veterans Administration	Proprietary format: contact Hirsch factory for details						
St Agnes Hospital / GTE	Proprietary format: contact Hirsch factory for details						
Antelope Valley Hospital	Proprietary format: contact Hirsch factory for details						
Kumahira	Proprietary format: contact Hirsch factory for details						
SEIWG-012	40	020206	OFF	**ON**	**ON**	**ON**	OFF
UNICAN/Camp Perry	Proprietary format: contact Hirsch factory for details						
Kumahira 017	Proprietary format: contact Hirsch factory for details						
Synergistics 018	Proprietary format: contact Hirsch factory for details						
Kumarhira 019	Proprietary format: contact Hirsch factory for details						
Kumahira 020	Proprietary format: contact Hirsch factory for details						
Hawaiian Airline 021 Track 2 pass-through	Proprietary format: contact Hirsch factory for details						

Table 7-16: MATCH S2 Banks Custom Settings

Custom Type	Vn	Date Code	S2 Bank				
			4	5	6	7	8
Wiegand Customs – S1 bank: SW7 = ON, SW8 = ON							
Pass-through, max 32 octal digits, no parity. *Requires Vn. 7.0.0 or later DIGI*TRAC*	38	010327	OFF	OFF	OFF	OFF	OFF
25-55 bits, no parity (compatible with DS47, V.980720 or later)	38	010327	OFF	OFF	OFF	OFF	**ON**
Pass-through, 3-digit facility code, 5-digit PIN, with parity (matches hotstamp)	38	010327	OFF	OFF	OFF	**ON**	OFF
Pass-through, 8 digits, no parity	38	010327	OFF	OFF	OFF	**ON**	**ON**
MultiProx, 26-bit or 32-bit, HID/Westinghouse	38	010327	OFF	OFF	**ON**	OFF	OFF
MultiProx 32-bit pass-through for HP/SAI	38	010327	OFF	OFF	**ON**	OFF	**ON**
CC34N8 CardKey 34-bit no parity (Old-style reader)	38	010327	OFF	OFF	**ON**	**ON**	OFF
CC34N8 CardKey 34-bit no parity (New-style reader)	38	010327	OFF	OFF	**ON**	**ON**	OFF
HID 5355 keypad & prox or Essex KTP-163 & any card reader. Uses standard parity algorithm to validate the card.	38	010327	OFF	OFF	**ON**	**ON**	**ON**
HID 5355 keypad & prox or Essex KTP-163 & any card reader. Uses “Corporate 1000” algorithm to validate card.	38	010327	OFF	**ON**	OFF	OFF	OFF
“WG_NP” 25-55 bits, no parity (compatible with old MATCH "WG_NP"). *Note: both WG_NP customs generate the same MATCH codes for bit lengths 29 and up.*	38	010327	OFF	**ON**	OFF	OFF	**ON**
“Corporate 1000” HID 35-bit	38	010327	OFF	**ON**	OFF	**ON**	OFF
HID 5355 keypad & prox or Essex KTP-163 & any card reader. Uses DS47 no parity algorithm to validate card.	38	010327	OFF	**ON**	**ON**	OFF	OFF
Caixa Geral de Depositos SSR-2210 (W) Bar Code Reader - Paradise Information & Communication Co., LTD.	Proprietary format: contact Hirsch factory for details						
New HID Corporate 1000 card	48	030911	OFF	**ON**	**ON**	**ON**	OFF
Bidirectional Interlock function-uses standard parity Wiegand card.	51	050224	OFF	**ON**	**ON**	**ON**	**ON**

Table 7-16: MATCH S2 Banks Custom Settings (Continued)

Custom Type	Vn	Date Code	S2 Bank				
			4	5	6	7	8
GSA 75-bit + WGN000 (pass-through). GSA 75-bit + 128-bit UUID + WGN000 (pass-through).	61 71	060928 130127	**ON**	OFF	OFF	**ON**	OFF
GSA 75-bit + standard Wiegand. GSA 75-bit + 128-bit UUID + standard Wiegand.	63 71	061030 130127	**ON**	OFF	**ON**	OFF	OFF
GSA 75-bit + parity pass-through. GSA 75-bit + 128-bit UUID + parity pass-through.	63 71	061030 130127	**ON**	OFF	**ON**	OFF	**ON**
GSA 75-bit + 64-bit FASCN/PIV pass-through. GSA 75-bit + 128-bit UUID + 64-bit FASCN/PIV pass-through.	63 71	061030 130127	**ON**	OFF	**ON**	OFF	**ON**
64-bit FASCN/PIV + WGN000 (pass-through). 64-bit FASCN/PIV + 128-bit UUID + WGN000 (pass-through).	70 71	120305 130127	**ON**	**ON**	OFF	OFF	OFF
64-bit FASCN/PIV + standard Wiegand. 64-bit FASCN/PIV + 128-bit UUID + standard Wiegand.	70 71	120305 130127	**ON**	**ON**	OFF	OFF	**ON**
64-bit FASCN/PIV + parity pass-through. 64-bit FASCN/PIV + 128-bit UUID + parity pass-through.	70 71	120305 130127	**ON**	**ON**	OFF	**ON**	OFF
200-bit FASCN/PIV + WGN000 (pass-through). 200-bit FASCN/PIV + 128-bit UUID + WGN000 (pass-through).	70 71	120305 130127	**ON**	**ON**	OFF	**ON**	**ON**
200-bit FASCN/PIV + standard Wiegand. 200-bit FASCN/PIV + 128-bit UUID + standard Wiegand.	70 71	120305 130127	**ON**	**ON**	**ON**	OFF	OFF
200-bit FASCN/PIV + parity pass-through. 200-bit FASCN/PIV + 128-bit UUID + parity pass-through.	70 71	120305 130127	**ON**	**ON**	**ON**	OFF	**ON**

Table 7-16: MATCH S2 Banks Custom Settings (Continued)

The MATCH also contains a dedicated RS-232 port next to the S1 switch bank. The P1 connector accommodates an ESC1 cable, which includes a three-pin adapter on one end and a DB25 on the other. Use this port to connect the MATCH to a Card Enrollment station on a PC, as shown in “Enrollment Station Installation” on page 7-325.

The MATCH also contains a dedicated RS-232 port marked P2 which is located to the left of the P1 port. The P2 port uses an ESC1 cable to connect to the DIGI*TRAC Annunciator. For more about this installation, see “DIGI*TRAC Annunciator Installation” starting on page 7-330.

ScramblePad/MATCH Addressing Conventions

Addresses are assigned to ScramblePads and MATCHs according to user discretion, but always following these protocols:

- ❑ 16 Addresses are available
  - Addresses 1 – 8 are used for entry ScramblePads and MATCH interfaces
  - Addresses 9 – 16 are used for exit ScramblePads

So, for example, to assign a MATCH the address 7 on the S1 bank, leave SW1 OFF then turn SW2, SW3, and SW4 to ON. The controller understands the reader connected to Channel 1 is on the entry side of the door, and a reader connected to Channel 2 is on the exit side of the door.

- ❑ If two readers are attached to a MATCH, the entry reader address is assigned to the address on the MATCH.
- ❑ If one ScramblePad is attached to a MATCH, the ScramblePad must be assigned the same address as the MATCH. For example, if a MATCH is allocated Address 1, then the ScramblePad must be set as Address 1.
- ❑ If two ScramblePads are connected to the same MATCH, then the lowest of the two addresses must also be assigned to the MATCH. For example, if ScramblePads on opposite sides of a door have been assigned Addresses 1 and 9 (per the rule for addressing entry and exit ScramblePads), then the MATCH to which these two ScramblePads are connected must be assigned Address 1; similarly, the MATCH to which ScramblePads addressed as 2 and 10 must be allocated Address 2, and so on.

Mounting the MATCH

There are three ways to mount the MATCH interface:

- ❑ MRIA in a Hirsch mounting box
- ❑ MRIB in a universal J-Box
- ❑ MR11LA

To Mount the MRIA:

The Hirsch MATCH Reader Interface Assembly (MRIA) includes an MRIB with mounting base and bezel, physical tamper switch, and blank faceplate. This assembly enables you to mount the MRIB directly behind an indoor mag stripe reader like the Hirsch CR11L or MR11L, where room permits.

1. Select the mounting box you require. Available models are MB1 and MB2. For more about this, see “MRIA/MRIB Mounting” on page 2-63.
2. Install and secure the selected mounting box using the instructions earlier in this chapter. Refer to “Installing the Mounting Box” on page 7-97.
3. Route cable from the controller through the back box.
4. Using the enclosed screws, insert and secure the MRIB to the mounting box.
5. Connect ScramblePads and Card Readers to the MRIB as required. For more about this, see the next section, “Wiring the MATCH” on page 7-140.
6. Connect the MRIB to the controller.

To Mount the MRIB:

The MRIB is the bare board version of the MATCH. It is usually mounted inside a J-Box and located above the ceiling line.

1. Locate the MRIB in close proximity to the readers and ScramblePads, if used. The MRIB should be located at the Door or Access Point. If you want to protect the board from the environment, place it inside a J-Box above the ceiling or in the wall.

   For every foot of separation between the MRIB and ScramblePad, the distance between the Controller and the MRIB must be decreased by one foot.
2. Install and secure the J-Box.
3. Route cable from the controller through the box.
4. Using the enclosed screws, insert and secure the MRIB to the mounting box.
5. Connect ScramblePads and Card Readers to the MRIB as required. For more on this, see the following section.
6. Connect the MRIB to the Controller.2.

To Mount the MR11LA:

The indoor magstripe reader (MR11LA) includes its own integrated MRIB, behind the reader.

1. Select the mounting box you require. Available models are MB1 and MB2. For more about this, see “MRIA/MRIB Mounting” on page 2-63.
2. Install and secure the selected mounting box using the instructions earlier in this chapter. Refer to “Installing the Mounting Box” on page 7-97.
3. Route cable from the controller through the back box and connect it to the MRIB as described in the next section, “Wiring the MATCH” on page 7-140.
4. If you need to connect a second reader or a ScramblePad to the MR11LA’s MRIB, route the wiring from the second reader through the back box and connect it to the MRIB as described in the next section, “Wiring the MATCH” on page 7-140.

Wiring the MATCH

Wiring the MATCH is a three-step process:

- ❑ Connecting the MATCH to one or two readers
- ❑ Connecting the MATCH to an optional ScramblePad
- ❑ Connecting the MATCH to a controller

To Connect the MATCH to Readers:

1. Connect the reader to the end of the flying lead cable. For information on doing this, refer to your reader’s installation manual.
2. Attach the cable connector (the other end of the flying lead cable) to the Channel 1 or Channel 2 input port on the MATCH.
3. If the distance between the MATCH and the reader is greater than the 12-inch flying lead connector, an additional cable must be provided and soldered to the flying lead cable.
4. Install the cable between the MATCH and the one or two readers this board will connect.

The distance from the MATCH to the Reader is a function of the specific reader. Some readers, like the Hirsch CR11L, can be up to 150 feet (45m) from the MATCH using wire gauge no smaller than 24 AWG. Reader distances vary. Check the specifications for your Reader to determine allowable wire distances.

Note: As a general rule, when using 5V readers, limit the voltage drop in the cable run to 0.2V.

Make sure the cable connector conforms to this specification:

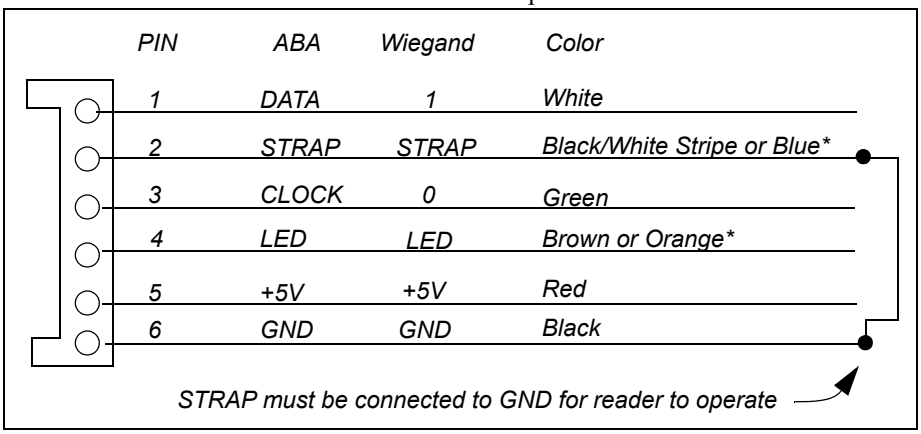


Figure 7-67: Reader Connector Wiring

* Notice that wires 2 and 4 can be one of two colors depending on whether the cable supplied by Hirsch or by the reader manufacturer. Wire 2 can be either black/white or blue; wire 4 can be either brown or orange.

Note: If you are using a DS47L or DS47L-SPX, attach readers to the back of the keypad using the same procedure as detailed above. The DS47L-series ScramblePads contain an integrated MATCH.

To Connect the MATCH to a ScramblePad:

1. Remove the green connector from the KEYPAD terminal block.
2. Attach wires from one end of the ScramblePad cable to the connector. Make sure the wiring corresponds to this pinout arrangement:

ScramblePad Terminal	Description	Wire Color	MATCH Terminal
1	GND	Black	G
2	+	Red	+
3	Data A	Green	A
4	Data B	White	B
5	Shield Drain	Shielded	S

3. Reattach the connector to the MATCH's Keypad terminal block.
4. Connect the other end of the cable into the back of the ScramblePad.

5. To attach a second ScramblePad to this board, insert and secure the second set of wires into the MATCH's KEYPADS terminal blocks.

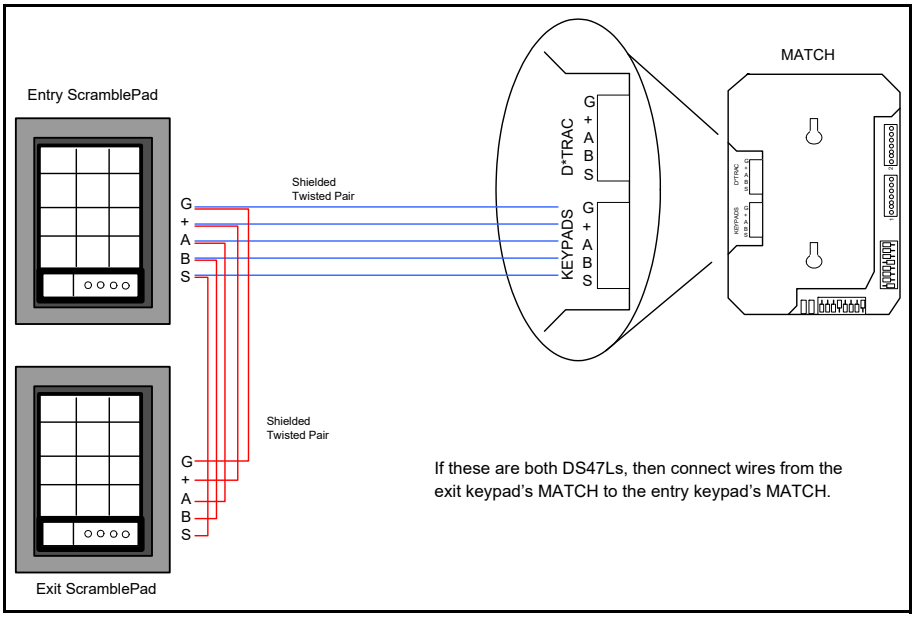


Figure 7-68: Connecting Entry and Exit ScramblePads

If one or both of the ScramblePads are DS47Ls, then the MATCH is integrated into the back of the keypad. Make sure to connect wires from the KEYPADS terminal block on the exit keypad's MATCH board to the KEYPADS terminal block on the entry keypad's MATCH board.

This 'doubling up' of wires will not affect communication between the two ScramblePads and the controller, since ScramblePad signals are digital and can be decoded by the controller.

If a ScramblePad is attached to a MATCH, the MATCH must be assigned the same address as the connected ScramblePad. For example, if a ScramblePad connected to a MATCH is allocated Address 1, then the MATCH must be set as Address 1.

If two ScramblePads are connected to the same MATCH, then the lowest of the two addresses must be assigned to the MATCH. For example, if ScramblePads on opposite sides of a door have been assigned Addresses 1 and 9 (per the rule for addressing entry and exit ScramblePads), then the MATCH to which these two ScramblePads are connected must be assigned Address 1; similarly, the MATCH to which ScramblePads addressed as 2 and 10 must be allocated Address 2, and so on.

For more on wiring the ScramblePad, refer to "ScramblePad Installation" on page 7-97.

To Connect the MATCH to the Controller:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Run the cable to the controller.

   For wiring and distances, refer to Chapter 2, "Design Considerations".
3. Remove the green connector from the D*TRAC terminal block on the MATCH board.
4. Attach wires from one end of the DIGI*TRAC cable to the terminal block.

Make sure the wiring corresponds to this pinout arrangement:

D*TRAC Terminal	Description	Wire Color	MRIB Terminal
1	GND	Black	G
2	+	Red	+
3	Data A	Green	A
4	Data B	White	B
5	Shield Drain	Shielded	S

5. Reattach the connector to the MATCH's D*TRAC terminal block.
6. Connect the other end of the cable into the DIGI*TRAC controller board.

For more about wiring the controller, refer to "Controller Installation" on page 7-17.

Powering the MATCH Locally

Most of the time, the attached controller provides sufficient power to the MATCH to run the attached readers. However, there are conditions which require more power than the controller can reasonably supply. This occurs if the wire run between the controller and the MATCH is more than 1800 feet.

When this happens, you should connect a local 24 VDC power supply into the MATCH's D*TRAC connector. To do this:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Locate a 24VDC – 27VDC (1 Amp) power supply near the MATCH.
3. Run a pair of wires (usually twisted pair) from the power supply to the MATCH.
4. Connect the G (black) and + (red) connectors at the power supply end.
5. Remove the D*TRAC terminal block from the MATCH's D*TRAC port.
6. Rewire the block in this way:
   - *Add* the G (black) wire from the power supply to the G (black) wire that already leads to the controller.
   - *Replace* the + (red) wire from the controller with the + (red) wire from the power supply.

Note: Do not use the red wire leading from the controller to the MATCH.

Figure 7-69 provides a schematic view of this arrangement:

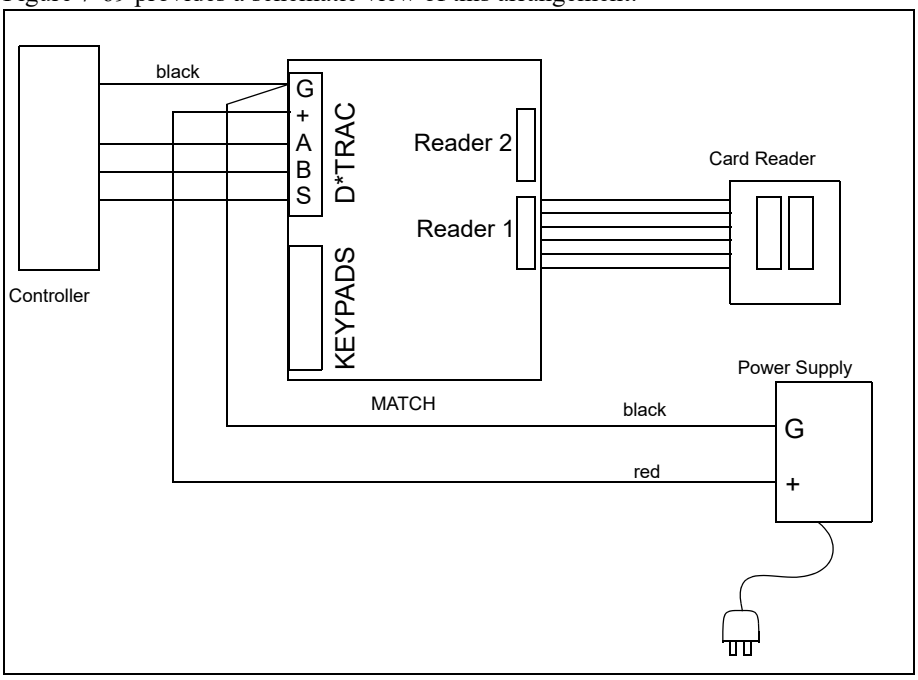


Figure 7-69: Powering the MATCH Locally (Schematic)

Figure 7-70 illustrates this same arrangement.

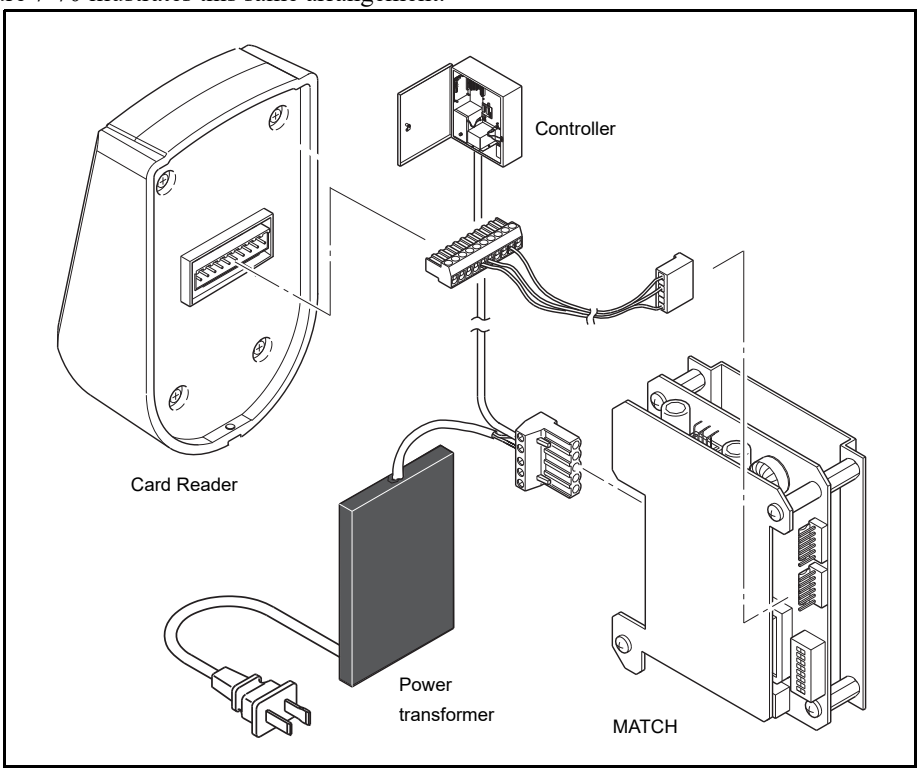


Figure 7-70: MATCH Connections using Local Power

7. Power up the system.

MATCH Reader Installation

There are a large number of readers provided by Hirsch and other manufacturers that are compatible with the MATCH.

A list of MATCH-compatible readers and their required wiring is provided in the following section.

Readers Setup

Some readers possess DIP switches and jumpers for pre-configuring, others do not. For specifics on setting up your reader, refer to the sheet or manual provided with the reader.

Specify how the MATCH Reader Interface handles each of its attached readers through MATCH switch settings (refer to “Setting Up the MATCH” on page 7-134). If there are one or two card readers attached to this MATCH, they must both use the same reader data format, since SW7-8 on the MATCH can only be set for one type of reader format. If the reader is a standard Wiegand, set SW7=OFF and SW8=ON; for ABA/ISO Mag Stripe set both SW7 and SW8 to OFF. The Wiegand and ABA/ISO are the two principle data formats.

Readers Mounting and Wiring

All readers have slight differences in the way they are mounted. For specifics on each reader, refer to the installation sheet provided with the reader you’ve purchased. In general, follow these instructions:

1. Use the supplied template or mounting base to prepare the reader for mounting.
2. Route the cable from the MATCH to the reader.
3. Connect the cable between the reader and MATCH as described earlier (refer to “Mounting the MATCH” on page 7-139).
4. If the Reader comes with a faceplate, attach that now.

For detailed information about wiring specific readers, refer to “MATCH-Compatible Readers Wiring” starting on page 7-145. For detailed information about wiring a MATCH-compliant keypad, refer to “MATCH-Compliant Keypads” on page 7-294.

MATCH-Compatible Readers Wiring

Drawings in this chapter are shown for both MATCH and MATCH2 boards, since connections between readers and MATCH boards vary according to which version you employ. Wiring distances are specified where appropriate.

This section gives wiring diagrams for integrating many of the more popular readers into the Hirsch DIGI*TRAC system. This chapter includes diagrams for the following types of readers:

Throughout this chapter, instructions on connections to MATCH boards, wiring, and reader configuration are shown in the accompanying notes in each diagram.

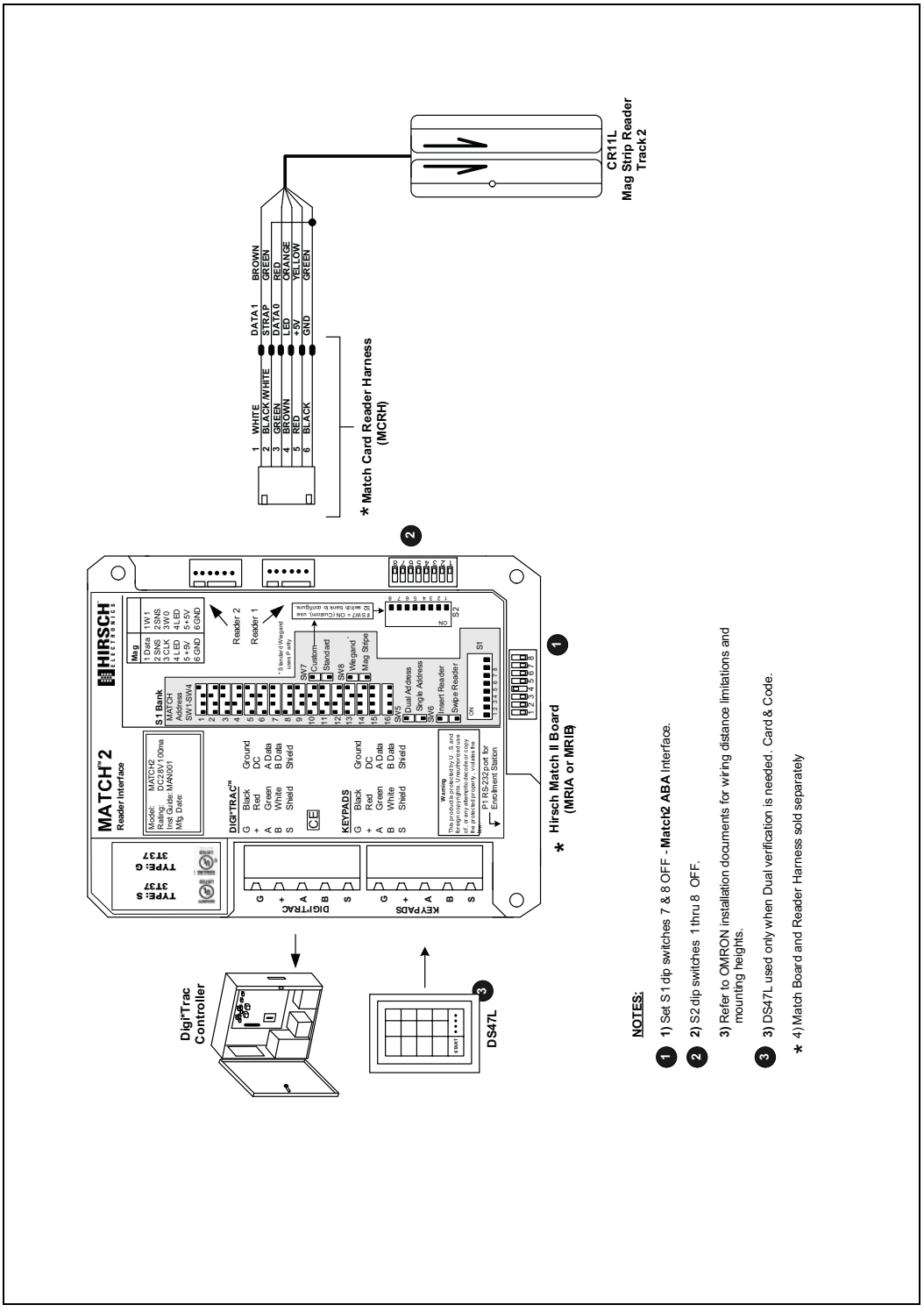
Note: The color coding of leads in the following diagrams varies from standard flying lead configurations. These drawings are for Hirsch assemblies with pre-fabricated custom cables.

Mag Stripe Card Readers

This section describes the MATCH wiring and settings information required to connect Hirsch-supported mag stripe readers. Diagrams for the following mag stripe card readers are shown:

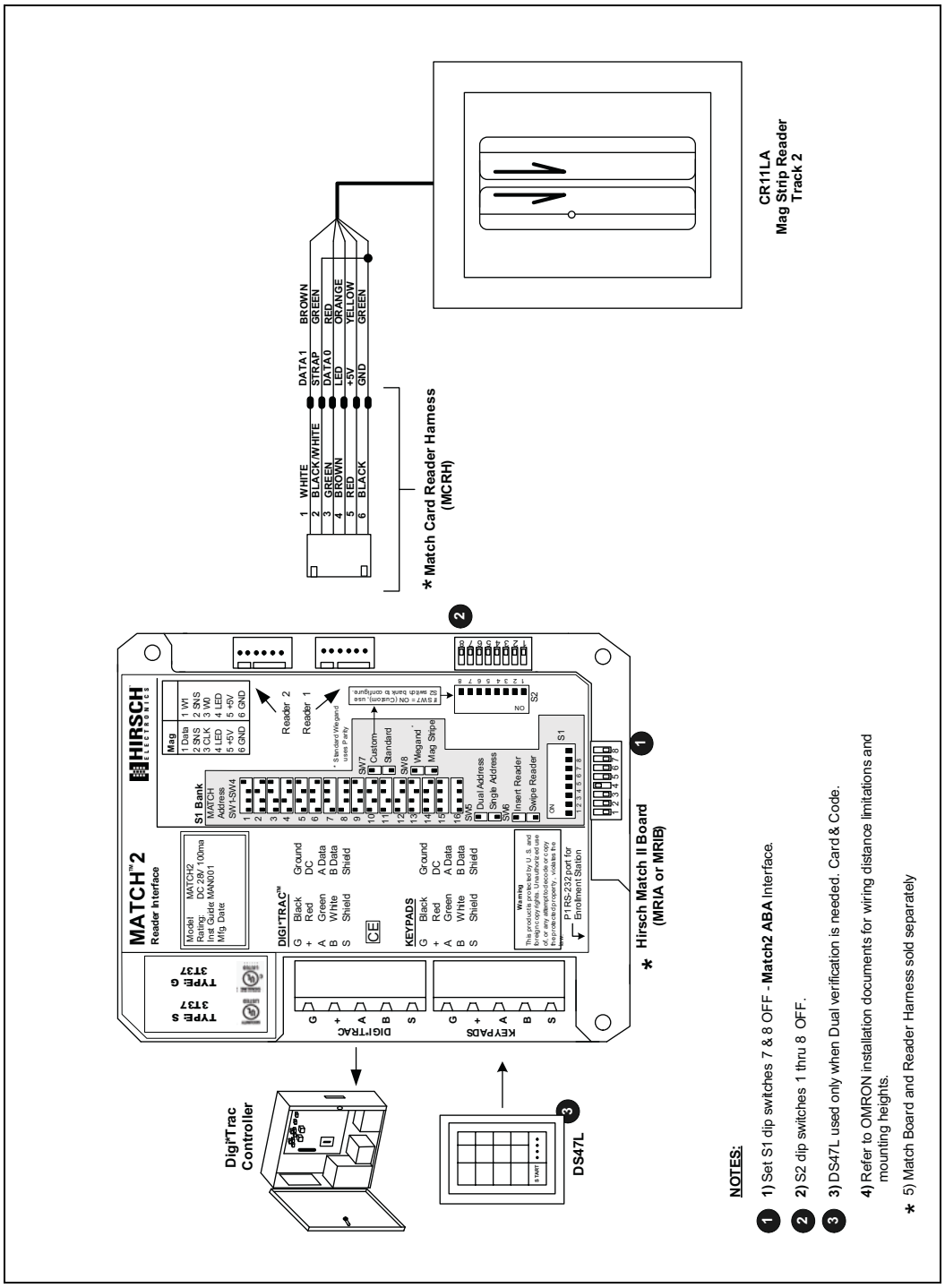
CRIlL Mag Stripe Reader

This diagram shows wiring for the CRIlL Mag Stripe Reader. This reader uses Track 2 mag stripe standards.



OMRON Mag Stripe Reader

This diagram shows wiring for the CRllLA OMRON Mag Stripe Reader.



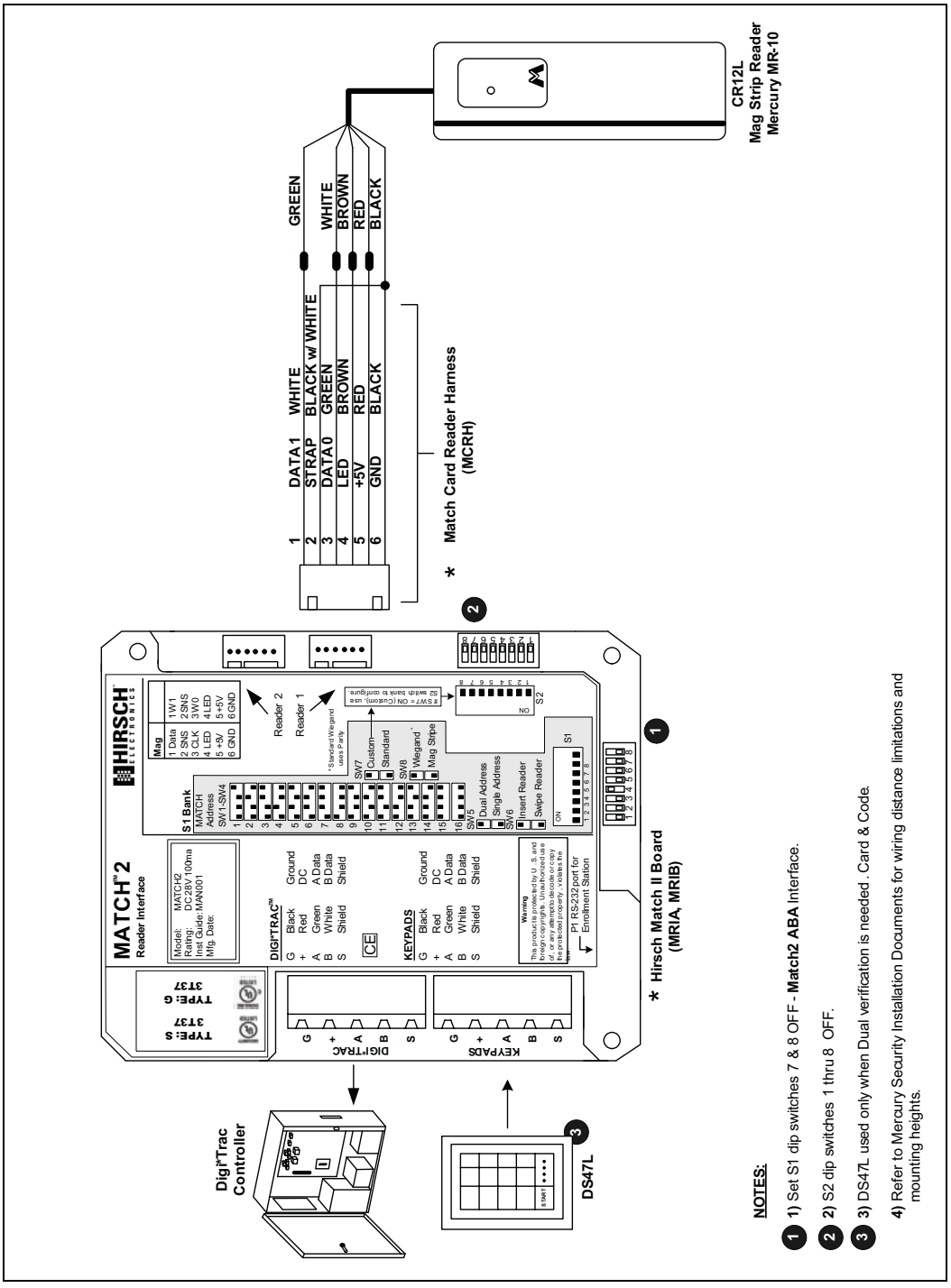
Mercury Mag Stripe Readers

This section gives diagrams for two different Mercury mag stripe readers:

- ❑ "CR12L Mag Stripe Reader" on page 7-149
- ❑ "CR12L-T1-28 Mag Stripe Reader" on page 7-150

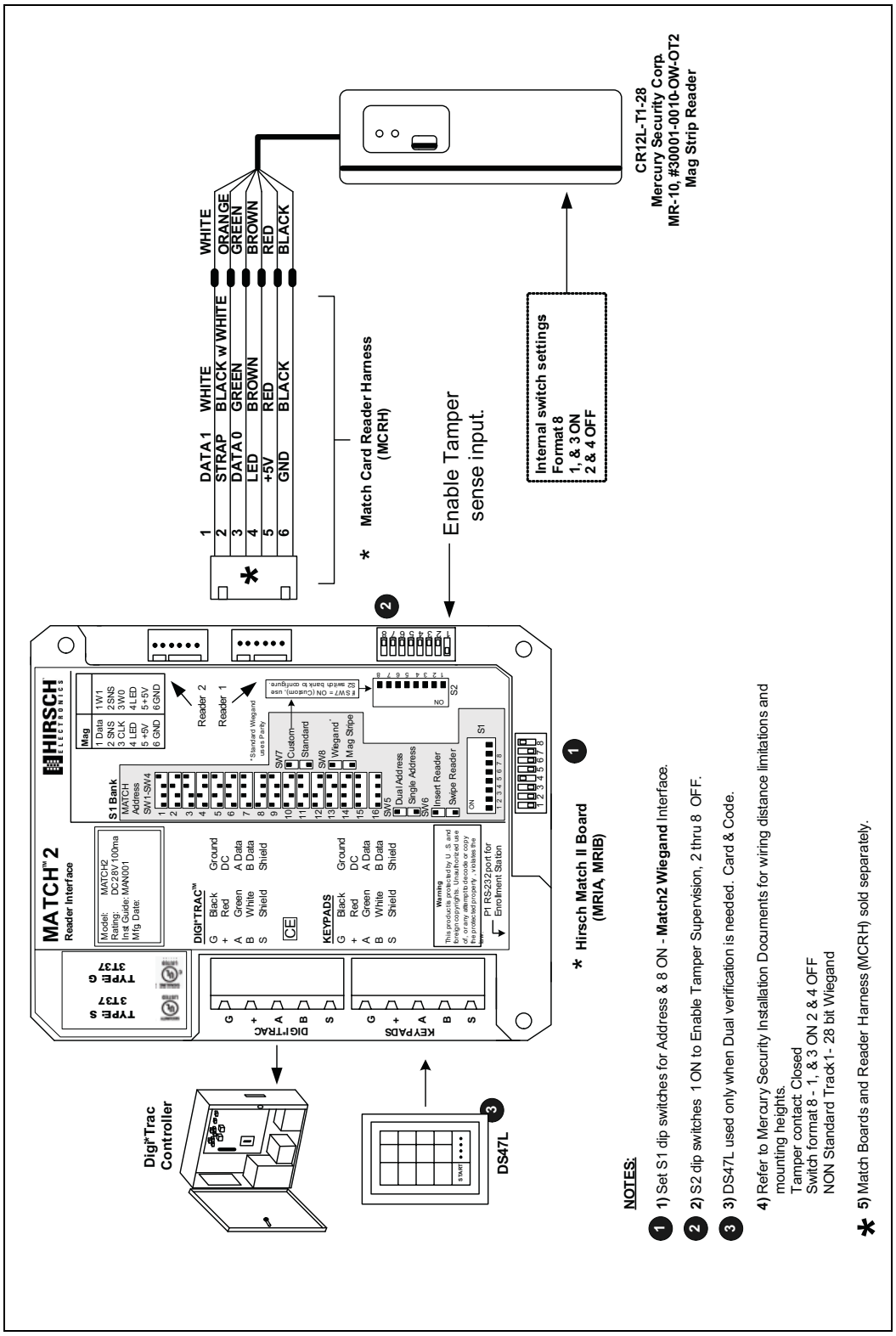
CR12L Mag Stripe Reader

This diagram shows wiring for the CR12L Mercury Mag Stripe Reader.



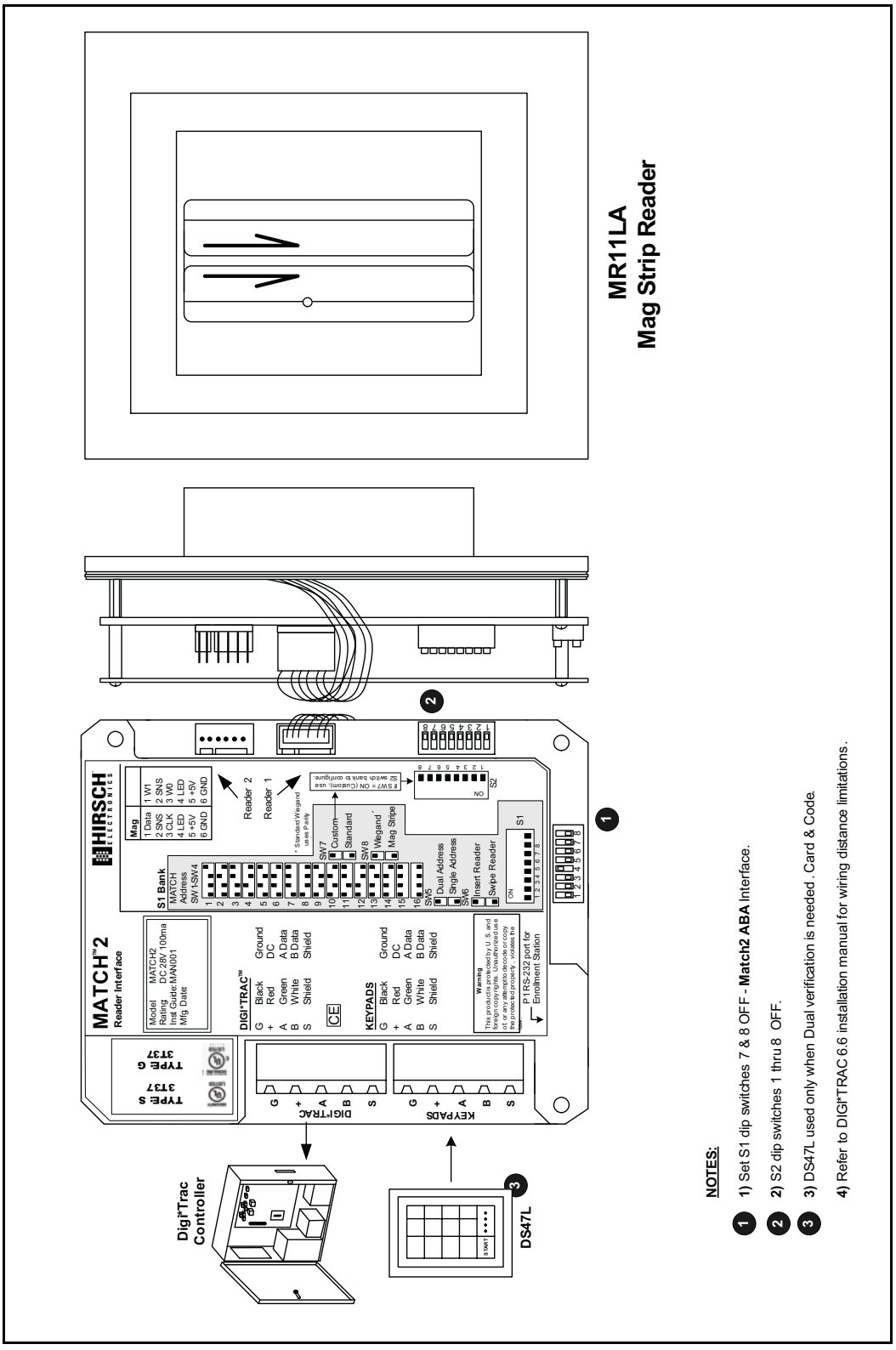
CR12L-T1-28 Mag Stripe Reader

This diagram shows wiring for the CR12L-T1-28 Mercury Mag Stripe Reader.



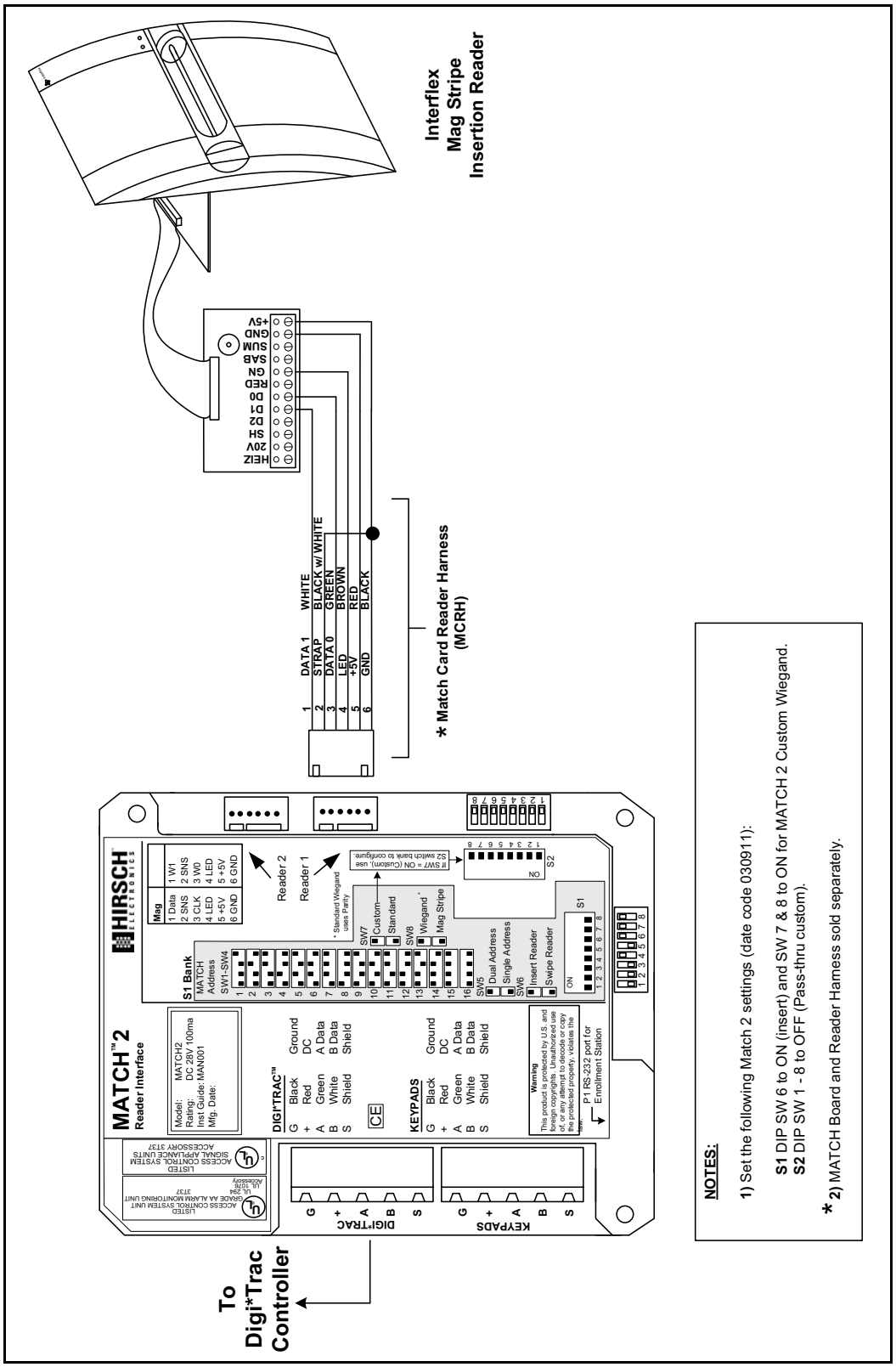
MR11LA Mag Stripe Reader

This diagram shows wiring for the MR11LA Mag Stripe Reader.



Interflex Mag Stripe Insertion Reader

This diagram shows wiring for the Interflex Mag Stripe Insertion Reader.



Proximity Card Readers

This section describes the MATCH wiring and settings information required to connect Hirsch-supported proximity card readers. Diagrams for the following proximity card readers are shown:

HID Proximity Readers

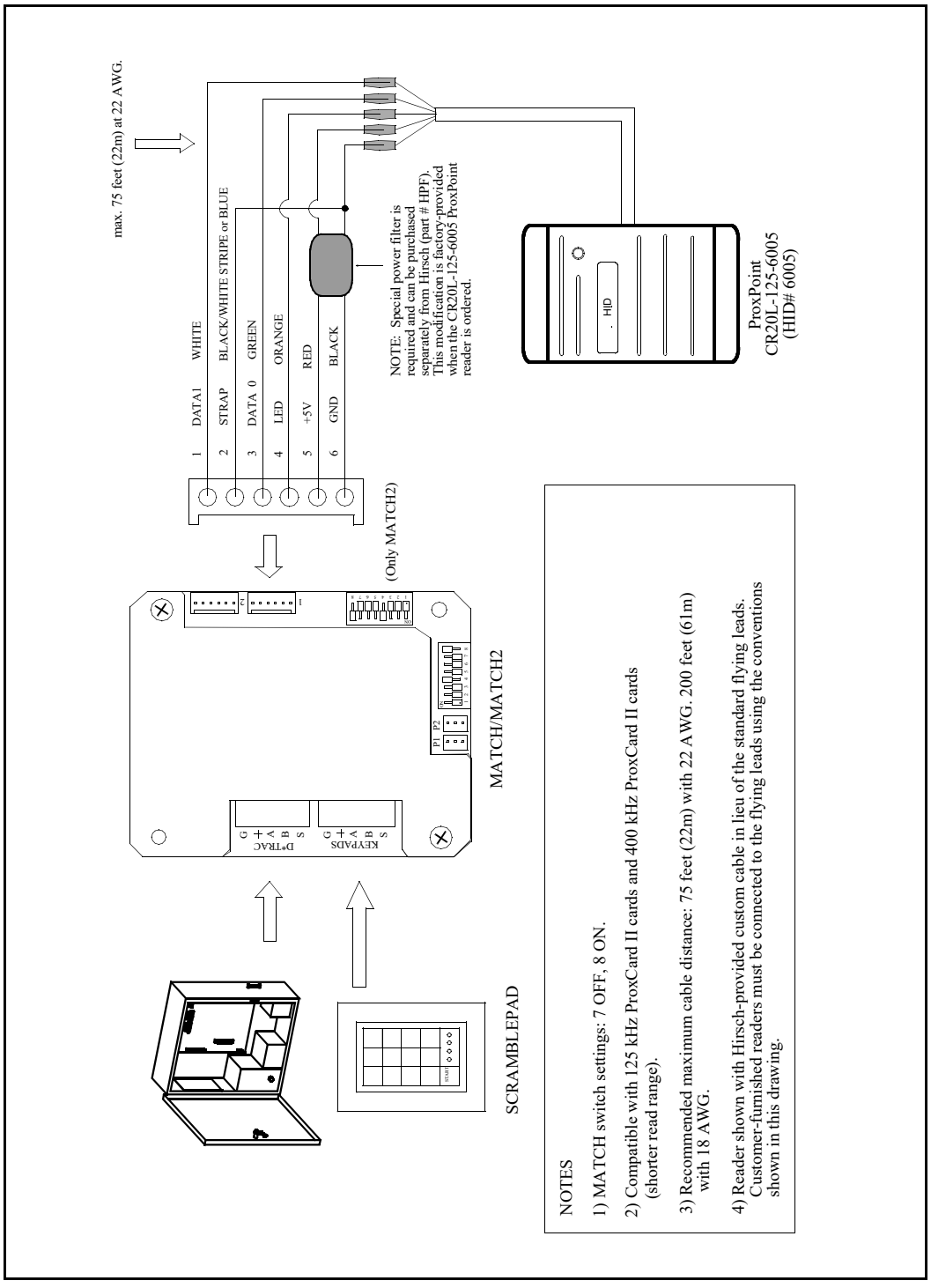
This section gives wiring diagrams for the following HID proximity readers:

HID ProxPoint 6005 Readers

This section shows wiring diagrams for the following HID ProxPoint 6005 Readers:

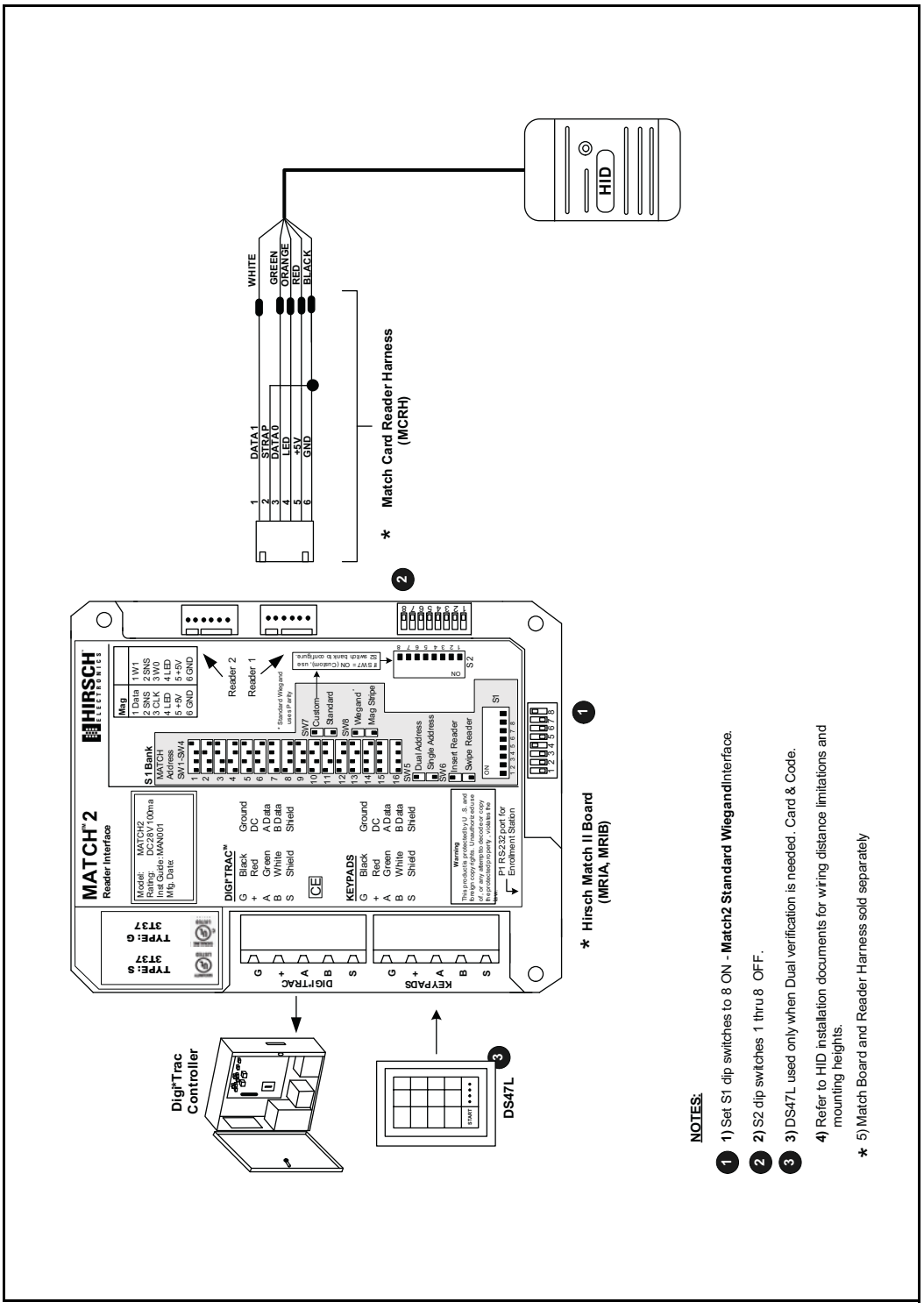
CR20L HID ProxPoint 6005 Reader

This diagram shows wiring for the CR20L HID ProxPoint 6005 Reader.



CR20L-BG HID ProxPoint 6005 Reader

This diagram shows wiring for the CR20L-BG HID ProxPoint 6005 Reader.



NOTES:

1) Set S1 dip switches to 8 ON - **Match2 Standard Wiegand** interface.

2) S2 dip switches 1 thru 8 OFF.

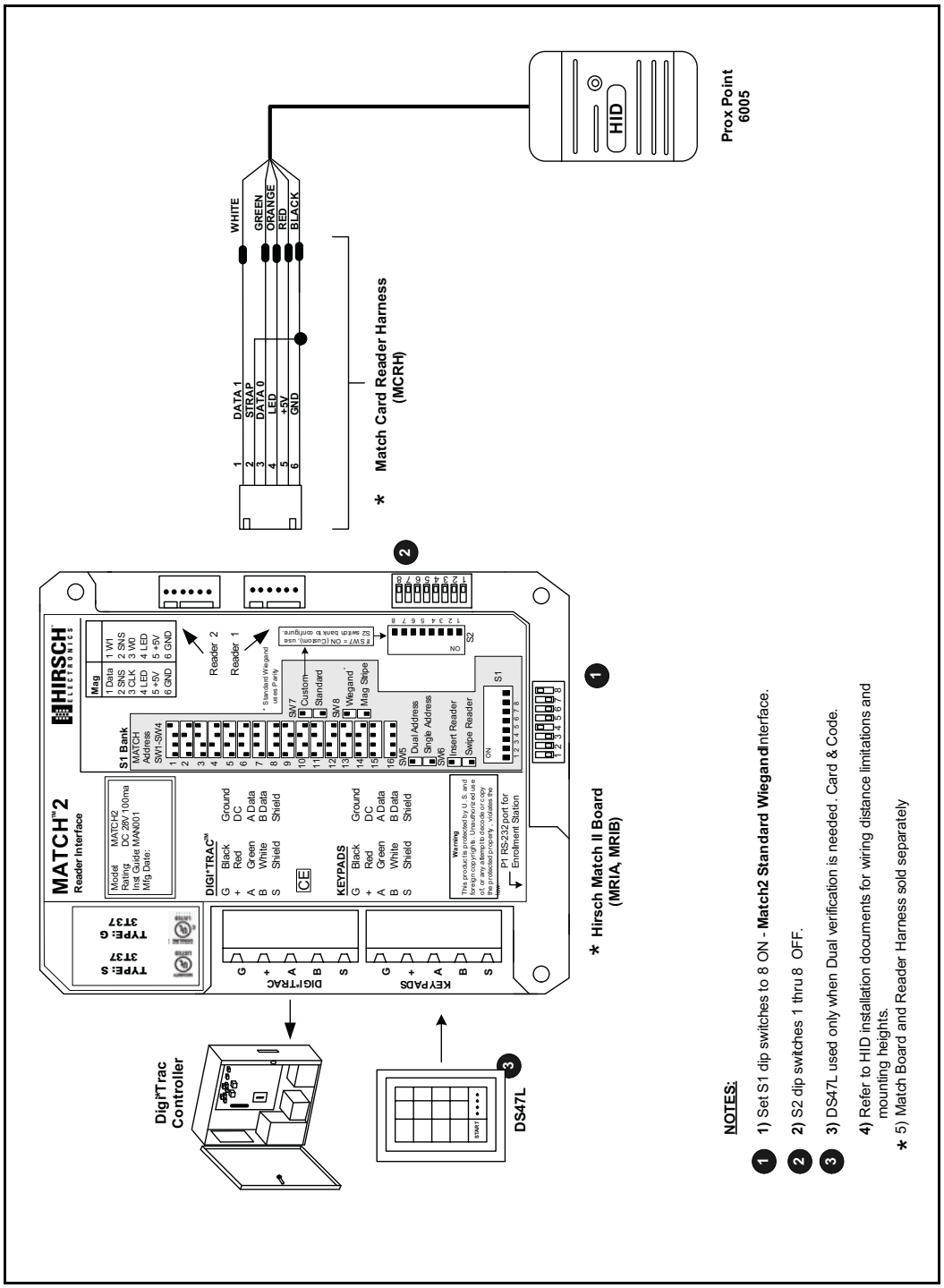
3) DS47L used only when Dual verification is needed. Card & Code.

4) Refer to HID installation documents for wiring distance limitations and mounting heights.

* 5) Match Board and Reader Harness sold separately

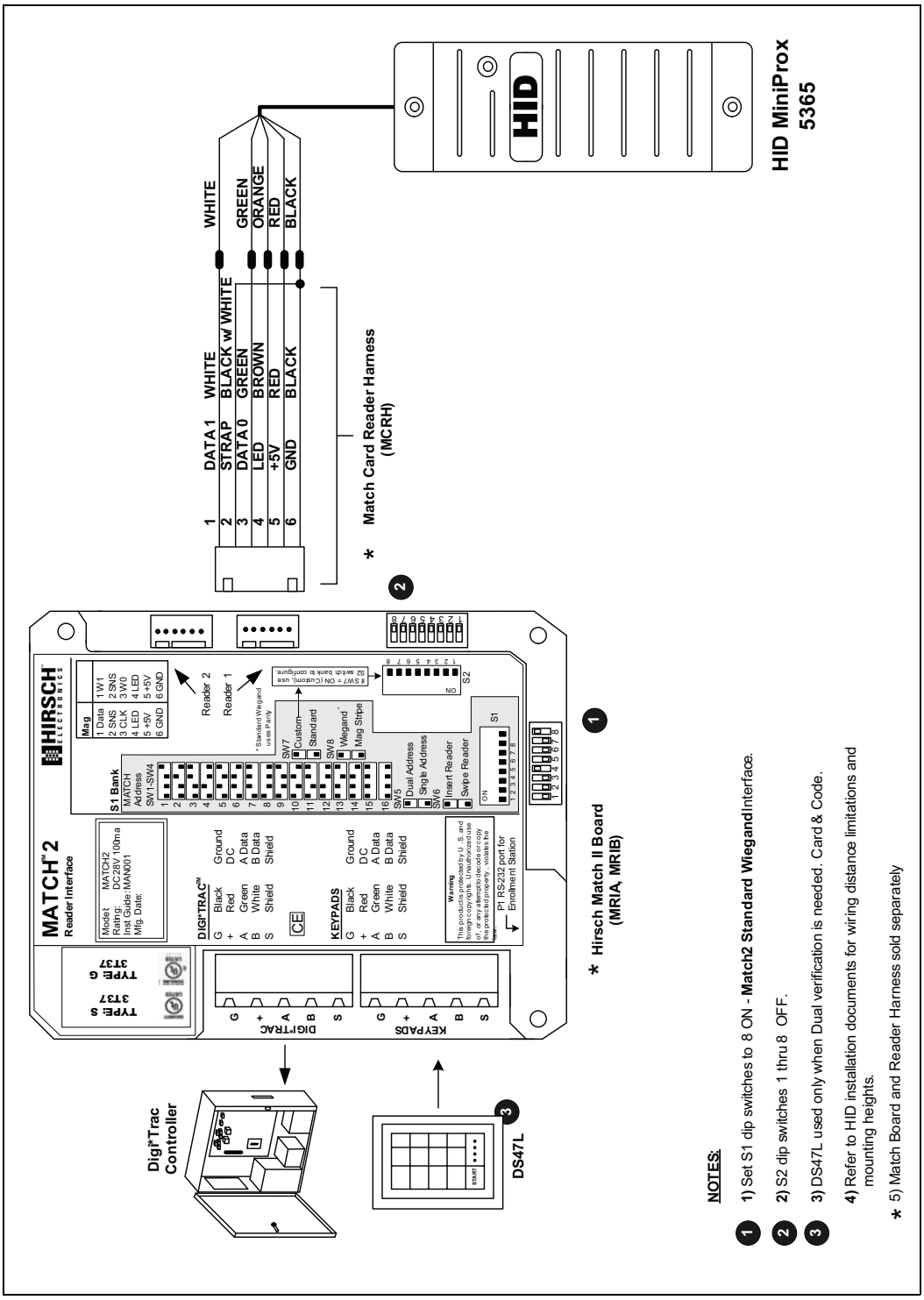
CR20L-BL HID ProxPoint 6005 Reader

This diagram shows wiring for the CR20L-BL HID ProxPoint 6005 Reader.



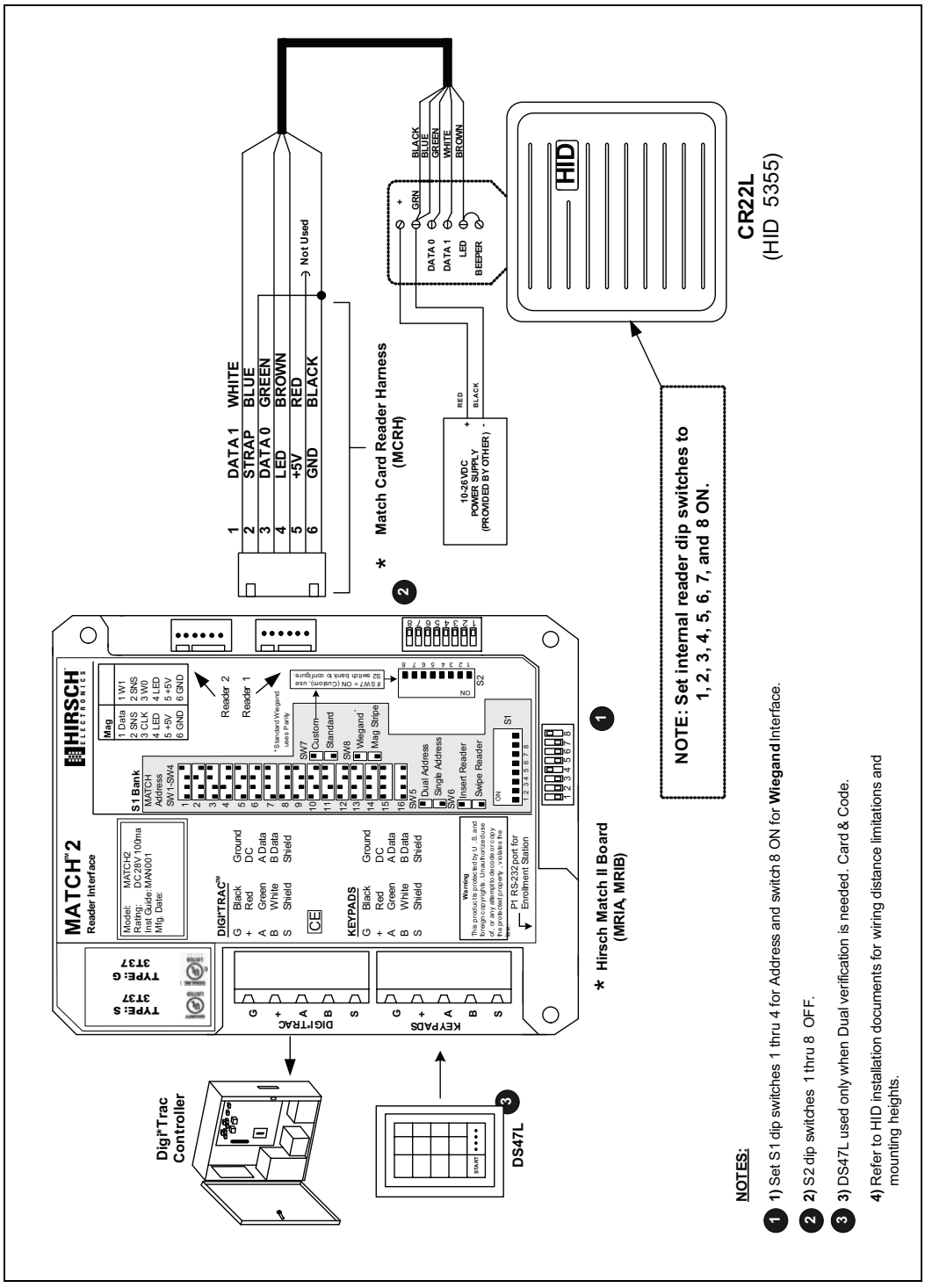
HID MiniProx 5365 Reader

This diagram shows wiring for the CR21L model HID MiniProx 5365 Reader.



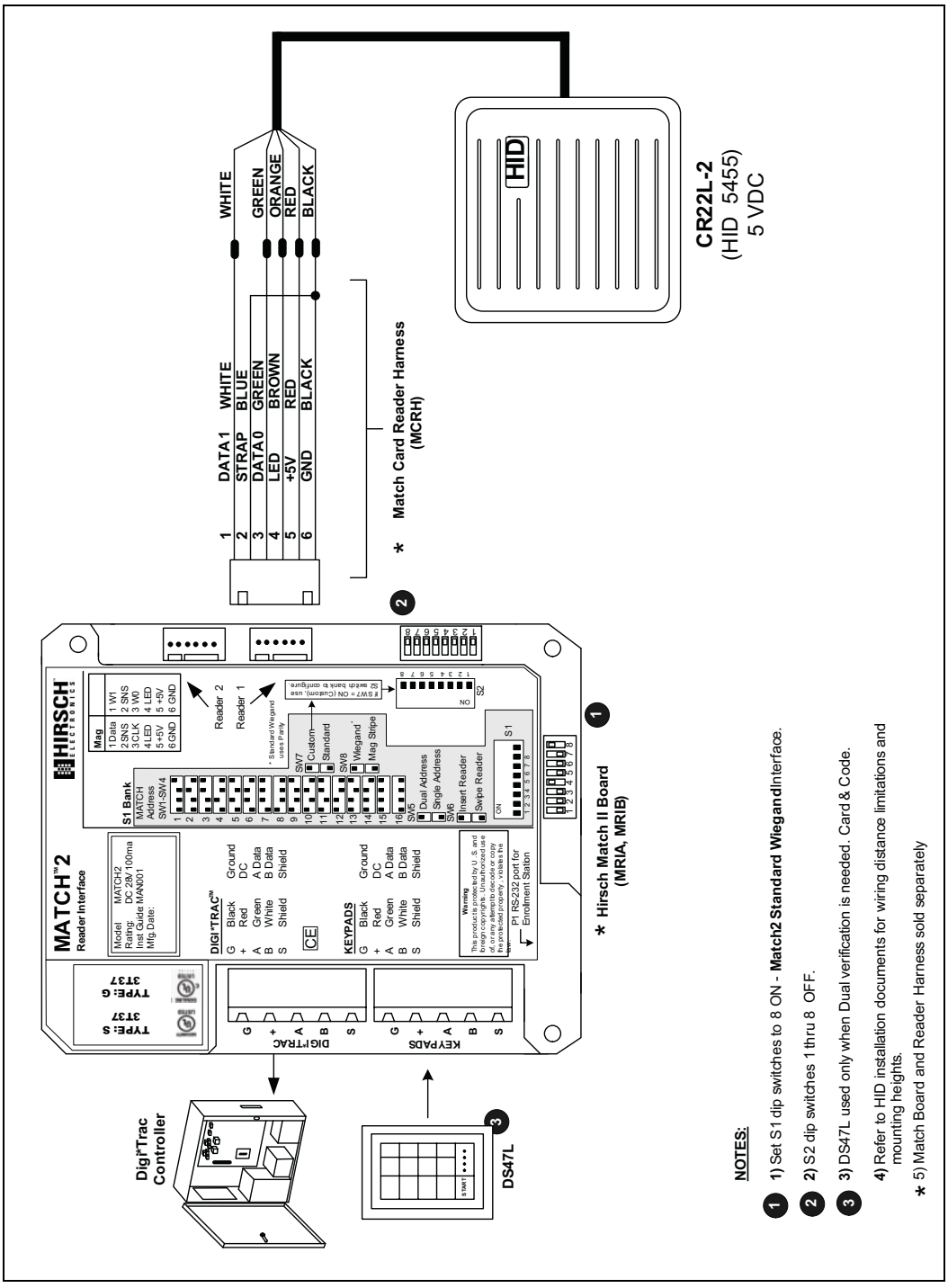
HID 5355 Proximity Reader

This diagram shows wiring for the CR22L model.



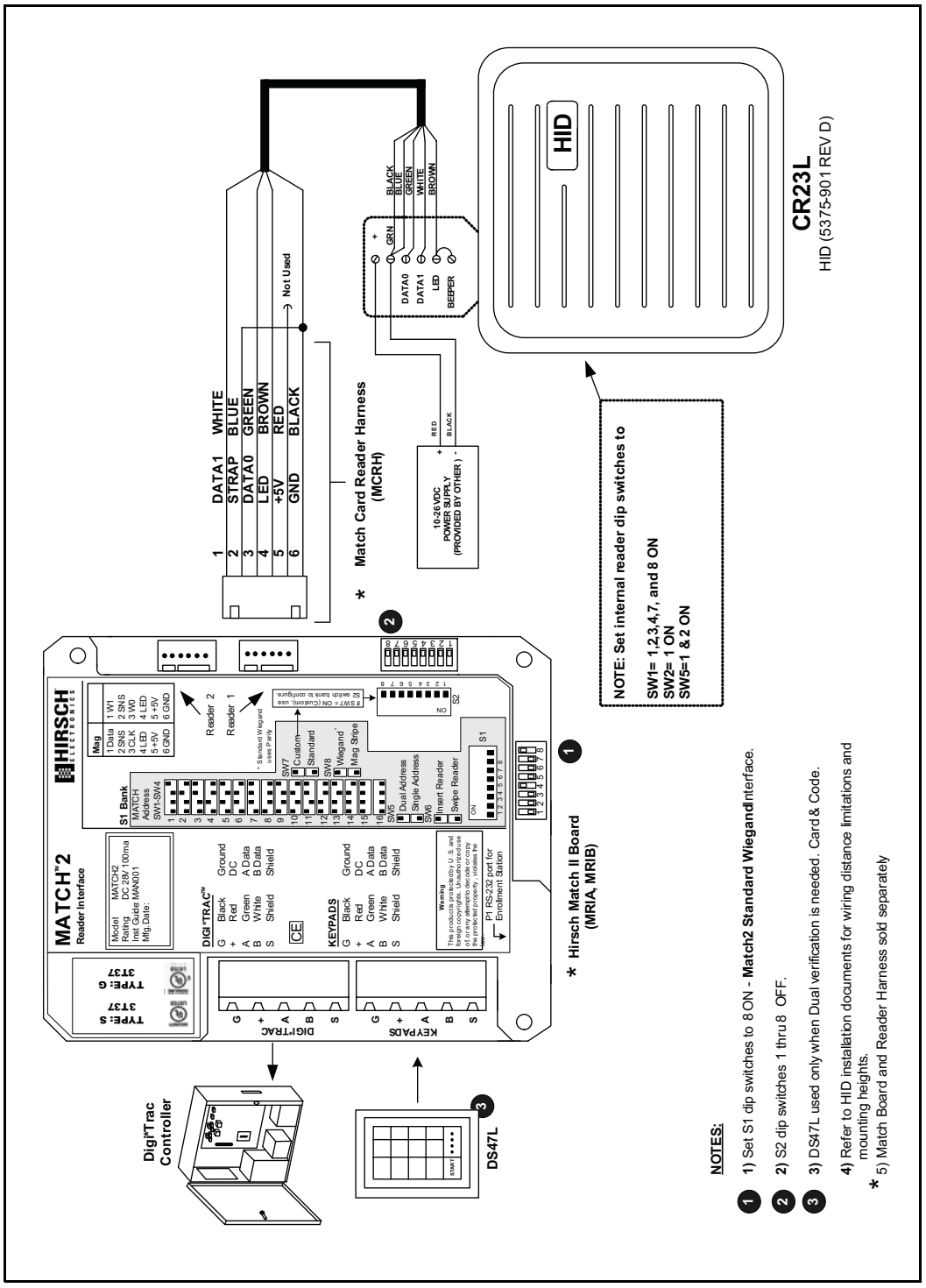
HID 5455 Medium-Range Proximity Reader

This diagram shows the wiring for the CR22L-II model.



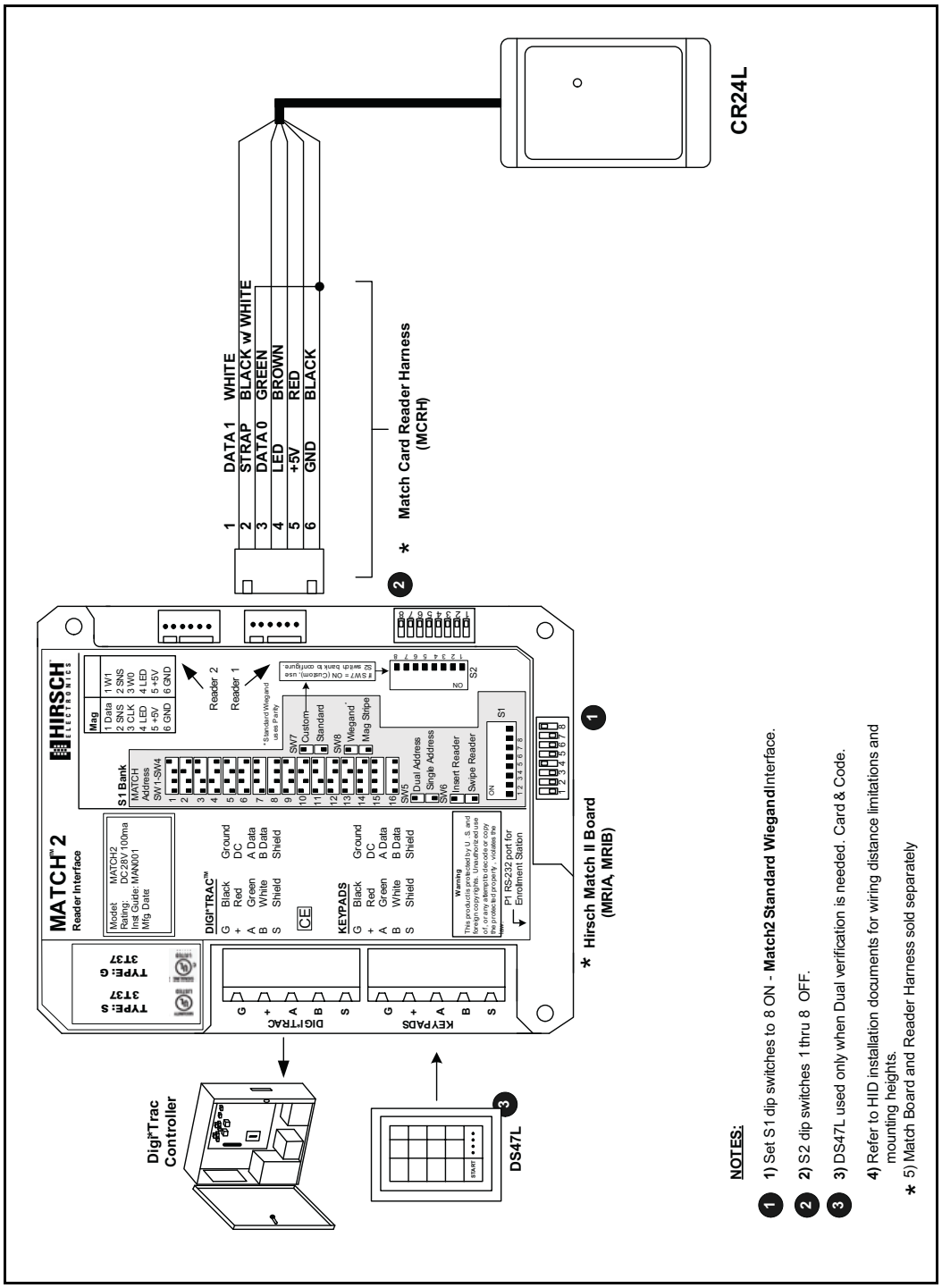
HID Proximity Reader

This diagram shows the wiring for the CR23L revision D model.



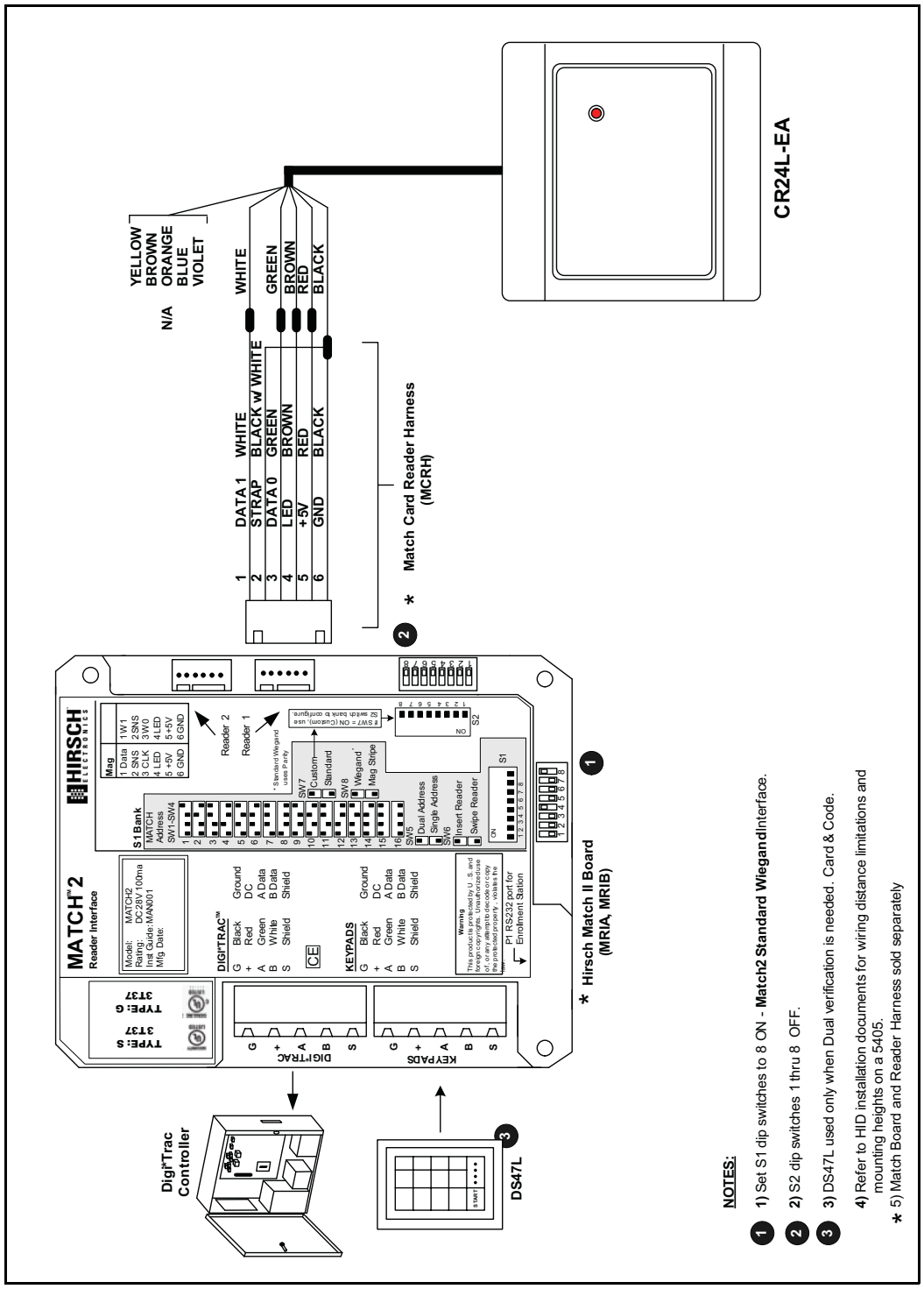
HID Proximity Thinline Reader

This diagram shows the wiring for the CR24L.



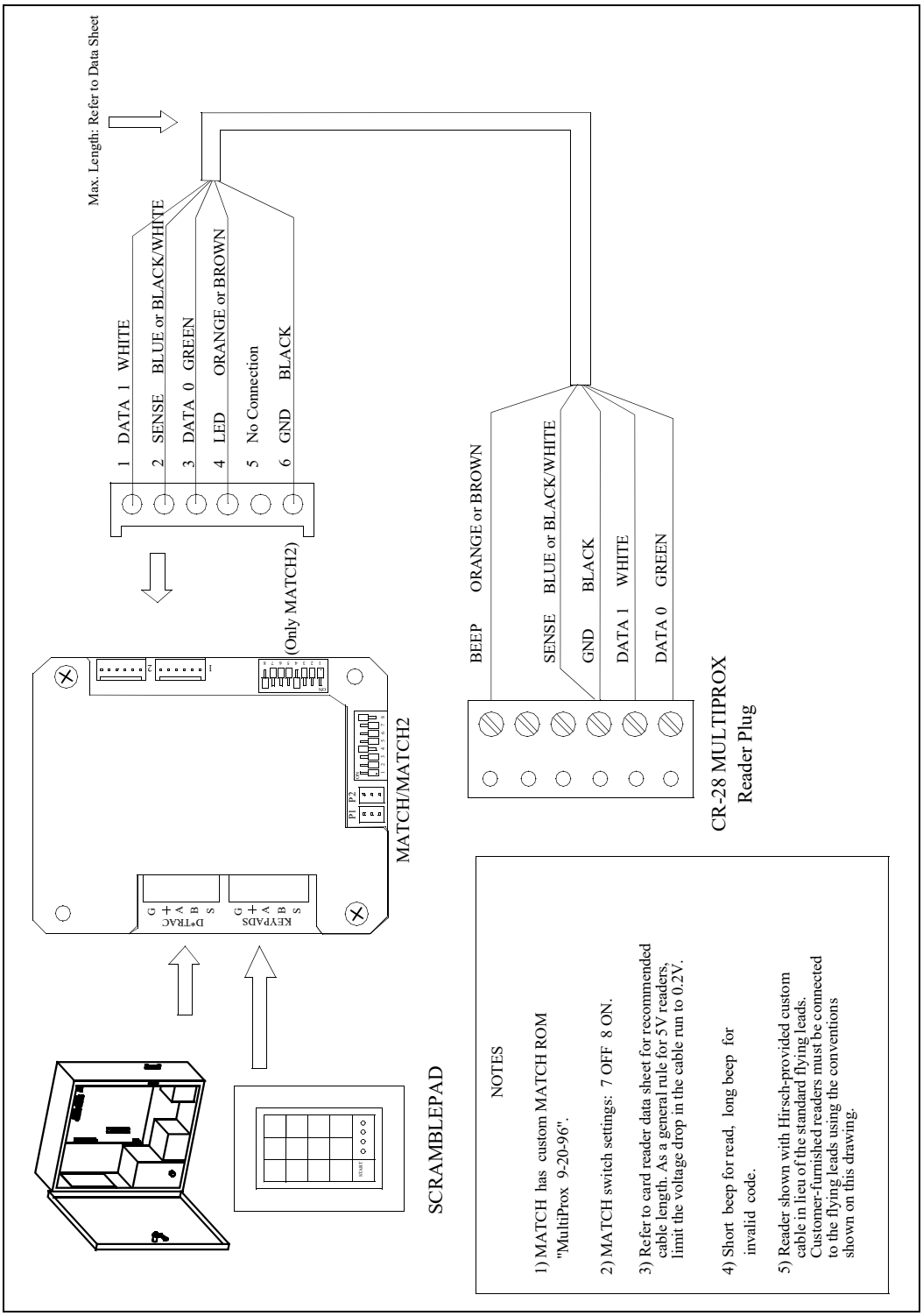
HID Proximity Thinline (Euro-Asian) Reader

This diagram shows the wiring for the CR24L-EA model.

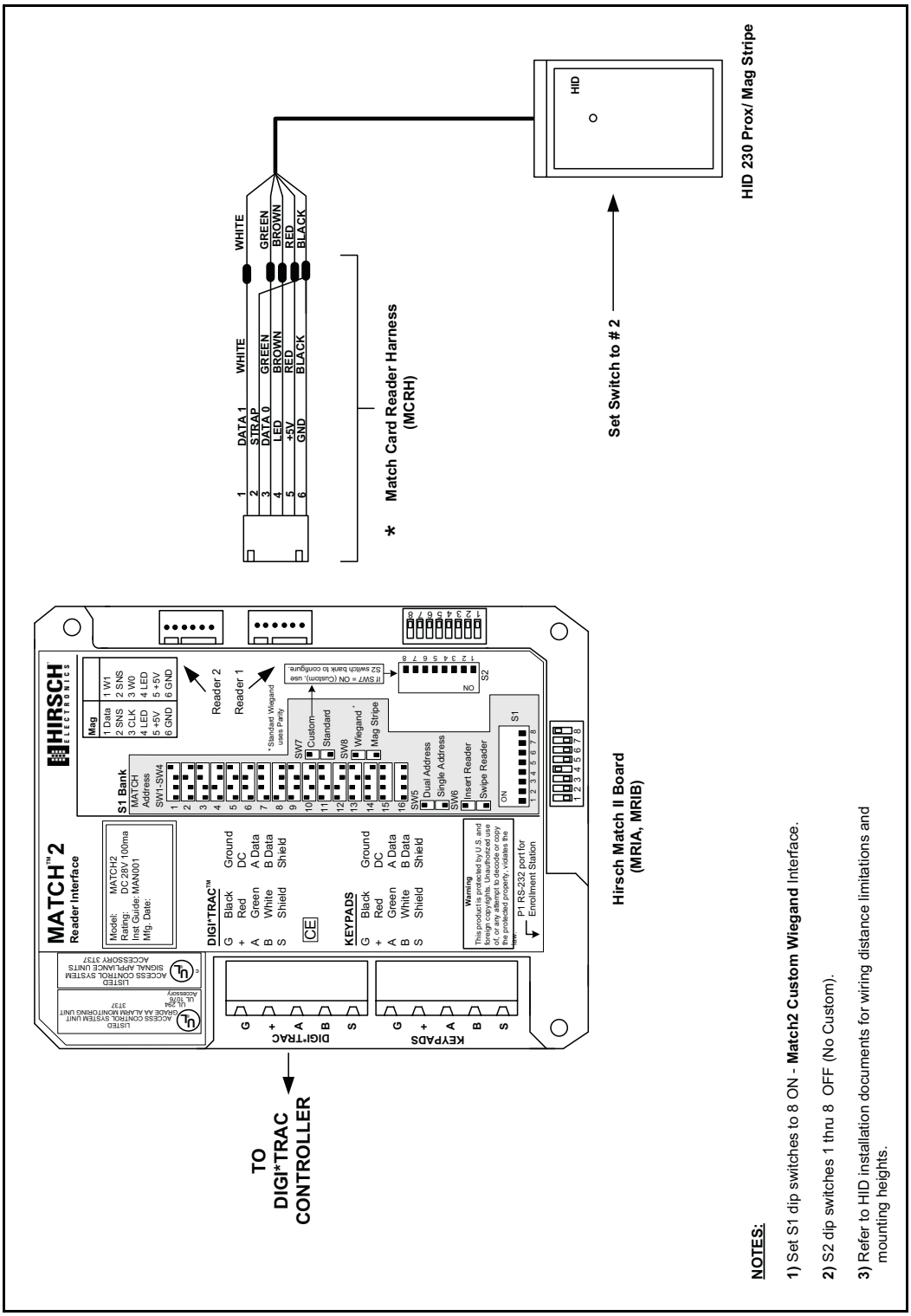


HID Multi-Prox Reader

This diagram shows the wiring for the CR28L model.



HID 230 Prox/Mag Stripe Card Reader



NOTES:

1) Set S1 dip switches to 8 ON - **Match2 Custom Wiegand** Interface.

2) S2 dip switches 1 thru 8 OFF (No Custom).

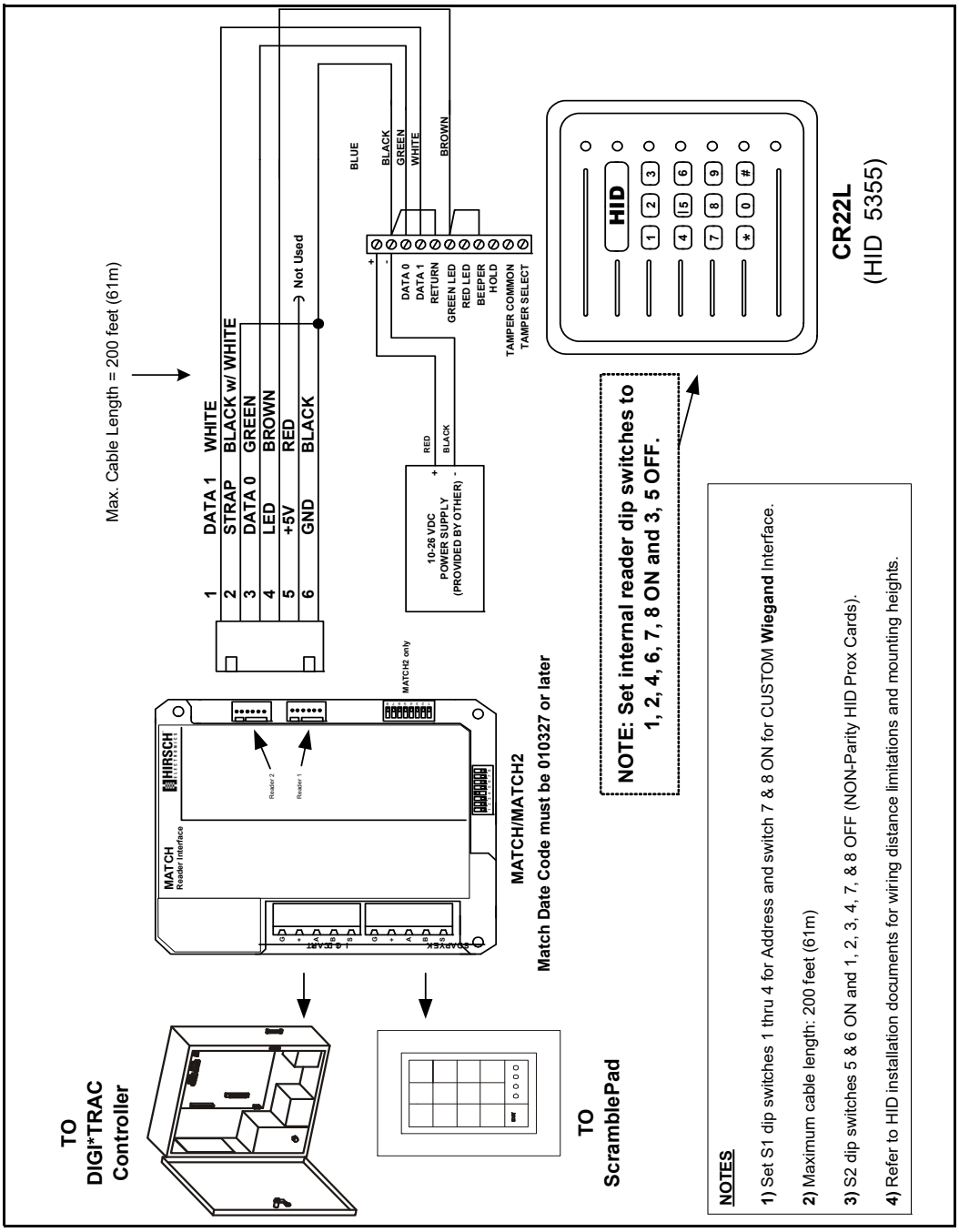
3) Refer to HID installation documents for wiring distance limitations and mounting heights.

HID Proximity Readers with Keypads

This section gives wiring diagrams for HID proximity readers with keypads. The following models are shown:

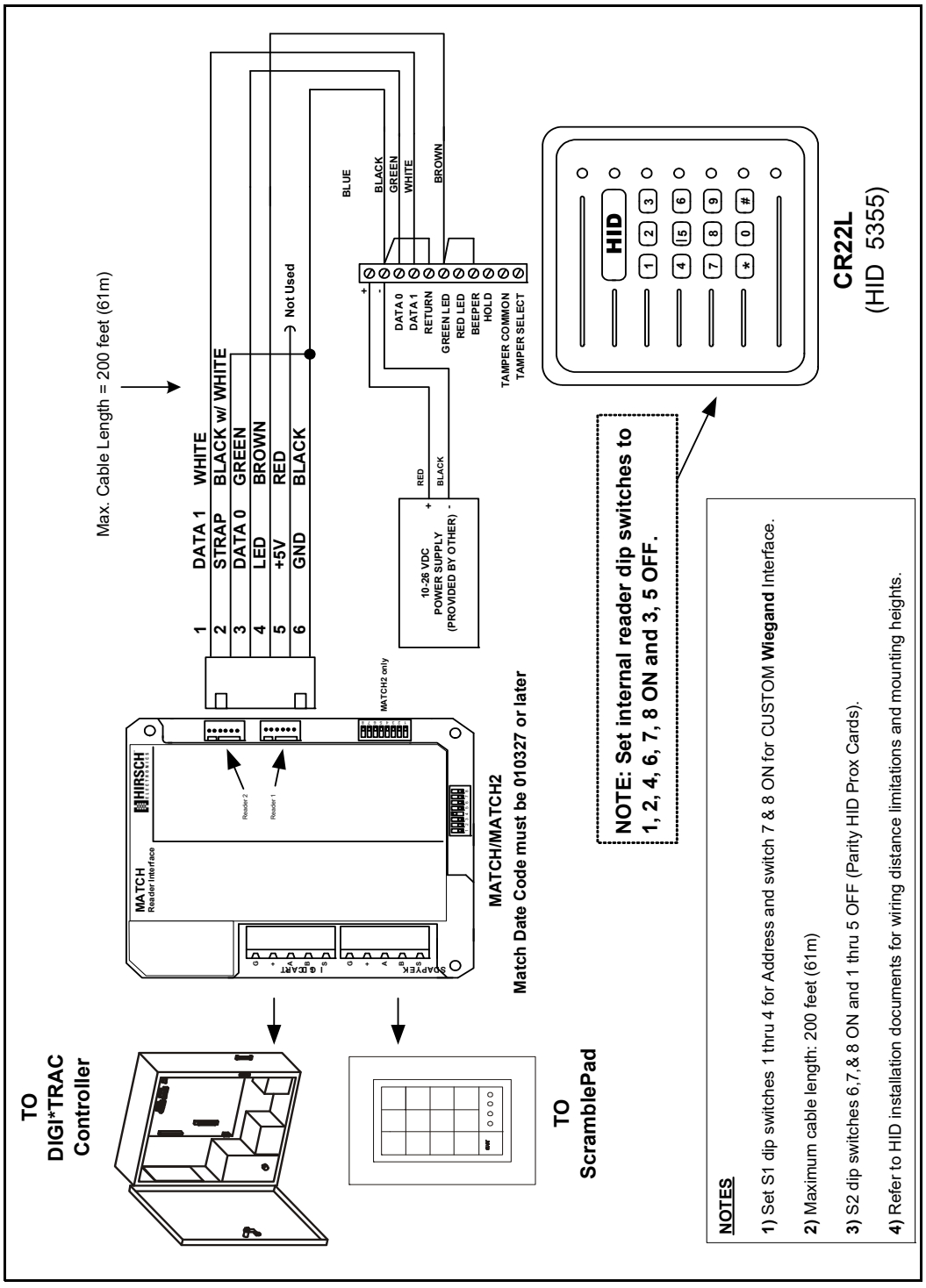
HID Prox with Keypad for Non-Parity Cards

This diagram shows the wiring for the CR22L with keypad for non-parity cards.



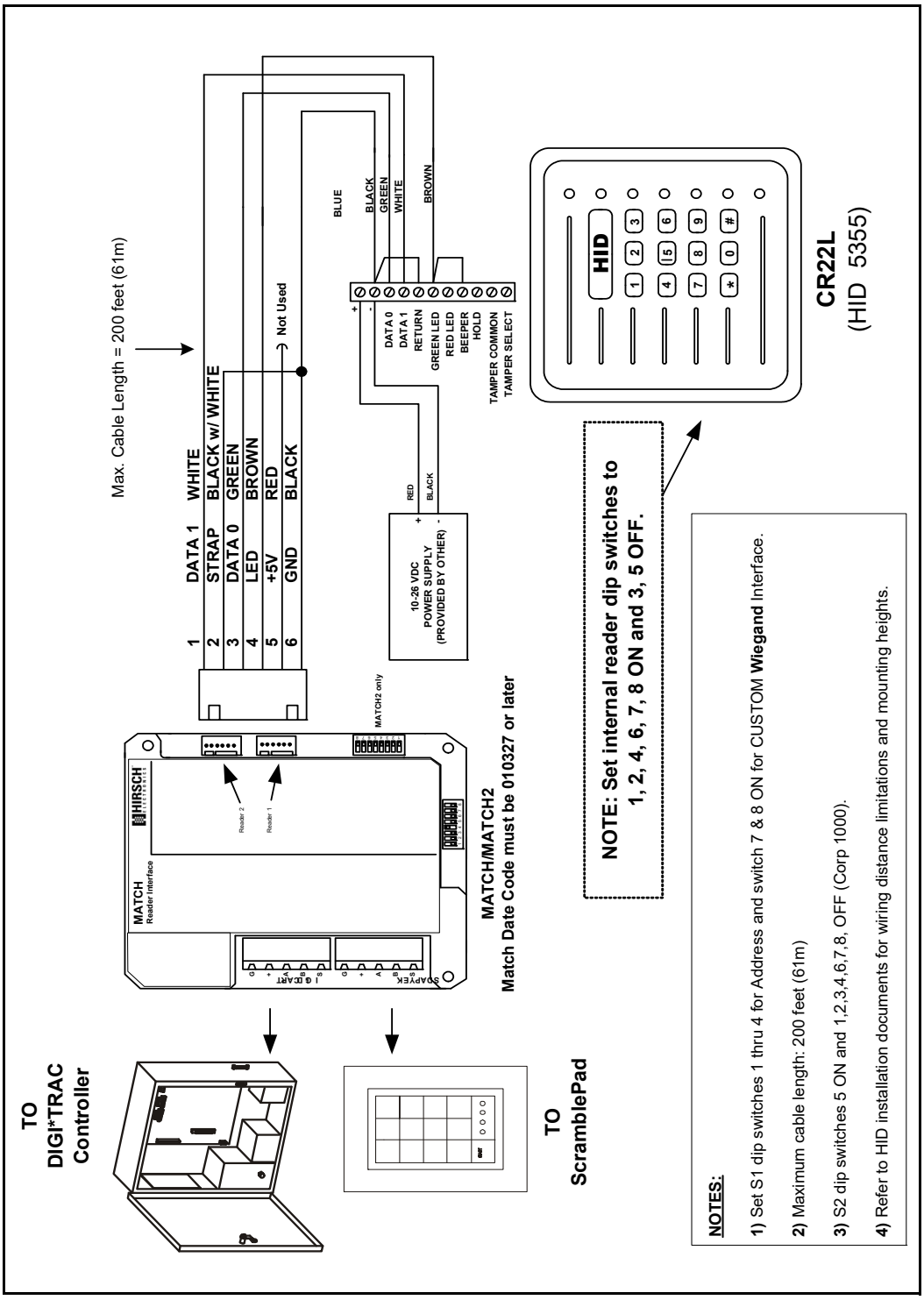
HID Prox with Keypad for Parity Cards

This diagram shows the wiring for the CR22L with keypad for parity cards.



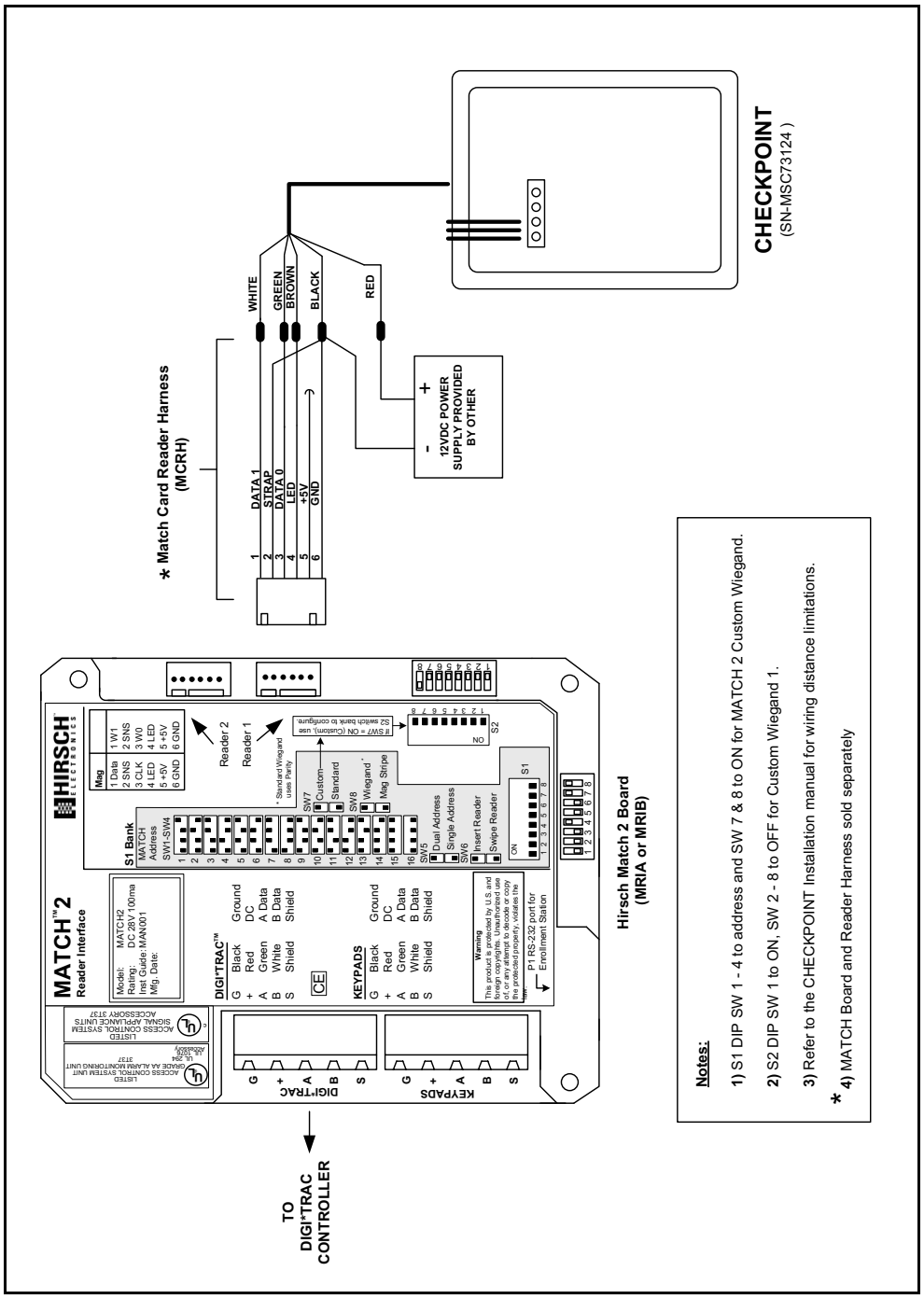
HID Prox with Keypad for Corporate 1000 Cards

This diagram shows the wiring for the CR22L with keypad for Corporate 1000 cards.



Checkpoint Proximity Reader

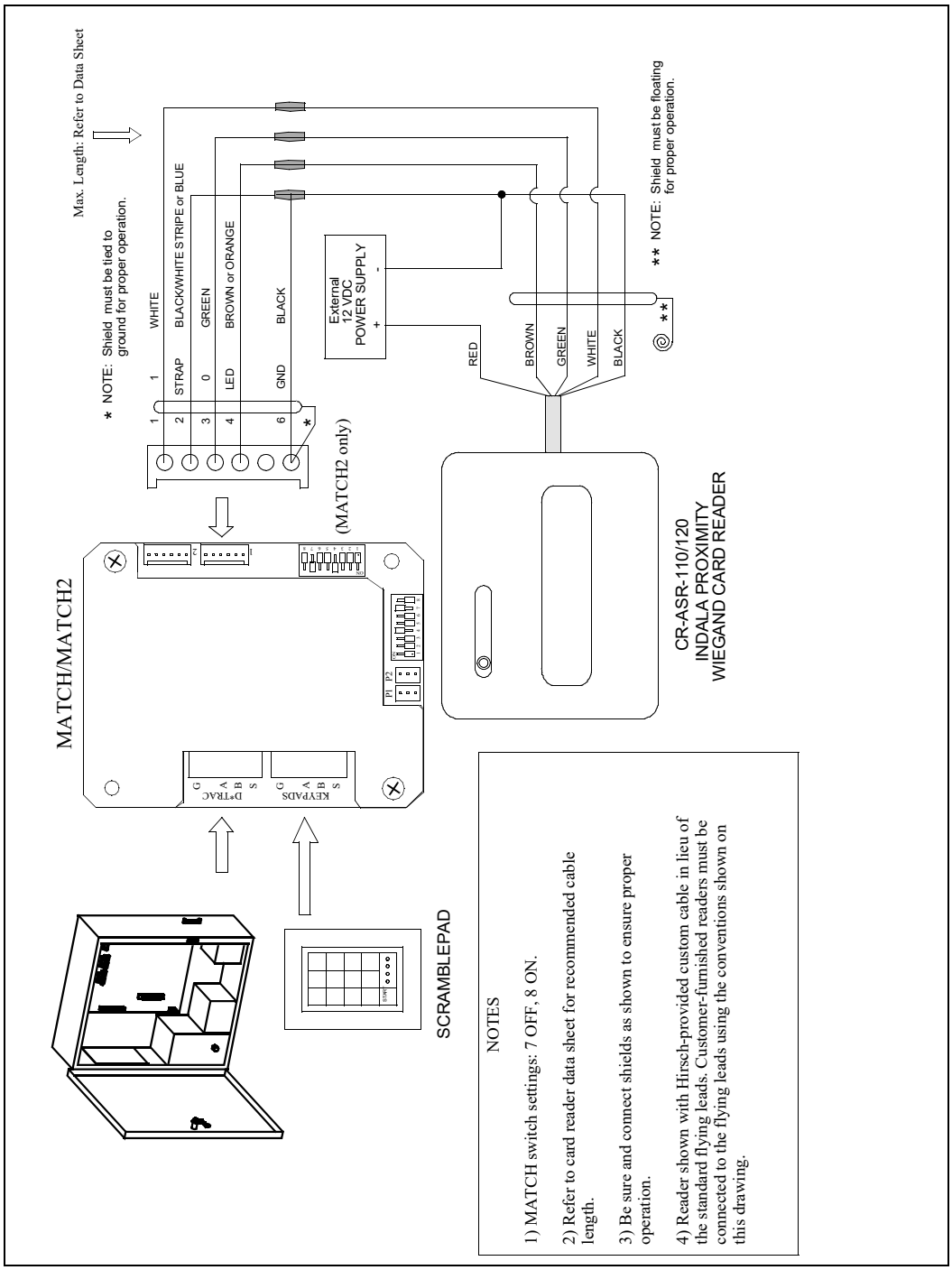
This diagram shows the wiring for the Checkpoint proximity reader.



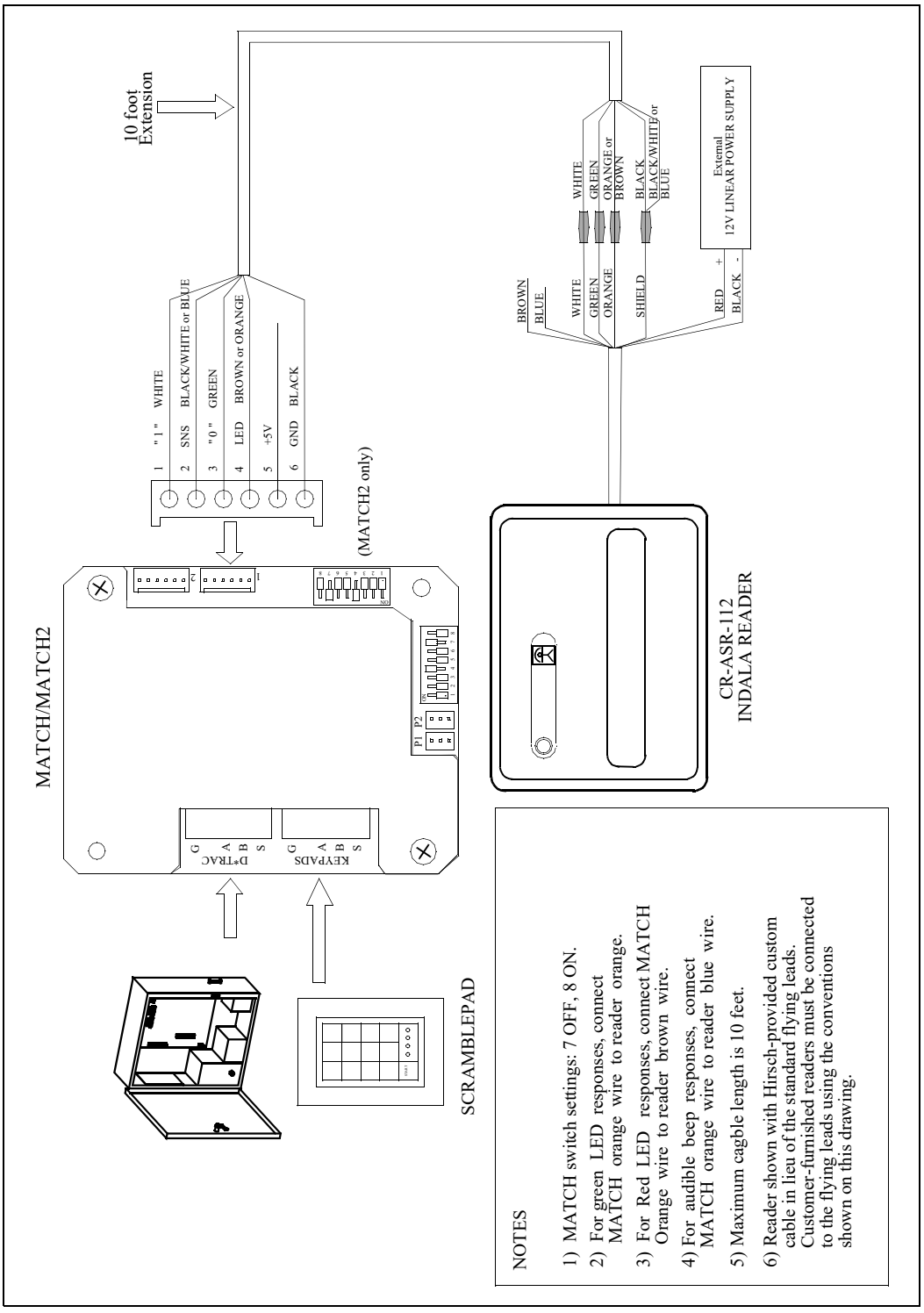
Indala Proximity Card Readers

This section gives wiring diagrams for Indala proximity card readers. The following models are shown:

CR-ASR-110/-120 Series Card Readers

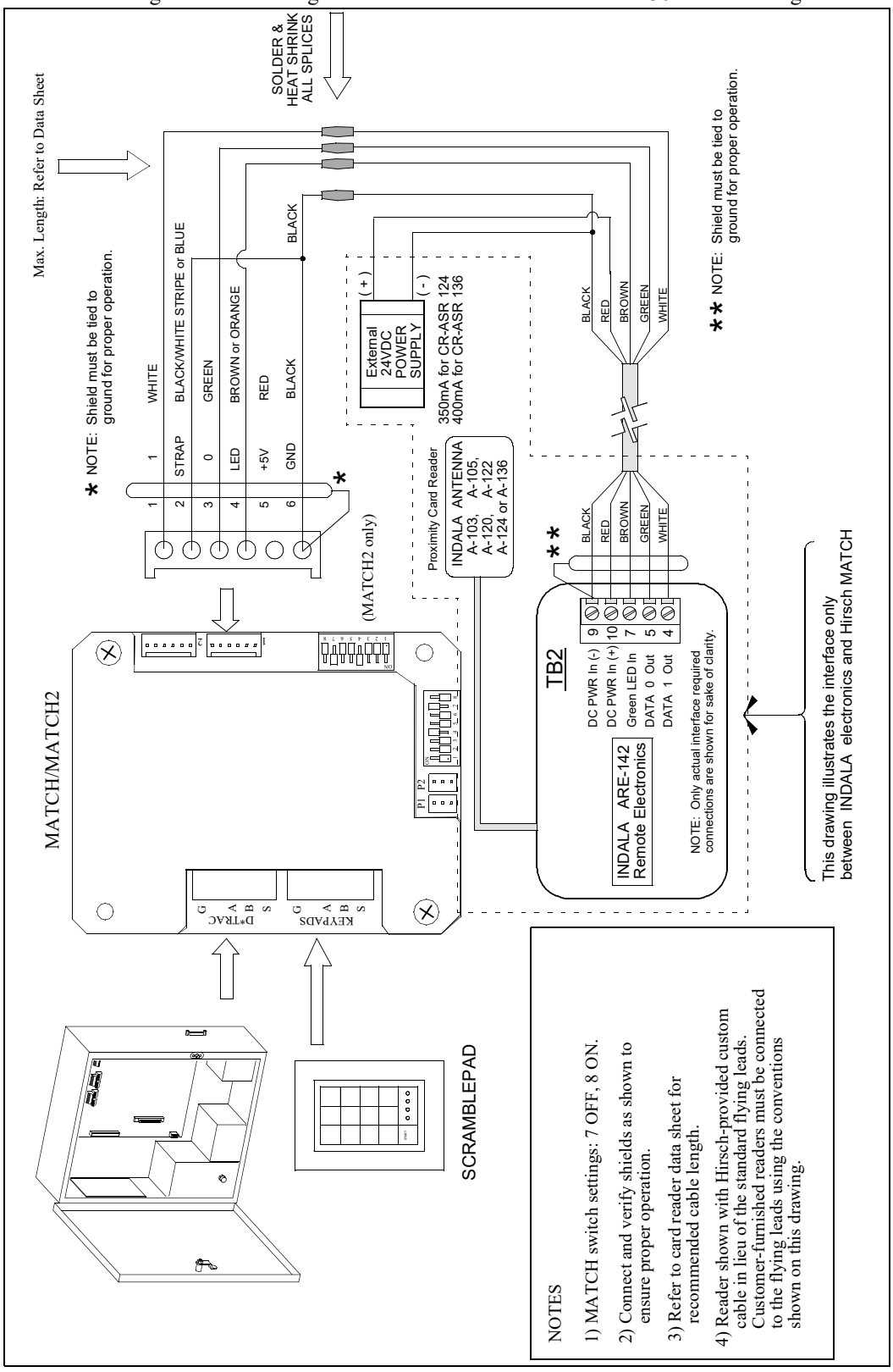


CR-ASR-112 Card Reader



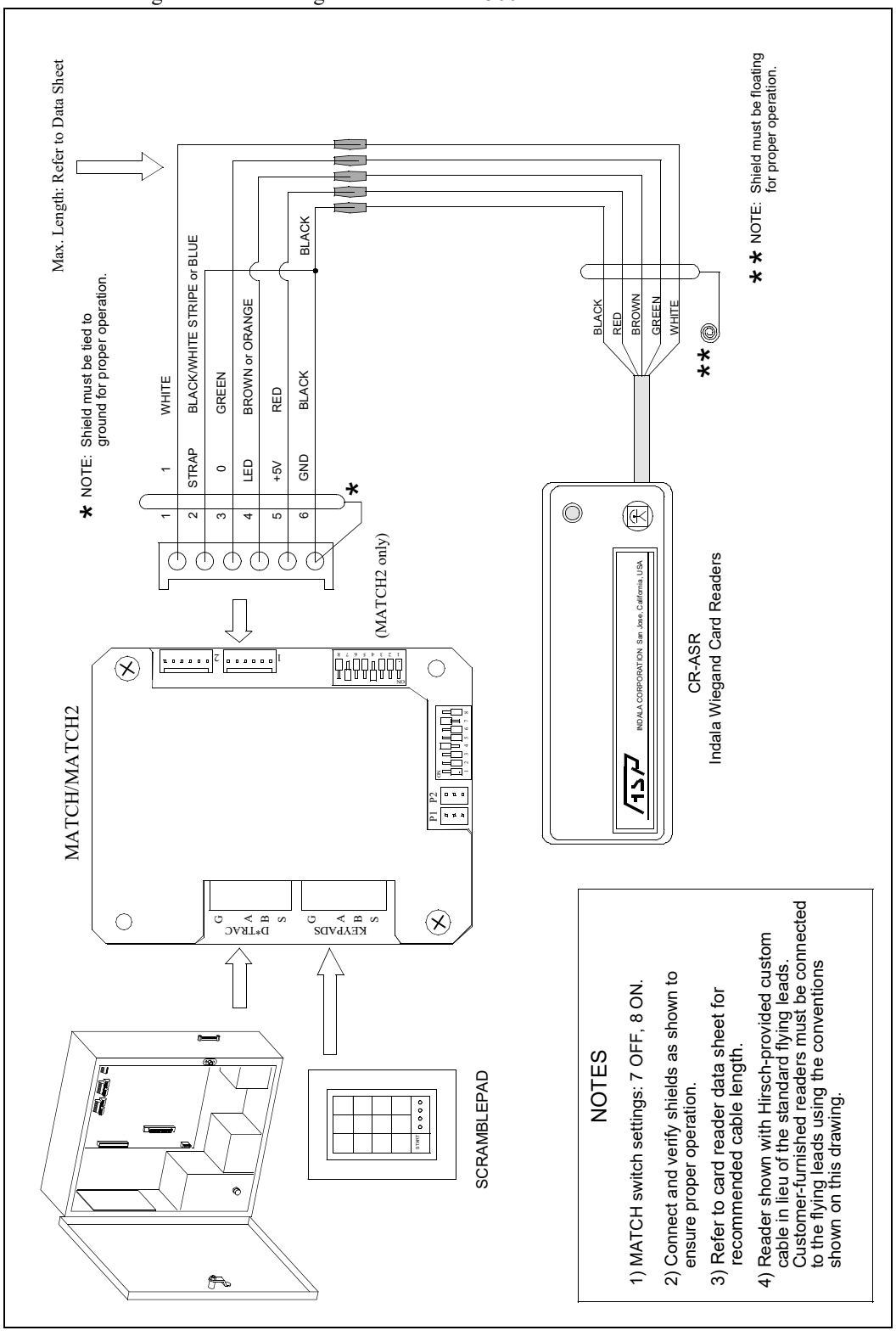
Extended Range Card Reader

This diagram shows wiring for the CR-ASR-124 and CR-ASR-136 extended range readers.



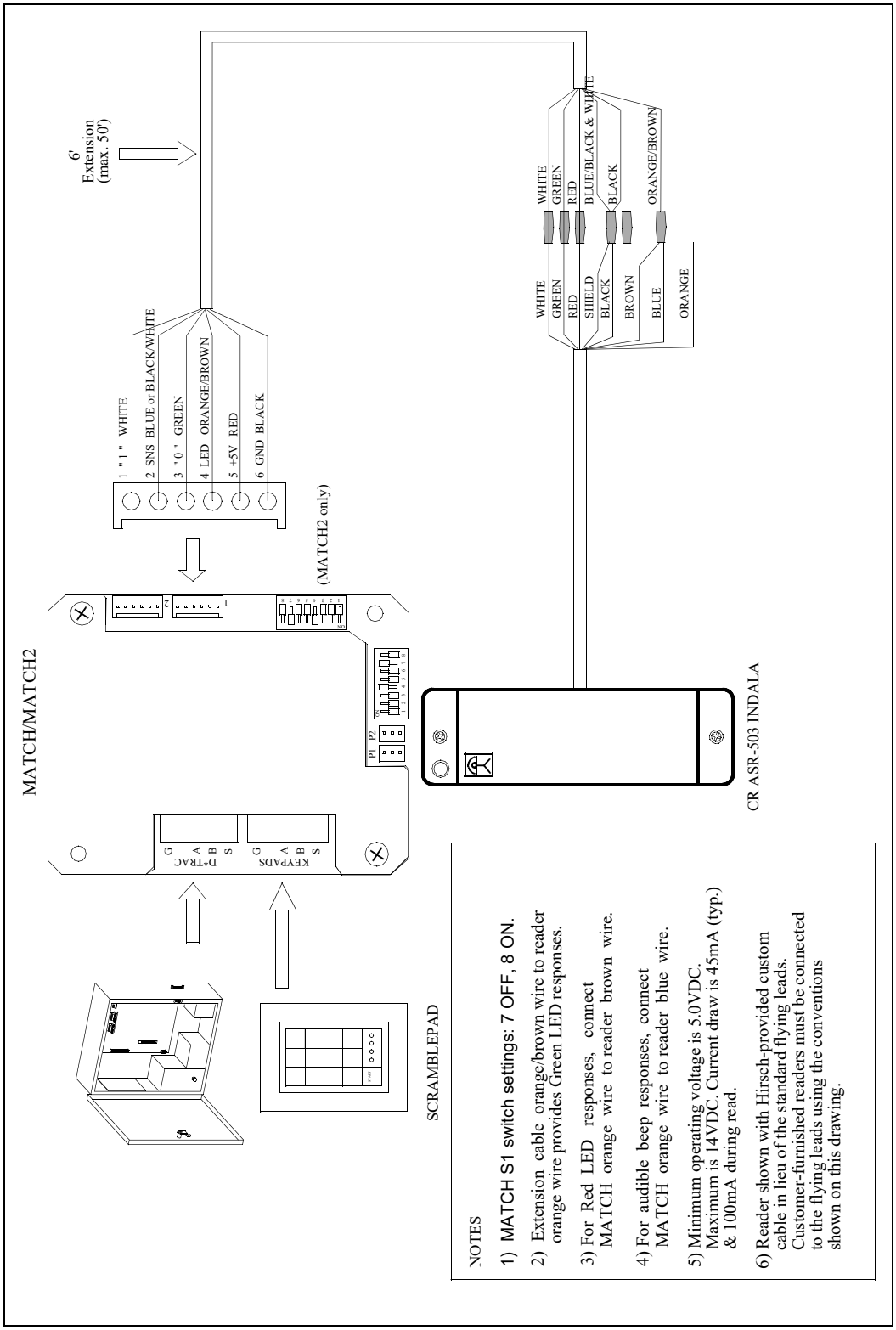
ValueProx Card Reader

This diagram shows wiring for the CR-ASR-500 ValueProx card reader.



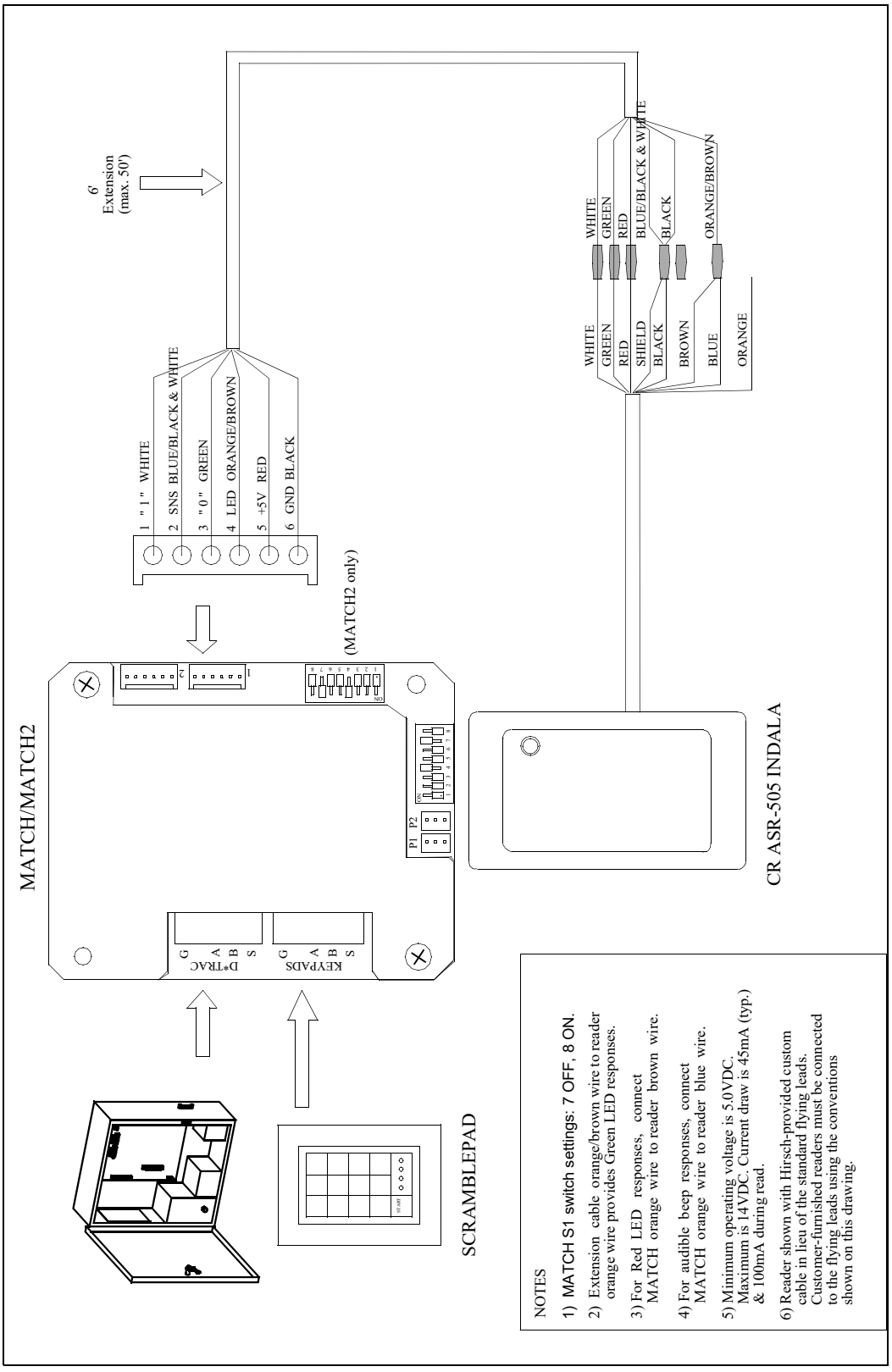
Slimline Card Reader

This diagram shows wiring for the CR-ASR-503 Slimline card reader.



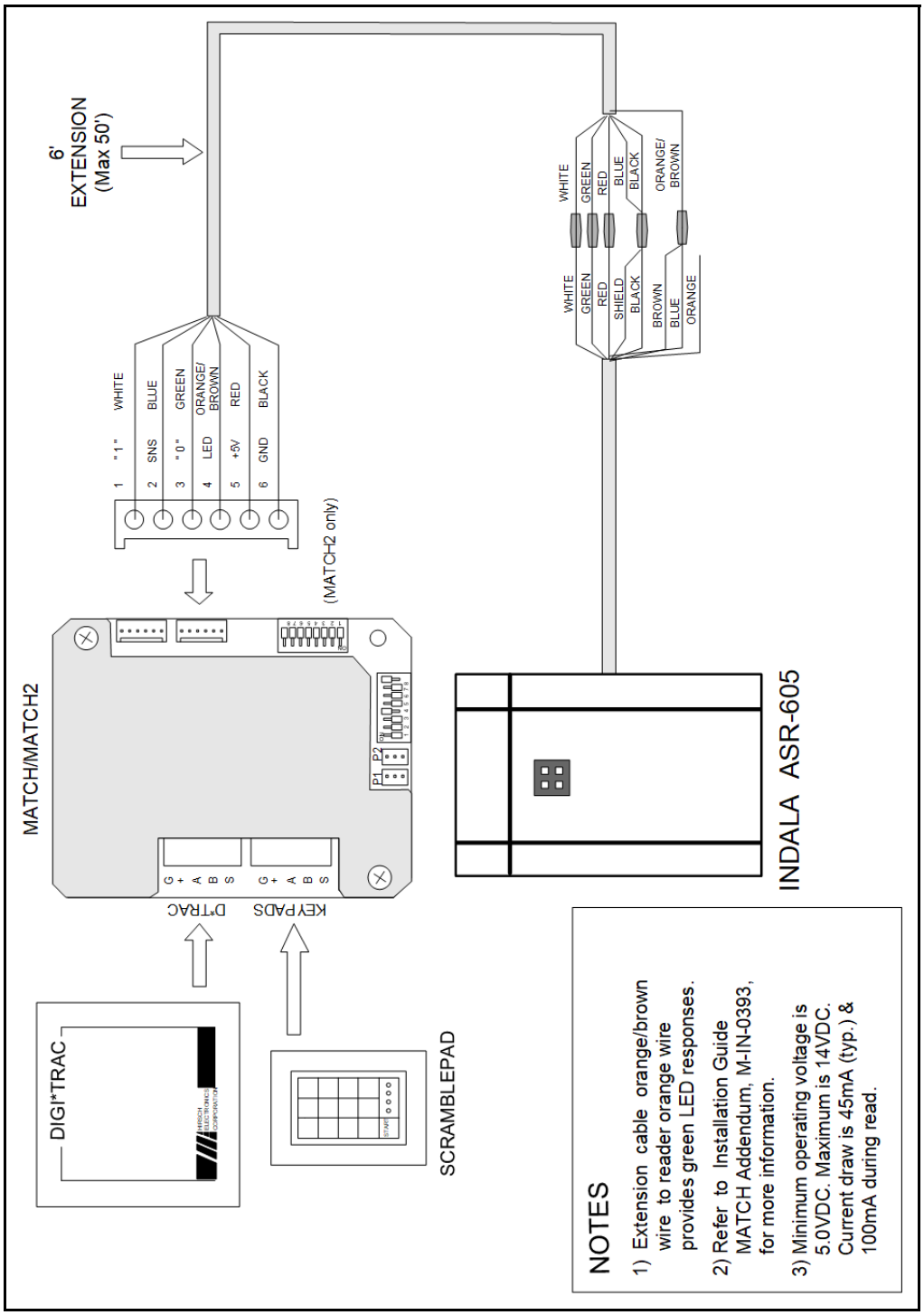
WallSwitch Card Reader

This diagram shows wiring for the CR-ASR-505 Wallswitch card reader.



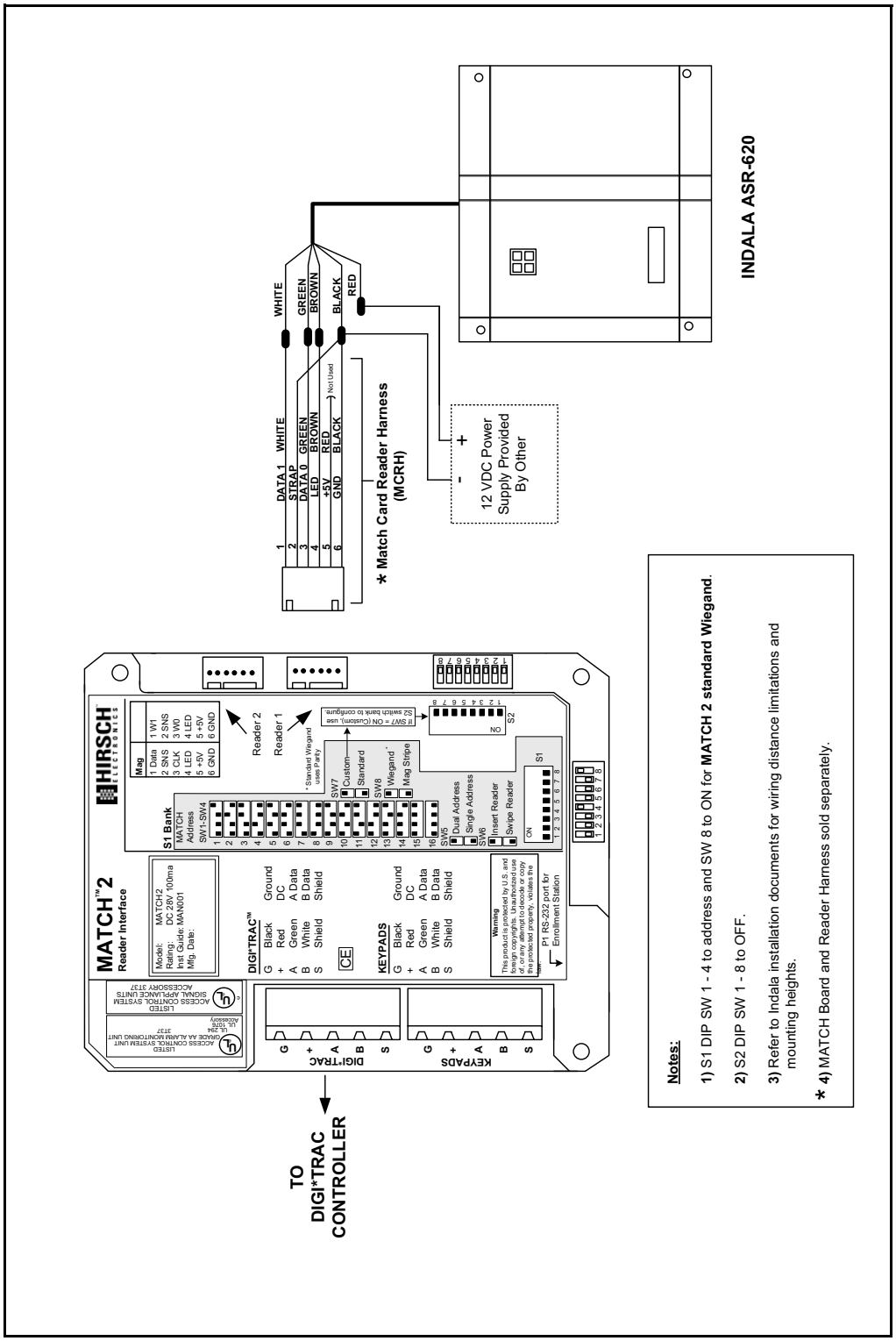
Arch Card Reader

This diagram shows wiring for the CR-ASR-605 Arch card reader.



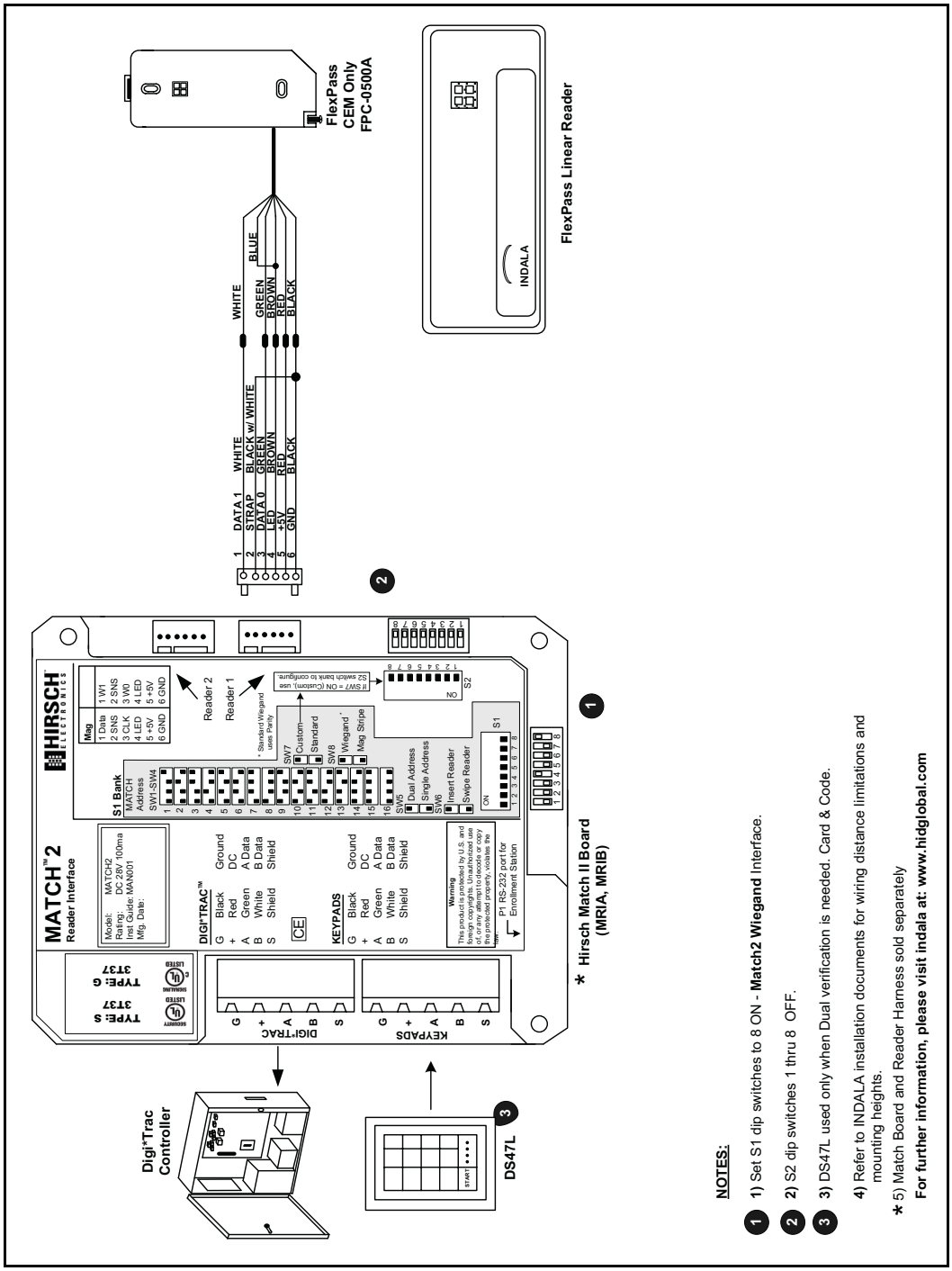
Proximity Card Reader

This diagram shows wiring for the CR-ASR-620-BL proximity card reader.



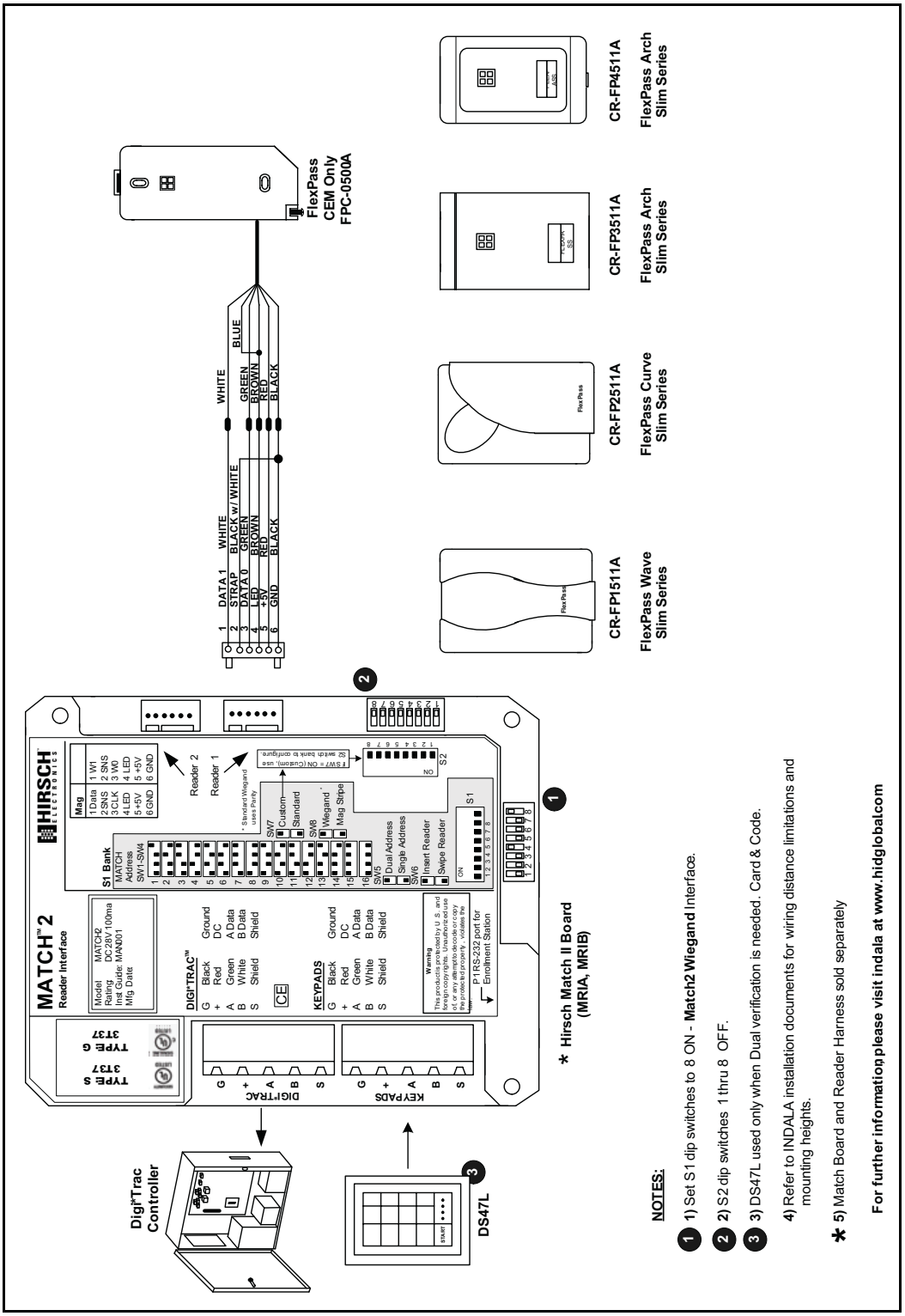
FlexPass Linear Card Reader

This diagram shows wiring for the Indala CR-FP4551A FlexPass Linear card reader (mag stripe style).



FlexPass Slim Series Proximity Readers

This diagram shows the wiring for the following Indala FlexPass Slim models: CR-FP1511A (FlexPass Wave), CR-FP2511A (FlexPass Curve), CR-FP3511A (FlexPass Arch), and CR-FP4511A (FlexPass Arch).

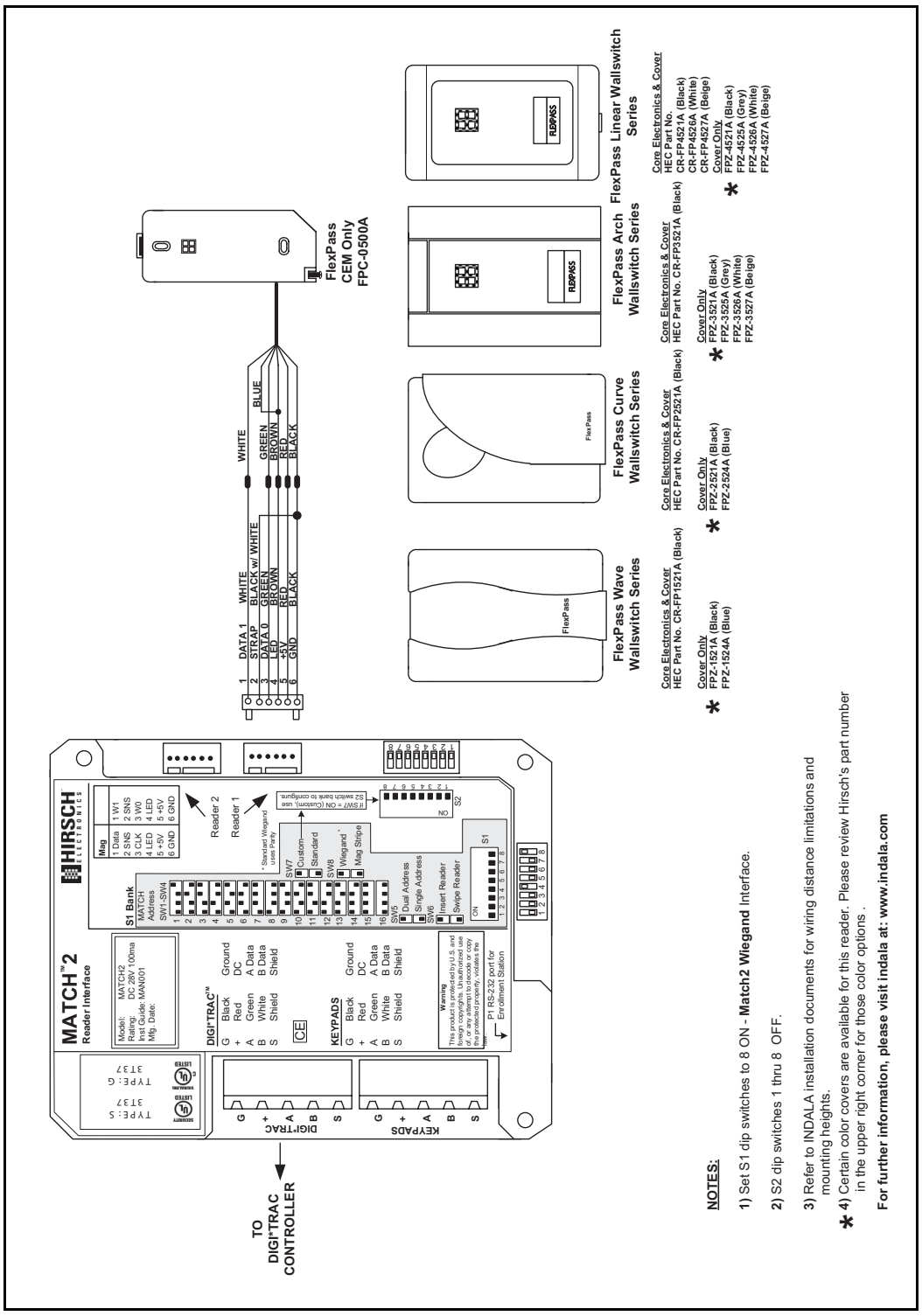


FlexPass Wallswitch Series Proximity Readers

This section gives wiring diagrams for the following Indala FlexPass Wallswitch series proximity readers:

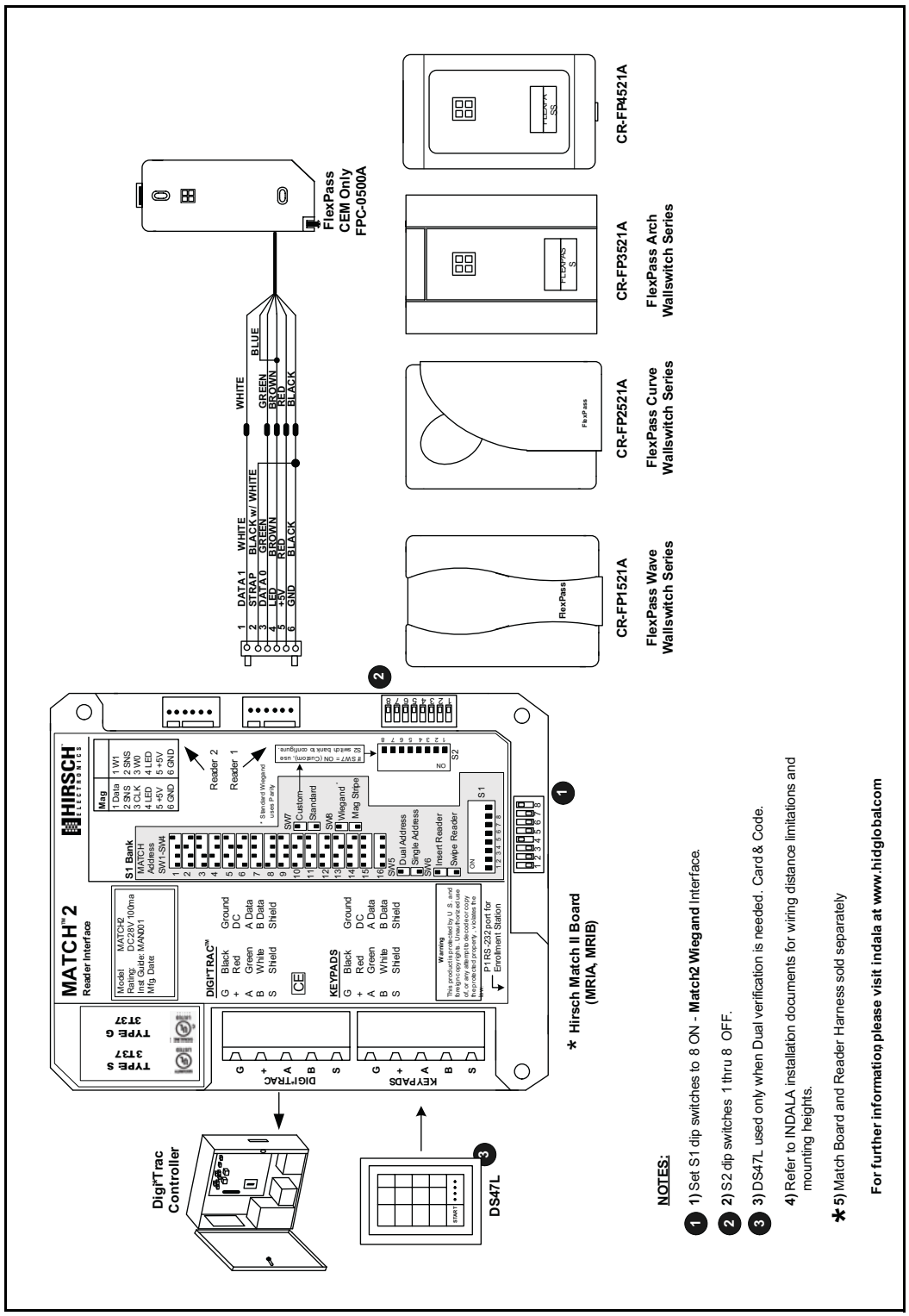
CR-FP1520, CR-FP2520, CR-FP3520, and CR-FP4520

This diagram shows the wiring for the following Indala FlexPass Wallswitch models: CR-FP1520 (FlexPass Wave), CR-FP2520 (FlexPass Curve), CR-FP3520 (FlexPass Arch), and CR-FP4520 (FlexPass Linear).



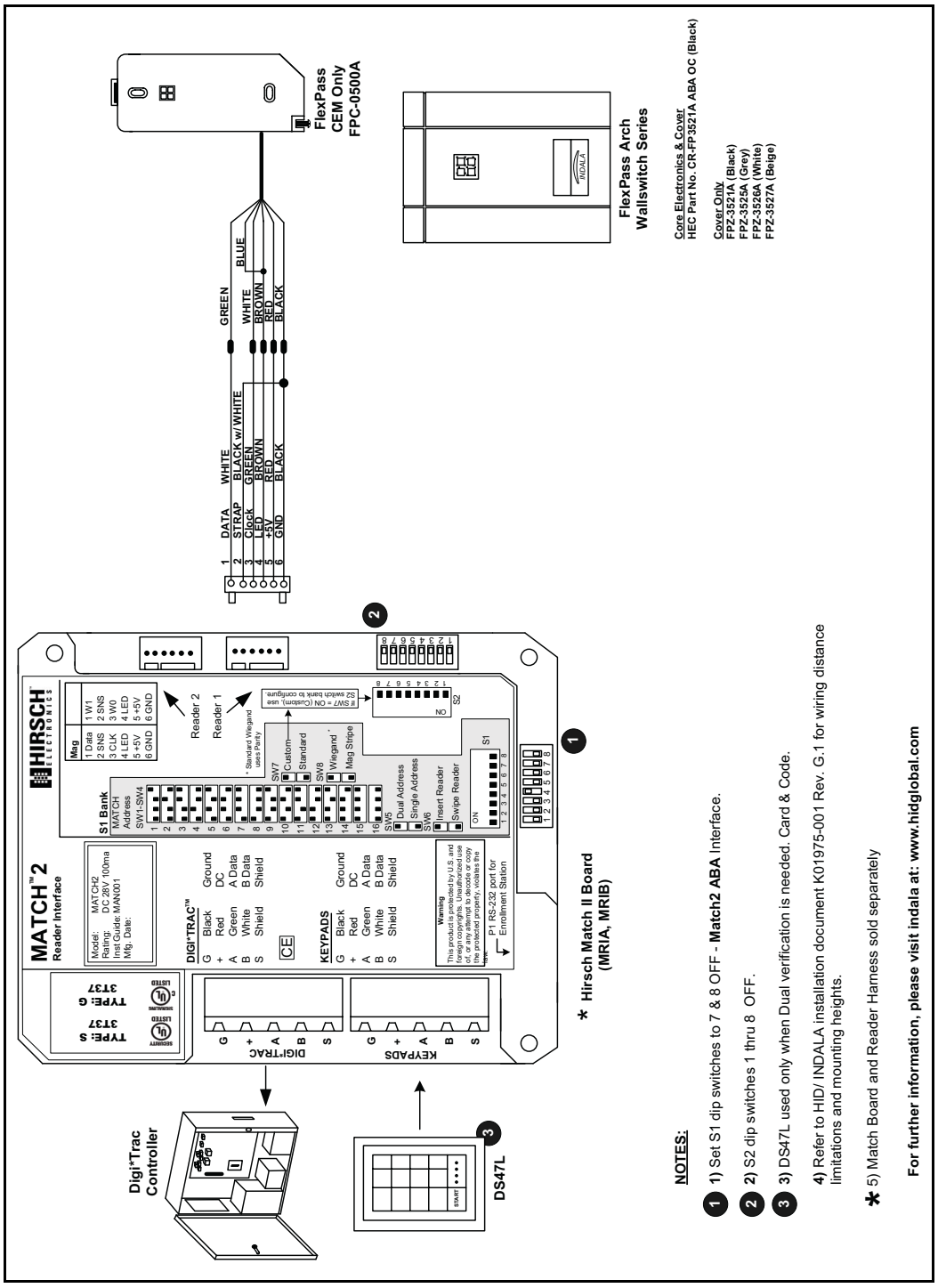
CR-FP1521, CR-FP2521, CR-FP3521, and CR-FP4521

This diagram shows the wiring for the following Indala FlexPass Wallswitch models: CR-FP1521 (FlexPass Wave), CR-FP2521 (FlexPass Curve), CR-FP3521 (FlexPass Arch), and CR-FP4521 (FlexPass Linear).



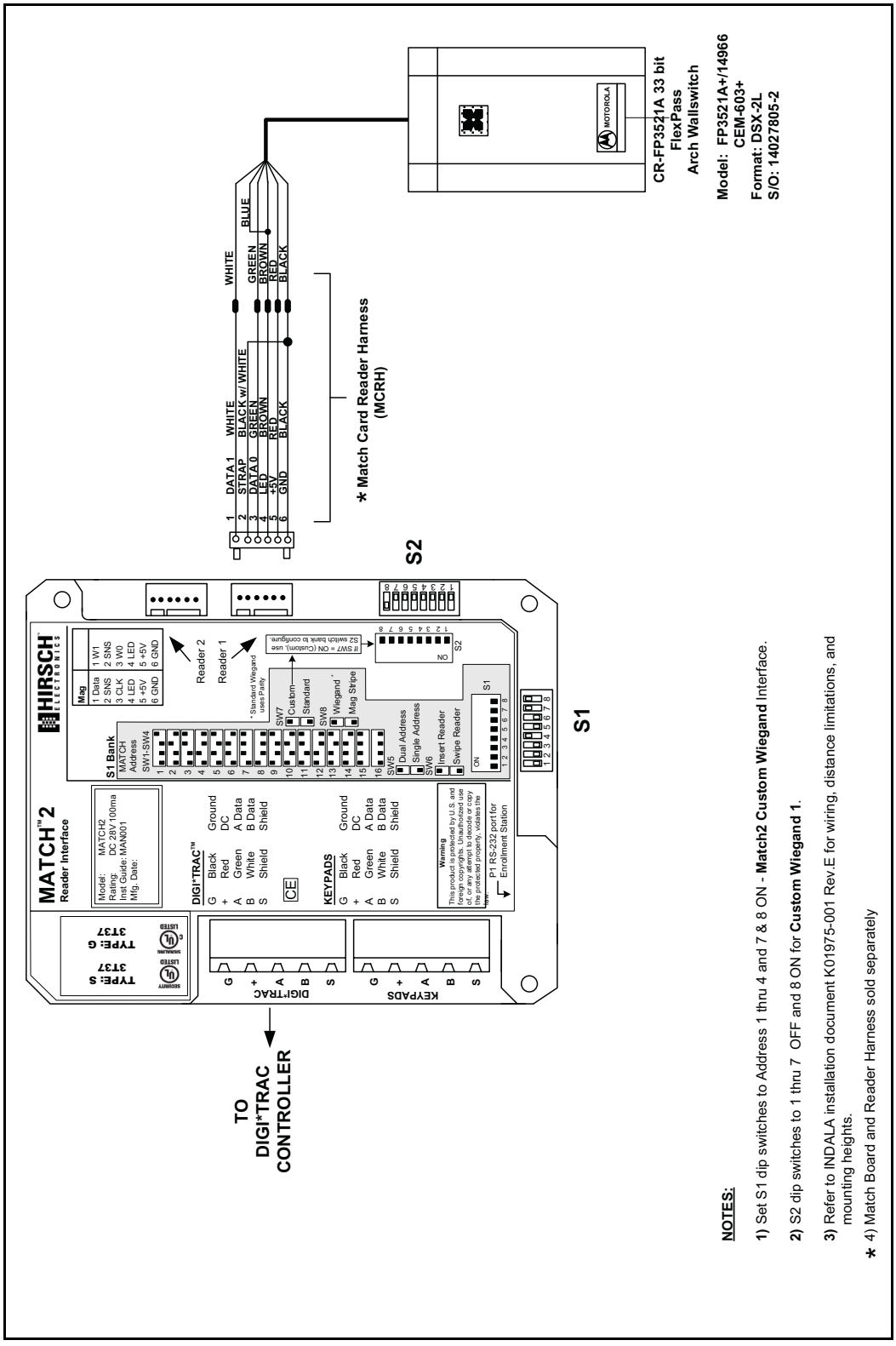
FlexPass Arch Wallswitch Reader

This diagram shows the wiring for the following Indala FlexPass Arch Wallswitch models FP3521A. This is specific to the ABA Track II OC standard.



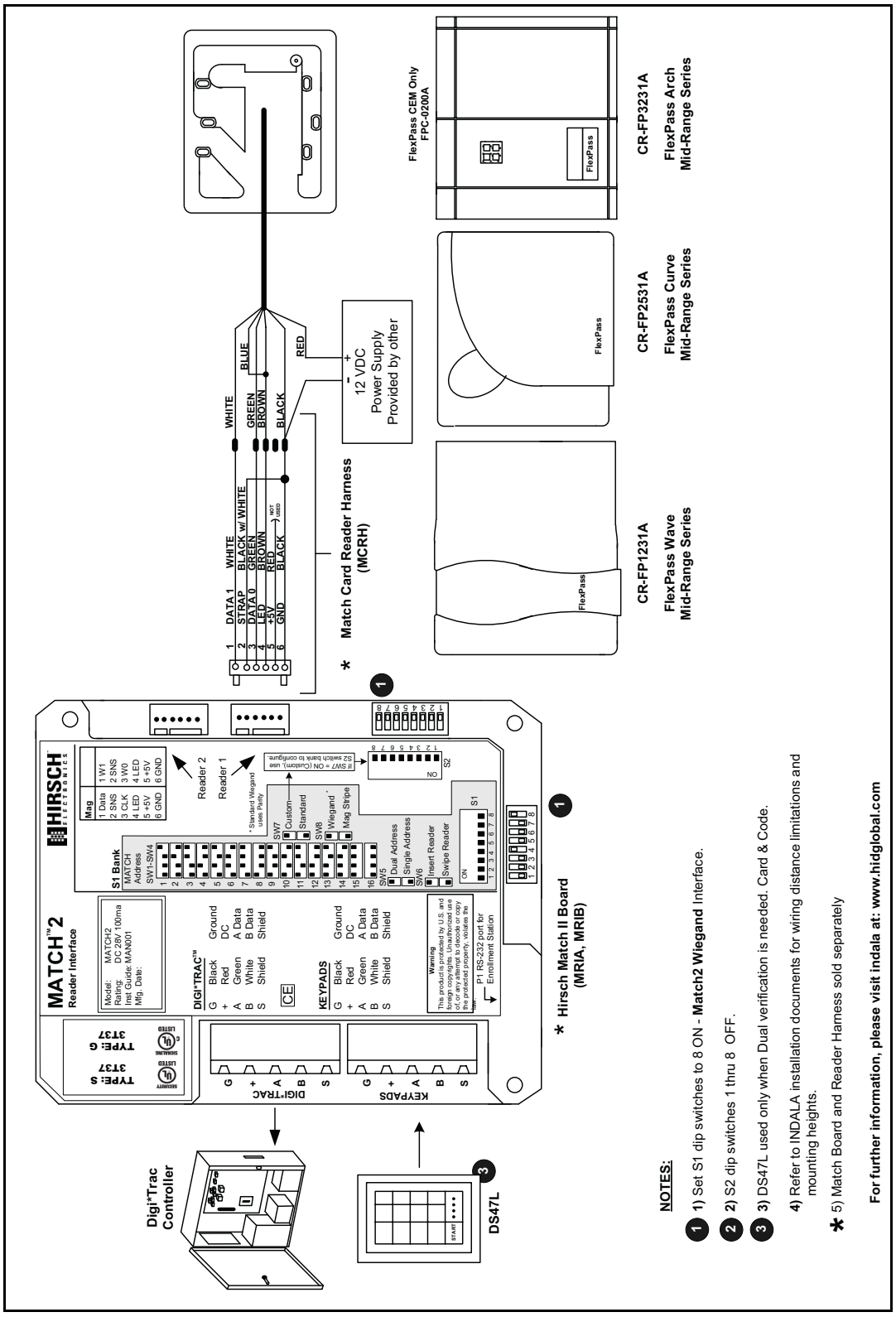
FlexPass Arch Wallswitch DSX-2L Reader

This diagram shows the wiring for the CR-FP3521A Indala/Motorola FlexPass DSX-2L Special 33-Bit Reader.



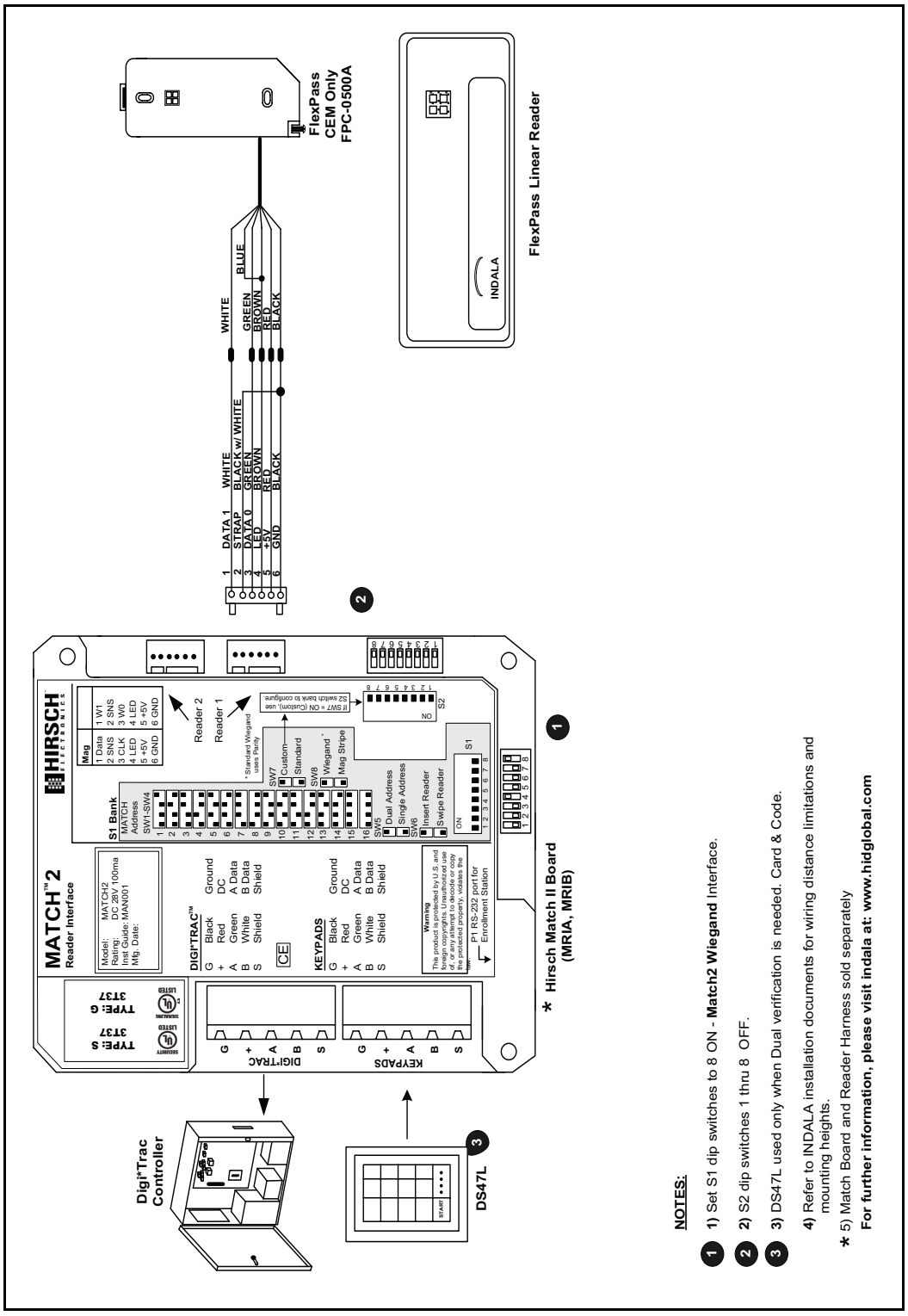
FlexPass Mid-Range Series Prox Readers

This diagram shows the wiring for the Indala FlexPass Mid-Range models: CR-FP1231A (FlexPass Wave), CR-FP2521A (FlexPass Curve), and CR-FP3231A (FlexPass Arch).



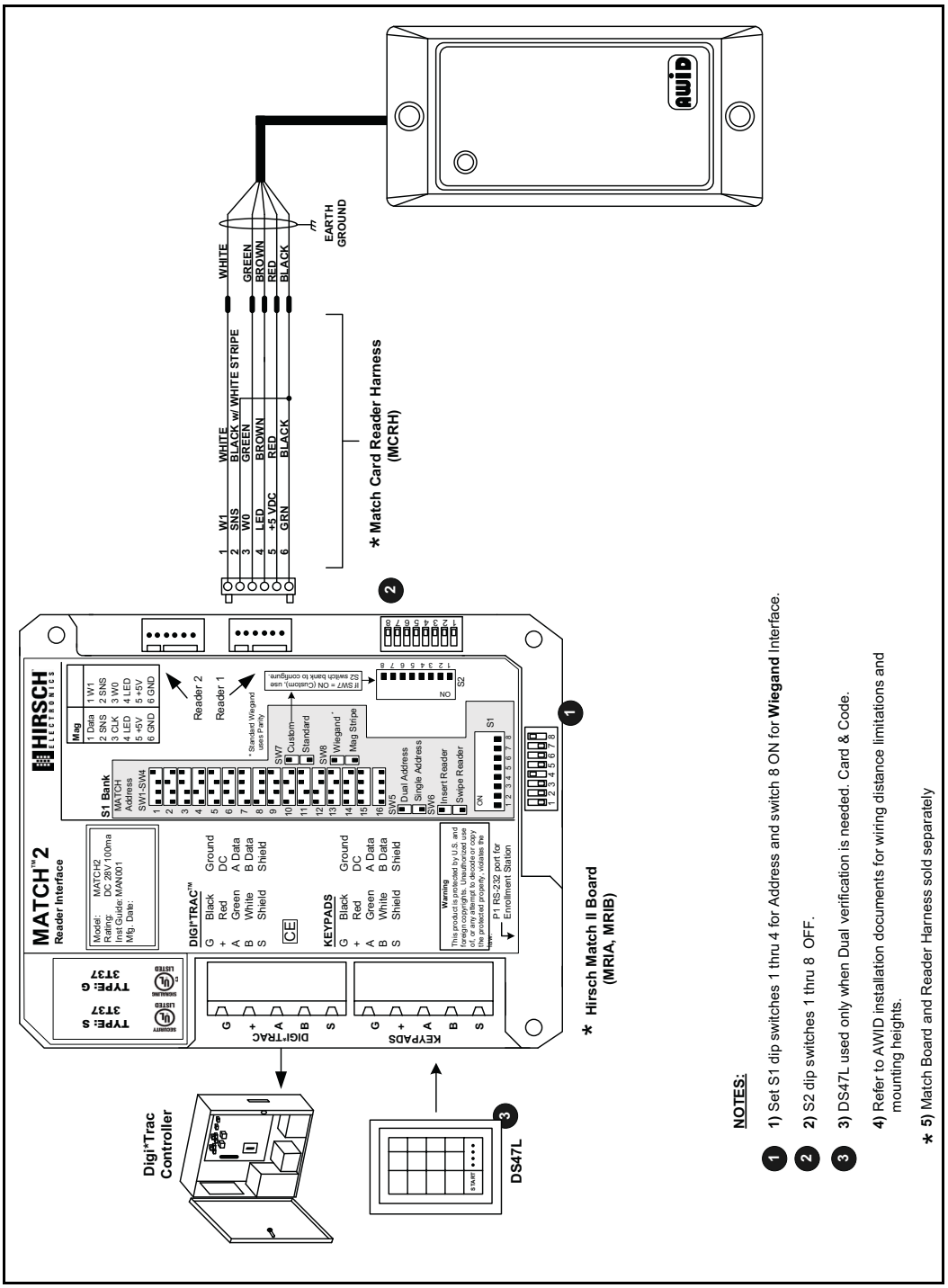
Motorola FlexPass Linear Reader

This diagram shows the wiring for the CR-FP4551A Motorola FlexPass Linear Reader.



AWID Proximity Reader

This diagram shows the wiring for the SR-2400 AWID Prox Reader.

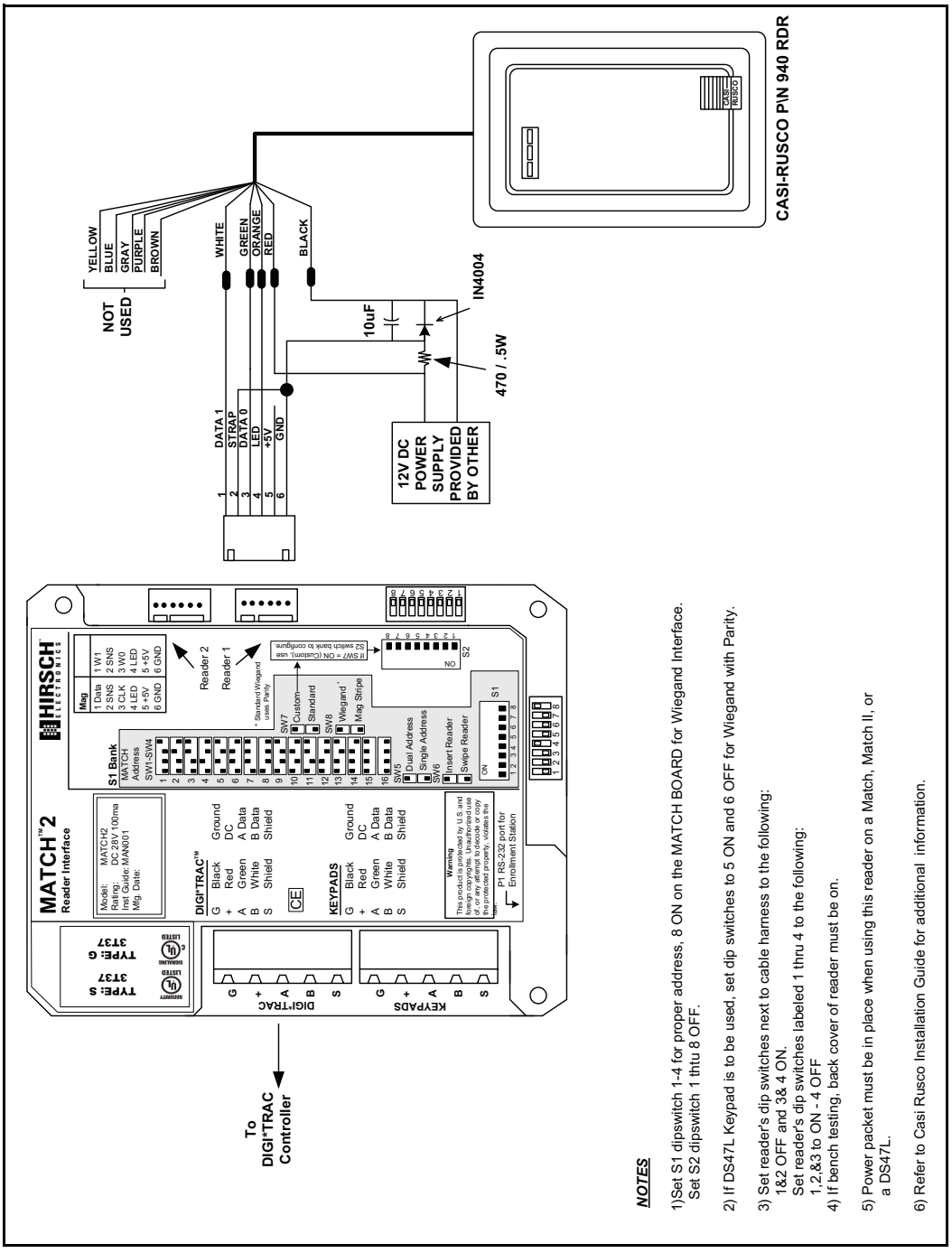


Casi-Rusco Card Readers

This section gives wiring diagram for the following Casi-Rusco card readers:

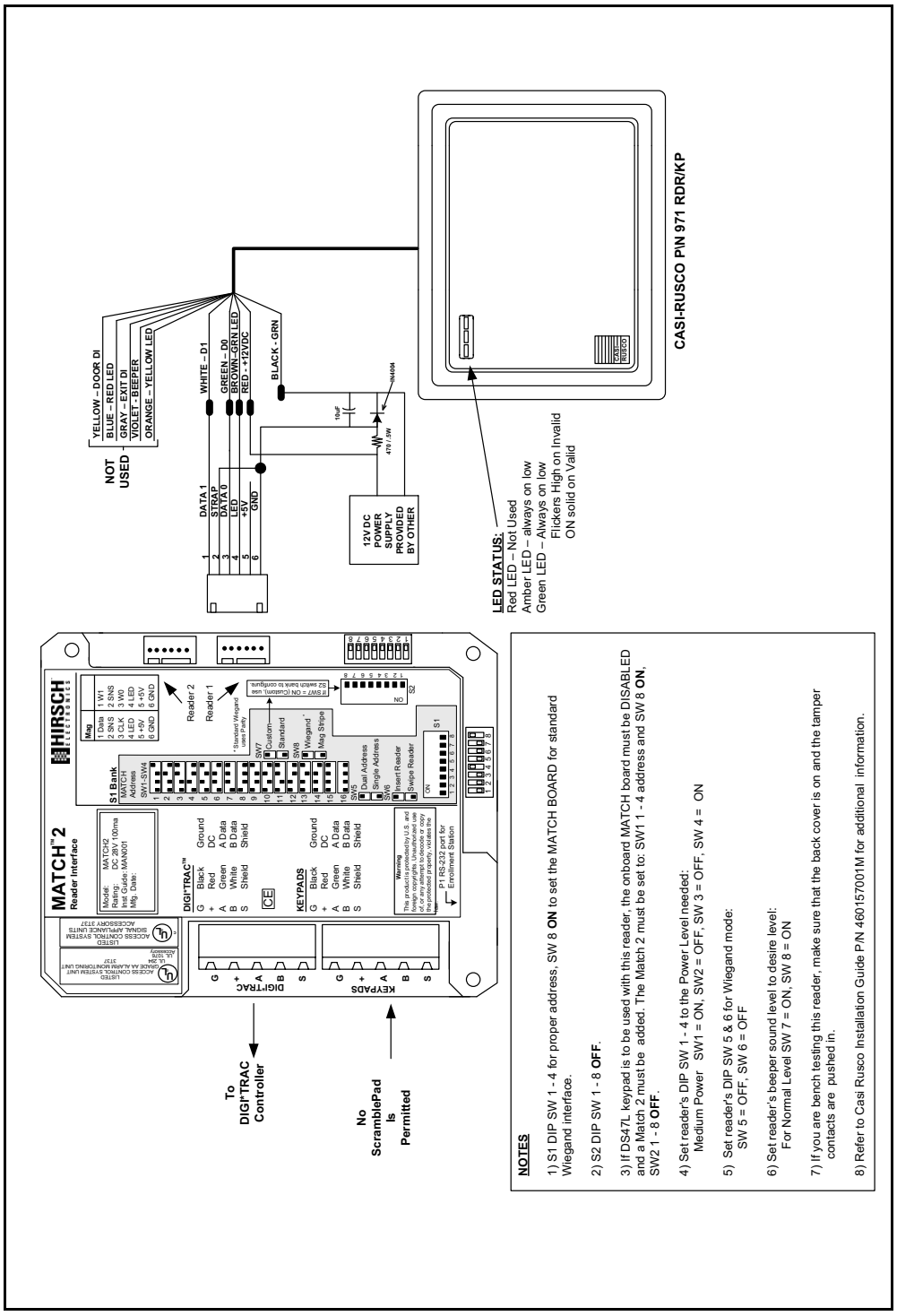
Casi-Rusco 940 Prox Perfect Reader

This diagram shows the wiring for the Casi-Rusco 940 Prox Perfect Reader.



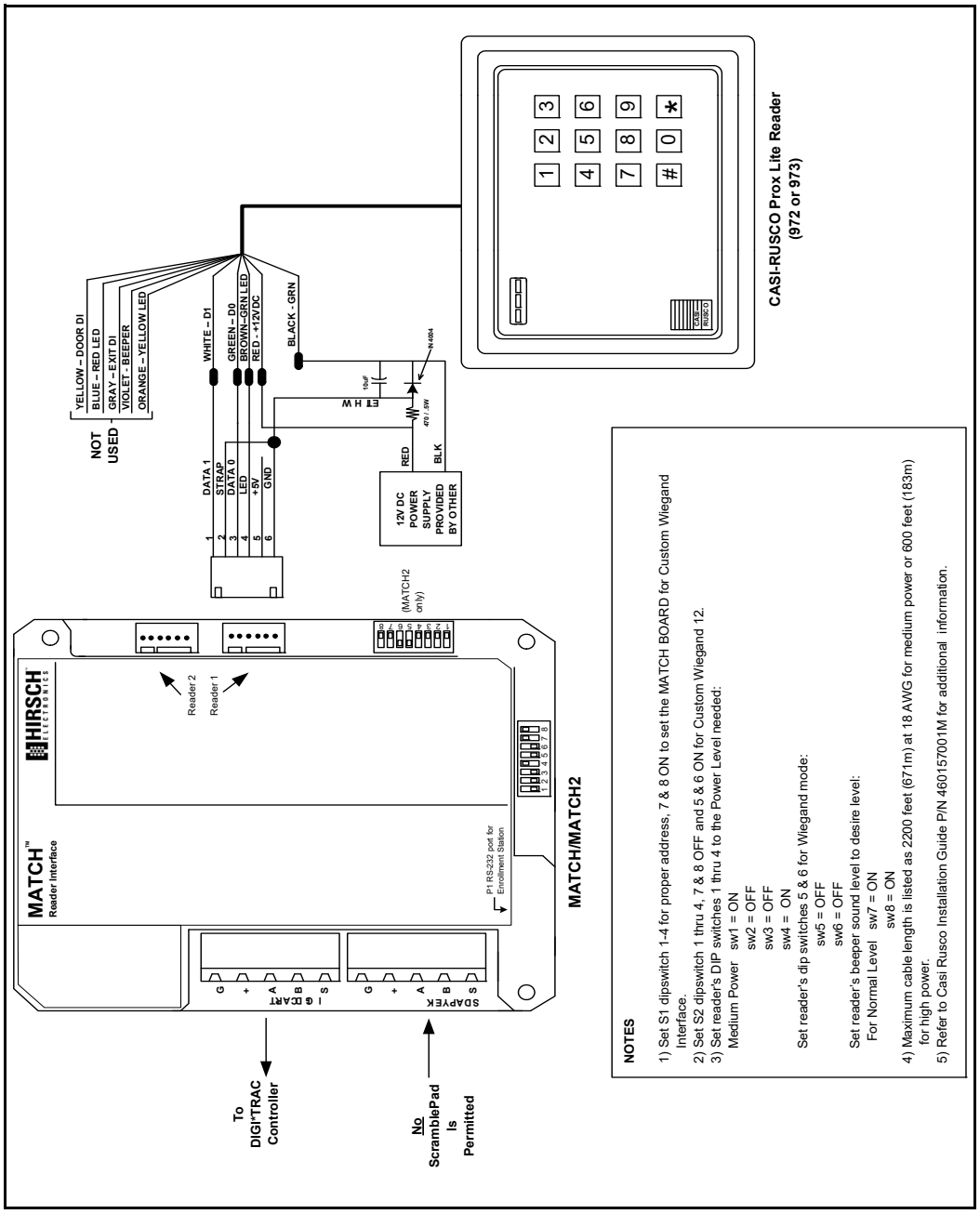
Casi-Rusco 971 Prox Reader

This diagram shows wiring for the Casi-Rusco 971 Prox Reader.



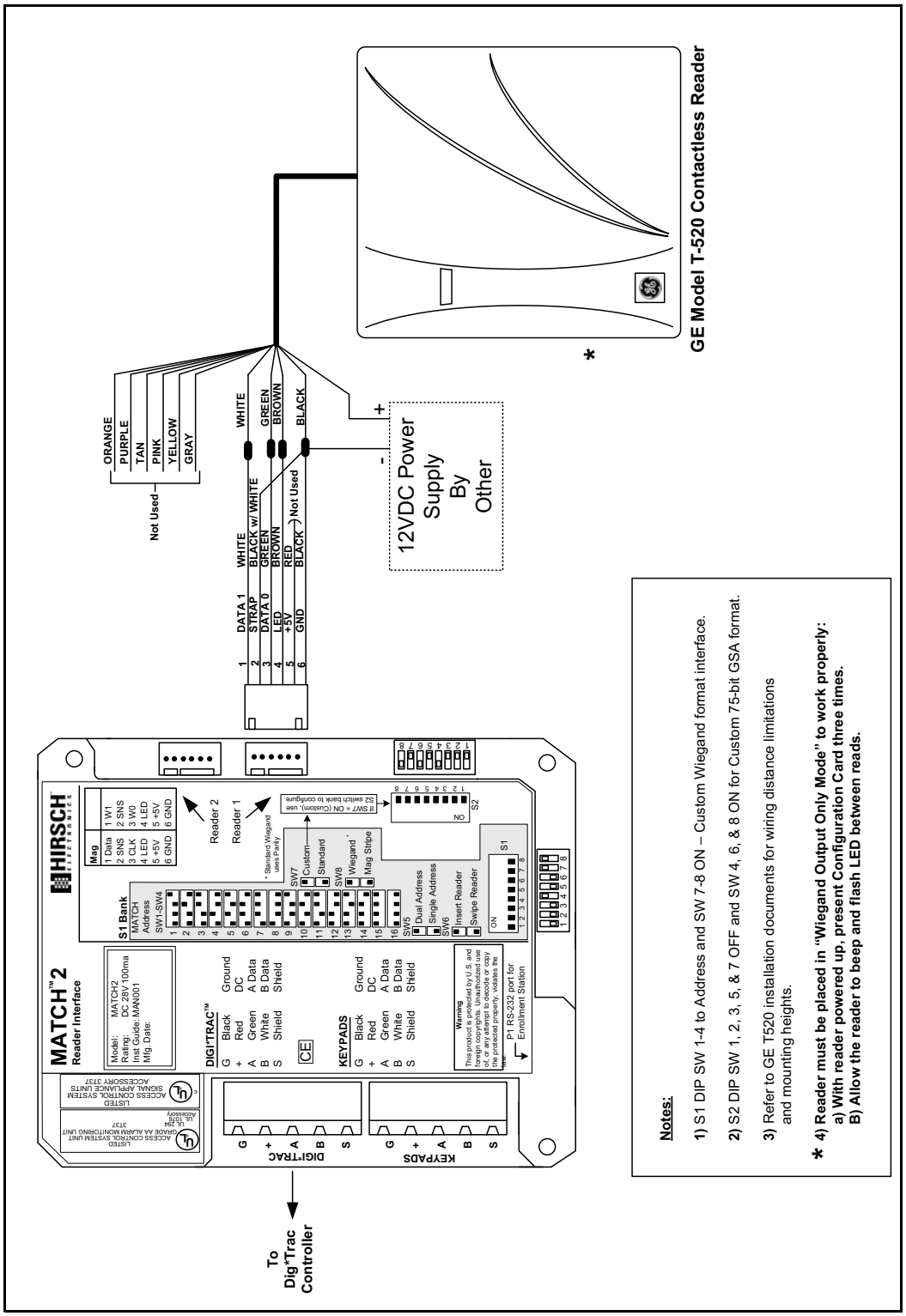
Casi-Rusco 972 and 973 Prox Lite Reader

This diagram shows wiring for the Casi-Rusco 972 and 973 Prox Lite Readers.



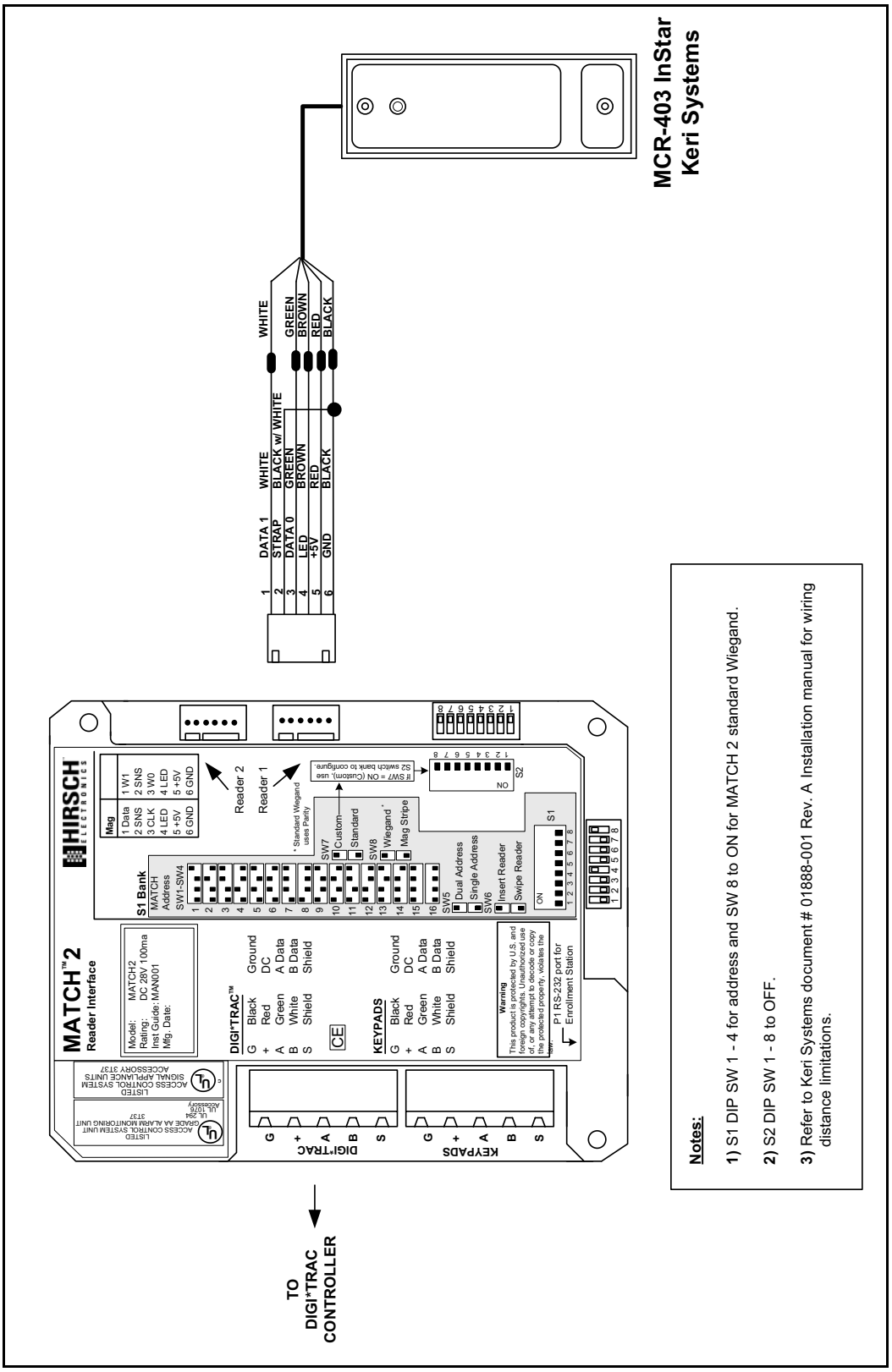
GE Contactless Reader

This diagram shows wiring for the GE model T-520 Contactless Reader.



Keri Systems InStar Prox Reader

This diagram shows wiring for the MCR-403 InStar Prox Reader from Keri Systems.



Notes:

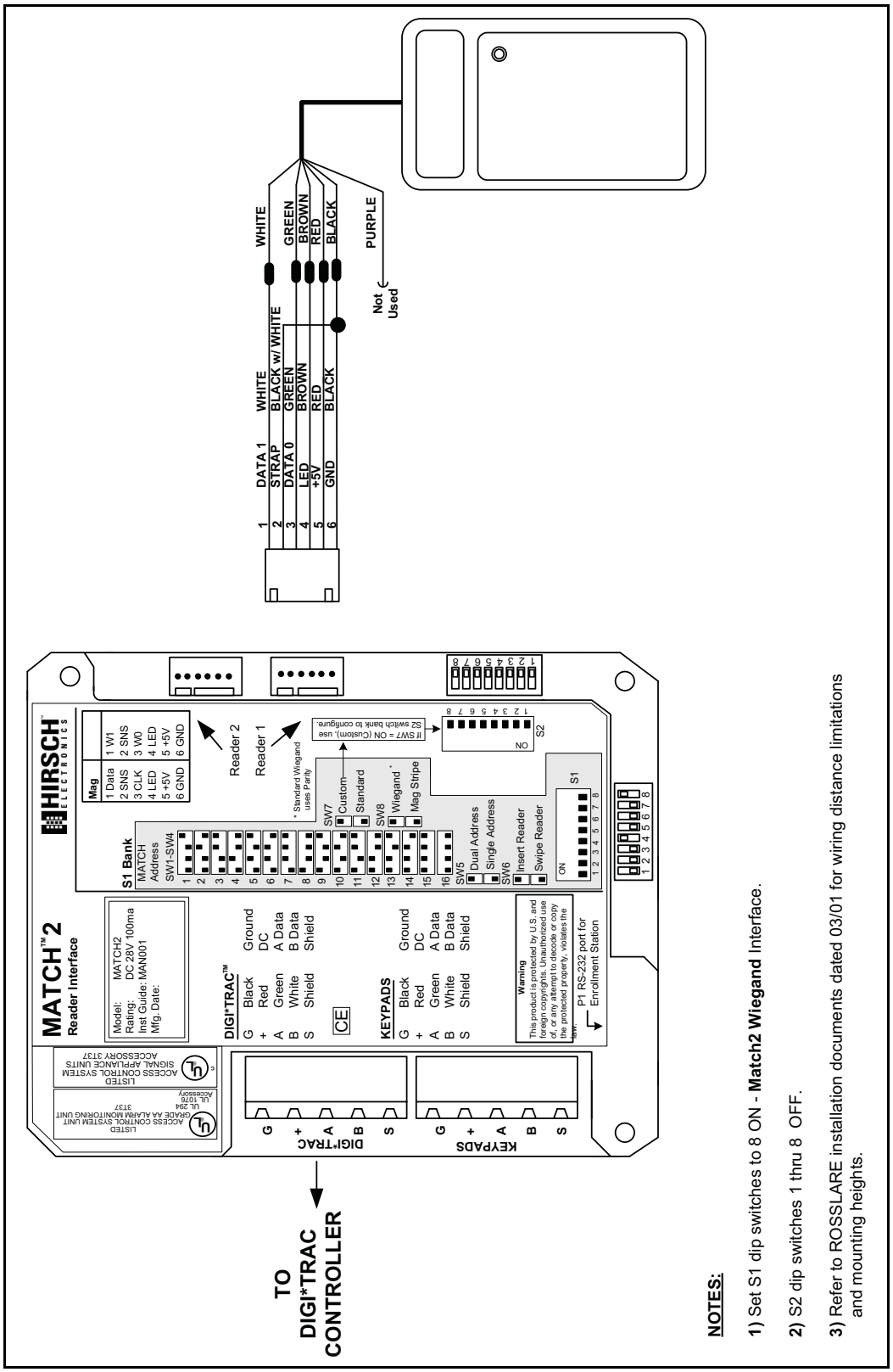
1) S1 DIP SW 1 - 4 for address and SW 8 to ON for MATCH 2 standard Wiegand.

2) S2 DIP SW 1 - 8 to OFF.

3) Refer to Keri Systems document # 01888-001 Rev. A Installation manual for wiring distance limitations.

Rosslare Prox Reader

This diagram shows wiring for the Rosslare AY-K12B 26-Bit Prox Reader.



NOTES:

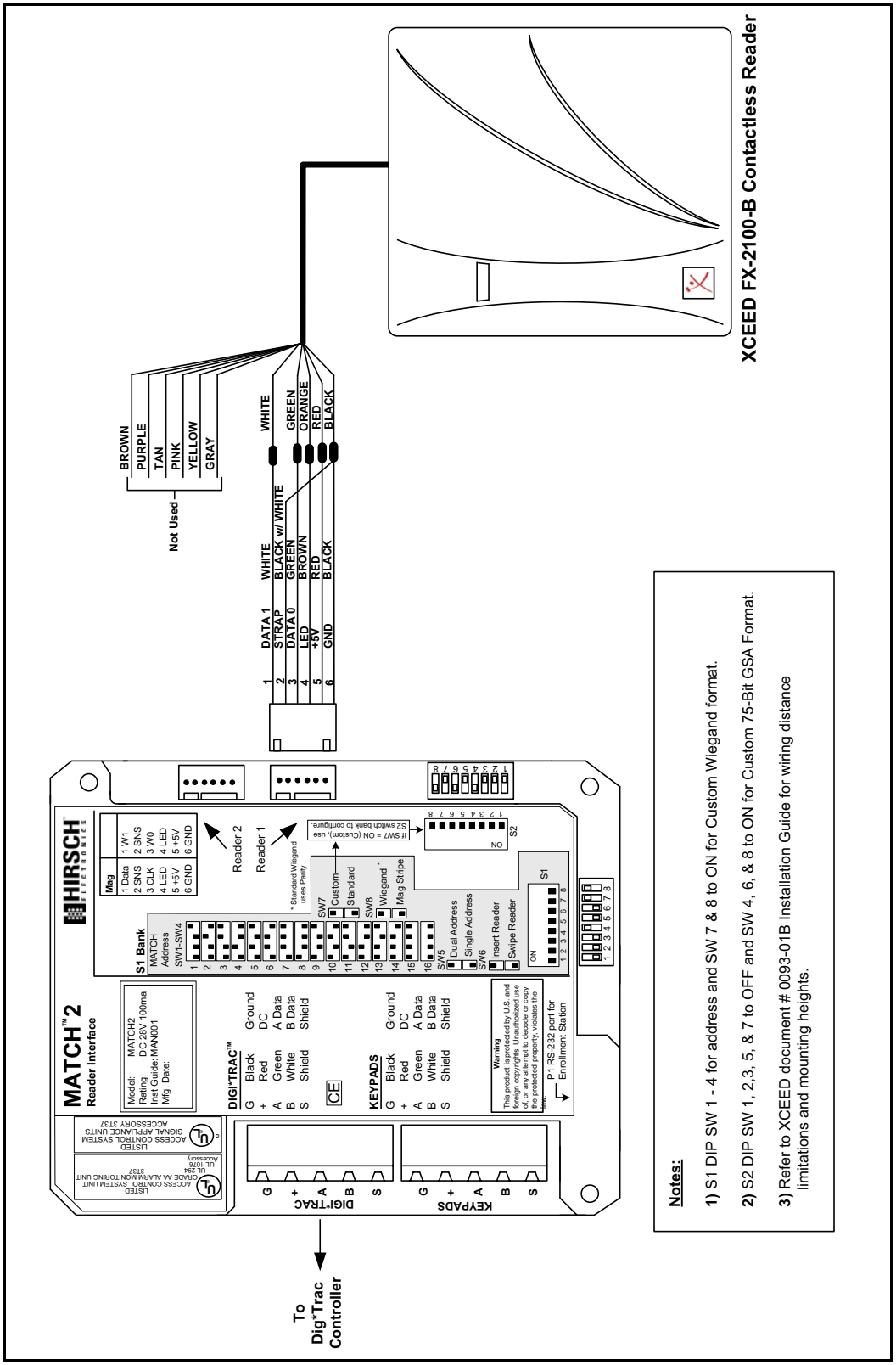
1) Set S1 dip switches to 8 ON - **Match2 Wiegand** Interface.

2) S2 dip switches 1 thru 8 OFF.

3) Refer to ROSSLARE installation documents dated 03/01 for wiring distance limitations and mounting heights.

XCEED Transition Series Multi-Technology Reader

This diagram shows wiring for the XCEED Transition Series XF-2100-B multi-technology reader.



Wiegand Readers

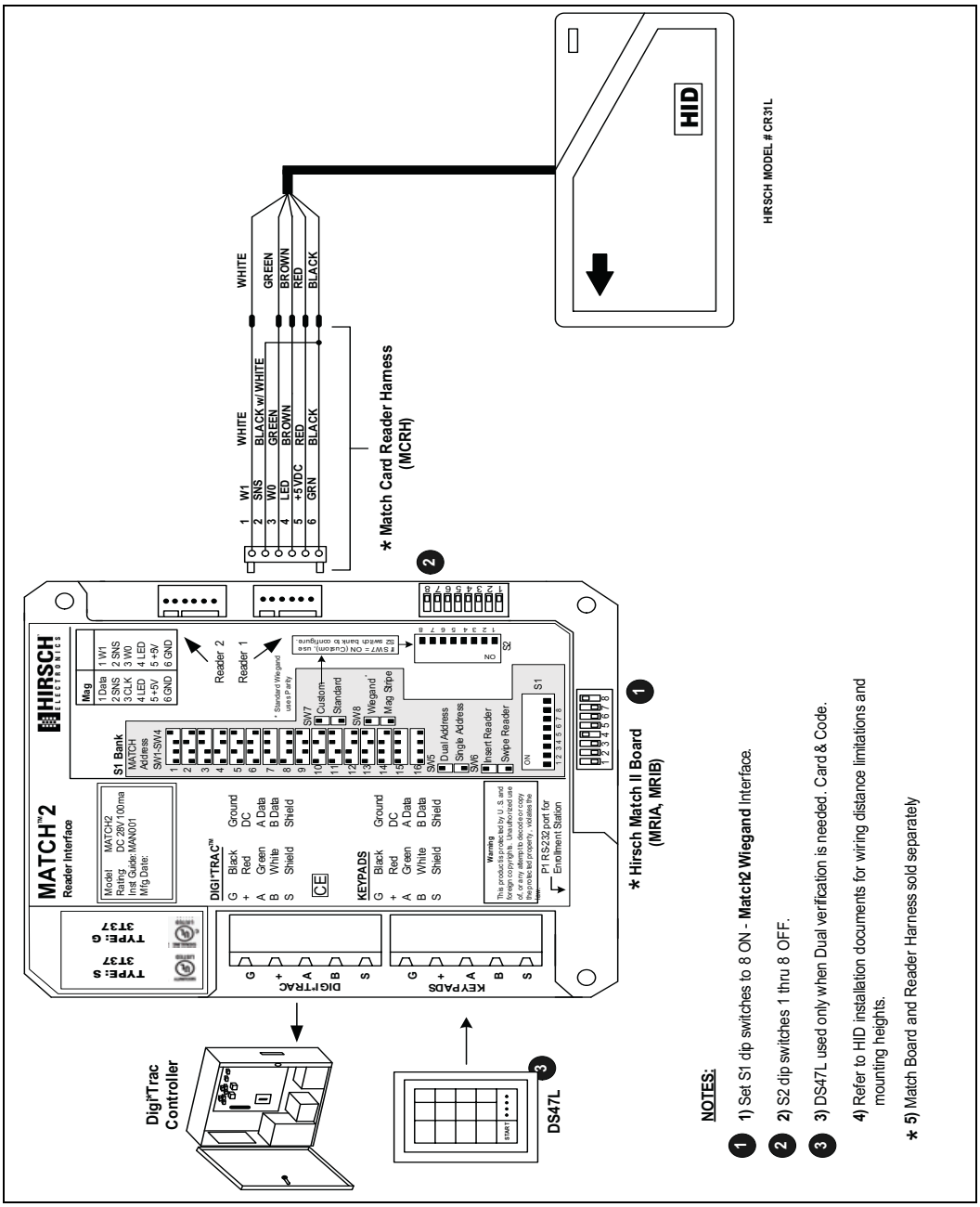
This section describes the MATCH wiring and settings information required to connect Hirsch-supported Wiegand card readers. Diagrams for the following readers are shown:

HID Wiegand Readers

This section gives diagrams for the following HID Wiegand readers:

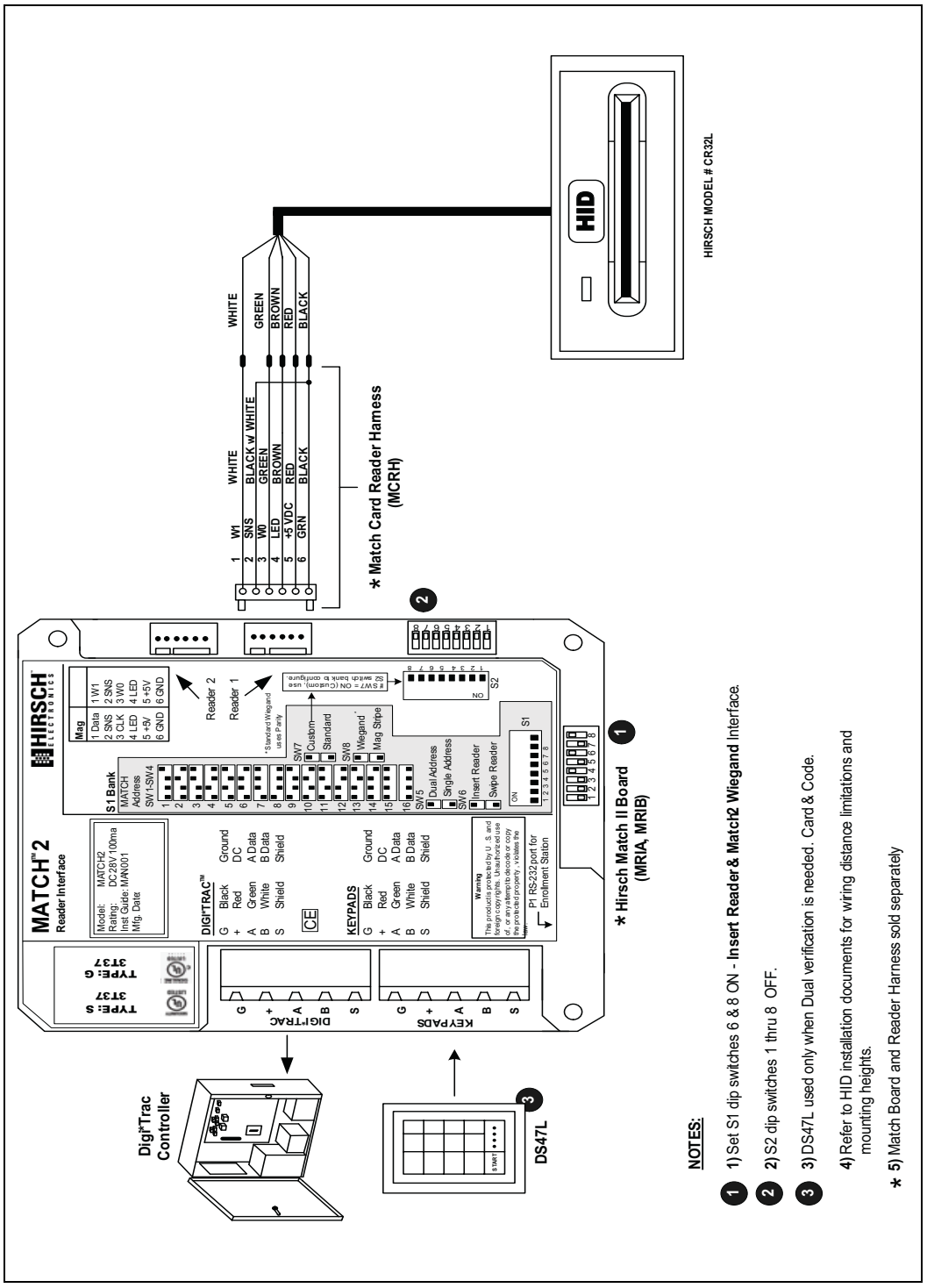
Wiegand Swipe Reader

This diagram shows wiring for the Wiegand Swipe Reader model CR31L.



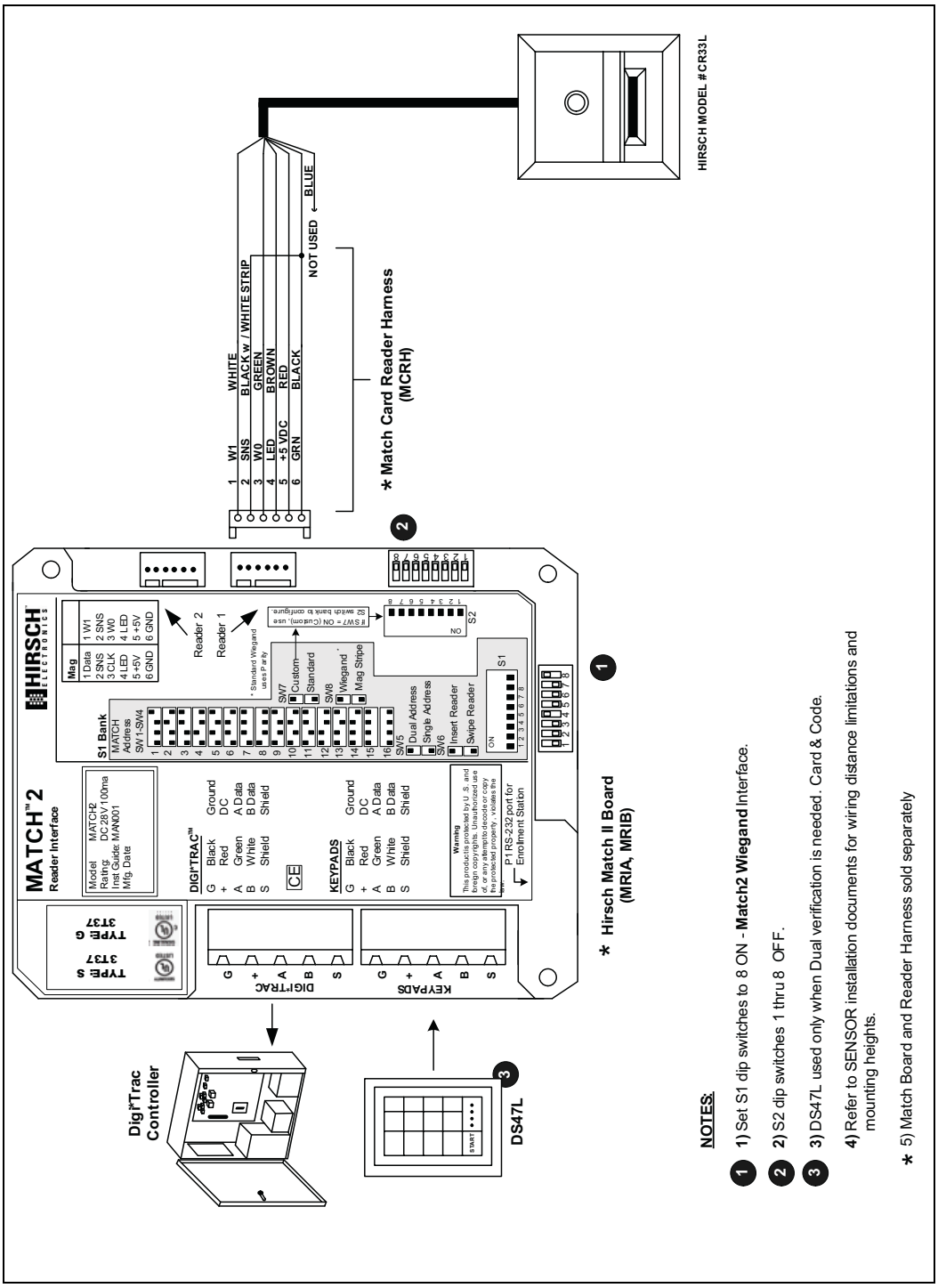
Wiegand Insertion Reader

This diagram shows wiring for the Wiegand Insertion Reader model CR32L.



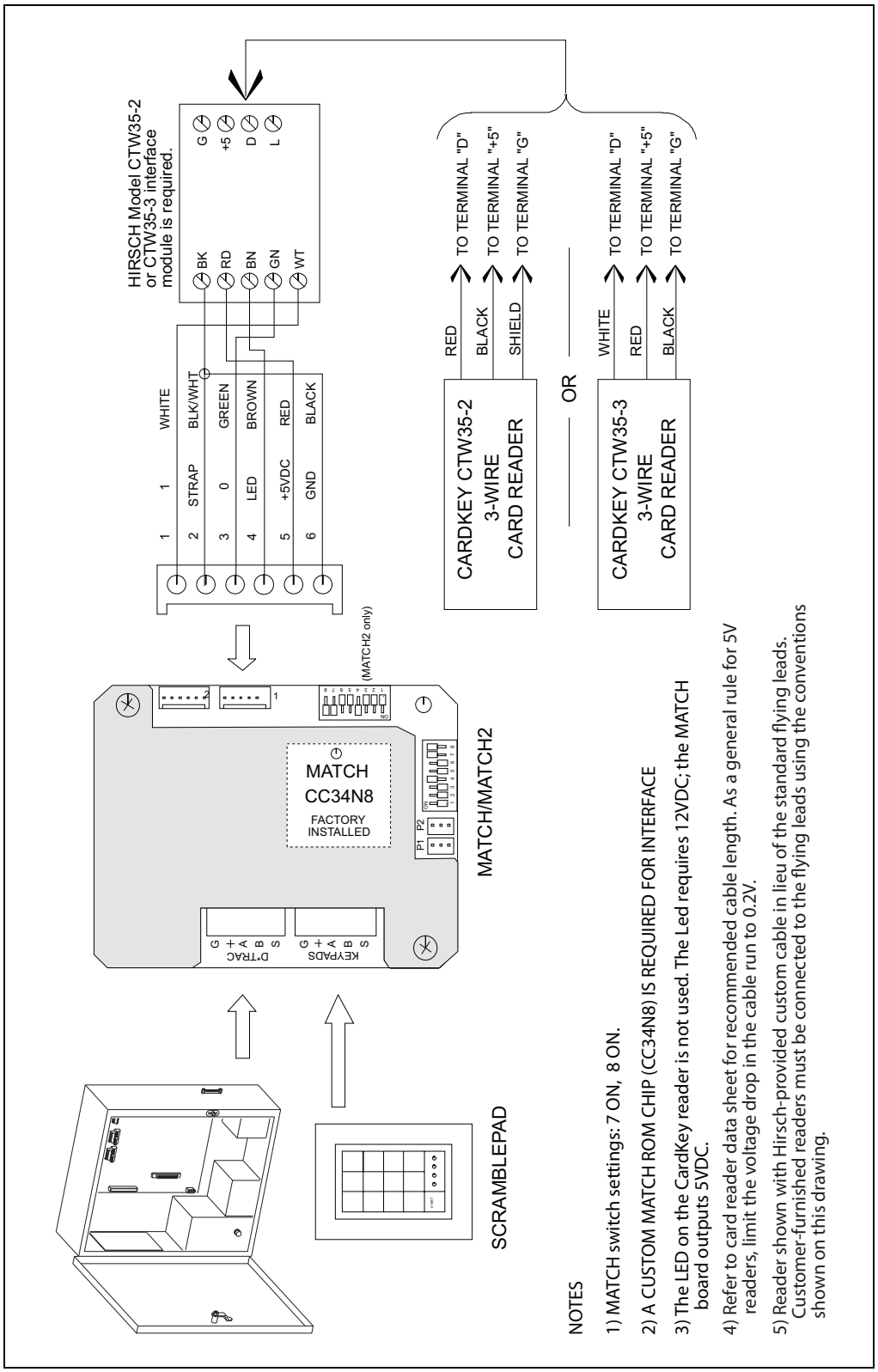
Wiegand Key Swipe Reader

This diagram shows wiring for the Wiegand Key Swipe Reader model CR33L.



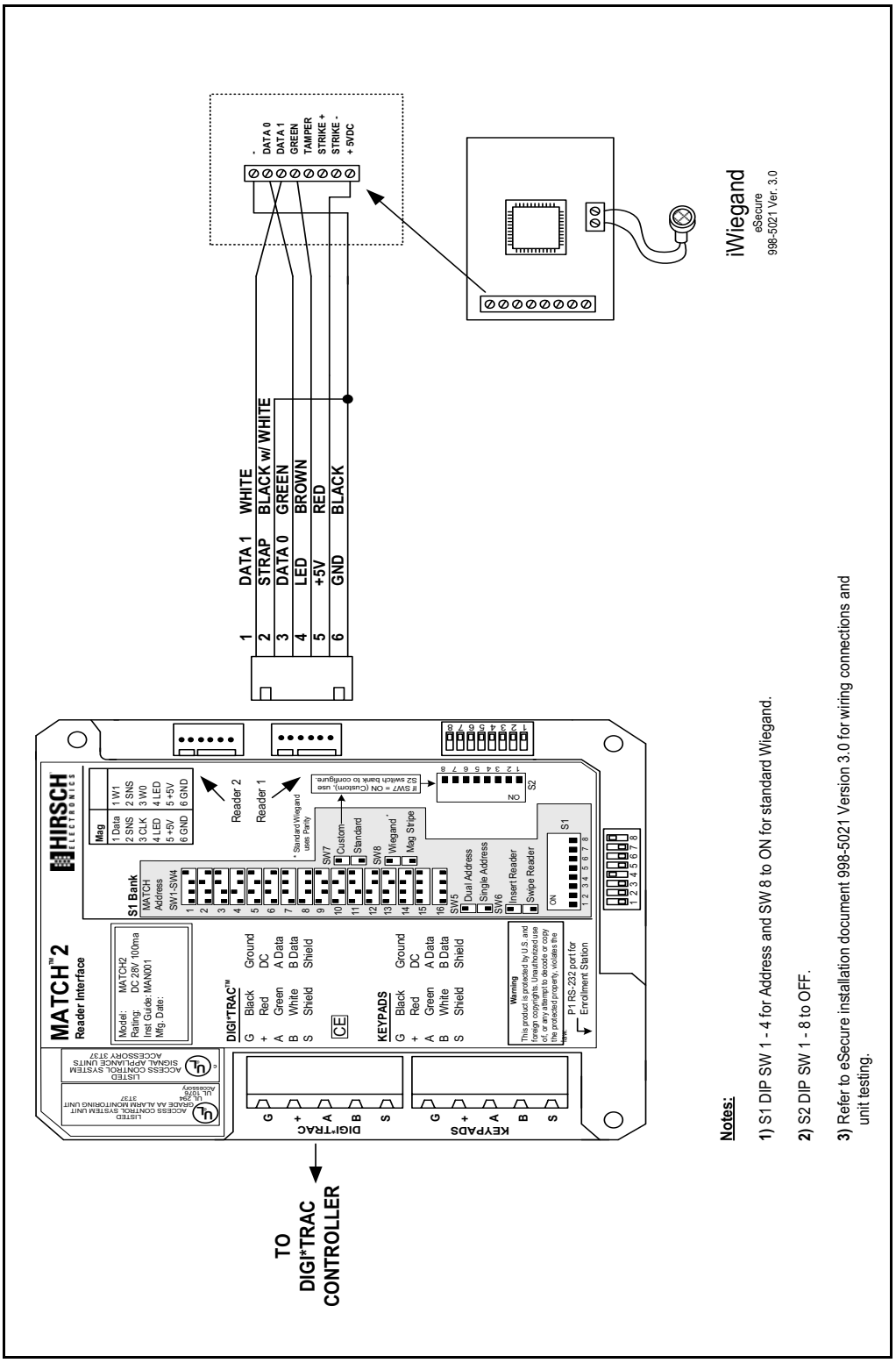
CardKey to Wiegand Card Reader Interface Module

This diagram shows wiring for the CardKey to Wiegand Card Reader Interface Module, model CTW35.



eSecure iWiegand Reader

This diagram shows wiring for the eSecure iWiegand Reader.



Barcode Swipe Card Readers

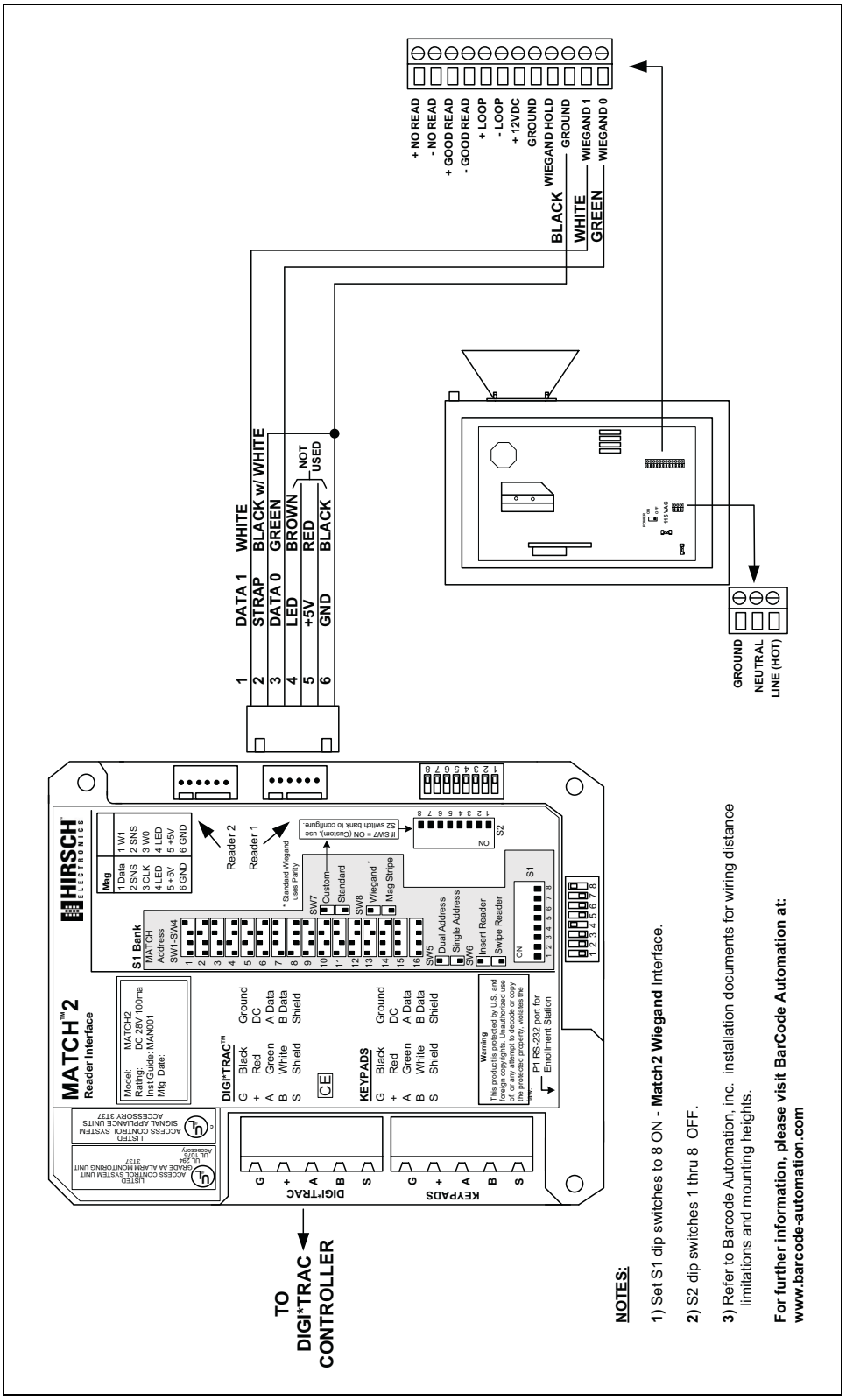
This section describes the MATCH wiring and settings information required to connect Hirsch-supported barcode swipe card readers. Wiring diagrams for the following barcode swipe card readers are shown:

Barcode Automation Readers

This section gives wiring diagrams for Barcode Automation readers, and includes the following models:

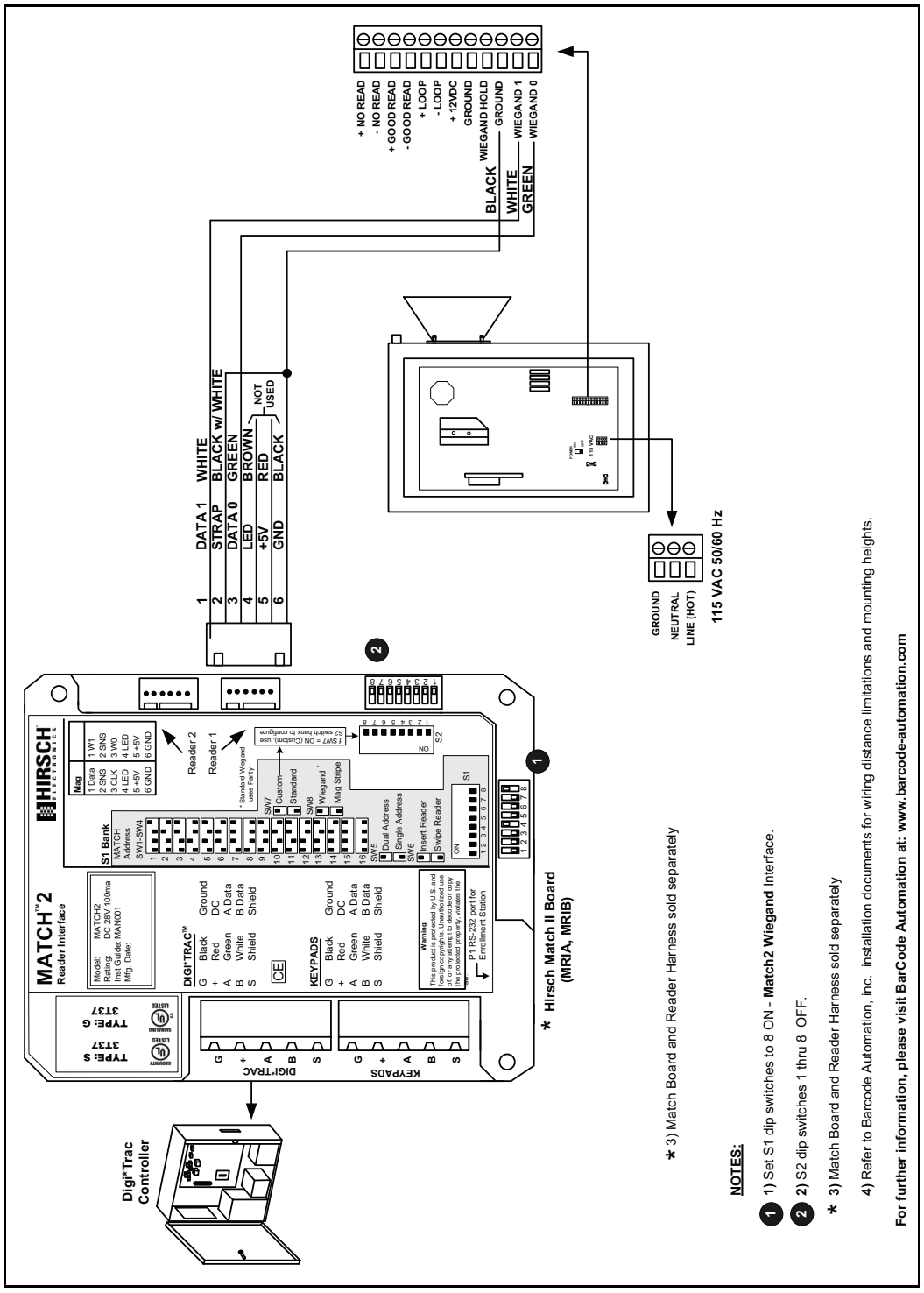
BAI Barcode Reader

This diagram shows wiring for the Barcode Automation BA-200 Barcode Reader.



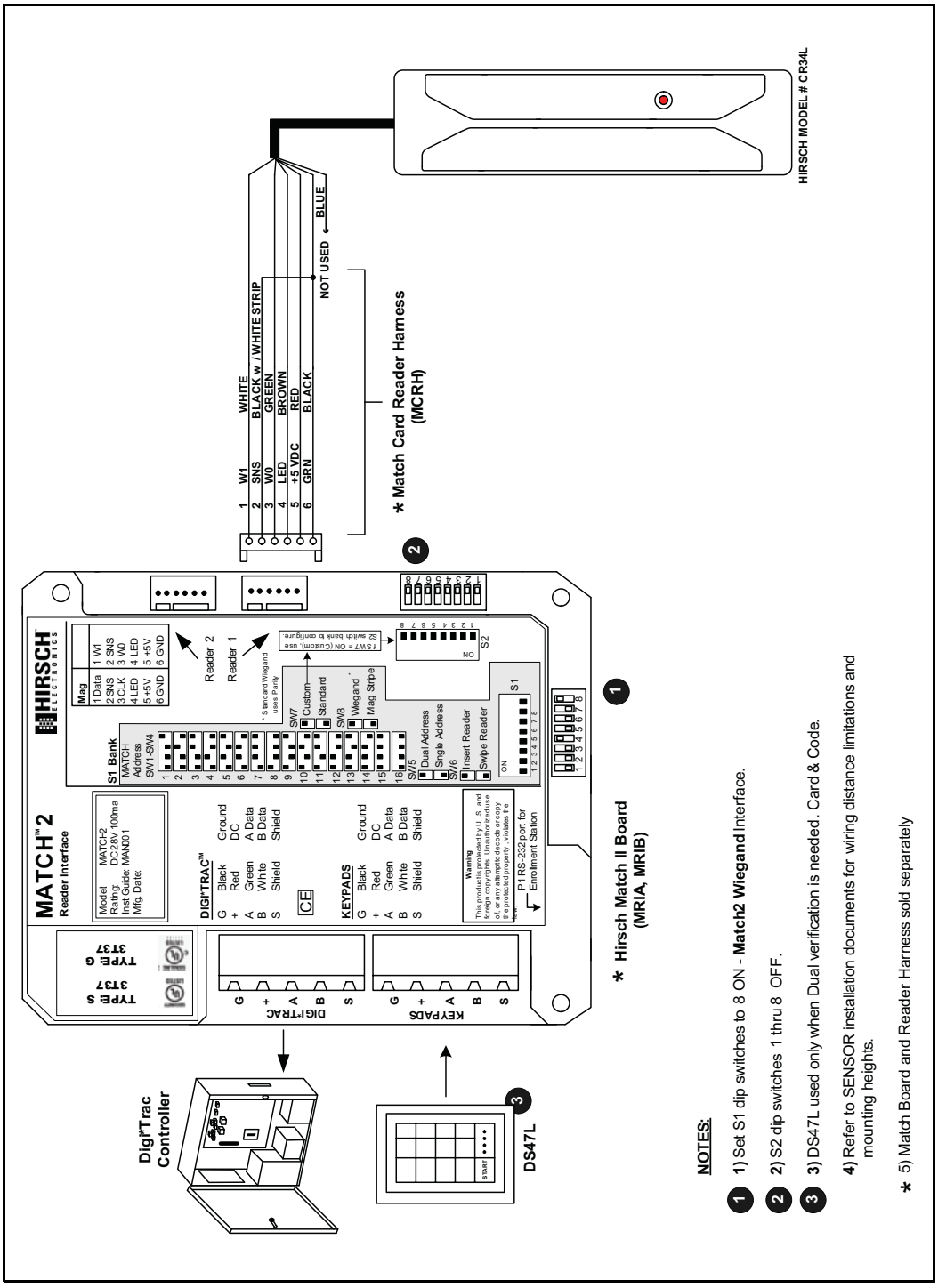
BAI Vehicle Barcode Reader

This diagram shows wiring for the CR-VBC model BAI Vehicle Barcode Reader.



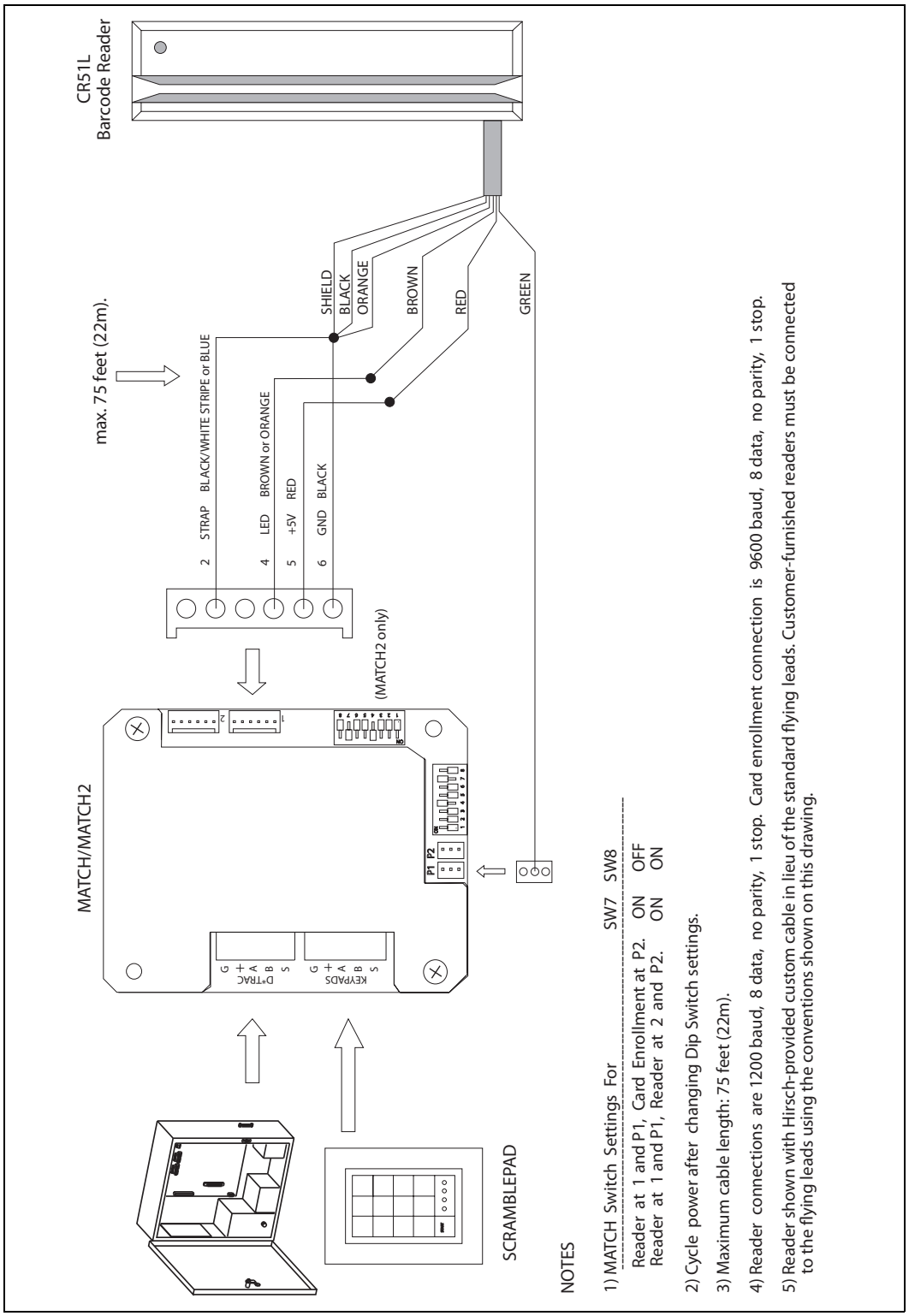
SENSOR Wiegand Turnstile Swipe Reader

This diagram shows wiring for the model CR34L SENSOR Wiegand Turnstile Swipe Reader.



CR51L Barcode Swipe Card Reader

This diagram shows wiring for the CR51L Bar Code Swipe Card Reader.

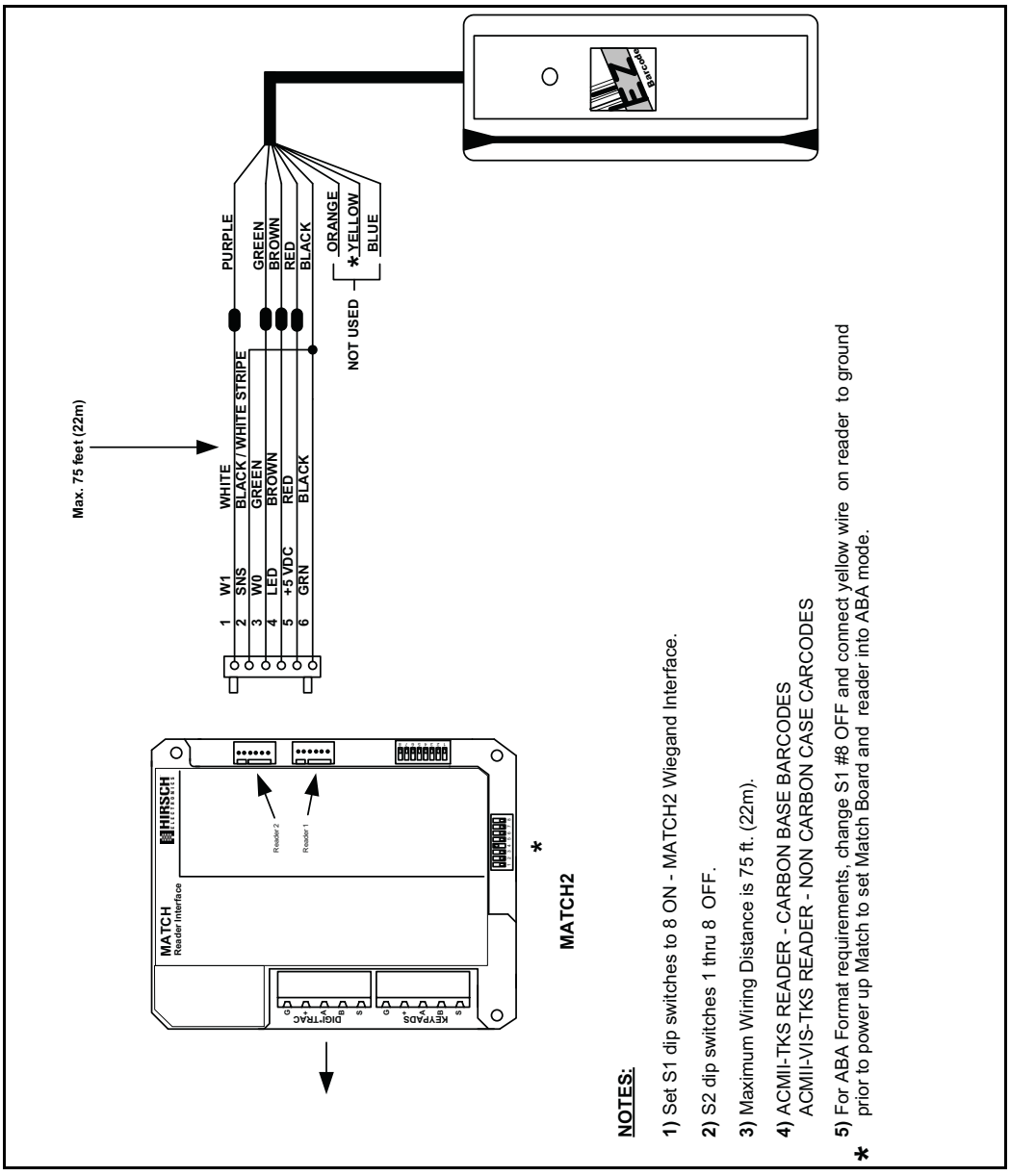


Time Keeping Systems Barcode Readers

This section gives wiring diagrams for the following Time Keeping Systems barcode readers:

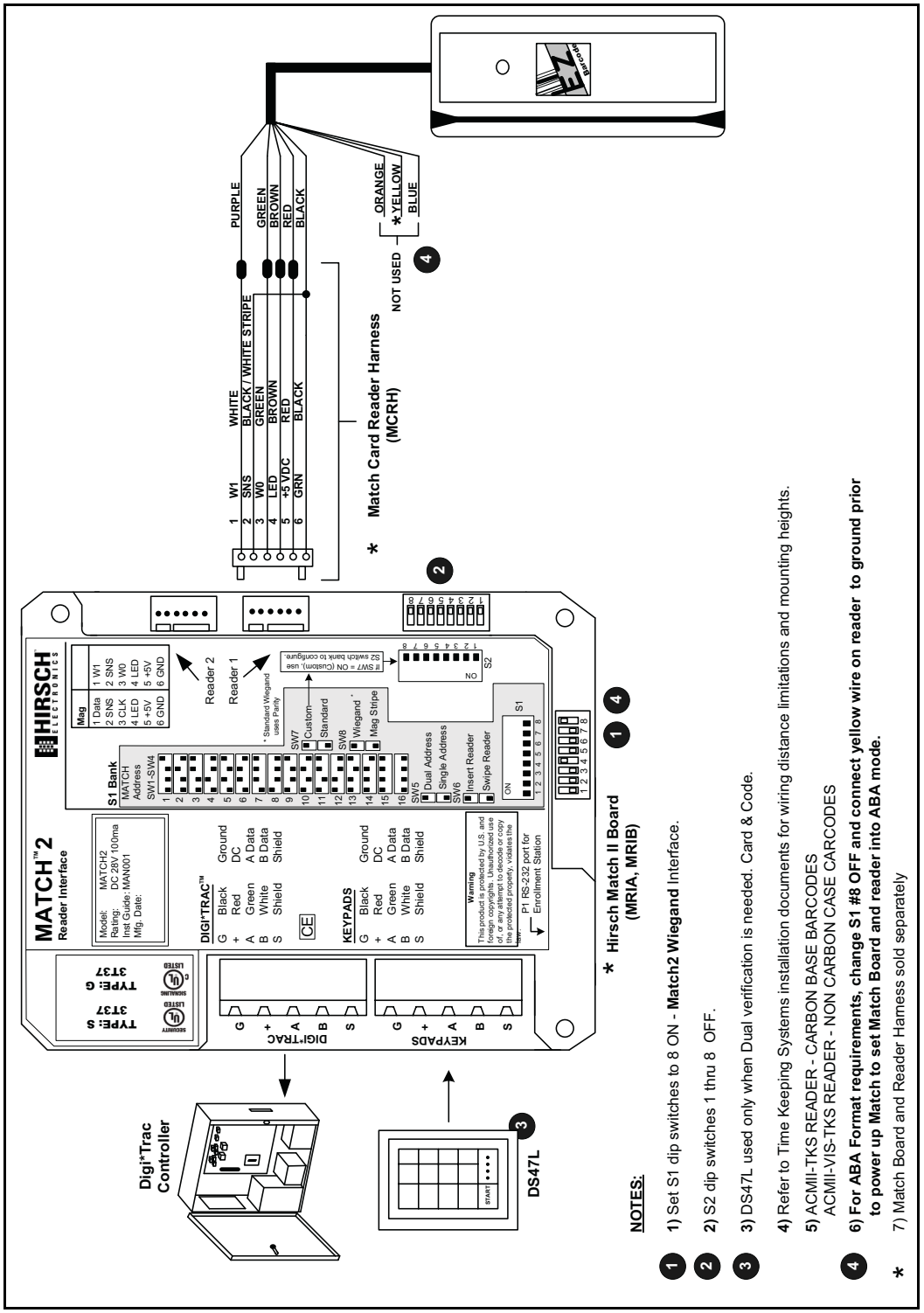
Bar Code Swipe Card Reader

This diagram shows wiring for the CR51VL Bar Code Swipe Card Reader.



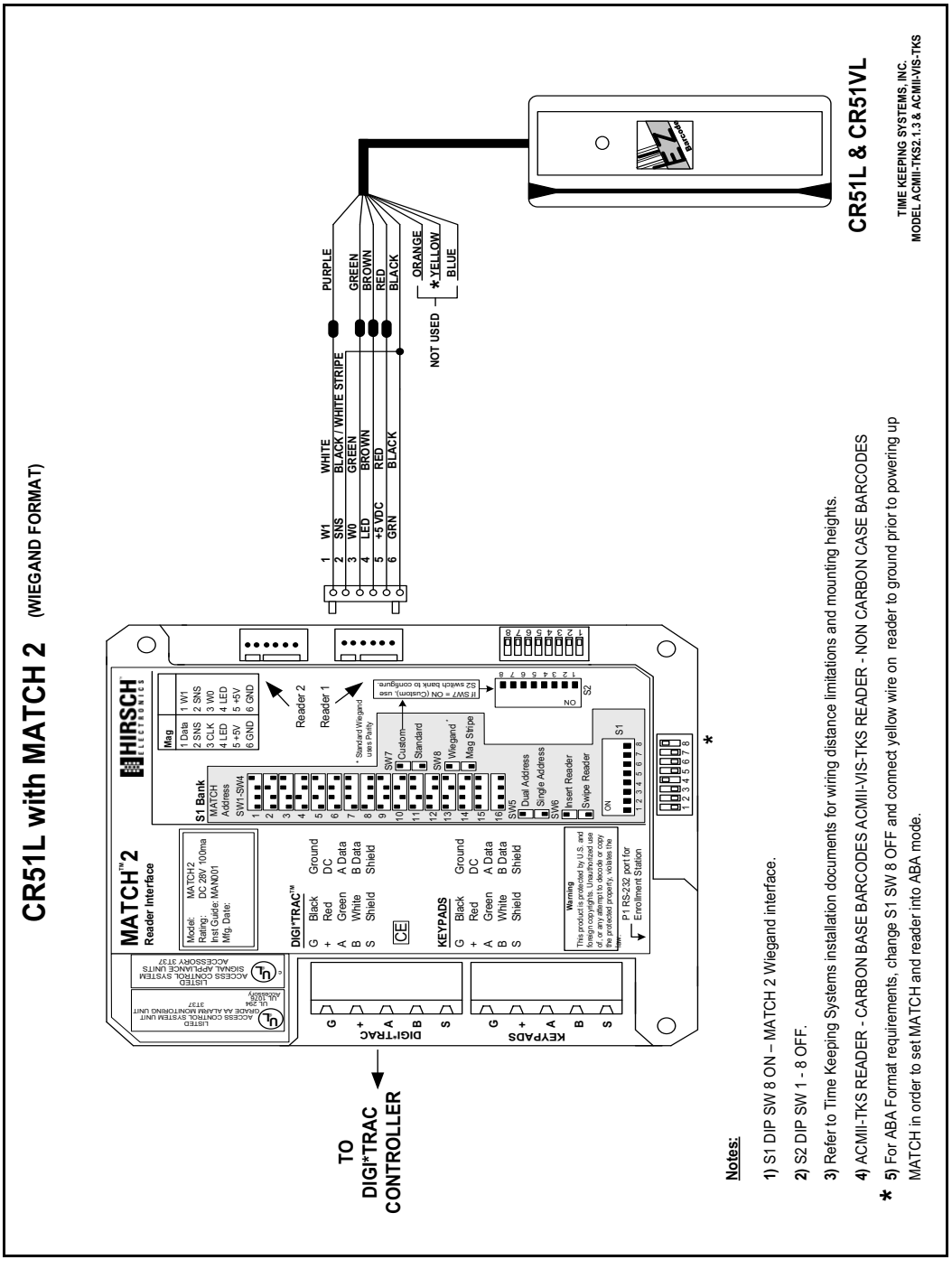
Barcode Reader (CR51L and CR51LV)

This diagram shows wiring for the Time Keeping Barcode Reader models CR51L and CR51LV.



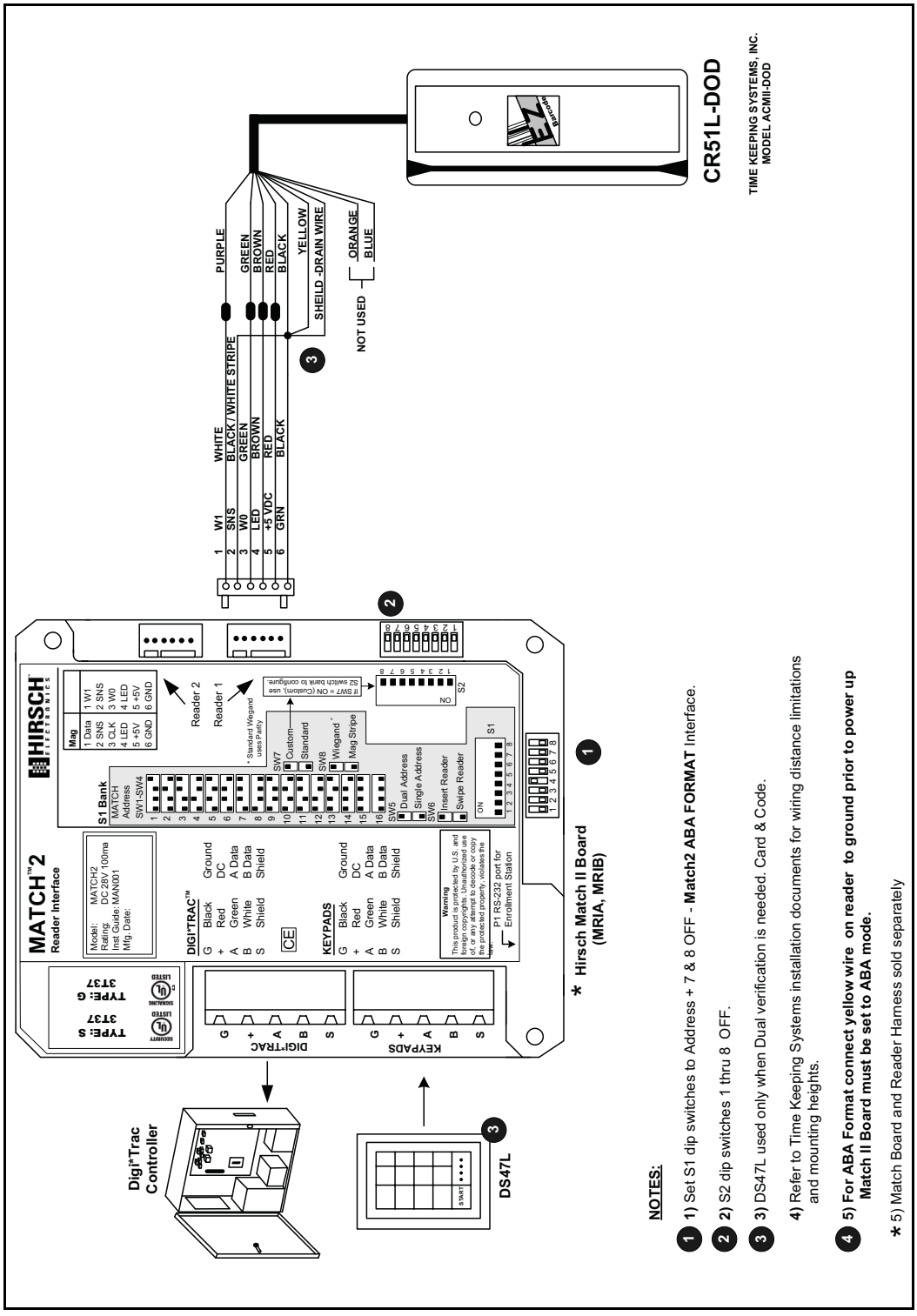
Bar Code Swipe Card Reader with MATCH2 for Wiegand

This diagram shows wiring for the CR51L/CR51VL Bar Code Swipe Card Reader with MATCH2 for Wiegand.



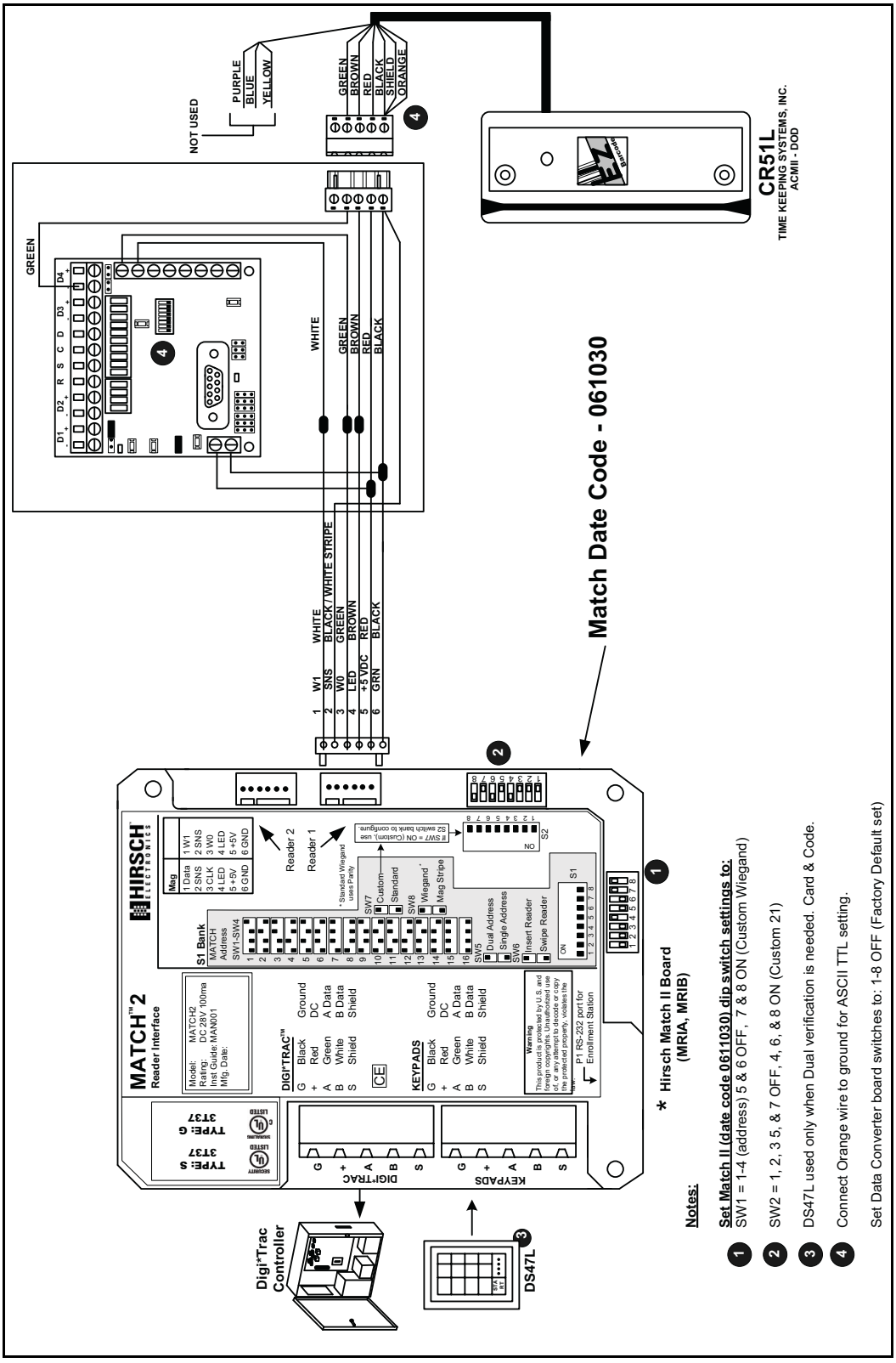
Barcode Reader DOD Model

This diagram shows wiring for the CR51L-DOD model Time Keeping Barcode Reader to MATCH2.



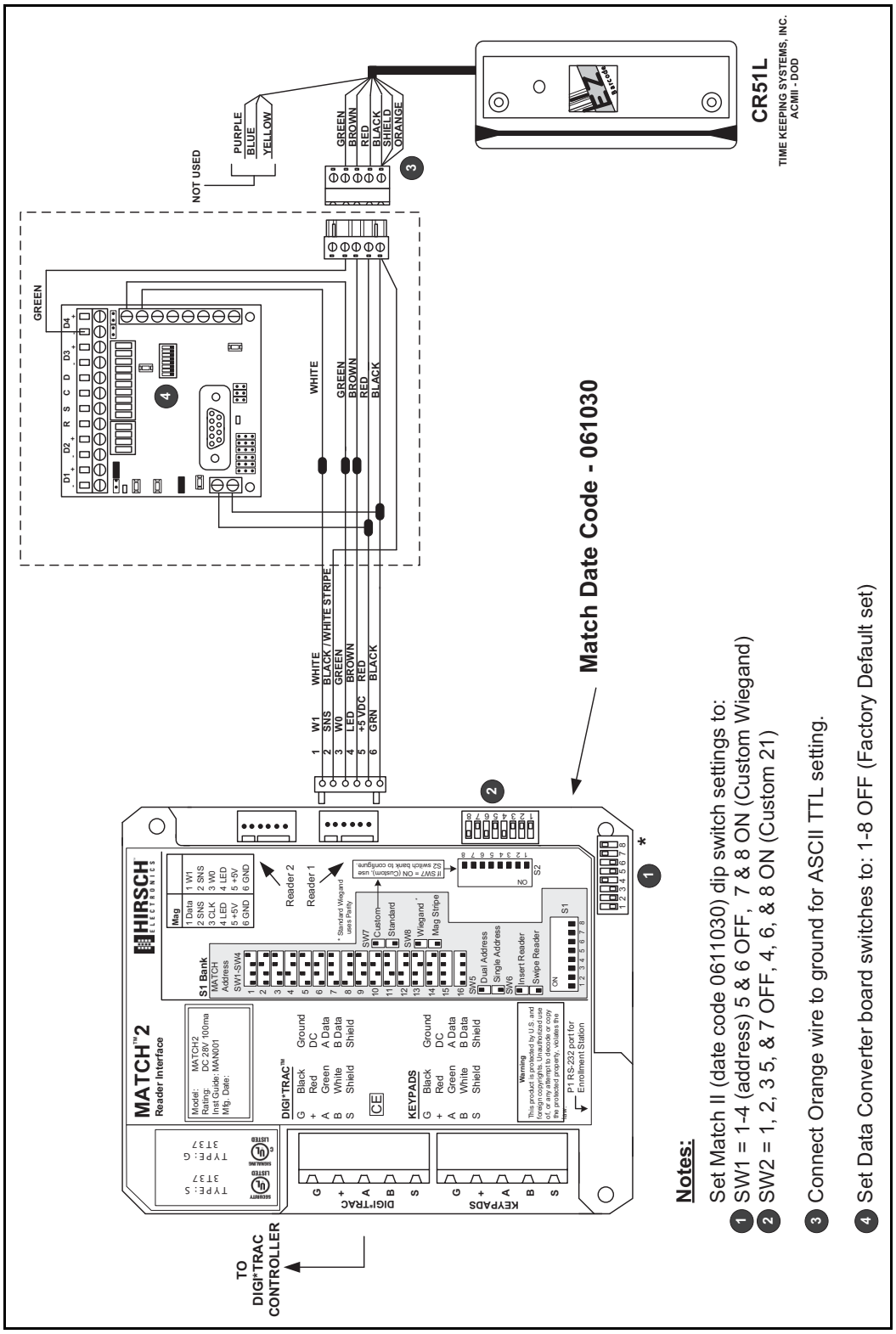
UT Barcode Data Converter

This diagram shows wiring for the CR-51L model with UT Barcode Data Converter (TTL to Wiegand Custom 21).



DOD TTL Barcode Reader

This diagram shows wiring for the CR-51L model DOD TTL Barcode Reader.



Biometric Readers

This section describes the MATCH2 wiring and settings for connecting Hirsch-supported biometric readers. These readers include:

Fingerprint Readers

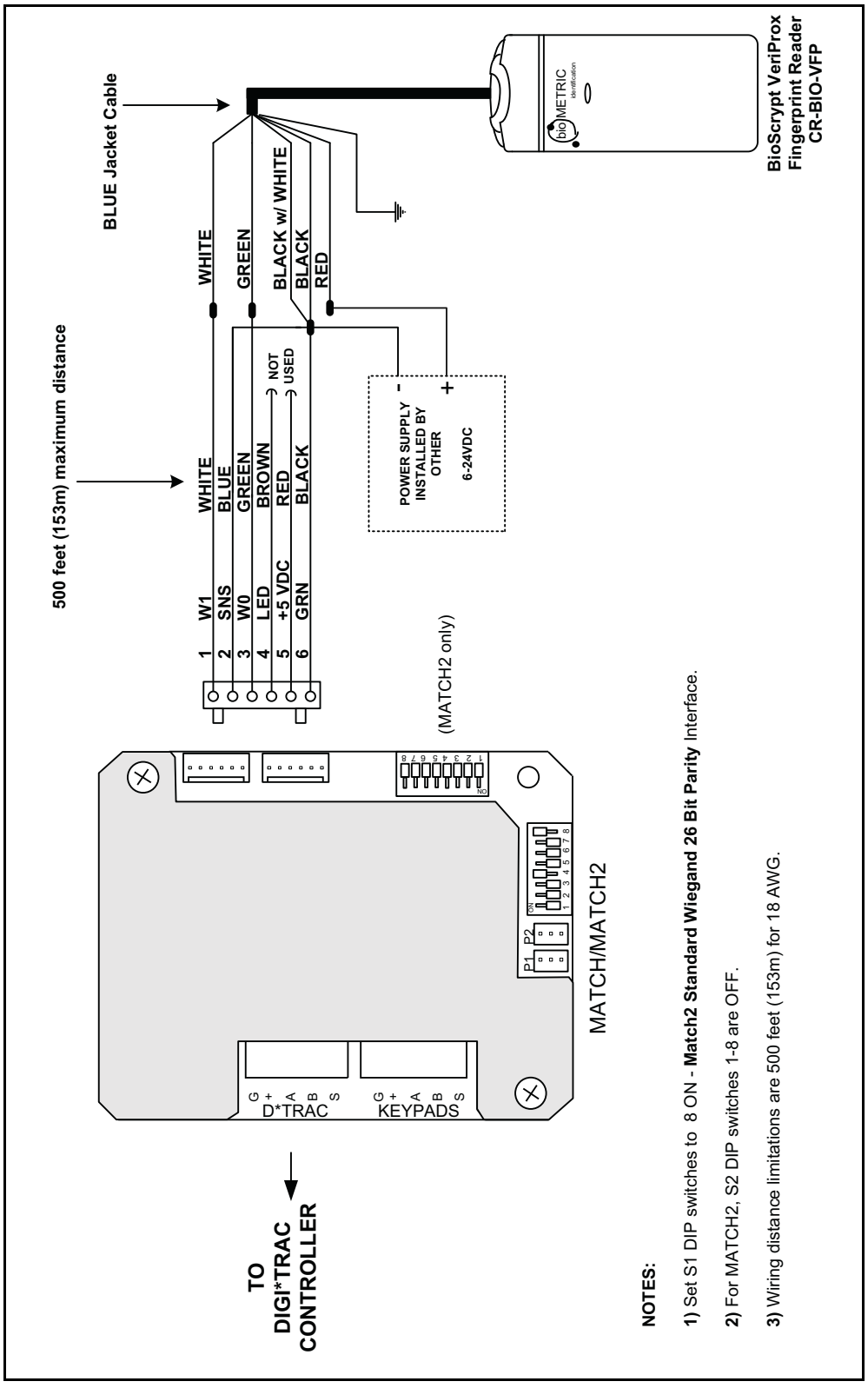
This section gives wiring diagrams for integrating commonly used fingerprint readers into the Hirsch DIGI*TRAC system. The following readers are diagrammed:

BioScrypt Fingerprint Readers

This section gives wiring diagrams and settings for the following BioScrypt Fingerprint readers:

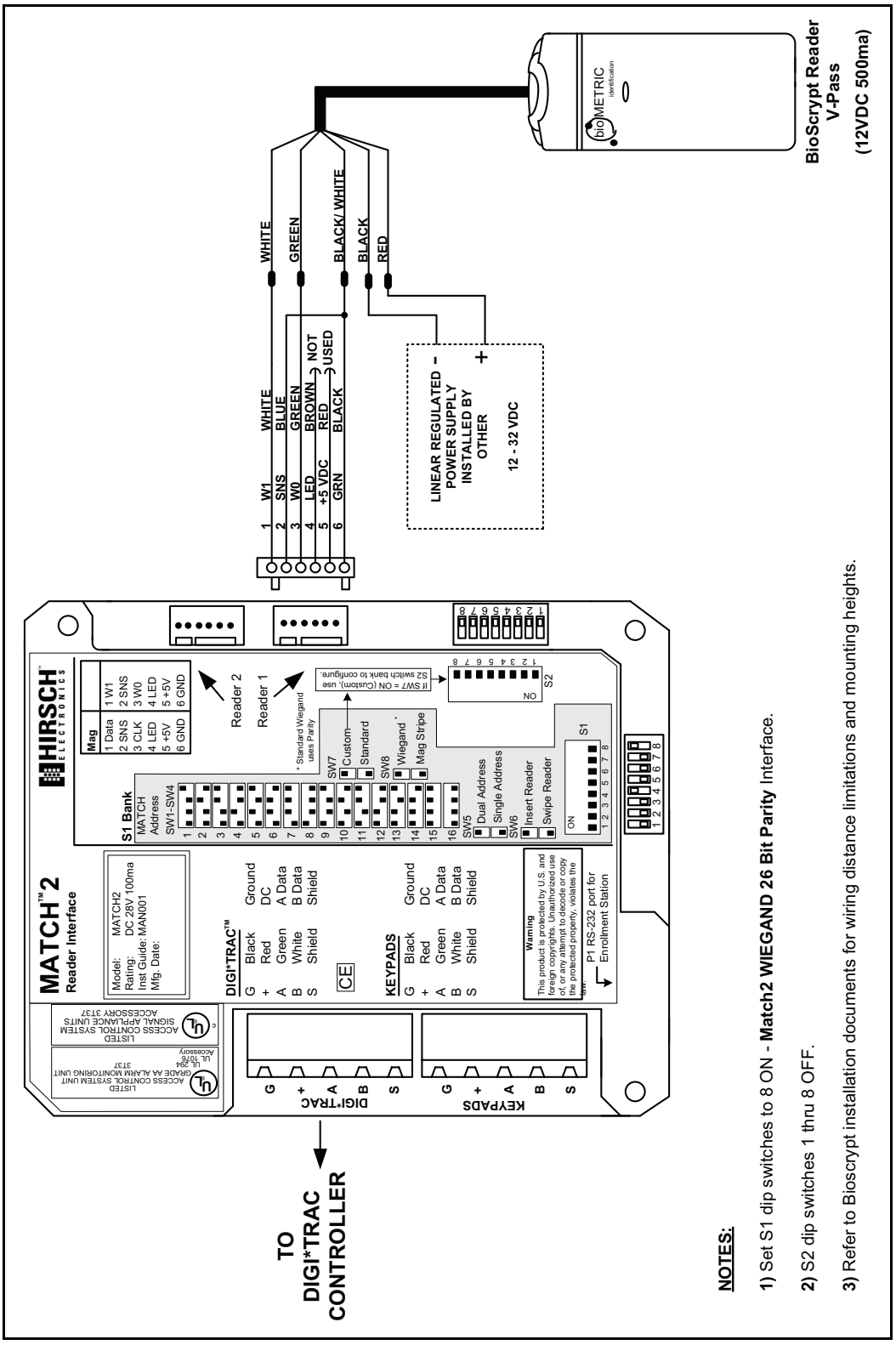
BioScrypt VeriProx Fingerprint Proximity Reader

This diagram shows wiring for the CR-BIO-VFP model BioScrypt VeriProx Fingerprint Proximity Reader.



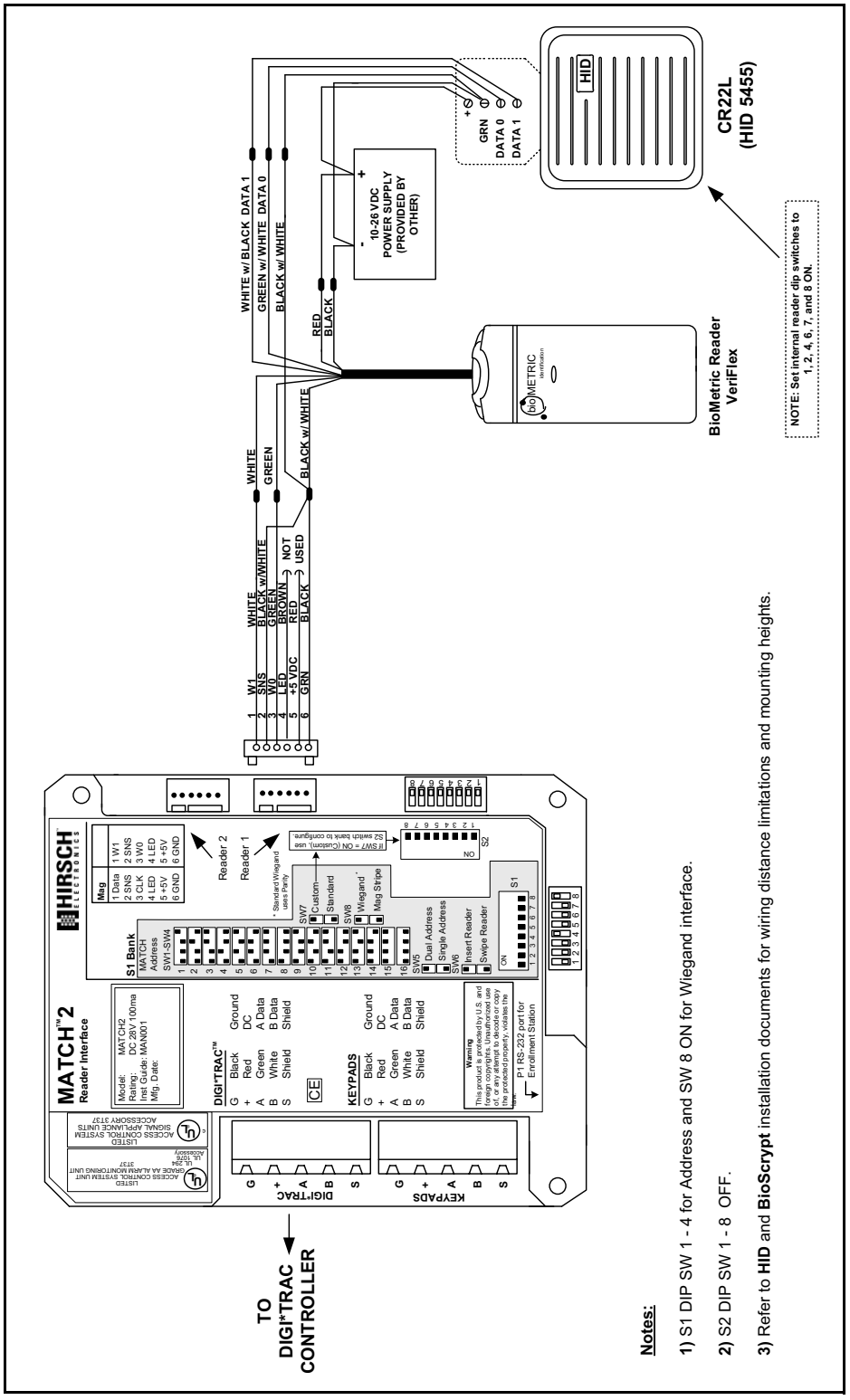
BioScrypt V-Pass Fingerprint Proximity Reader

This diagram shows wiring for the CR-BIO-VP model BioScrypt V-Pass Fingerprint Proximity Reader.



BioScrypt Veriflex with ScramblePad

This diagram shows wiring and settings for the CR22L model—the BioScrypt Veriflex with a ScramblePad for use with a MATCH2.



Notes:

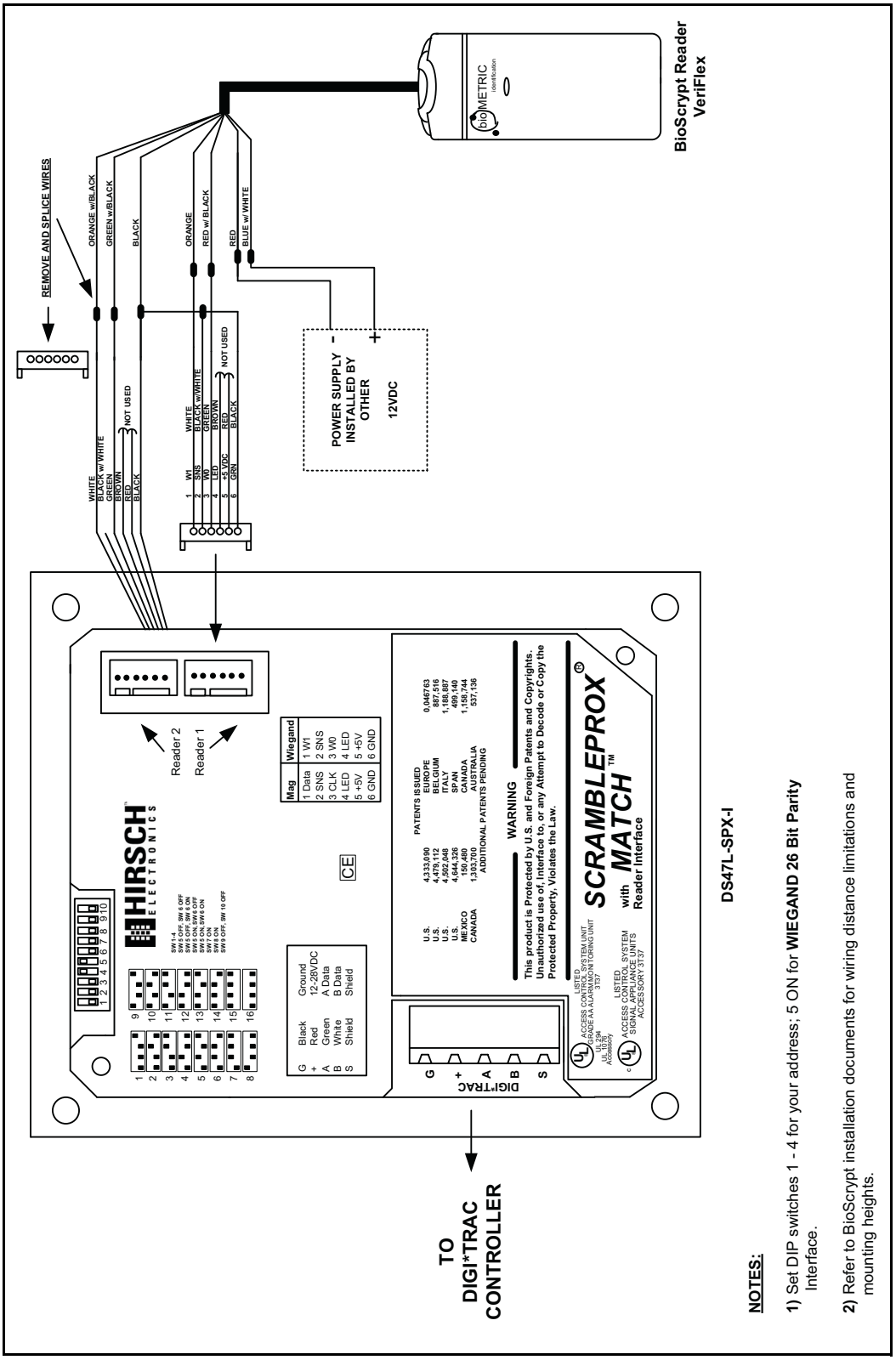
1) S1 DIP SW 1 - 4 for Address and SW 8 ON for Wiegand interface.

2) S2 DIP SW 1 - 8 OFF.

3) Refer to **HID** and **BioScrypt** installation documents for wiring distance limitations and mounting heights.

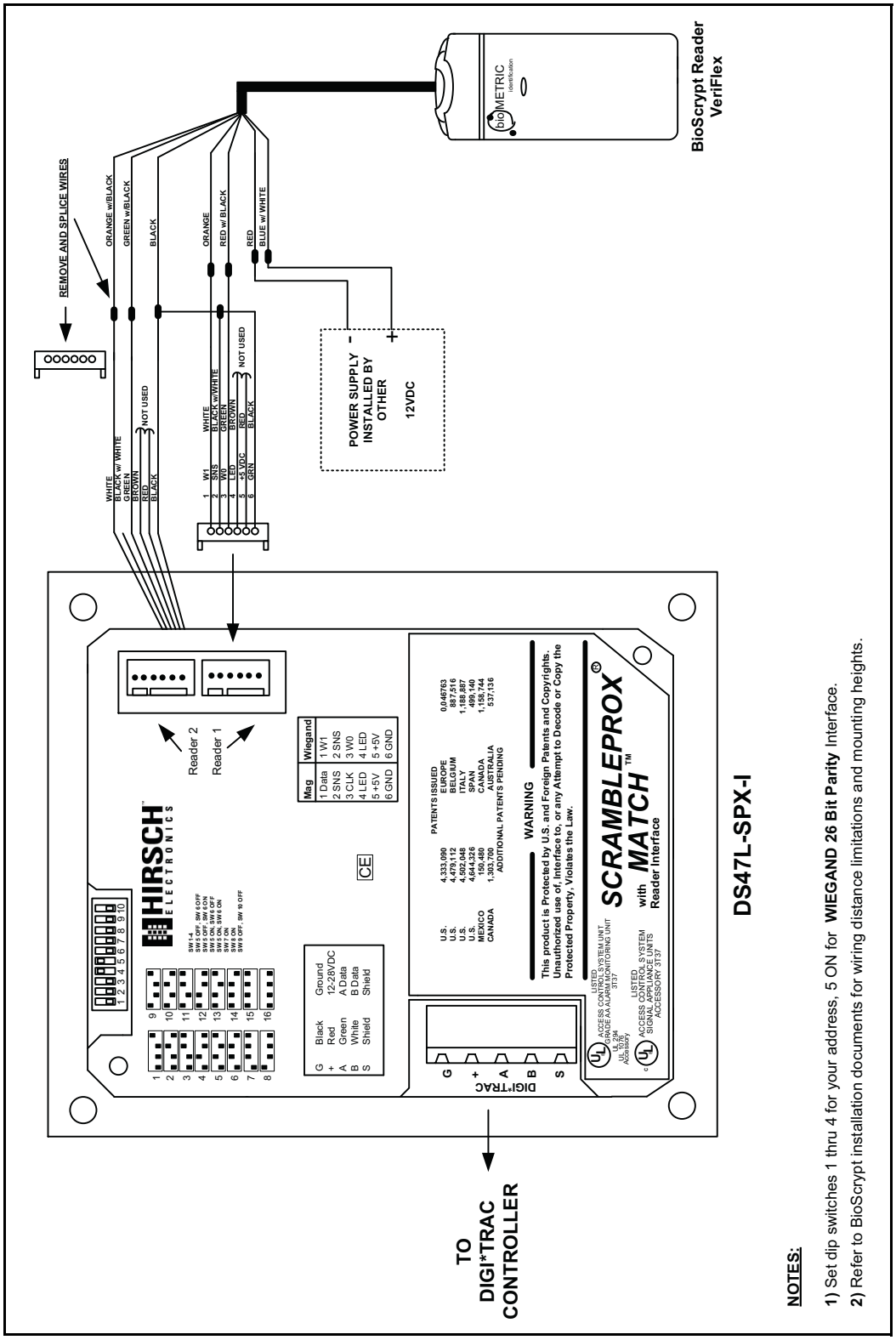
BioScrypt VeriFlex with HID-ScrambleProx

This diagram specifies the wiring and configuration of the HID prox card, fingerprint reader, and PIN code.



BioScrypt VeriFlex with Indala-ScrambleProx

This diagram specifies the wiring and configuration of the Indala prox card, fingerprint reader, and PIN code.

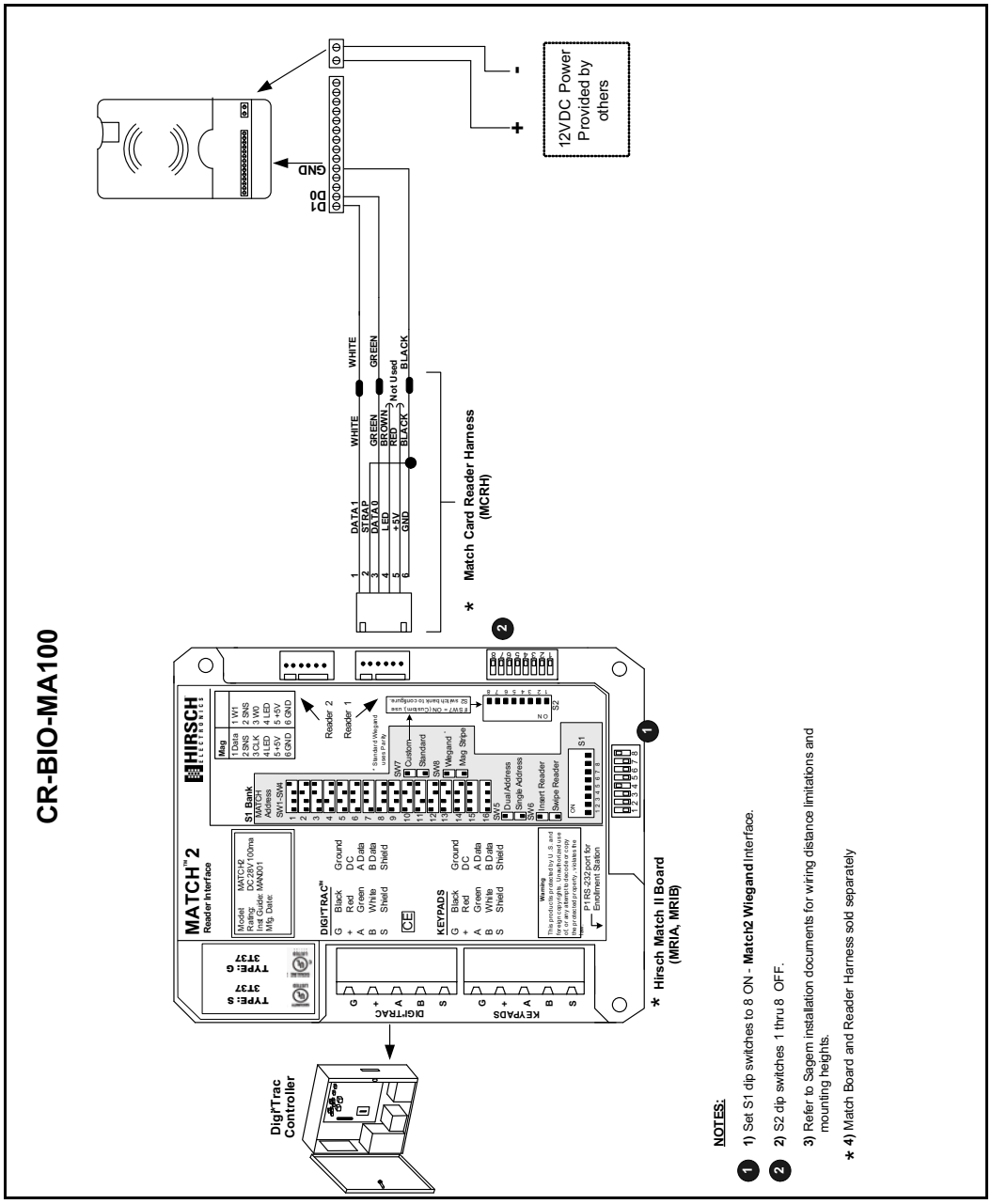


Sagem Fingerprint Readers

This section gives wiring diagrams and settings for the following BioScrypt Fingerprint readers:

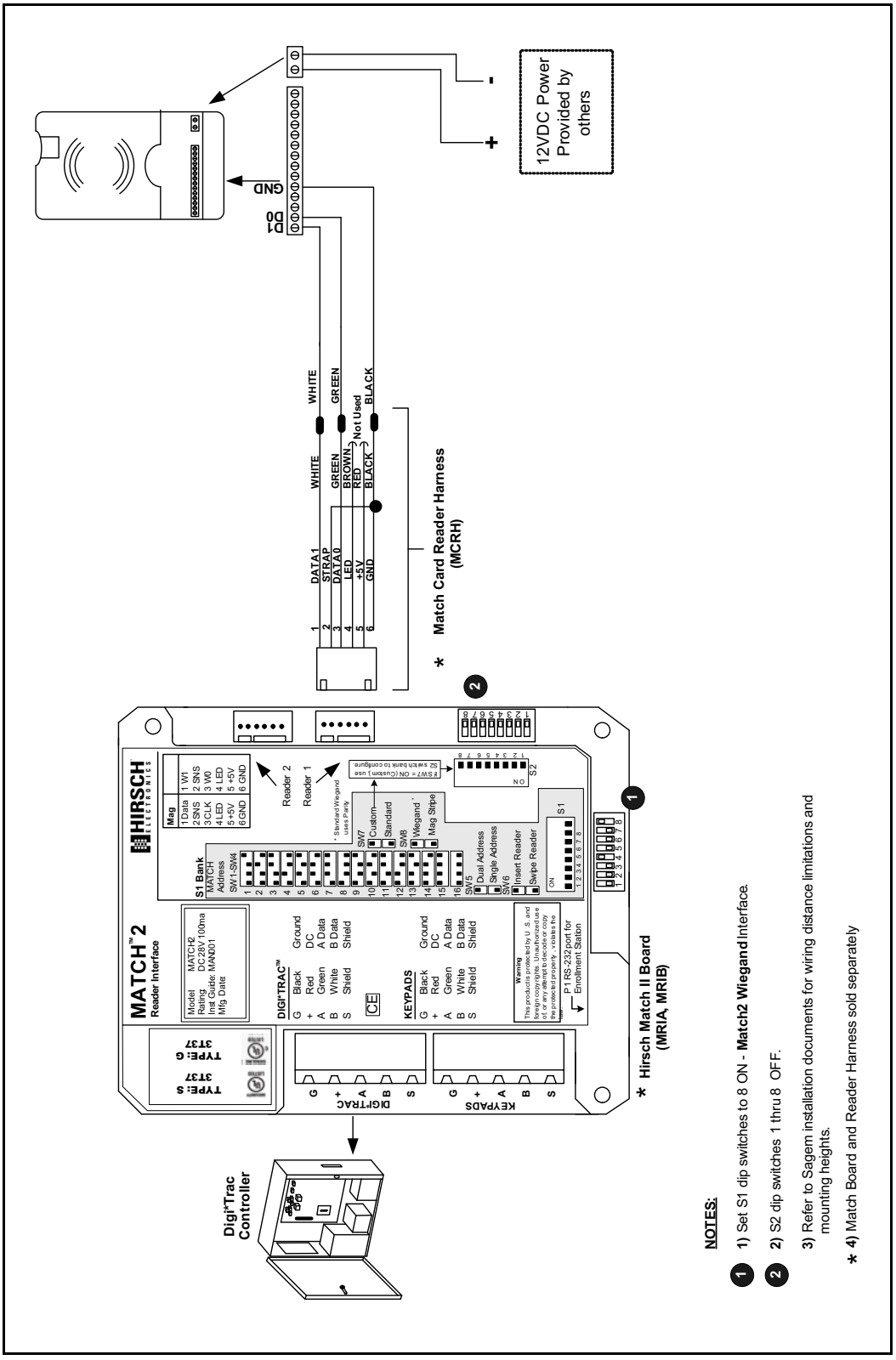
Sagem Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-MA100 Sagem Fingerprint Reader.



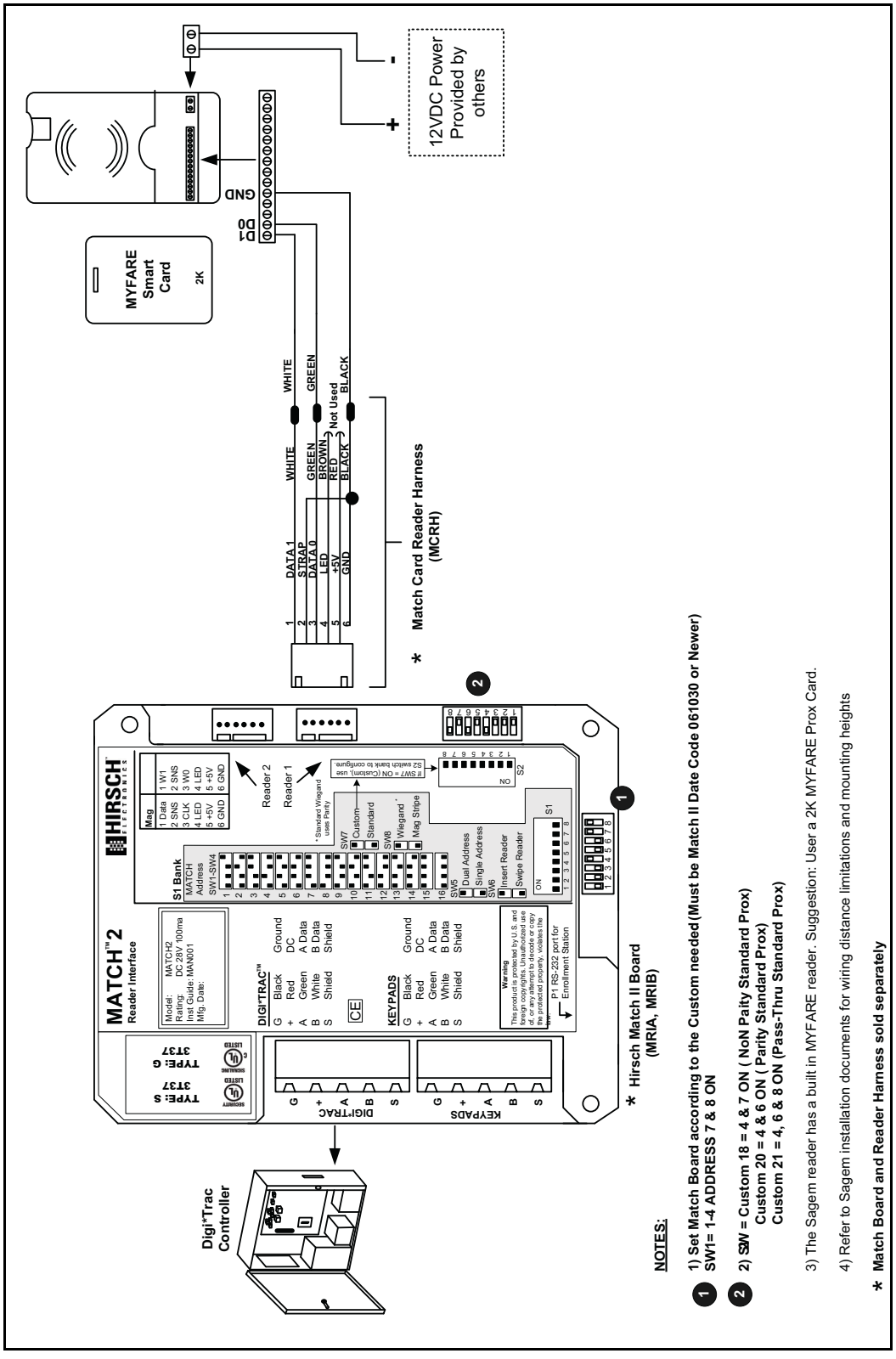
Sagem iClass-Compliant Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-MA110 Sagem iClass-Compliant Fingerprint Reader.



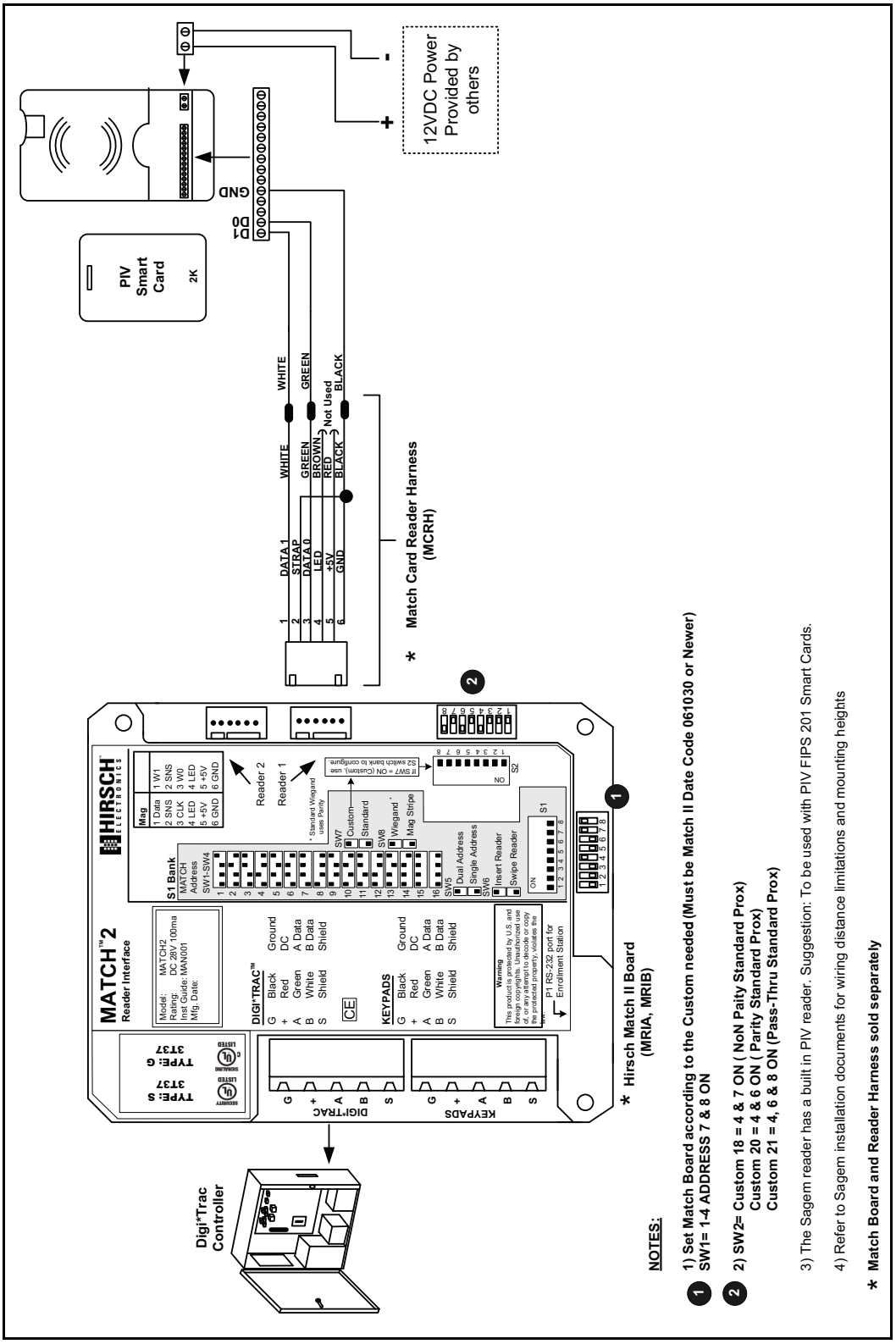
Sagem MiFare-Compliant Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-MA120 Sagem MiFare Fingerprint Reader.



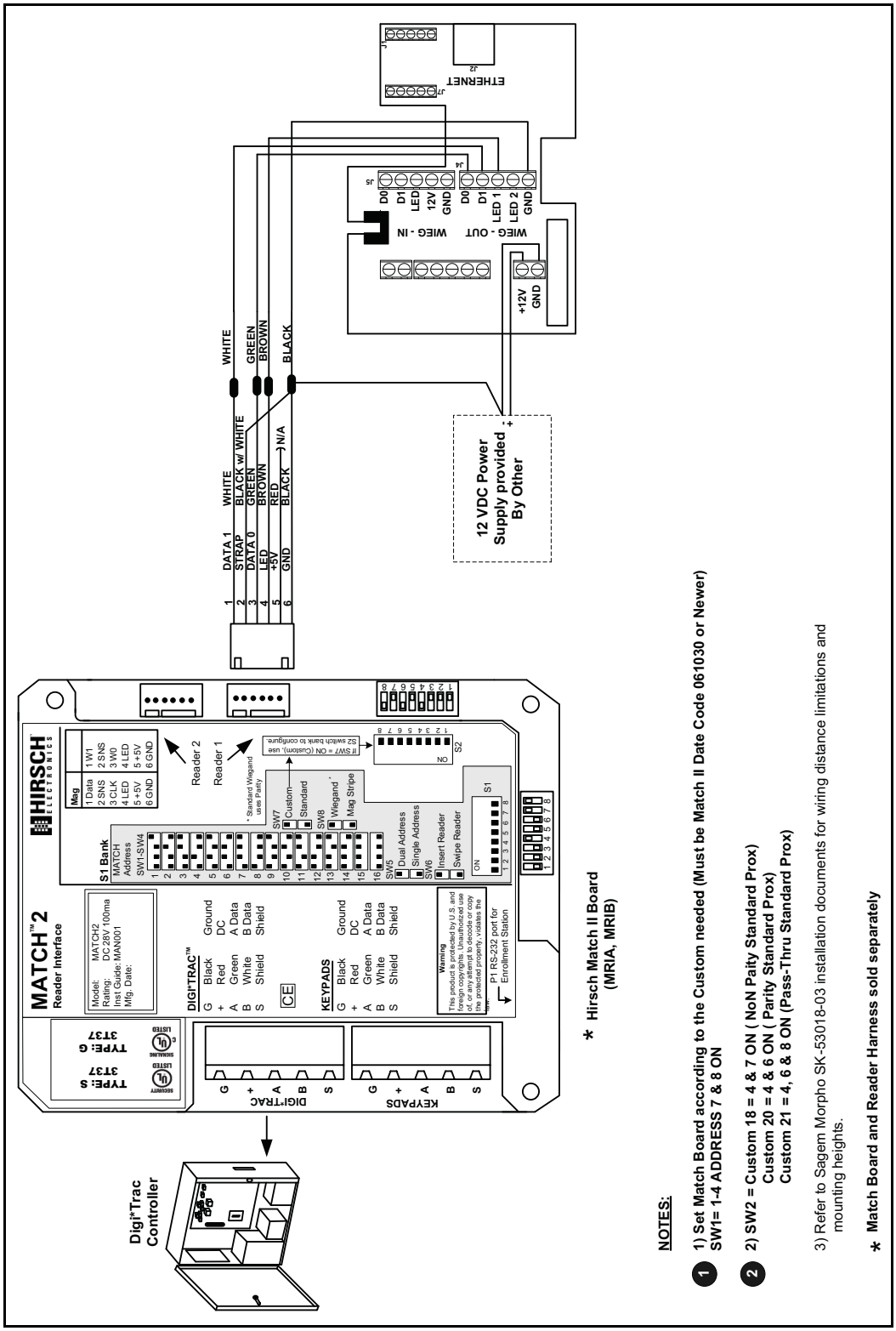
Sagem PIV-Compliant Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-MA120W Sagem PIV-Compliant Fingerprint Reader.



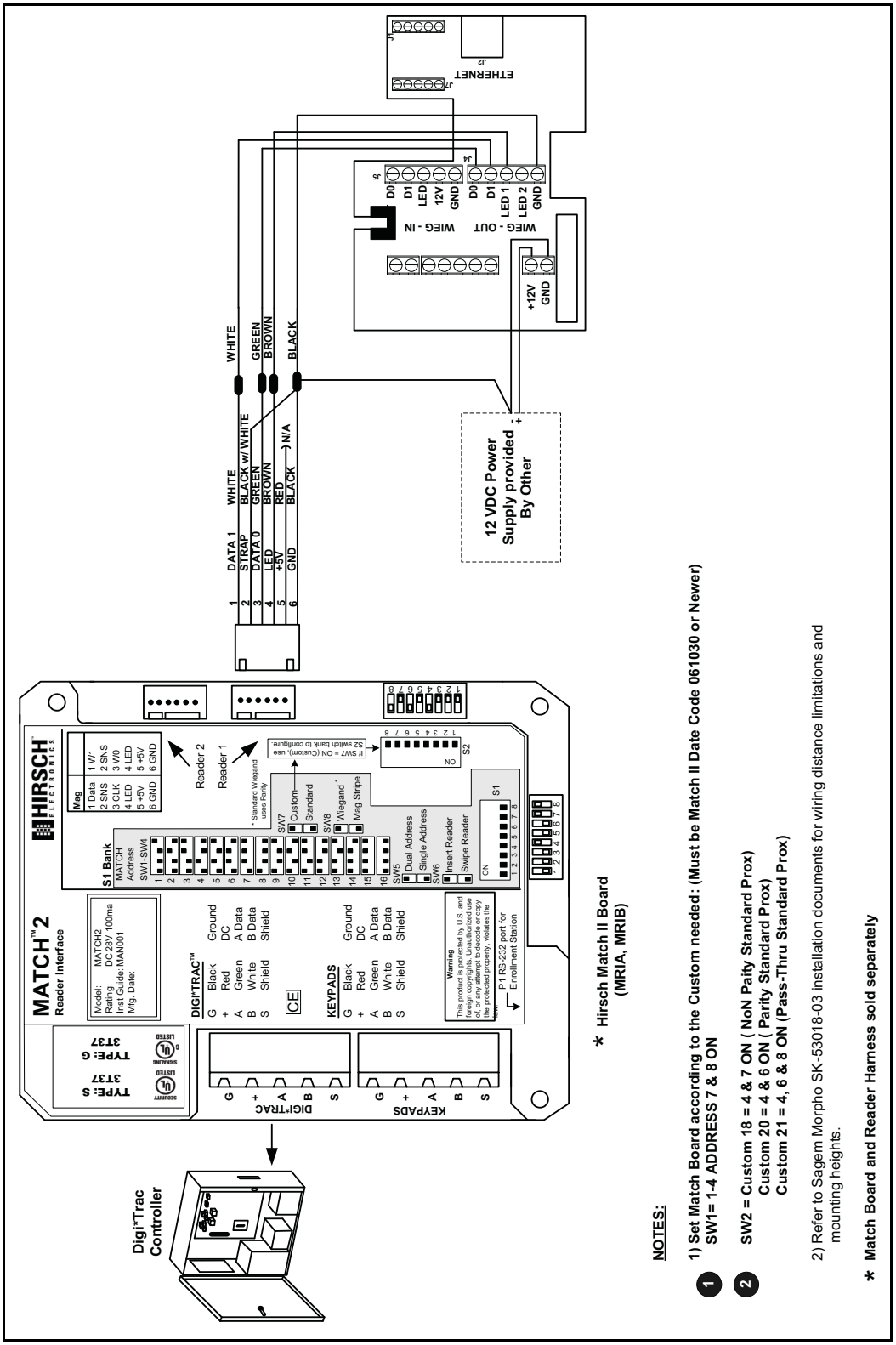
Sagem TWIC-Compliant SmartCard Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-MA521T Sagem TWIC-Compliant SmartCard Fingerprint Reader.



Sagem TWIC-Compliant SmartCard Outdoor Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-MA521T-O Sagem TWIC-Compliant SmartCard Fingerprint Reader.

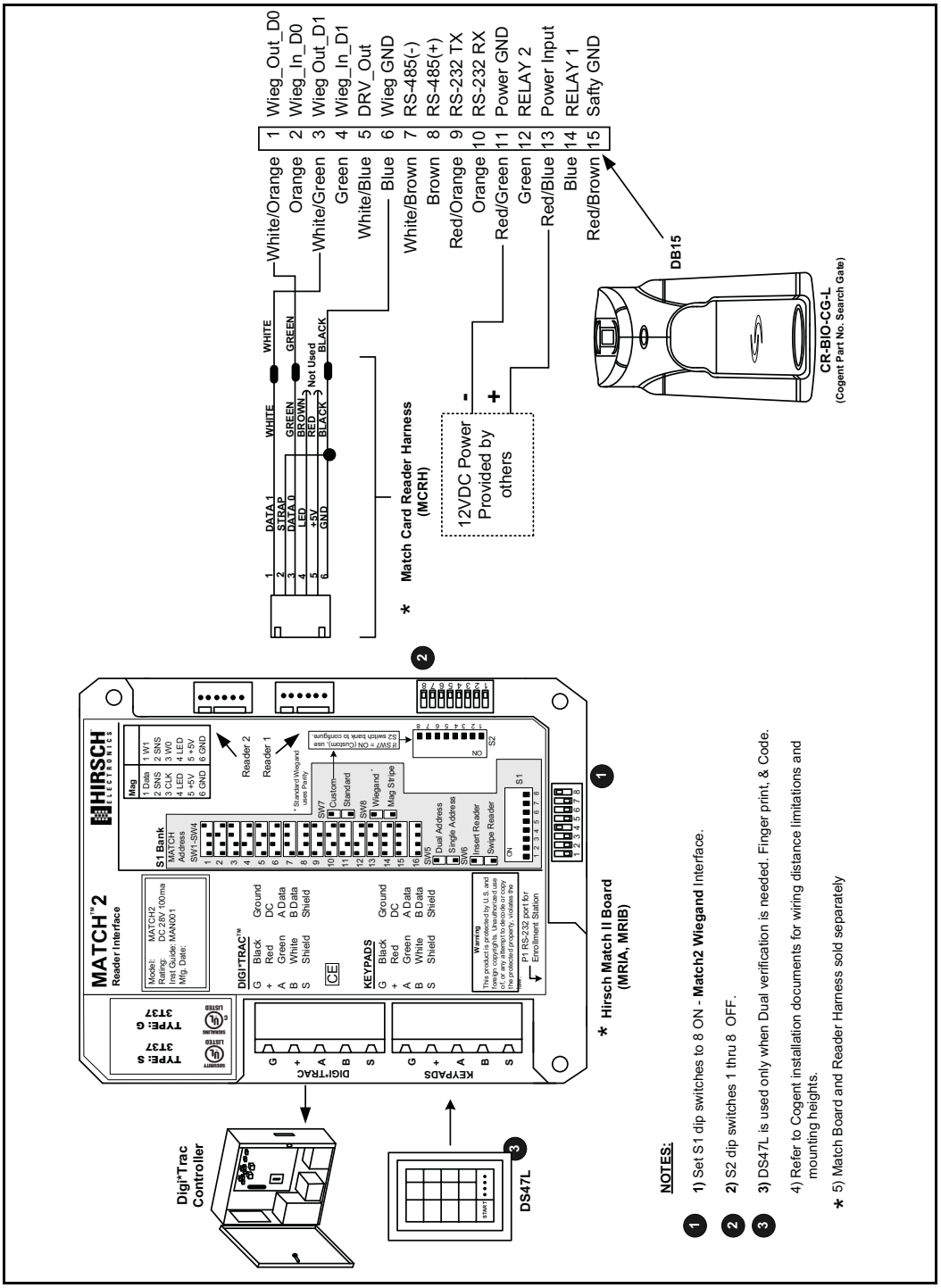


Cogent Fingerprint Readers

This section gives wiring diagrams and settings for the following Cogent Fingerprint readers:

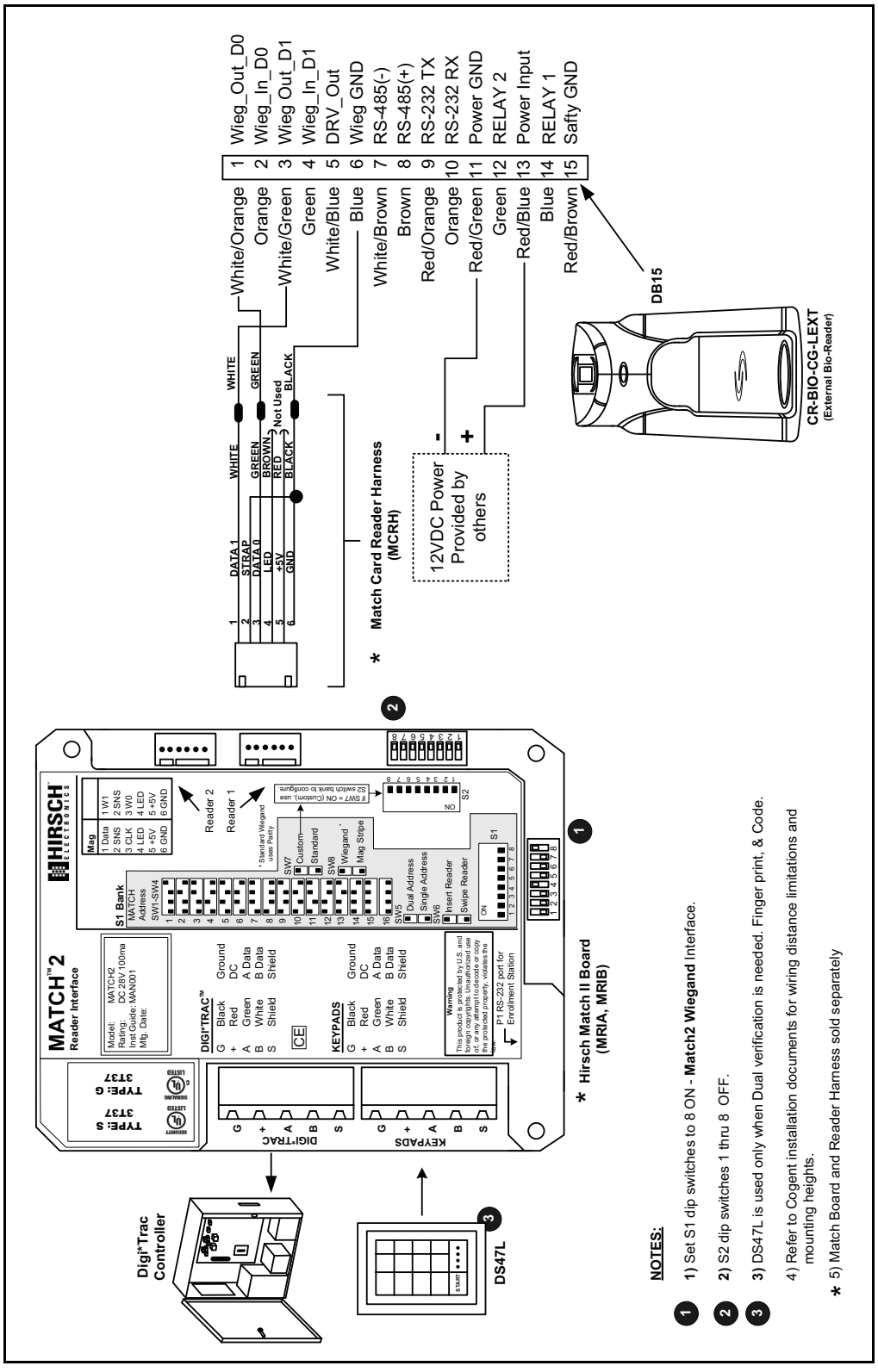
Cogent Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-CG-L Cogent Fingerprint Reader.



Cogent External Fingerprint Reader

This diagram specifies the wiring and configuration of the model CR-BIO-CG-LEXT Cogent External Fingerprint Reader.

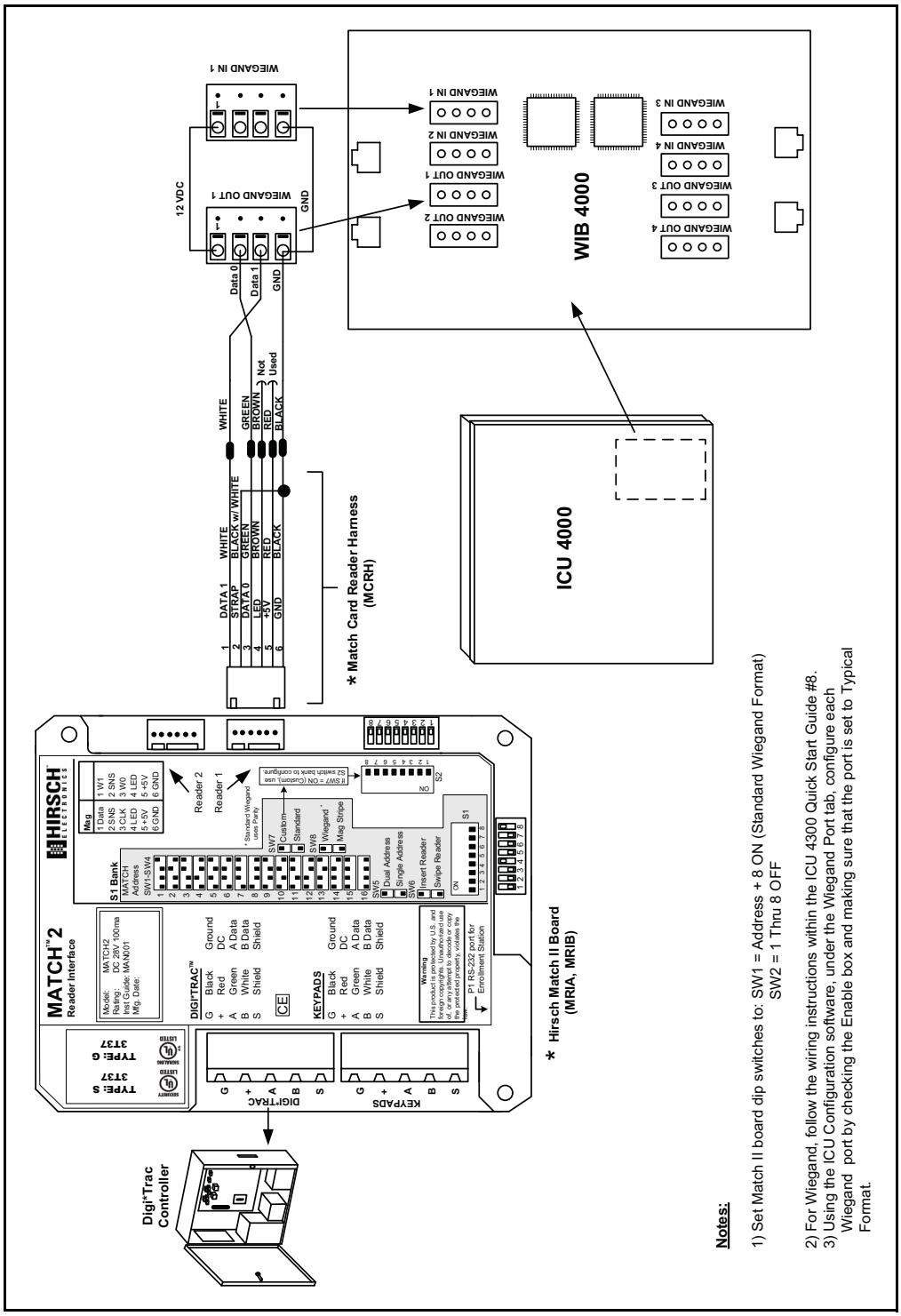


Iris Scan Readers

This section give diagrams for wiring and Match2 DIP switch settings for the following iris scan readers:

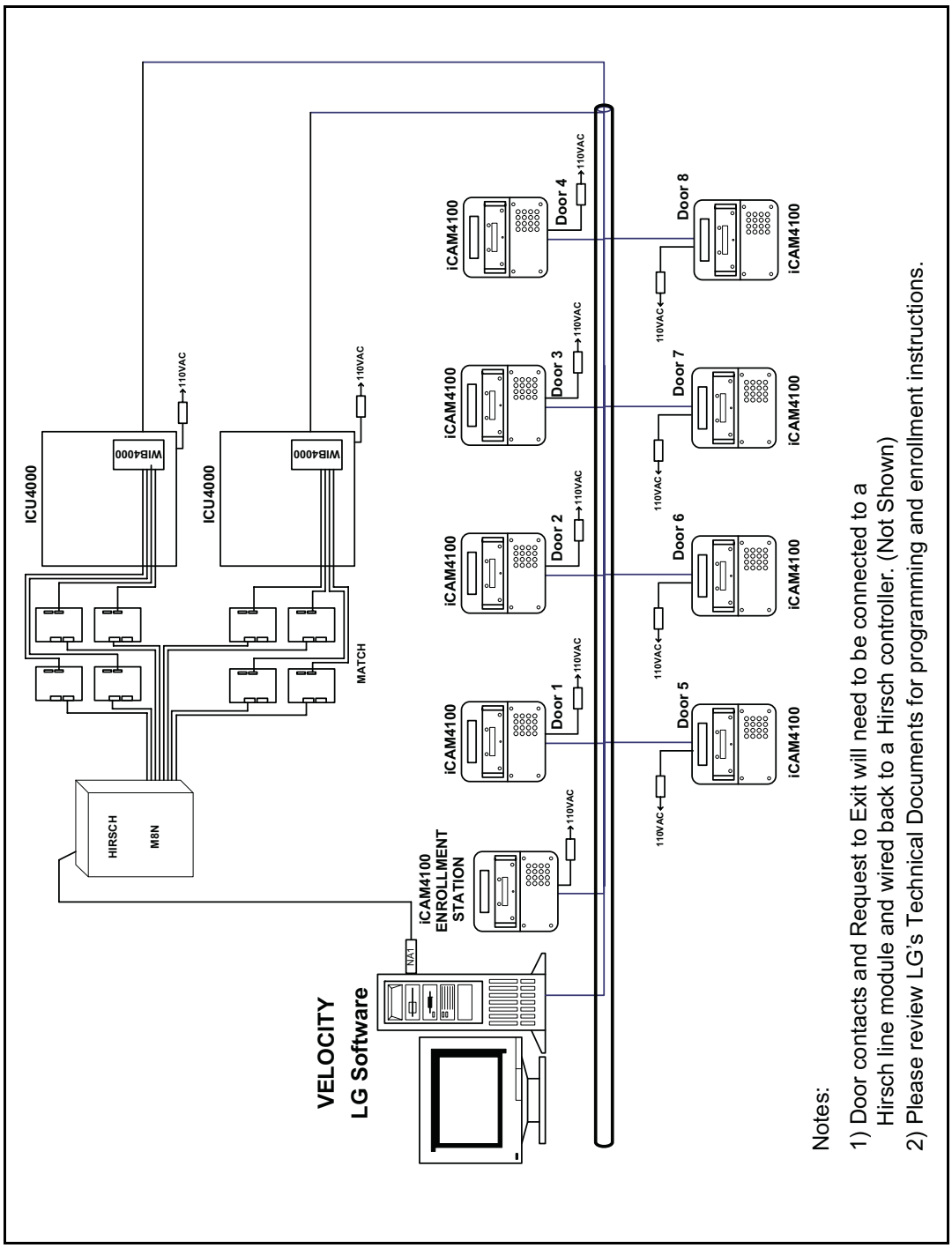
LG Iris Scan Reader

This diagram shows wiring and settings for the LG WIB 4000 Iris Scan Reader.



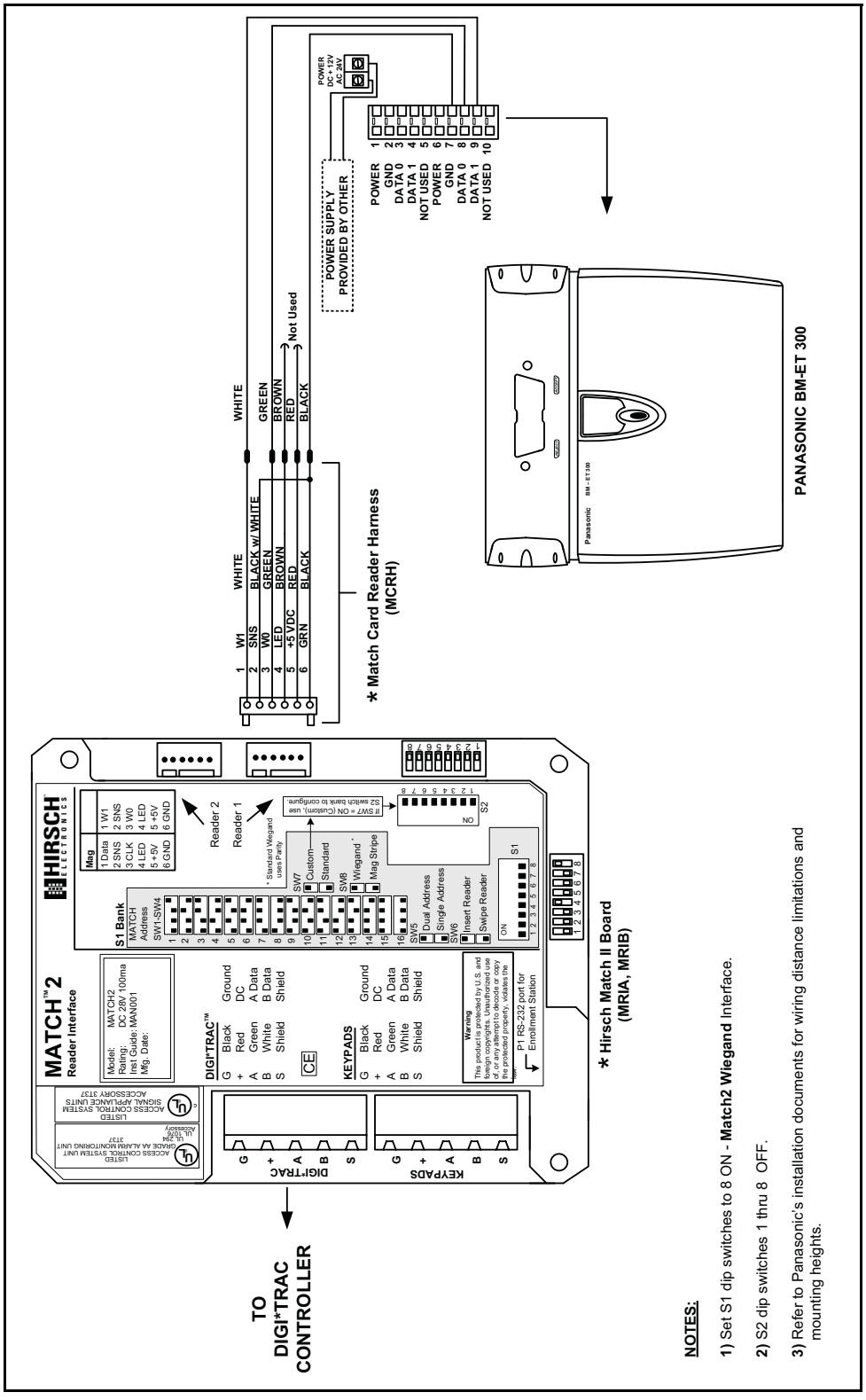
LG Iris Scan Reader Network

One or more LG iris scan readers can be connected to a network as shown in the following diagram. For instructions on connecting an LG iris recognition reader to a MATCH 2, refer to the previous diagram.



Panasonic Iris Reader

This diagram shows wiring and settings for the Panasonic BM-ET300 Iris Reader.

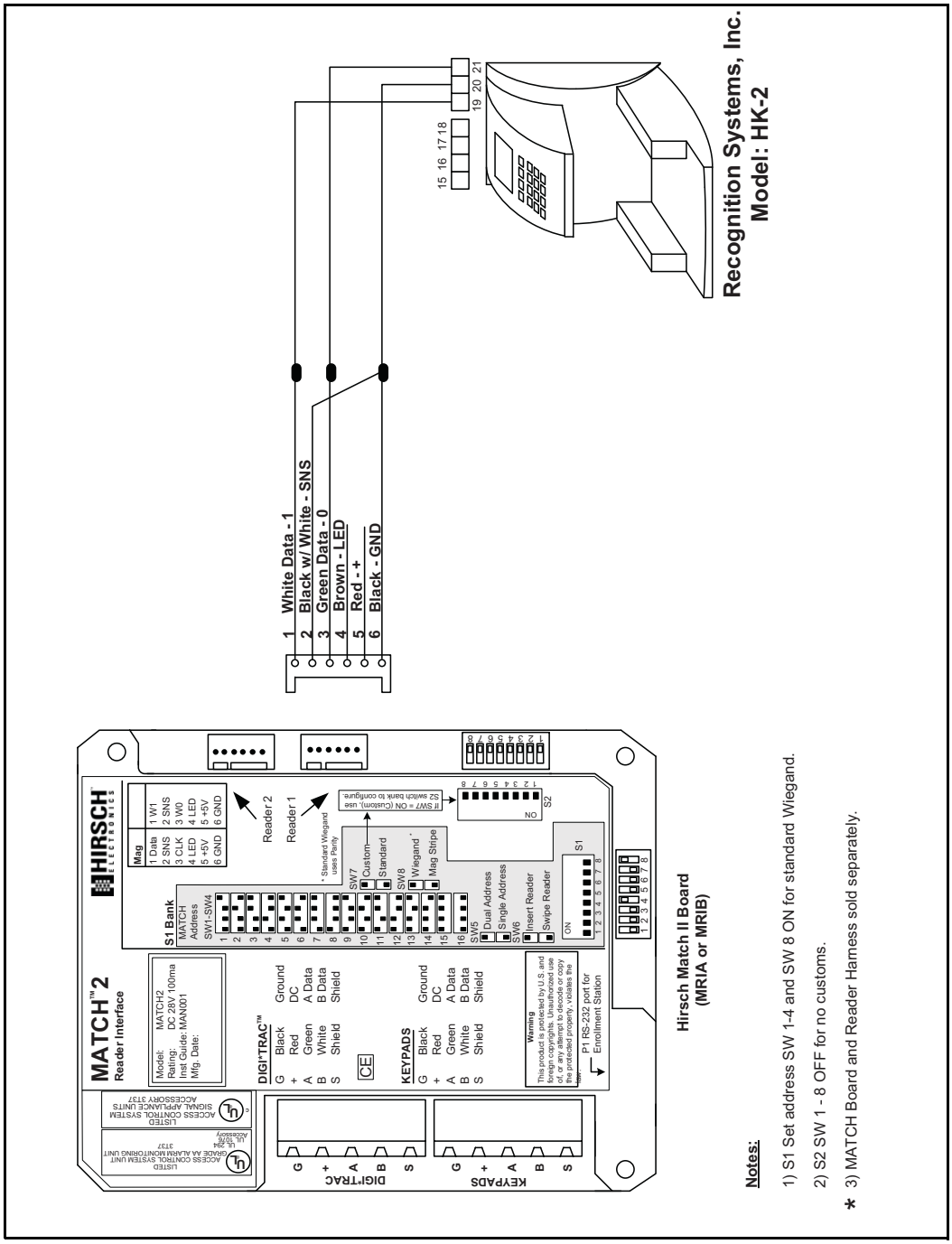


Hand Readers

This section give diagrams for wiring and Match2 DIP switch settings for the following hand readers:

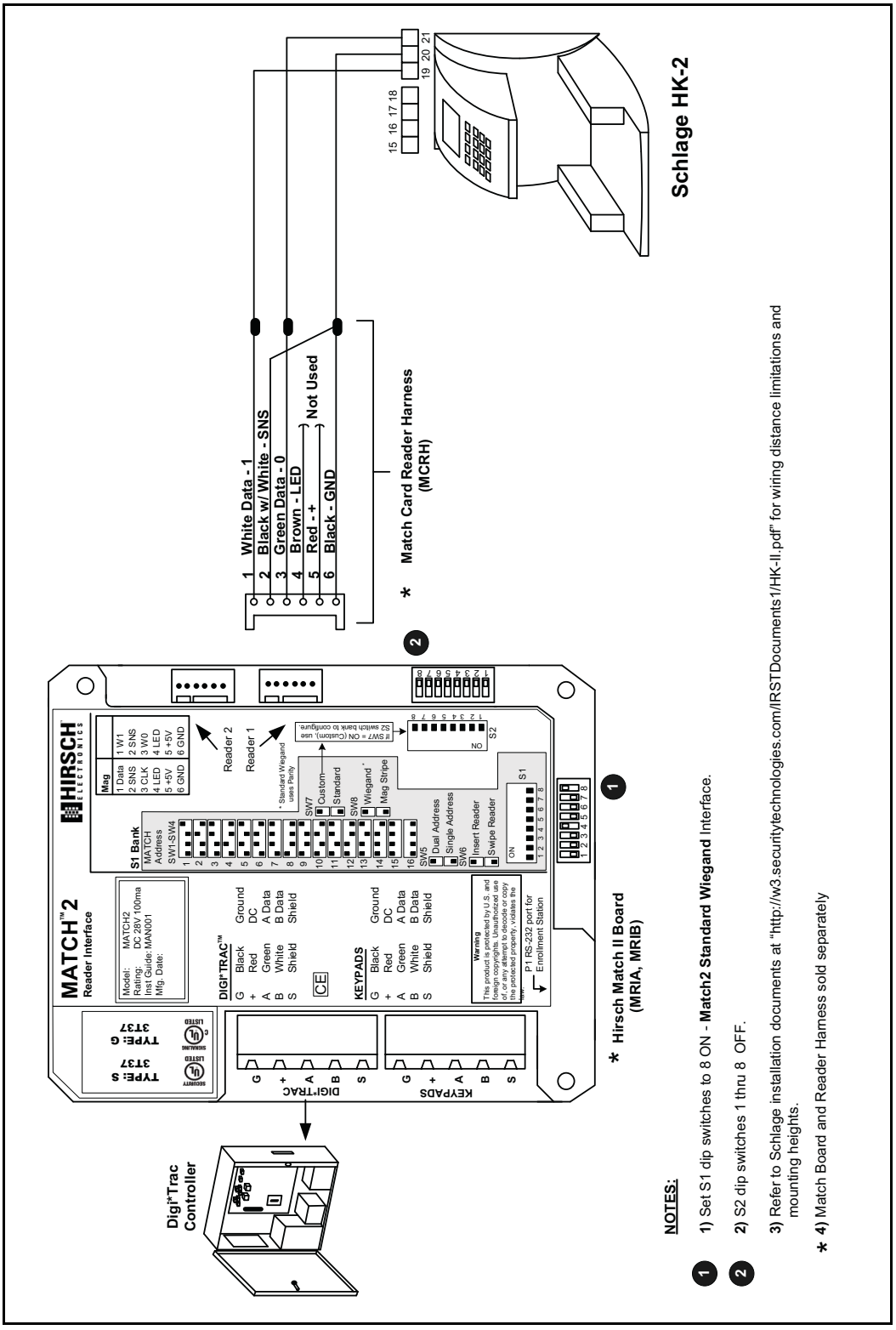
Recognition Systems Hand Key II Hand Reader

This diagram shows wiring and settings for the Recognition Systems HK-2 Hand Key II Hand Reader.

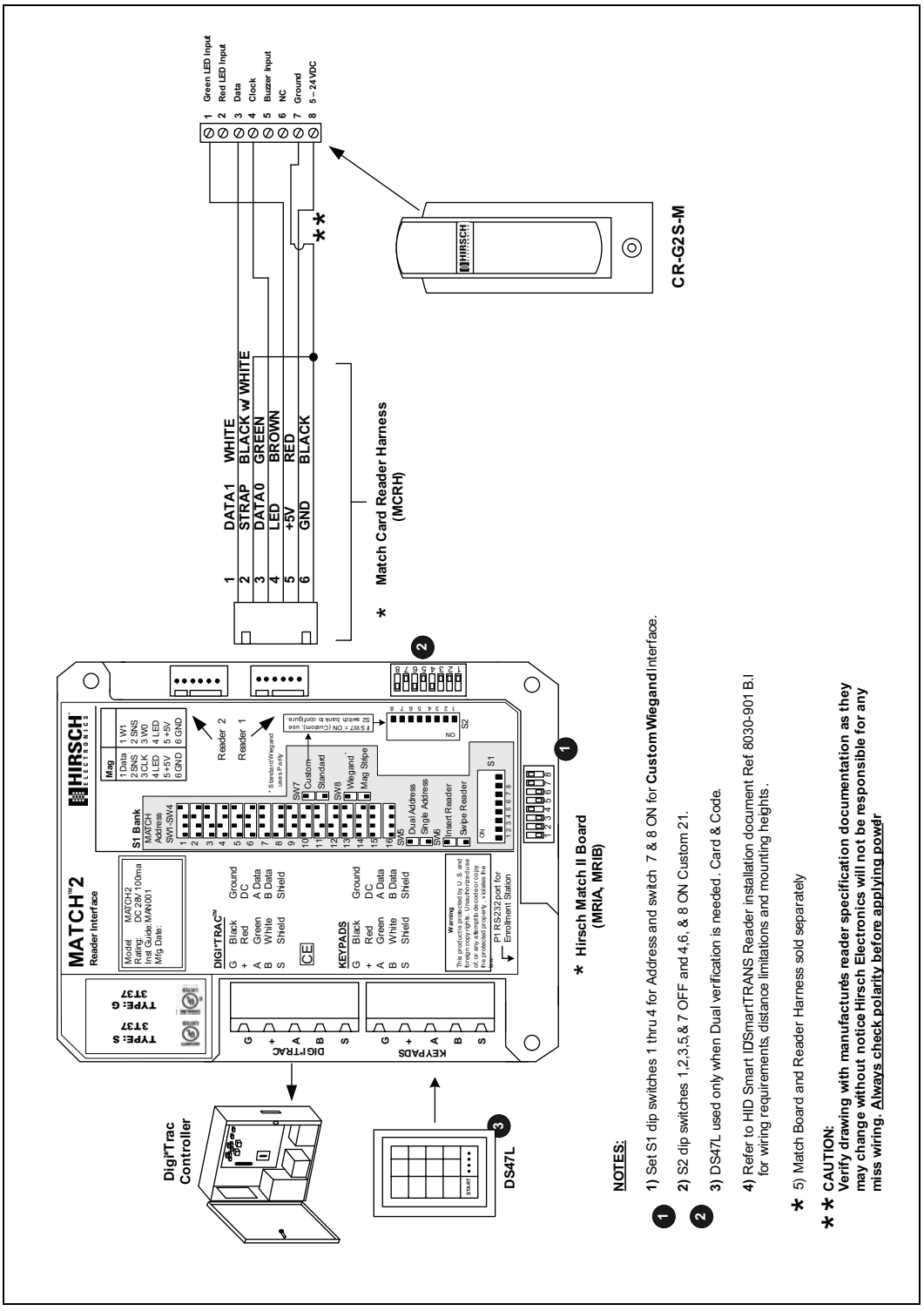


Schlage HK-2 Hand Reader

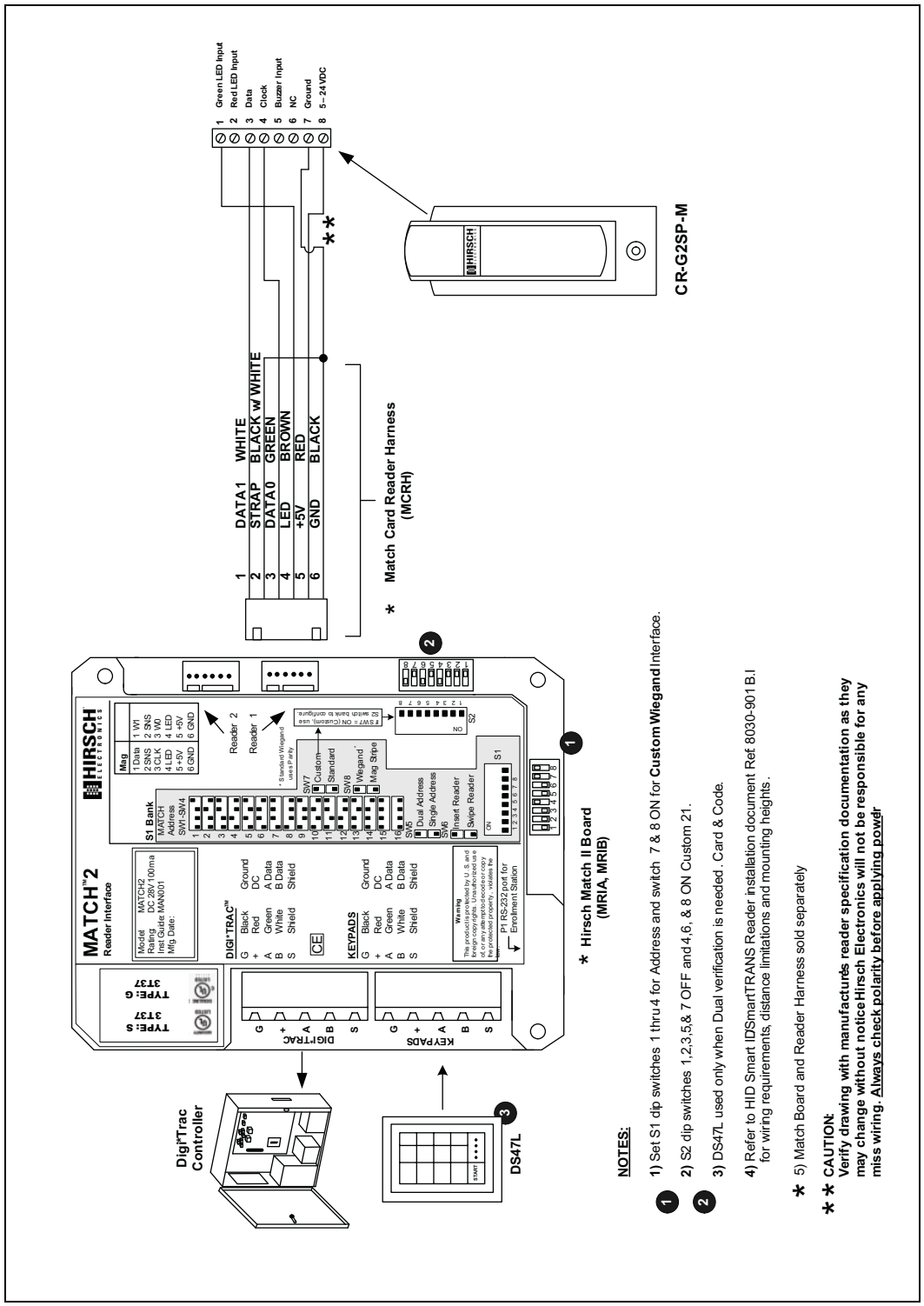
This diagram shows wiring and settings for the Schlage HK-2 Hand Reader, model CR-BIO-HAND.



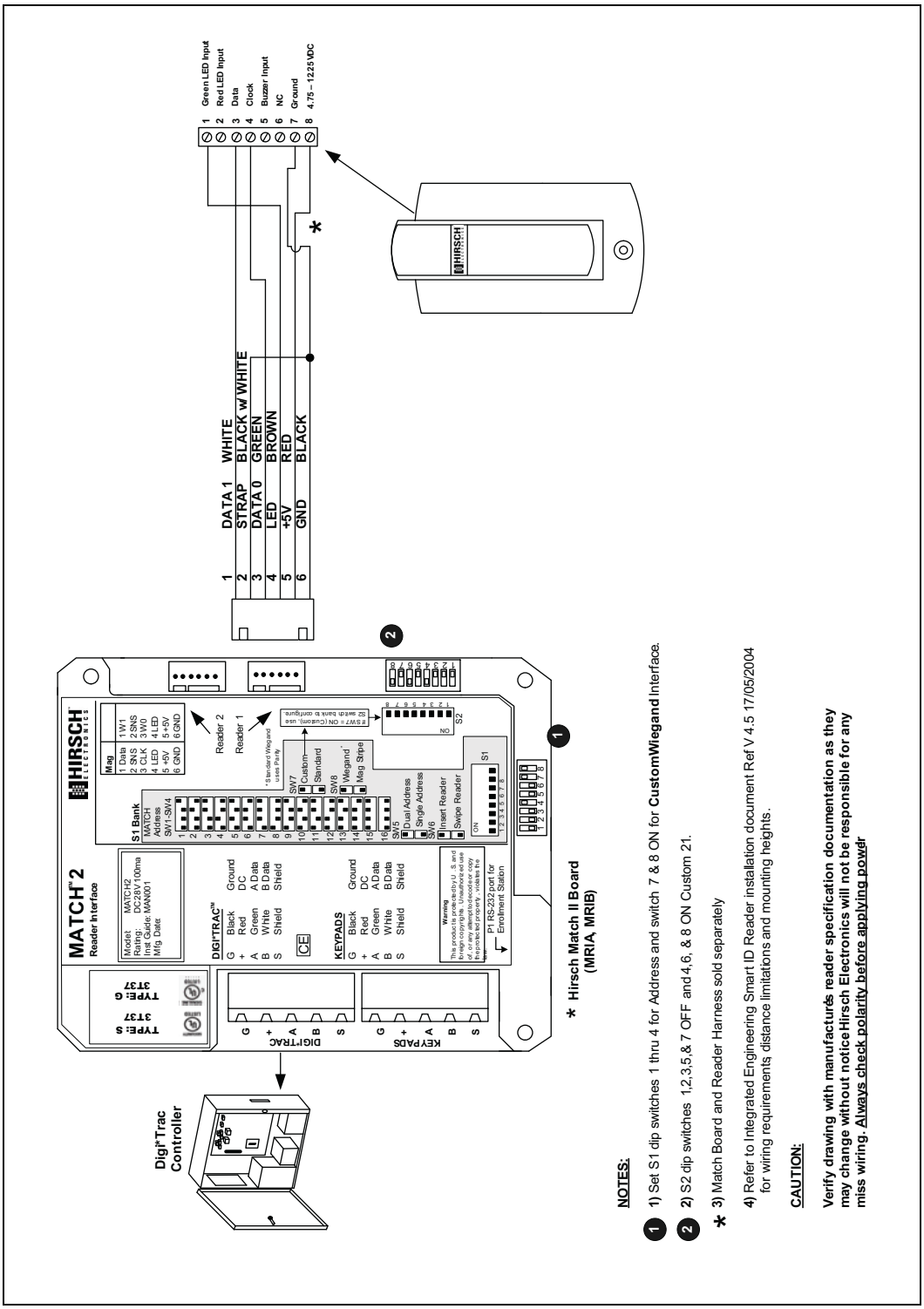
CR-G2S-M HID G2 DESFire / MIFARE SmartCard Reader



CR-G2SP-M HID G2 DESFire / MIFARE SmartProx Reader



CR-G2S-SGCP HID Single-Gang CP SmartCard Reader



NOTES:

1. **1)** Set S1 dip switches 1 thru 4 for Address and switch 7 & 8 ON for **CustomWiegand** Interface.
2. **2)** S2 dip switches 1,2,3,5,& 7 OFF and 4,6, & 8 ON Custom 21.

* **3)** Match Board and Reader Harness sold separately

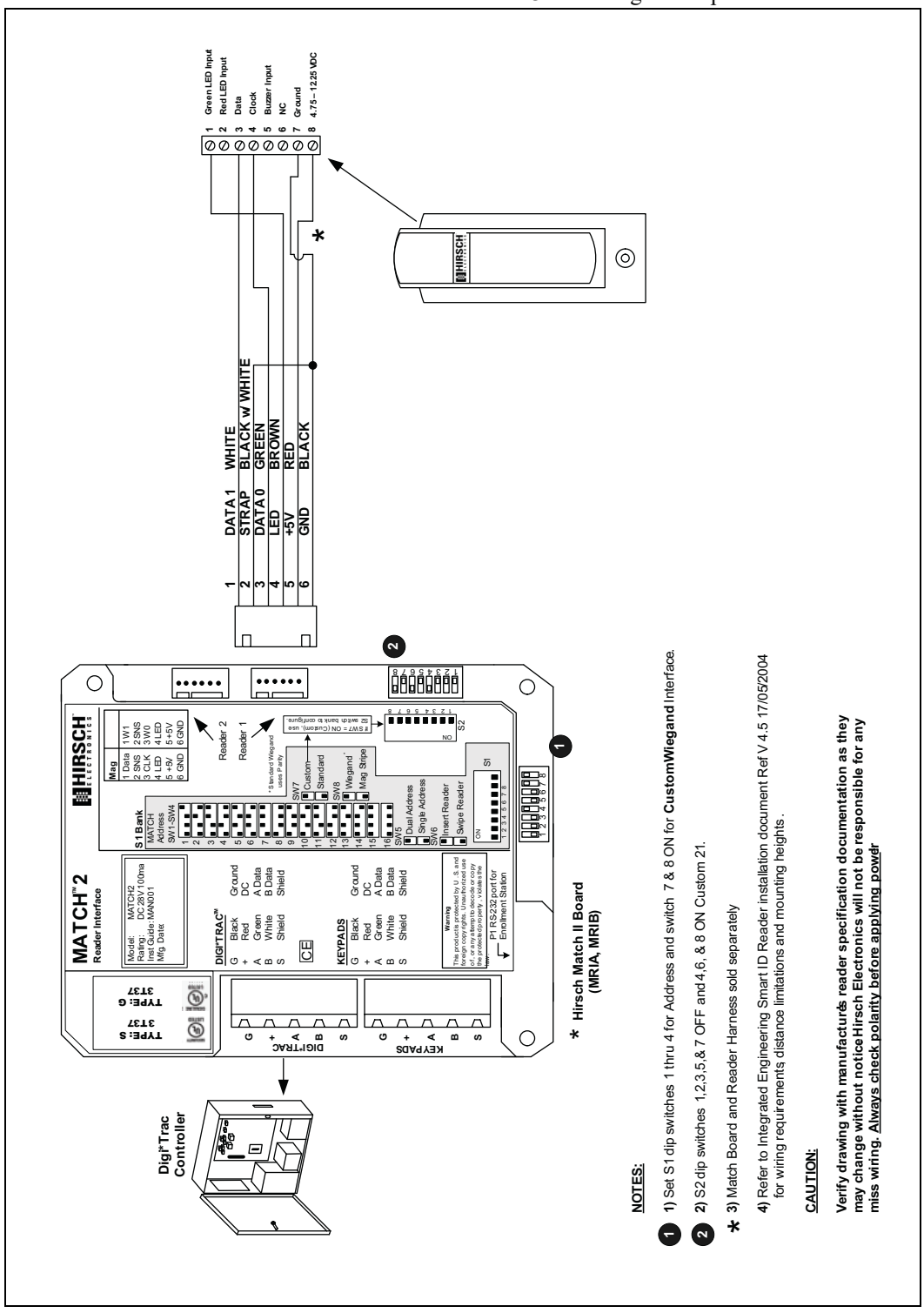
4) Refer to Integrated Engineering Smart ID Reader installation document Ref V 4.5 17/05/2004 for wiring requirements, distance limitations and mounting heights.

CAUTION:

Verify drawing with manufacturer's reader specification documentation as they may change without notice Hirsch Electronics will not be responsible for any miss wiring. Always check polarity before applying power

CR-G2SSN HID MIFARE SSN SmartCard Reader

This model reads MIFARE Serial Number with 34-bit Wiegand output.



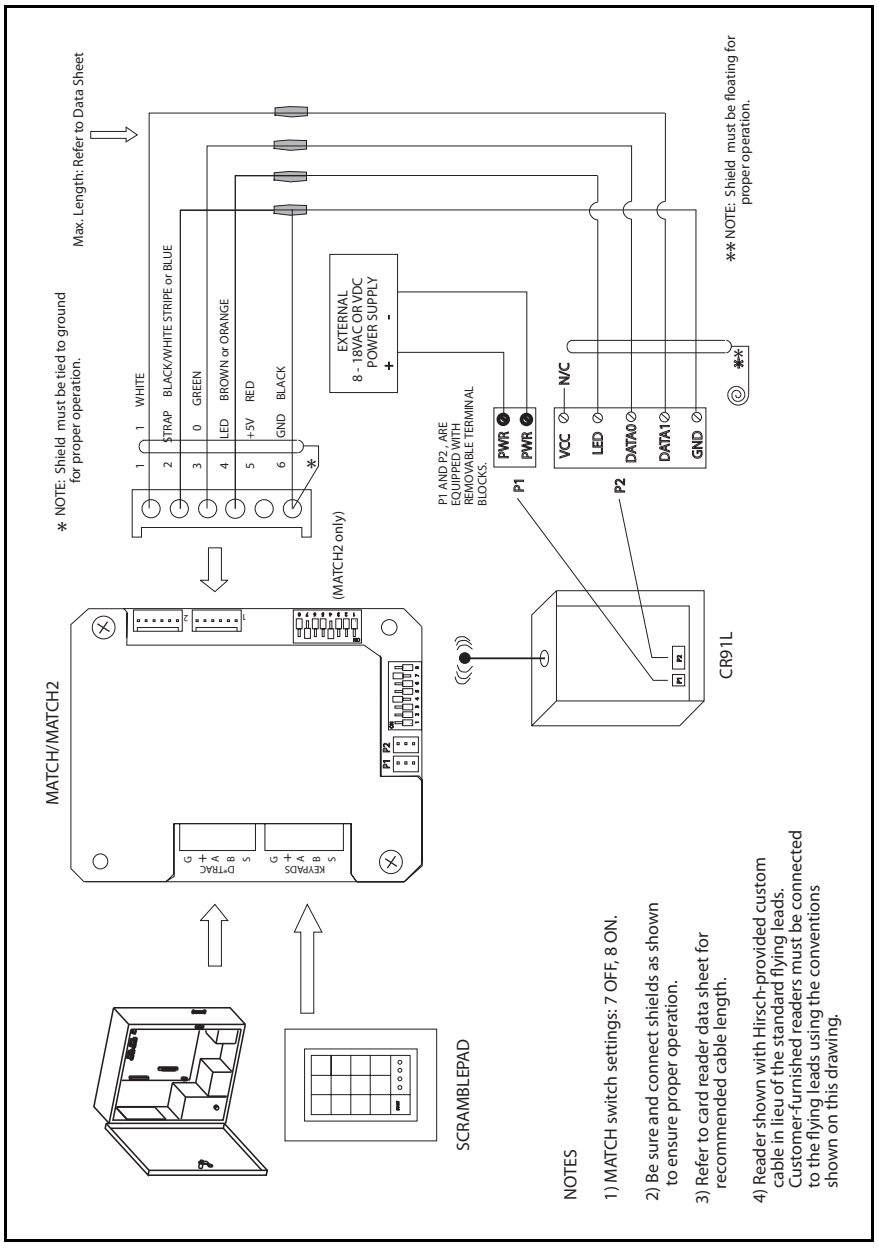
Infrared and Long-Range Readers

This section describes the MATCH wiring and settings information required to connect Hirsch-supported infrared and long-range card readers. These readers include:

- ❑ "Long-Range RF Receiver" on page 7-240
- ❑ "Nedap Transit Long-Range Readers" on page 7-241

Long-Range RF Receiver

This diagram shows wiring and settings for the Long Range RF Receiver, model CR91L.

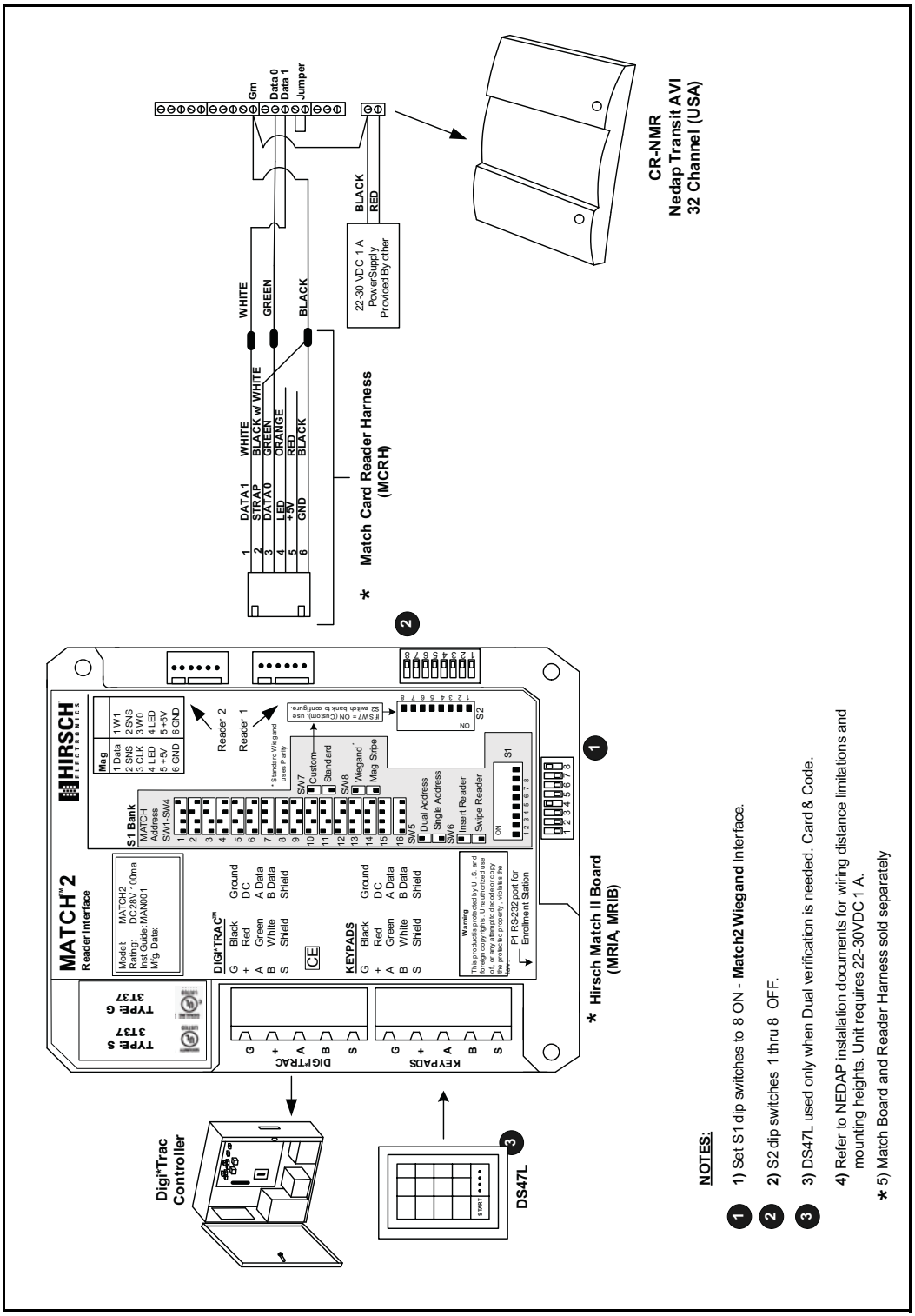


Nedap Transit Long-Range Readers

This section give diagrams for wiring and Match2 DIP switch settings for the following hand readers:

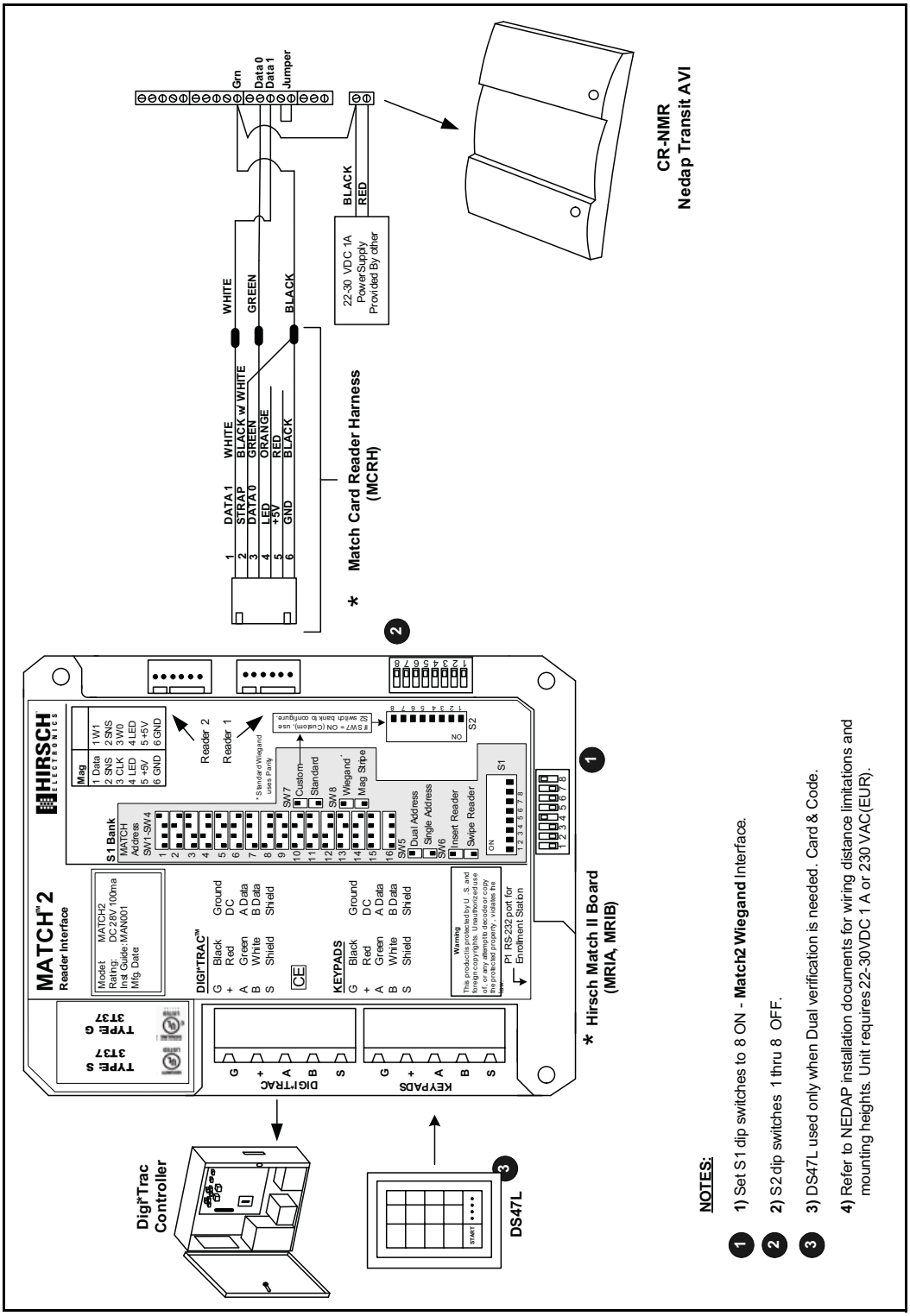
Nedap Transit AVI Long-Range Reader (American)

This diagram shows wiring and settings for the Nedap Transit AVI Long-Range Reader, model CR-NMRU.This is the American version of this reader.



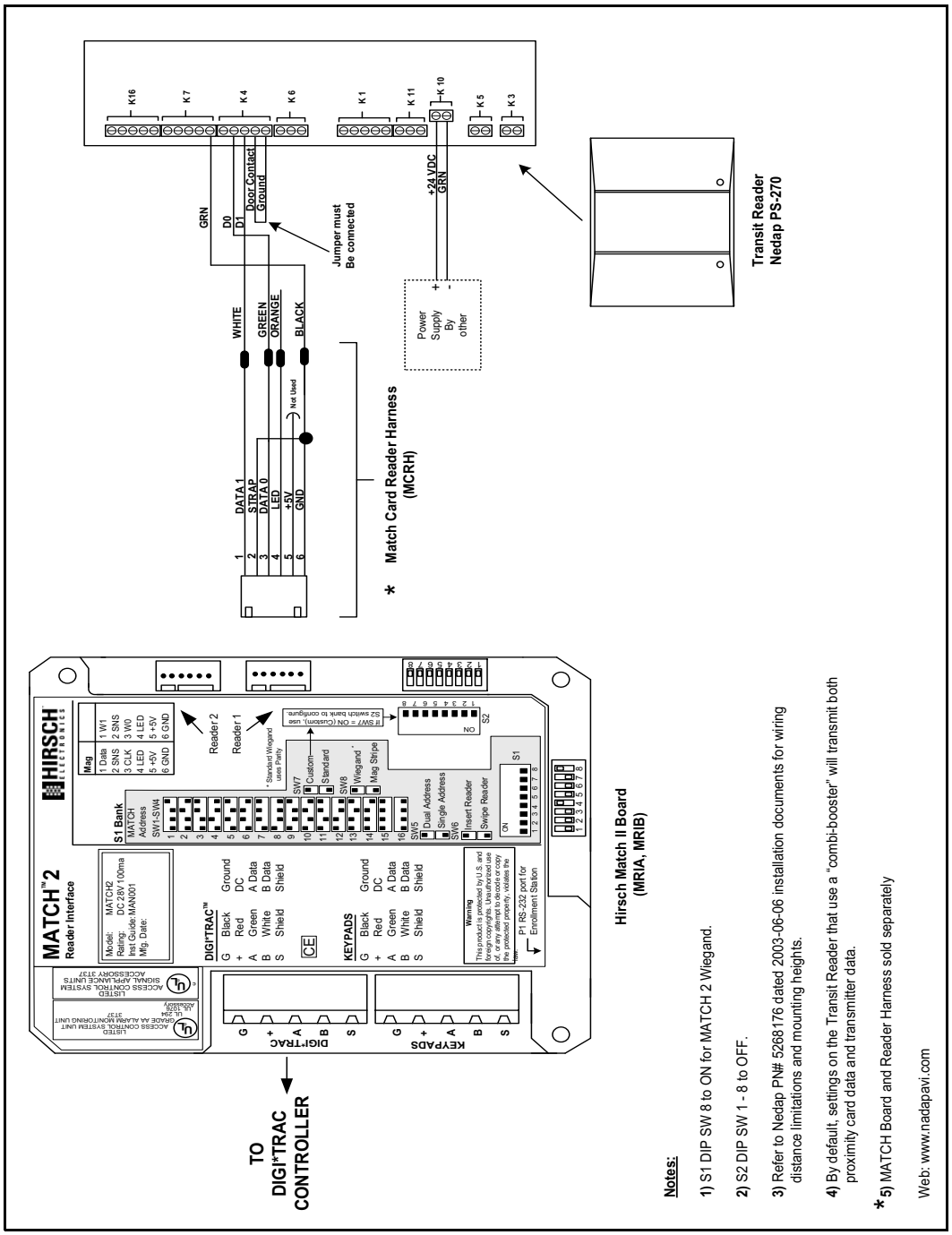
Nedap Transit AVI Long-Range Reader (European)

This diagram shows wiring and settings for the Nedap Transit AVI Long-Range Reader, model CR-NMR. This is the European version of this reader.



Nedap PS-270 Transit Reader

This diagram shows wiring and settings for the Nedap PS-270 Transit Reader.



Notes:

1) S1 DIP SW 8 to ON for MATCH 2 Wiegand.

2) S2 DIP SW 1 - 8 to OFF.

3) Refer to Nedap PN# 5268176 dated 2003-06-06 installation documents for wiring distance limitations and mounting heights.

4) By default, settings on the Transit Reader that use a "combi-booster" will transmit both proximity card data and transmitter data.

***5)** MATCH Board and Reader Harness sold separately

Web: www.nadapavi.com

Smart Card Readers

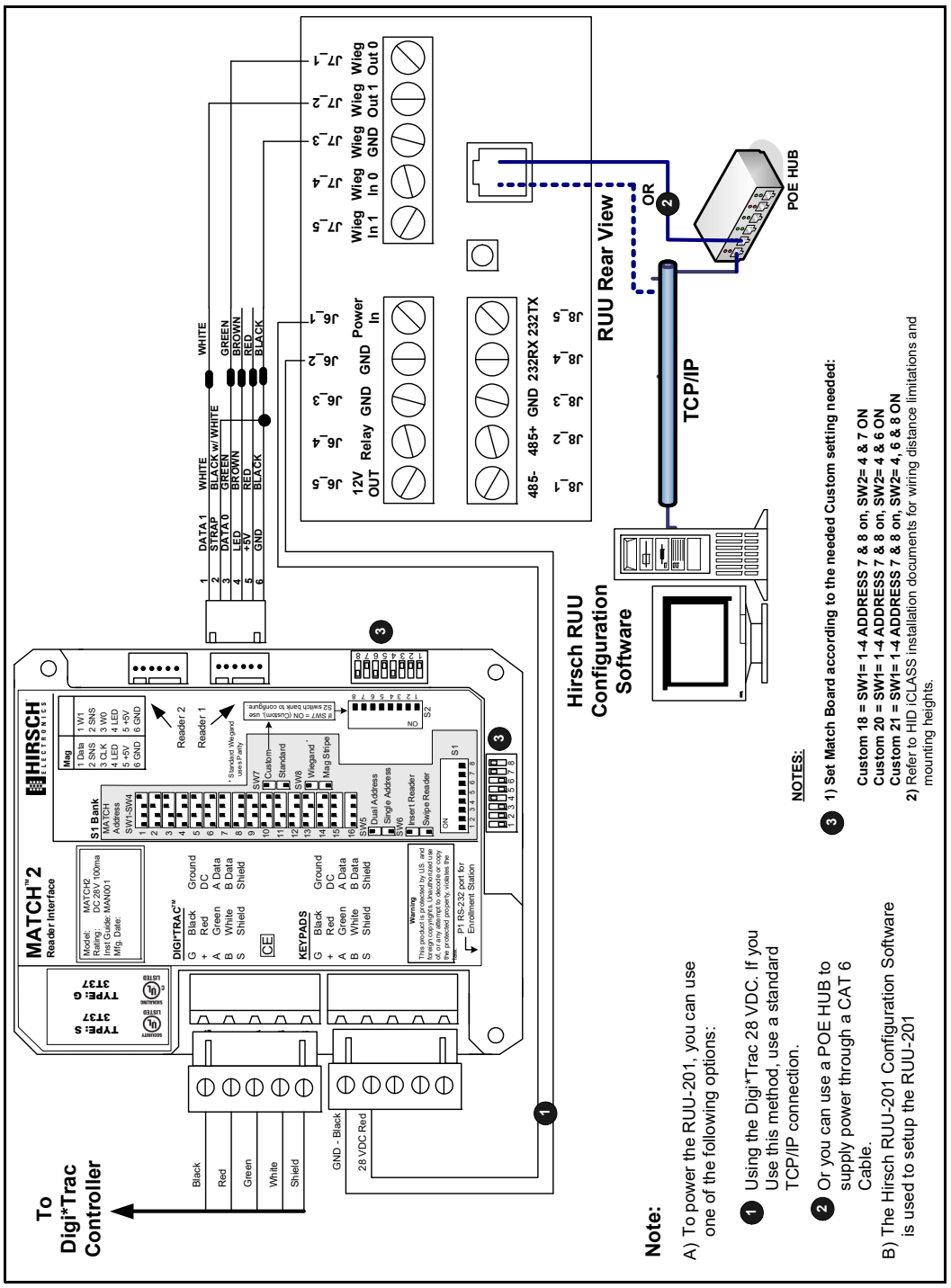
This section describes the MATCH wiring and settings information required to connect Hirsch-supported smart card readers. These readers include:

Hirsch Biometric SmartCard Readers

This section give diagrams for wiring and Match2 DIP switch settings for the following SmartCard readers:

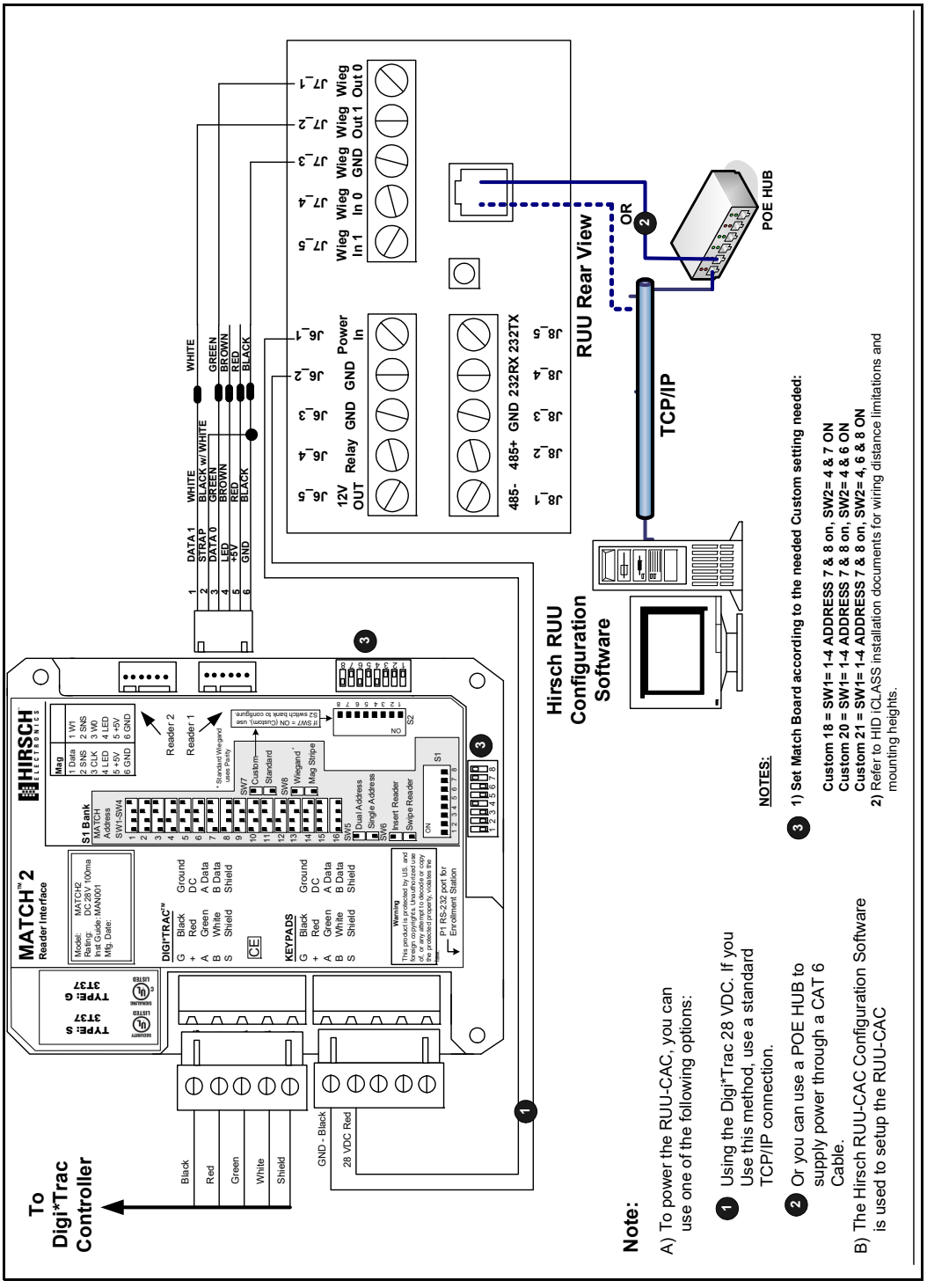
Hirsch PIV Biometric SmartCard Reader

This diagram shows wiring and settings for the Hirsch PIV Biometric SmartCard Reader, model CR-BIO-RUU-PIV. This can be powered by either the Hirsch DIGIT*TRAC controller or PoE hub.



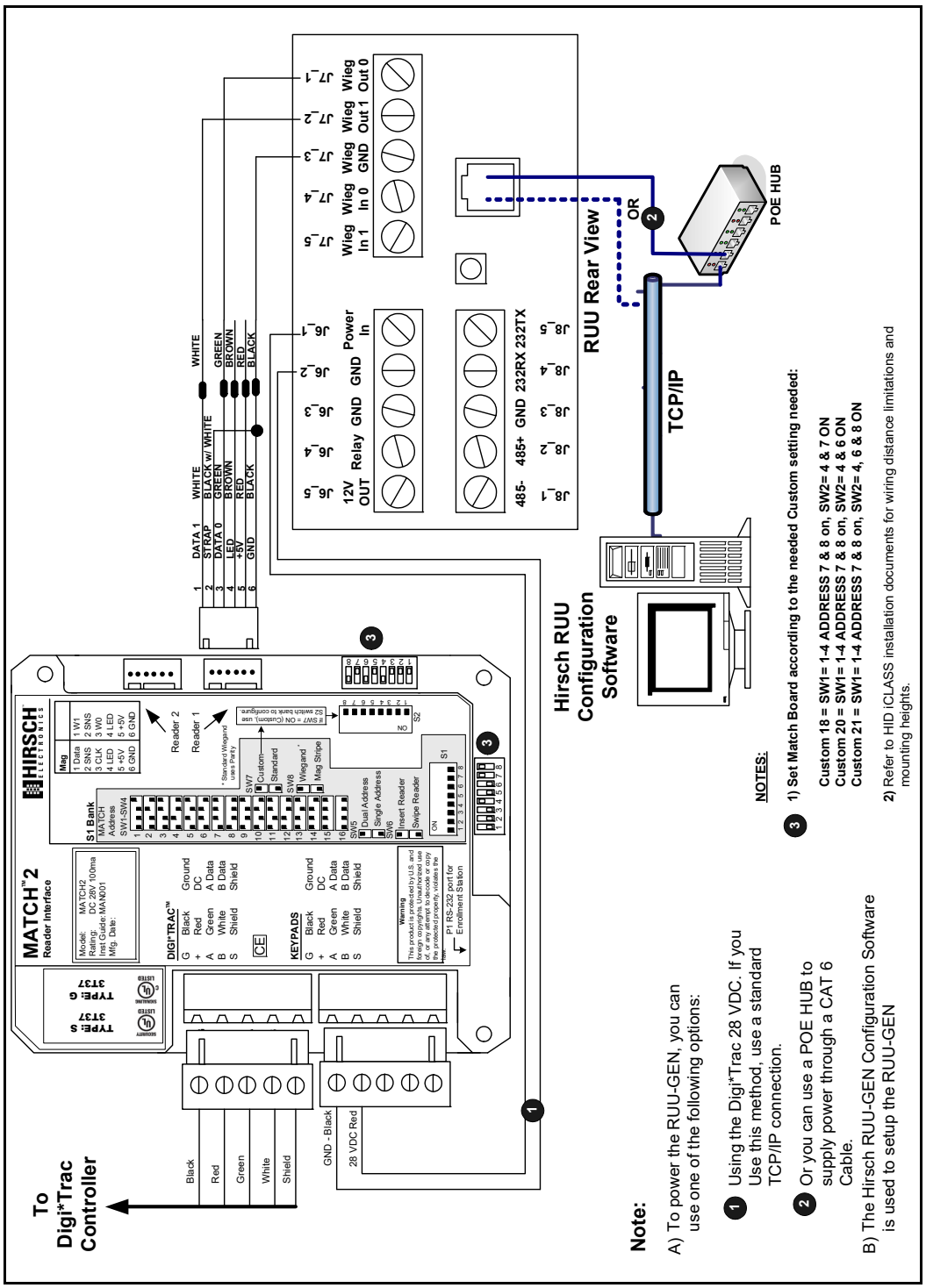
Hirsch CAC Biometric SmartCard Reader

This diagram shows wiring and settings for the Hirsch CAC Biometric SmartCard Reader, model CR-BIO-RUU-CAC. This can be powered by either the Hirsch DIGIT*TRAC controller or PoE hub.



Hirsch GEN Biometric SmartCard Reader

This diagram shows wiring and settings for the Hirsch GEN Biometric SmartCard Reader, model CR-BIO-RUU-GEN. This can be powered by either the Hirsch DIGIT*TRAC controller or PoE hub.



Cogent Smart Card Readers

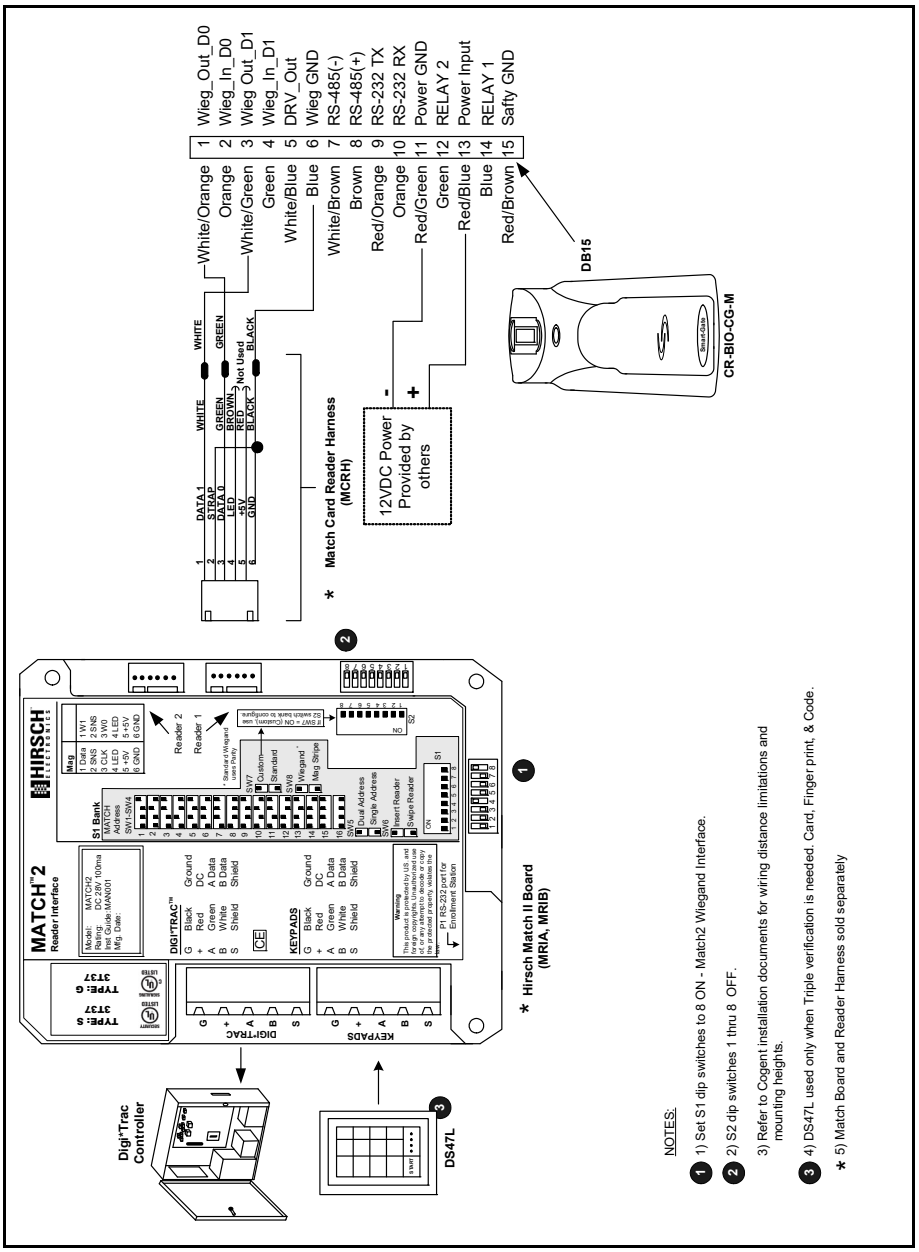
This section give diagrams for wiring and MATCH2 DIP switch settings for the following SmartCard readers:

❑ "Cogent MIFARE Fingerprint Smart Card Reader" on page 7-249

❑ "Cogent MIFARE External Fingerprint Smart Card Reader" on page 7-250

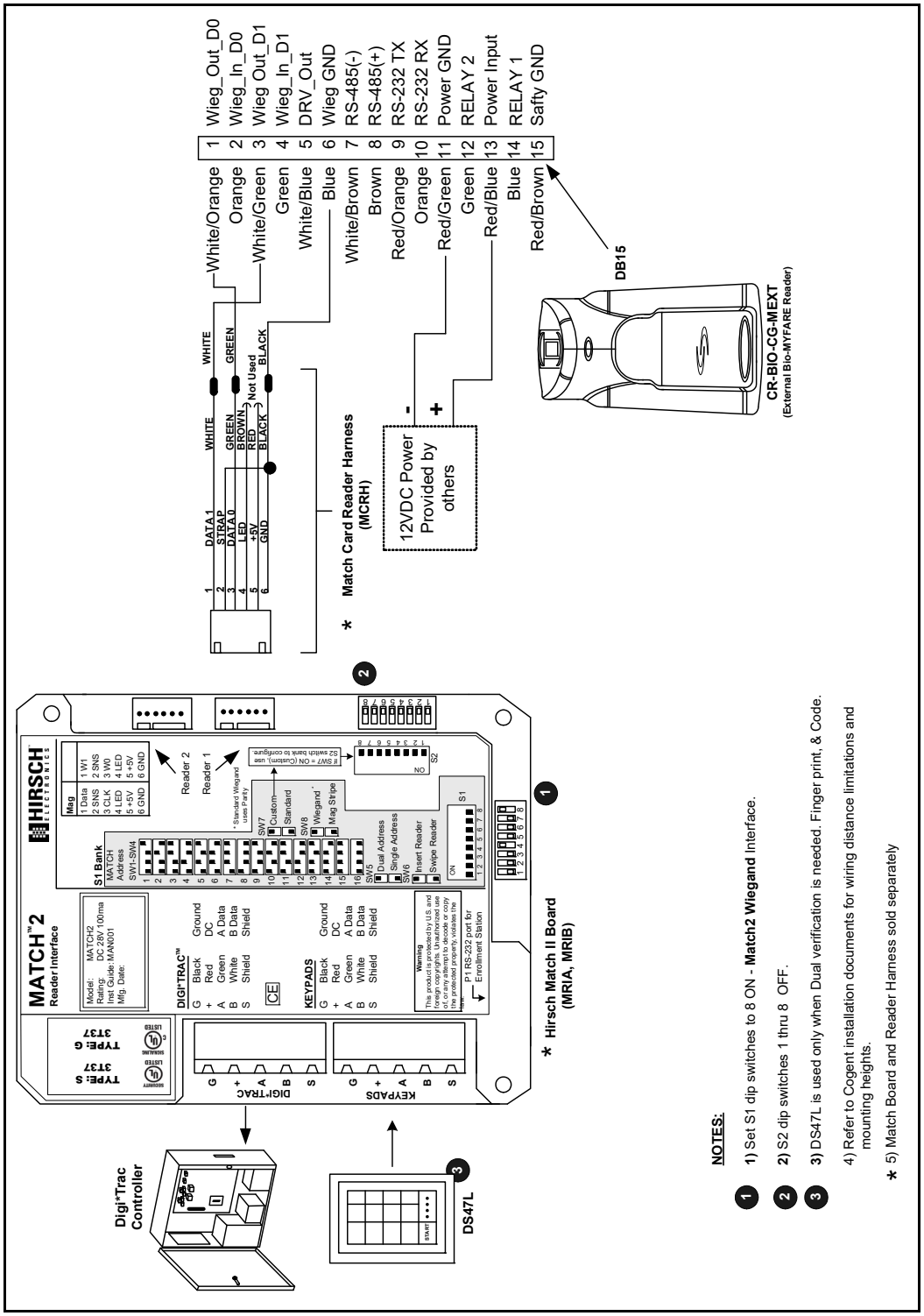
Cogent MIFARE Fingerprint Smart Card Reader

This diagram shows wiring and settings for the Cogent MIFARE Fingerprint SmartCard Reader, model CR-BIO-CG-M.



Cogent MIFARE External Fingerprint Smart Card Reader

This diagram shows wiring and settings for the Cogent MIFARE External Fingerprint Smart Card Reader, model CR-BIO-CG-MEXT.

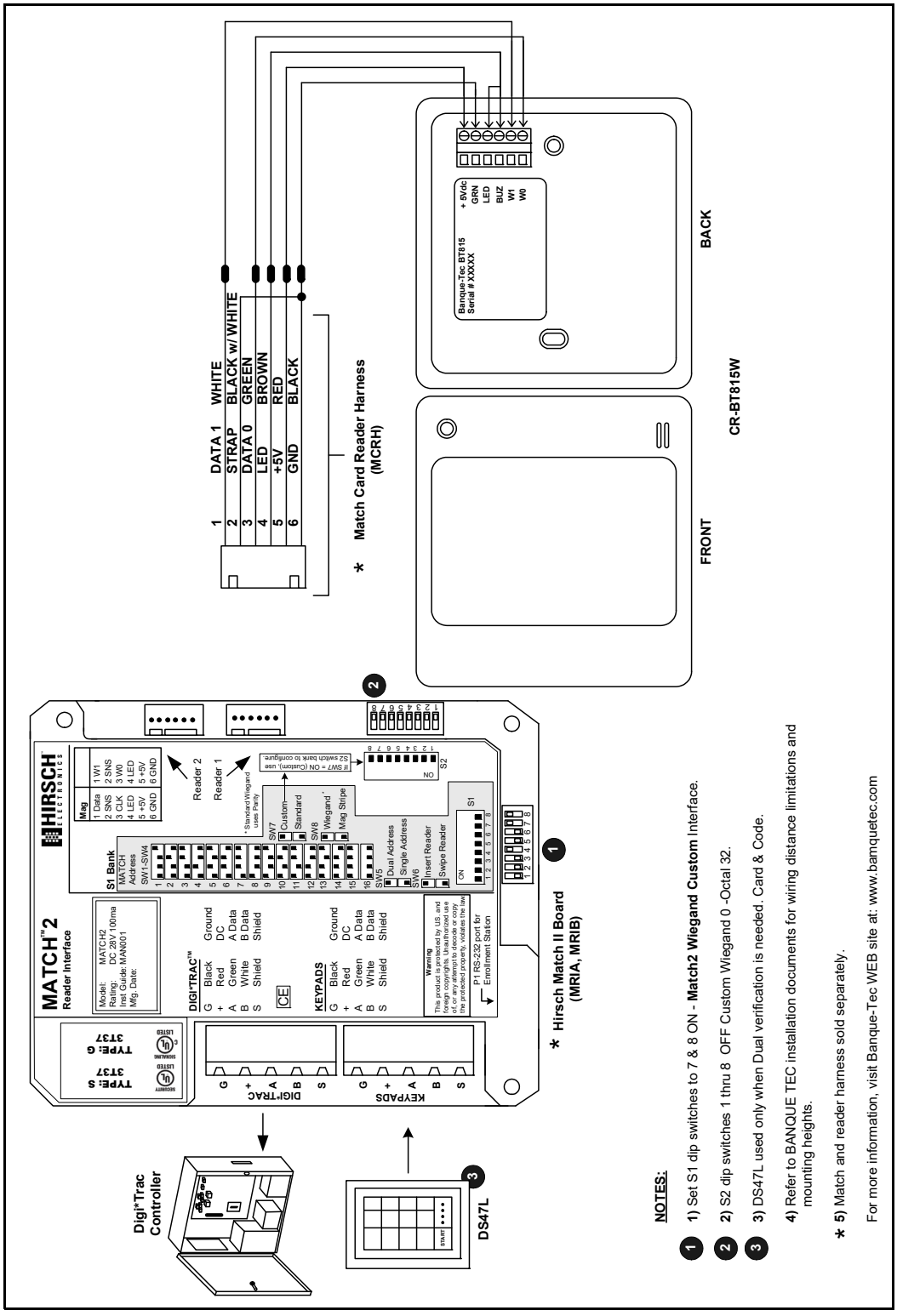


BanqueTec Smart Card Readers

This section give diagrams for wiring and Match2 DIP switch settings for the following SmartCard readers:

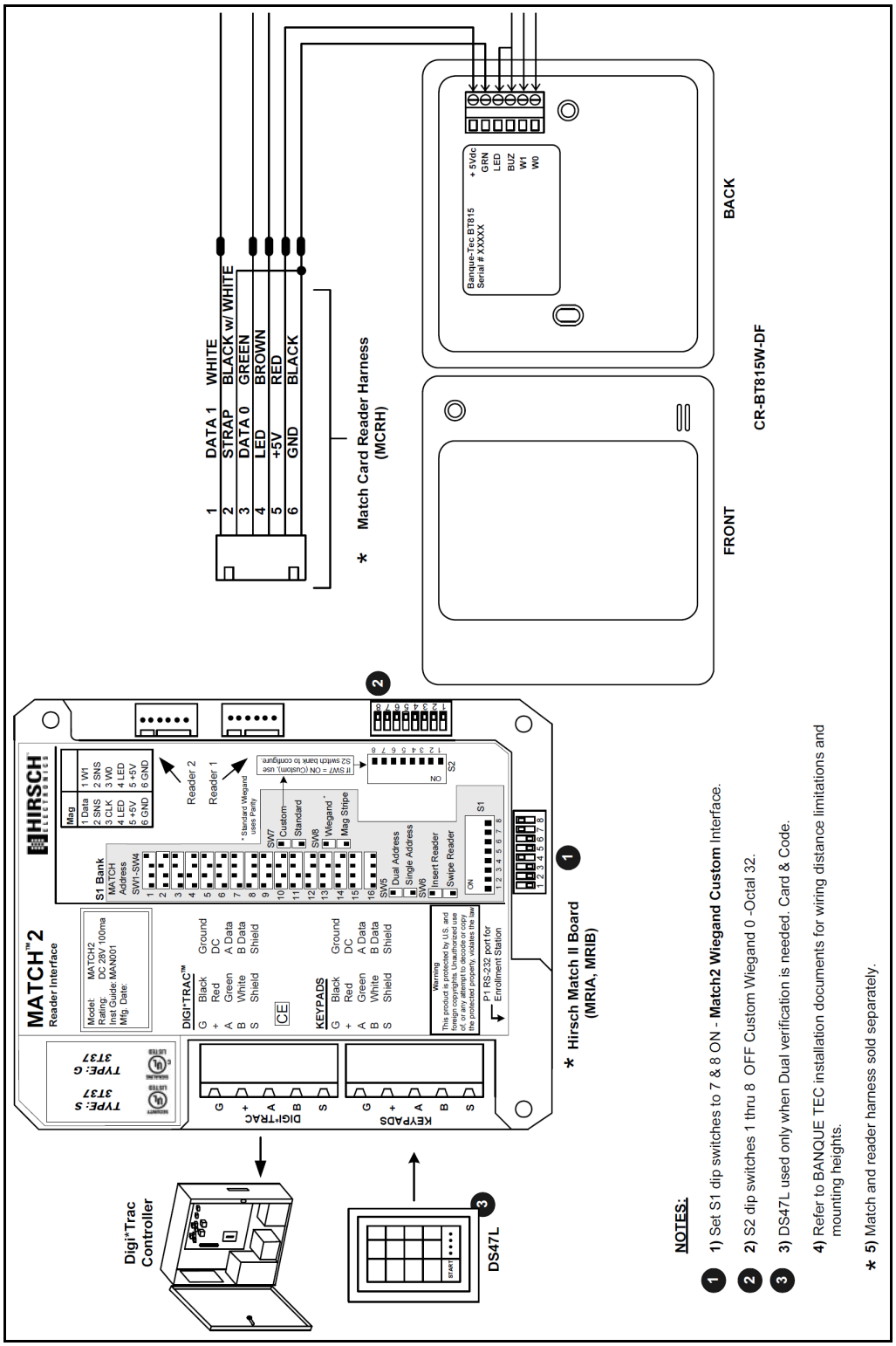
BQT MIFARE Smart Card Reader

This diagram shows wiring and settings for the BQT MIFARE Smart Card Reader, model CR-BT815W. This smartcard reader is compliant with Wiegand cards and readers.



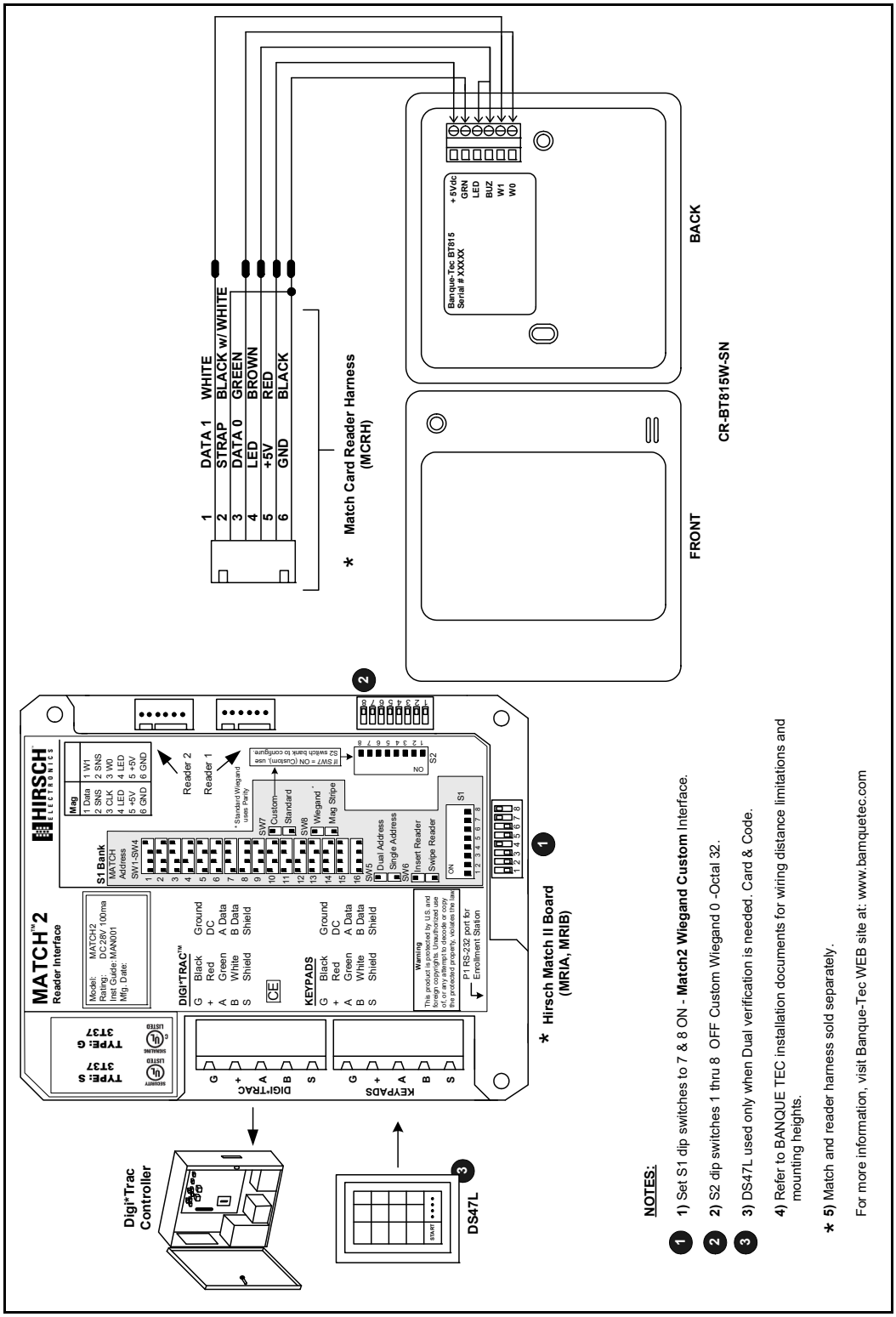
BQT DESFire Smart Card Reader

This diagram shows wiring and settings for the BQT DESFire SmartCard Reader, model CR-BT815W-DF.



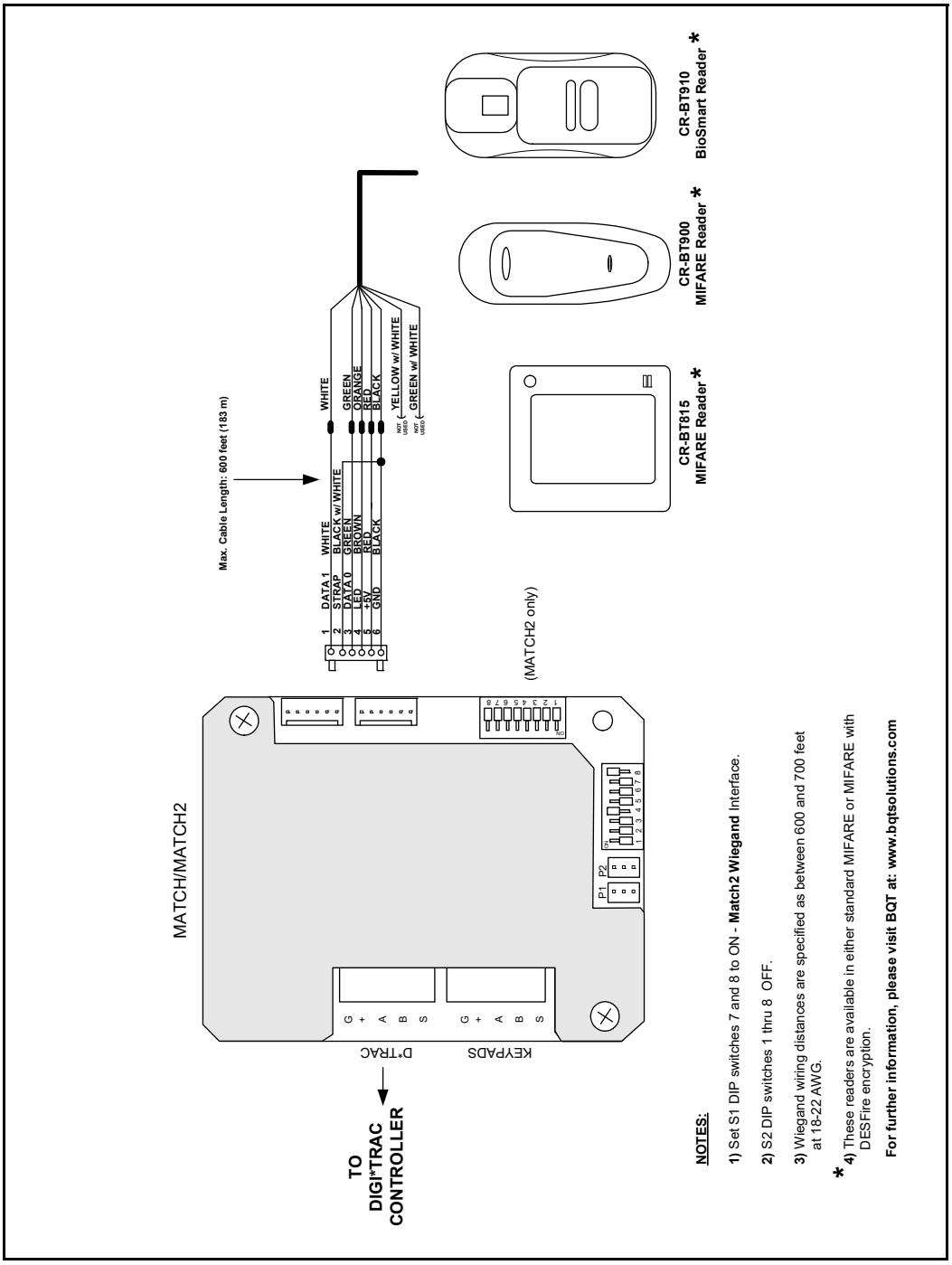
BQT DESFire/MIFARE Smart Card Reader

This diagram shows wiring and settings for the BQT DESFire/MIFARE SmartCard Reader, model CR-BT815W-SN.



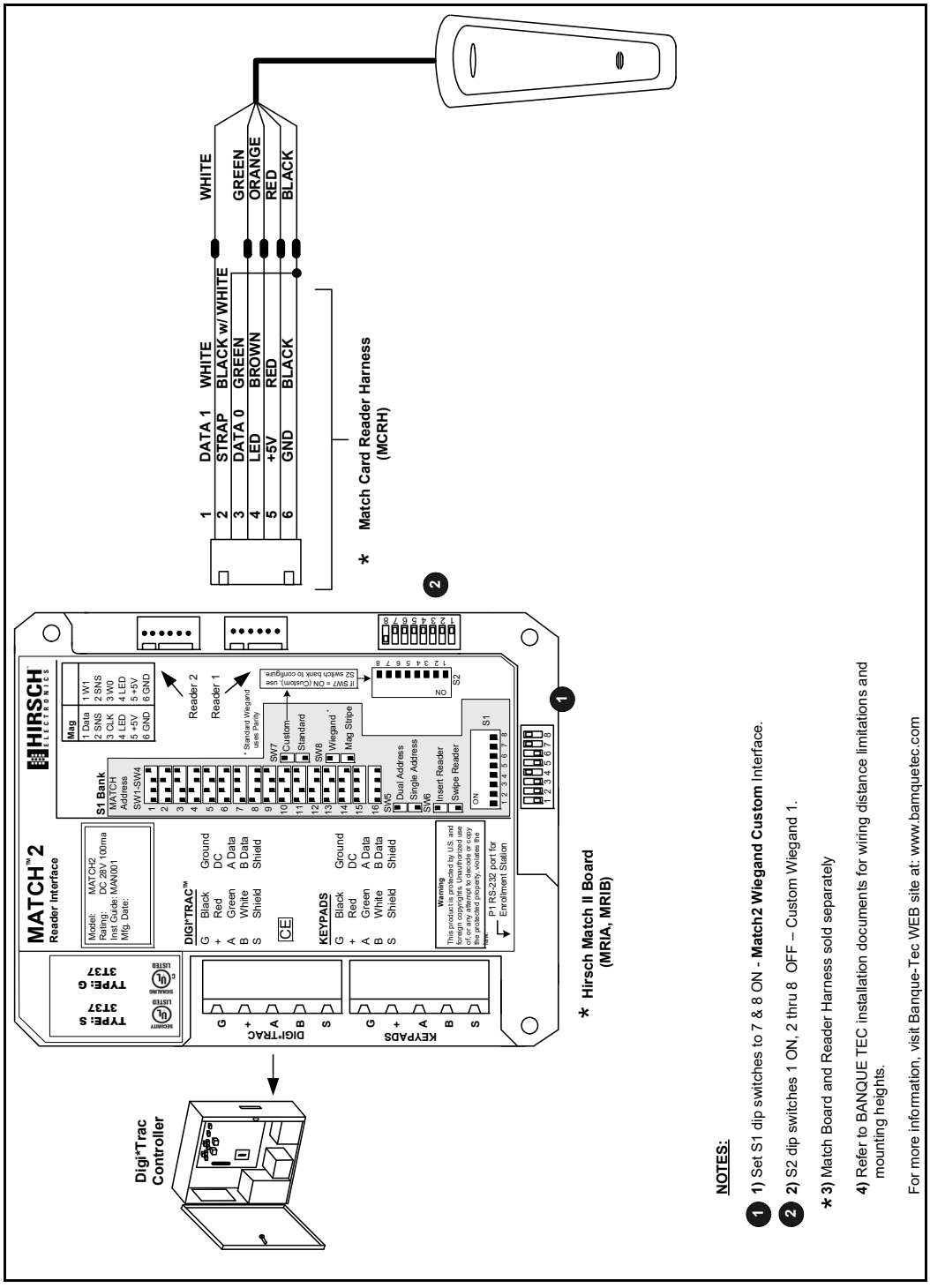
BQT MIFARE Contactless Smart Card Readers

This diagram shows wiring and settings for the BQT MIFARE Contactless SmartCard Readers, models CR-BT815, CR-BT900, and CR-BT910.



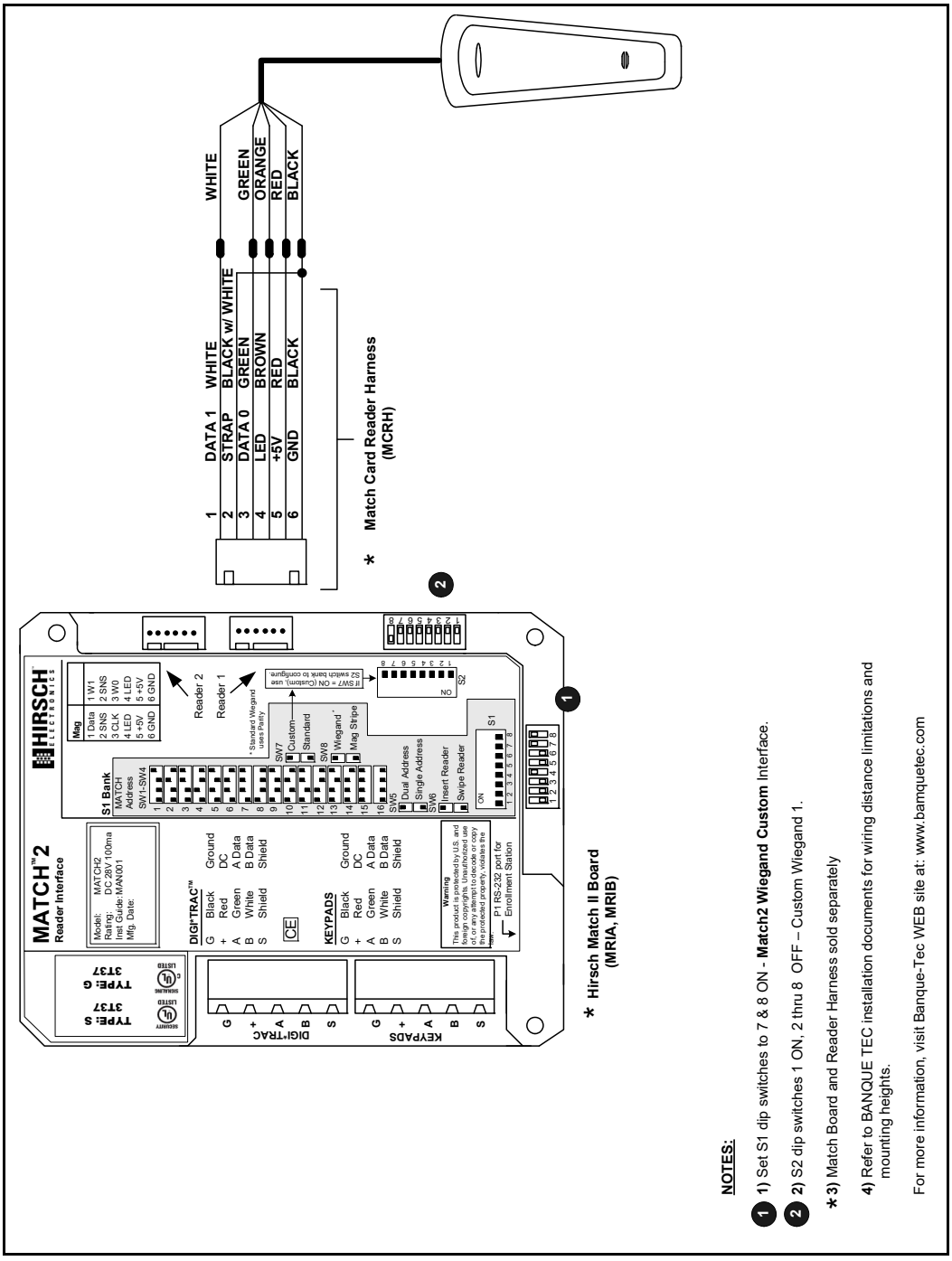
BQT BT900 DESFire Smart Card Reader

This diagram shows wiring and settings for the BQT BT900 DESFire Smart Card Reader, model CR-BT900W.



BT900 DESFire Smart Card Reader

This diagram shows wiring and settings for the BT900 DESFire SmartCard Reader, model CR-BT900W-DF.



NOTES:

1. **1)** Set S1 dip switches to 7 & 8 ON - **Match2 Wiegand Custom** Interface.
2. **2)** S2 dip switches 1 ON, 2 thru 8 OFF – Custom Wiegand 1.

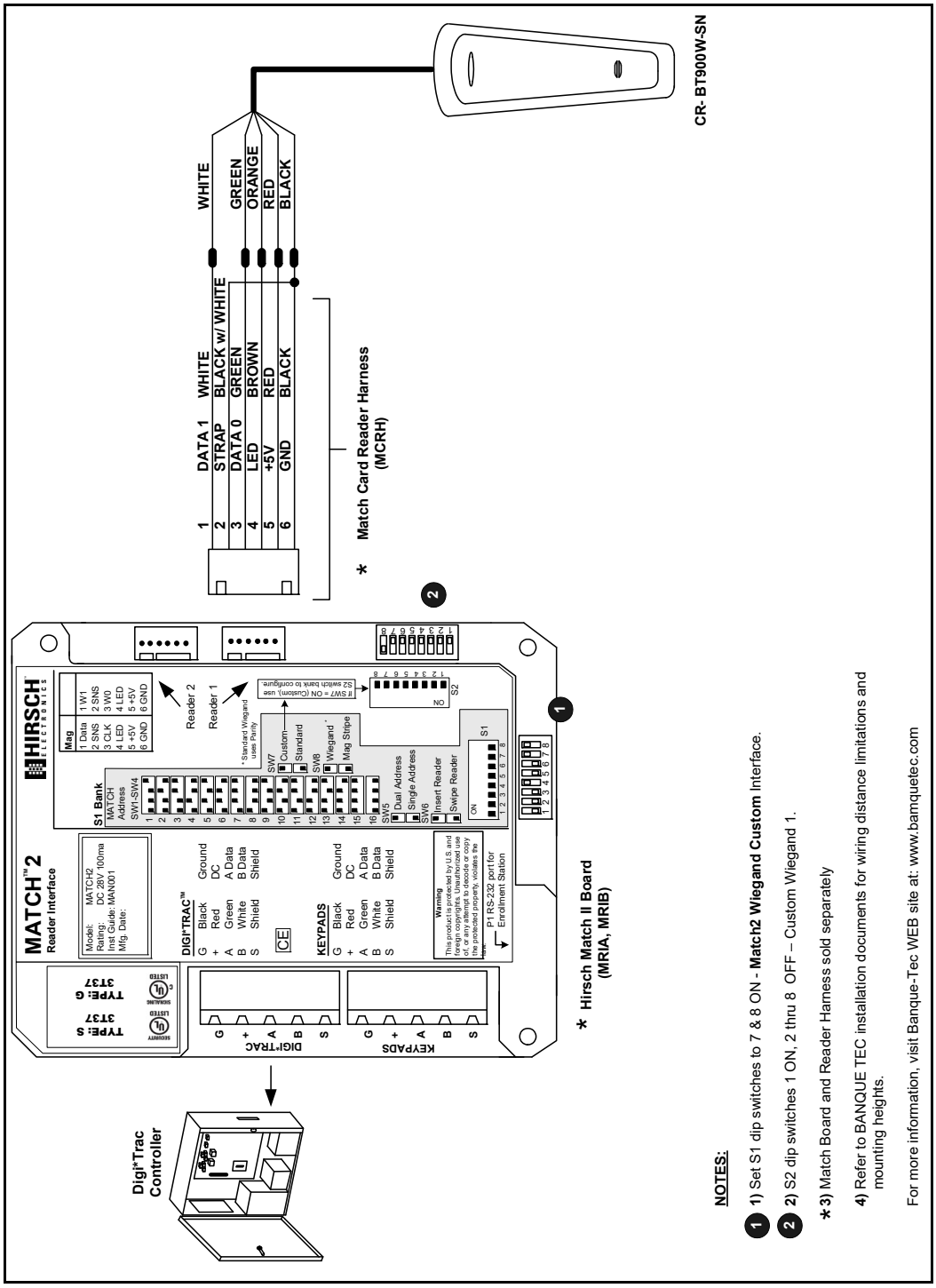
***3)** Match Board and Reader Harness sold separately

4) Refer to BANQUE TEC installation documents for wiring distance limitations and mounting heights.

For more information, visit Banque-Tec WEB site at: www.bamquetec.com

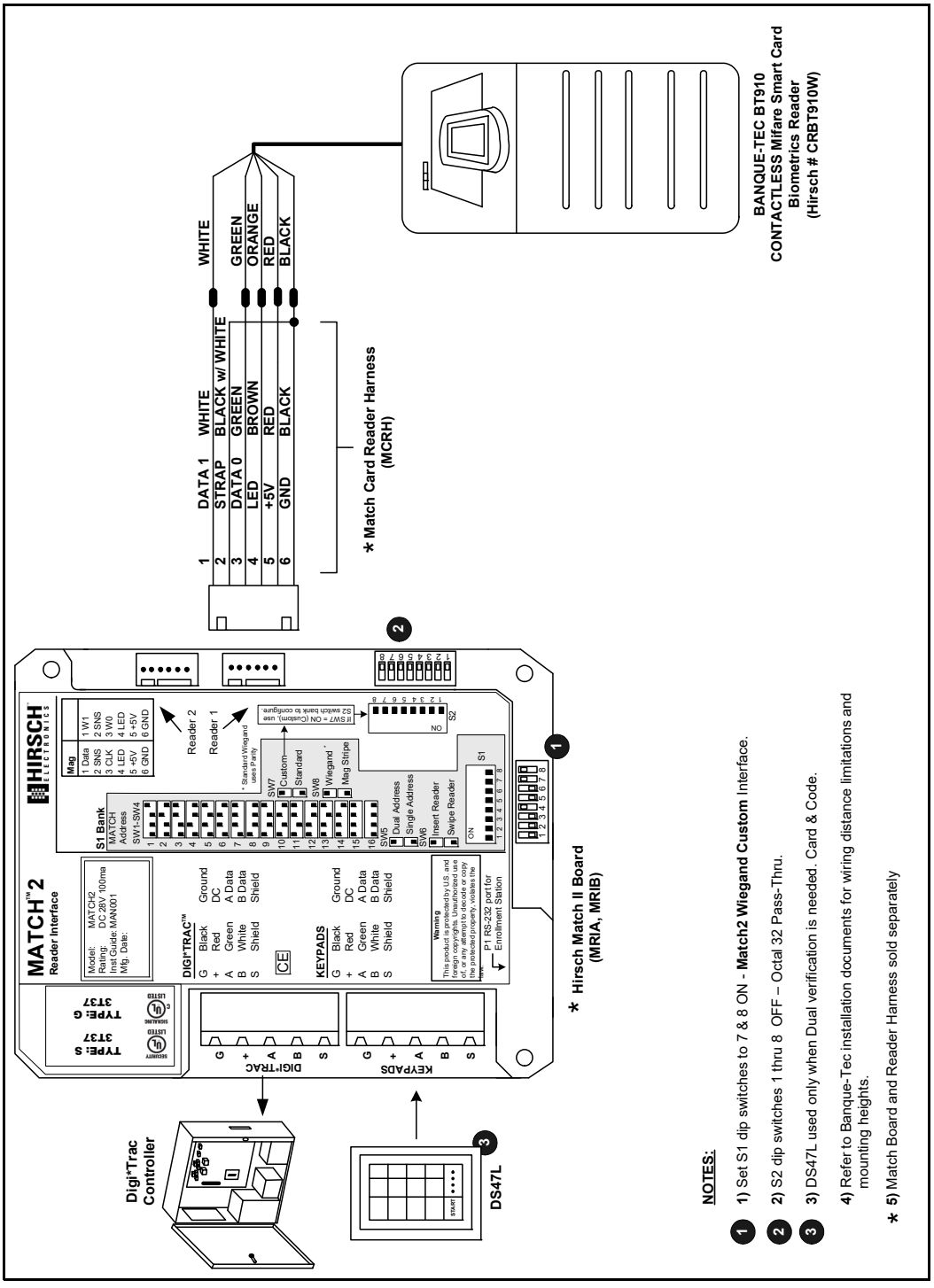
BT900 DESFire/MIFARE Smart Card Reader

This diagram shows wiring and settings for the BT900 DESFire/MIFARE Smart Card Reader, model CR-BT900W-SN.



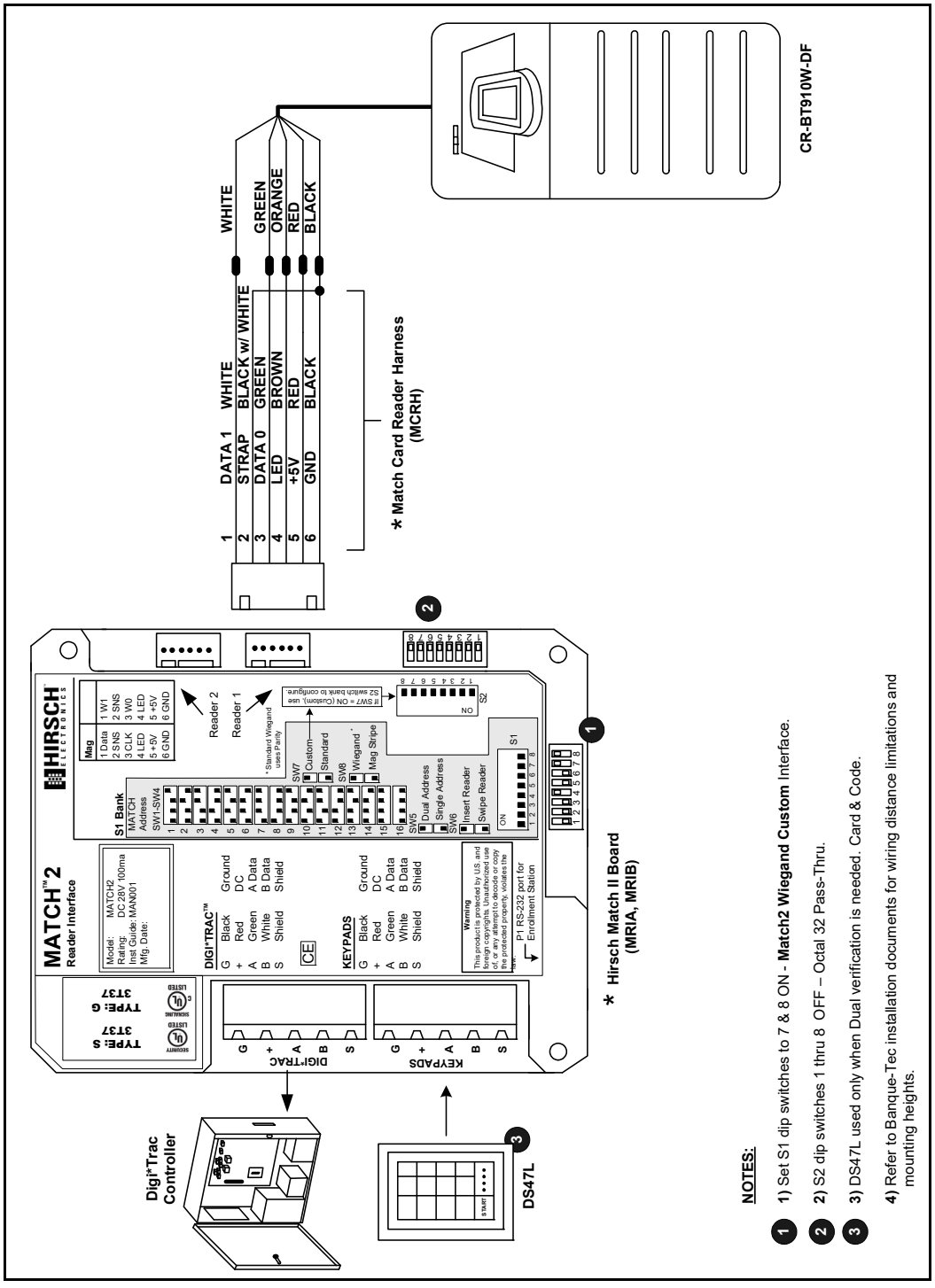
BQT BT910 MIFARE SmartCard Biometric Reader

This diagram shows wiring and settings for the BQT BT910 MIFARE Smart Card Biometric Reader, model CR-BT910W.



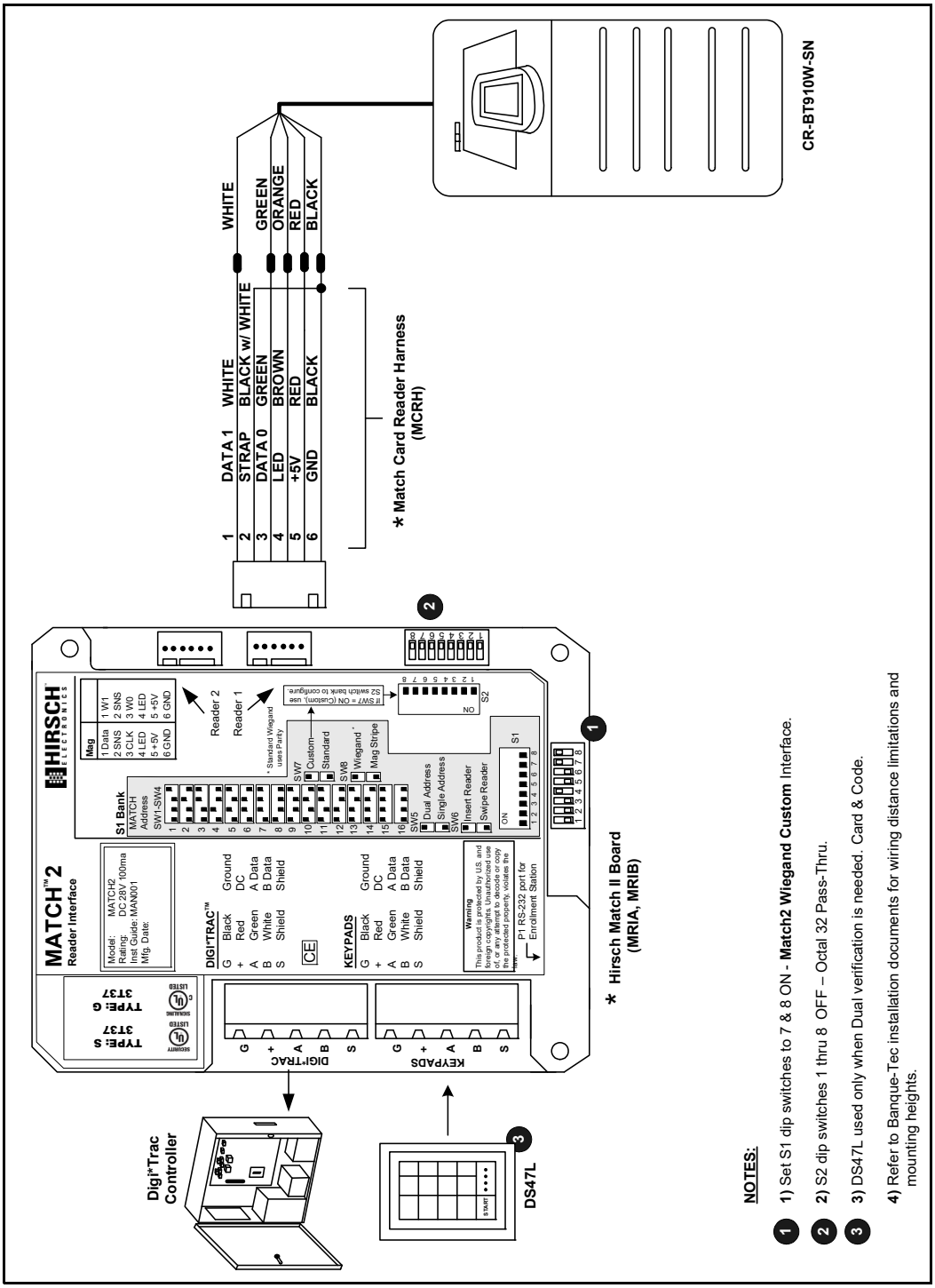
BQT DESFire Smart Card Biometric Reader

This diagram shows wiring and settings for the BQT DESFire SmartCard Biometric Reader, model CR-BT910W-DF.



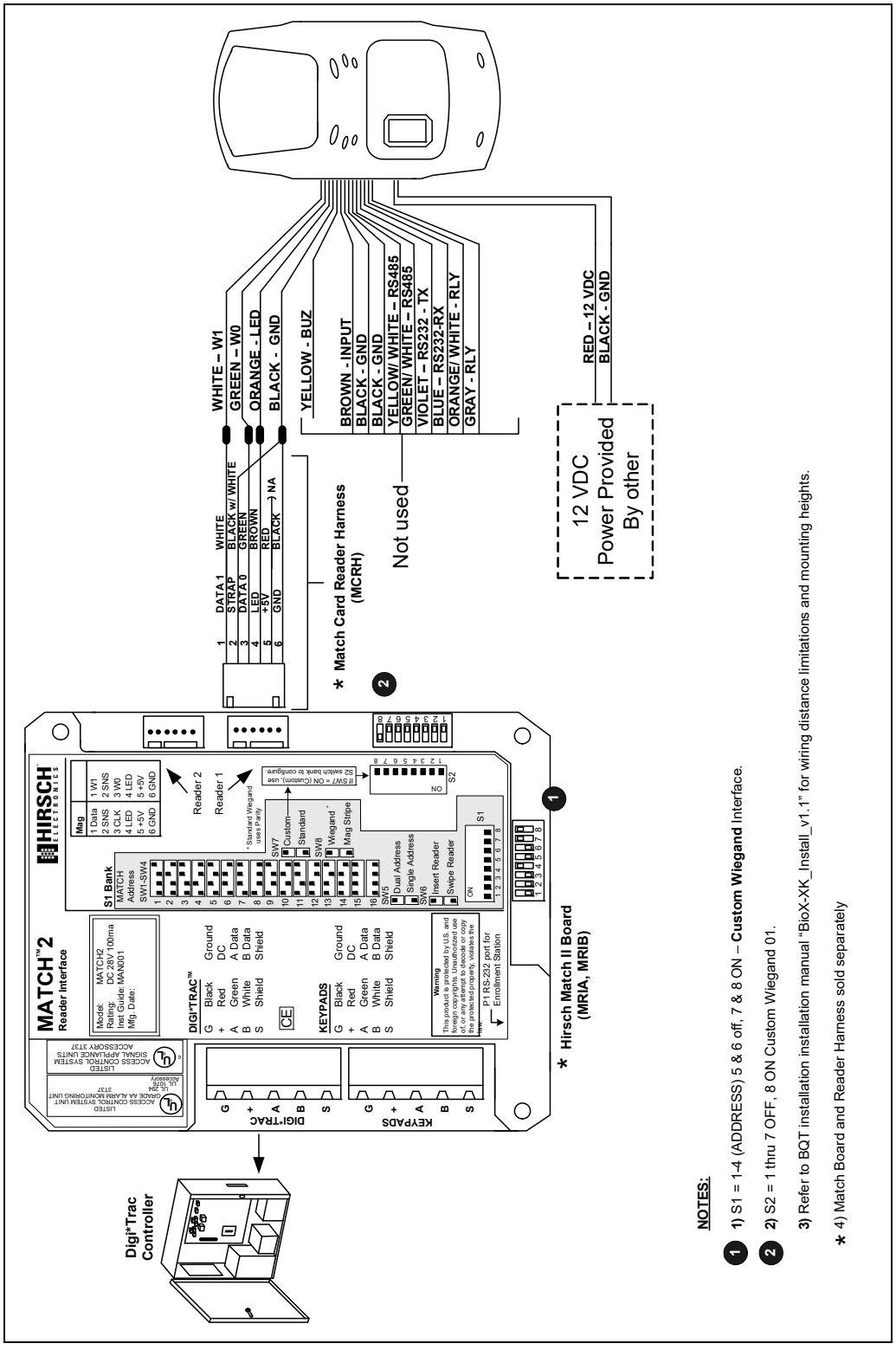
BQT DESFire/MIFARE Smart Card Biometric Reader

This diagram shows wiring and settings for the BQT DESFire/MIFARE SmartCard Biometric Reader, model CR-BT910W-SN.



BQT Smart Card Biometric Reader

This diagram shows wiring and settings for the BQT SmartCard Biometric Reader, model CR-BT910X.

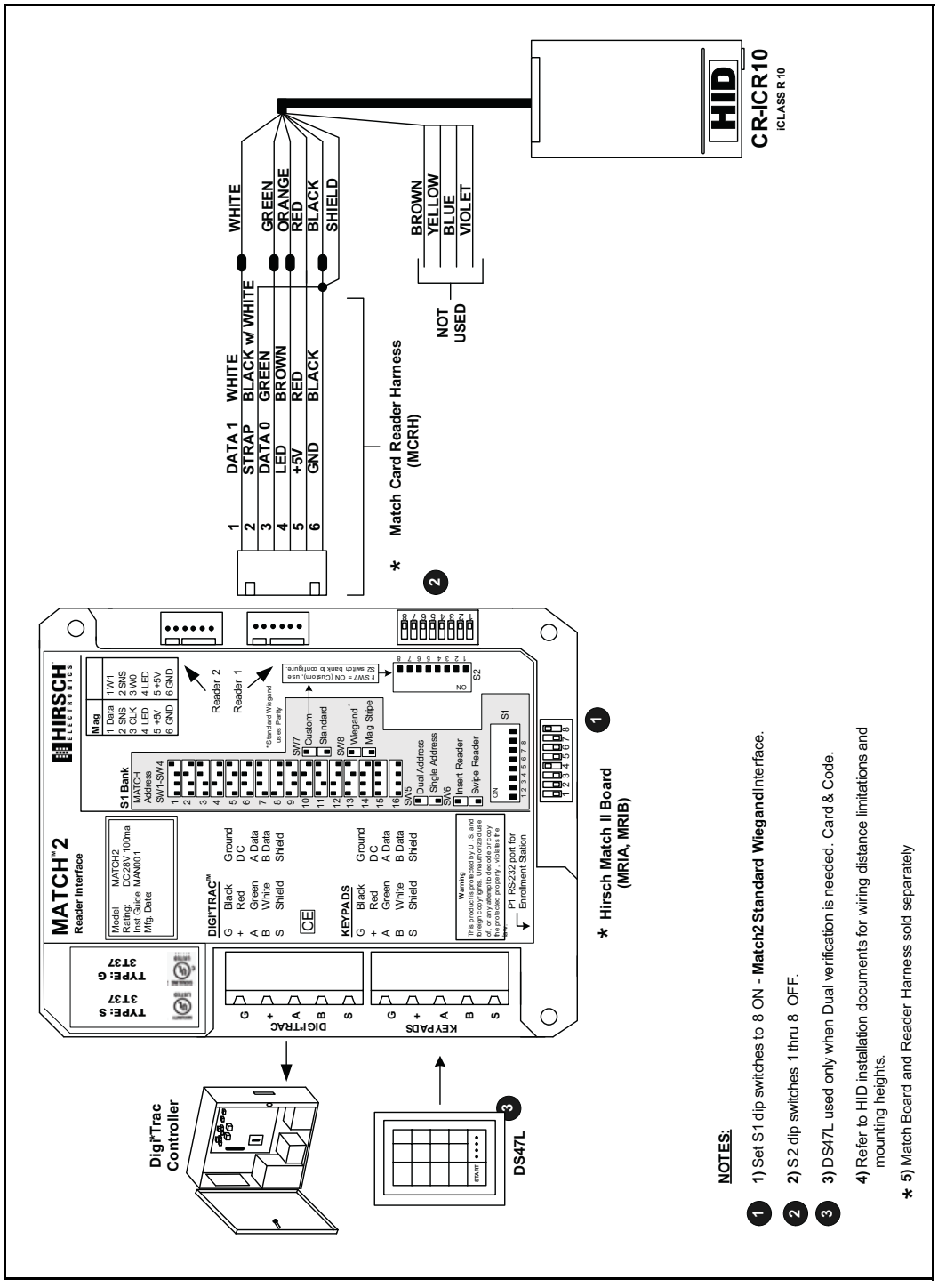


HID iClass Smart Card Readers

This section give diagrams for wiring and Match2 DIP switch settings for HID iClass Smart Card readers.

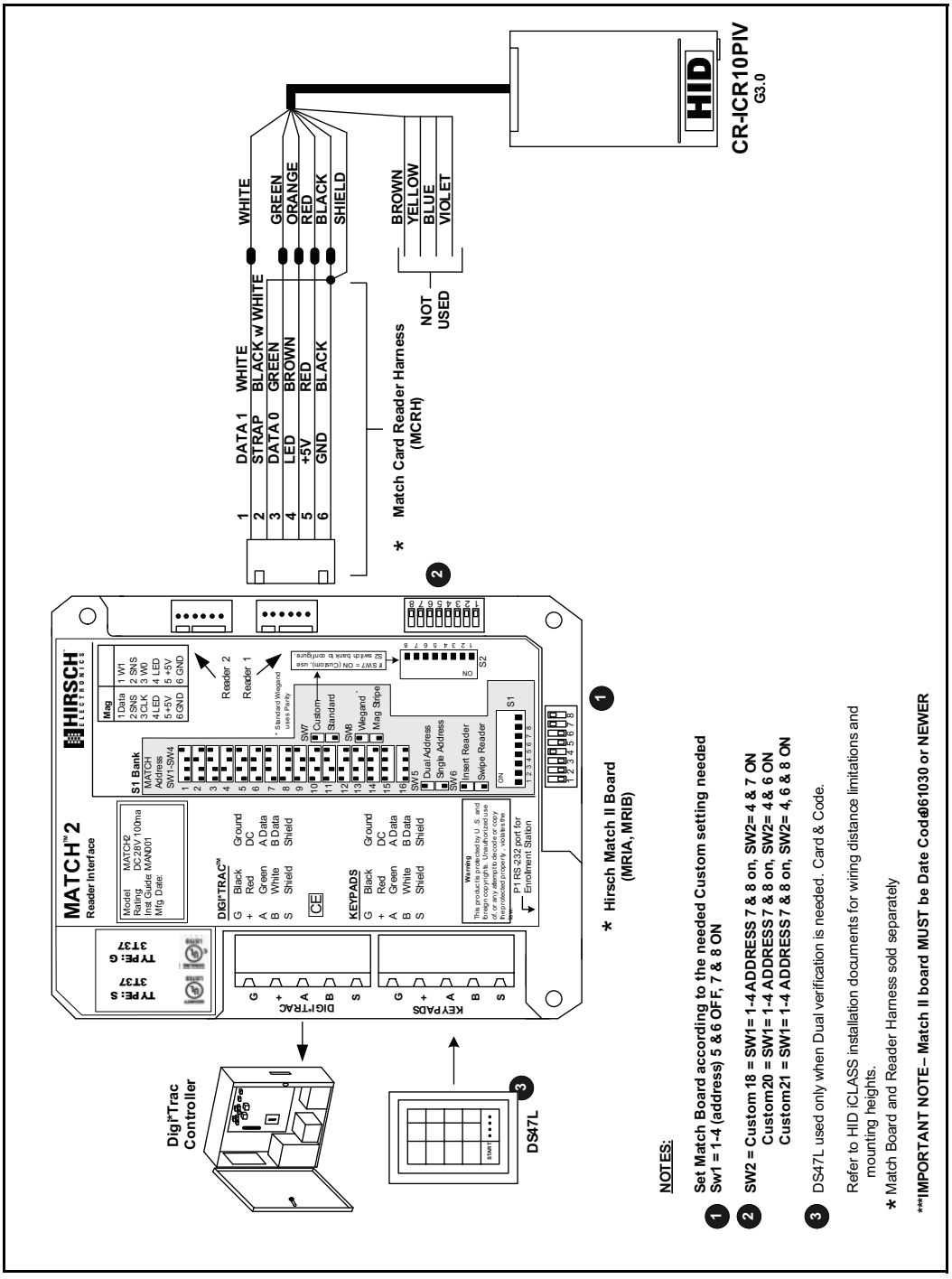
HID iClass Contactless Smart Card Reader

This diagram shows wiring and settings for the HID iClass Contactless Smart Card Reader, model CR-ICR10.



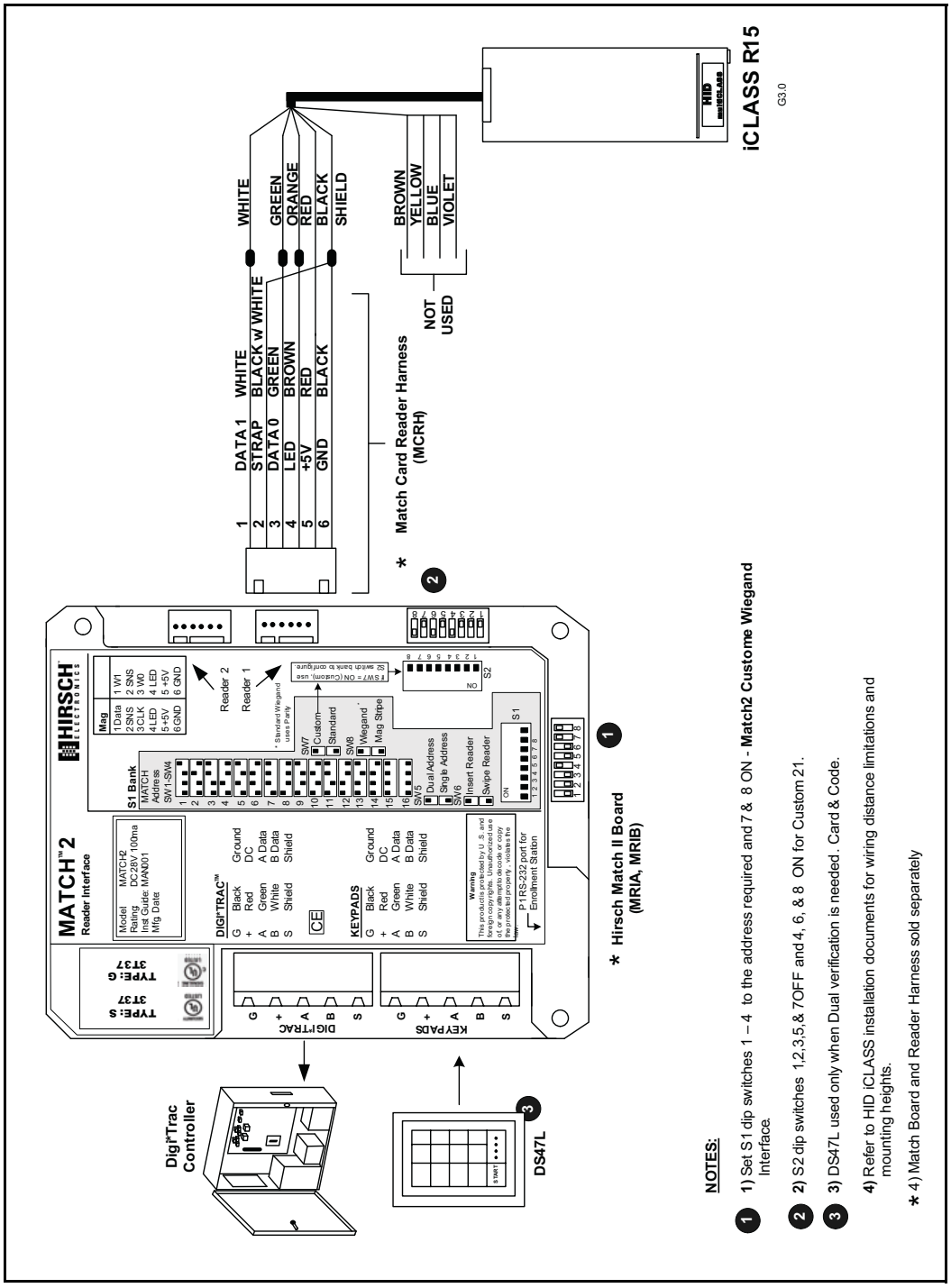
HID iClass PIV/DESFire Contactless Smart Card Reader

This diagram shows wiring and settings for the HID iClass PIV/DESFire Contactless Smart Card Reader, model CR-ICR10PIV. This device reads FIPS 201 PIV, DESFire FASC-N, and HID iCLASS cards.



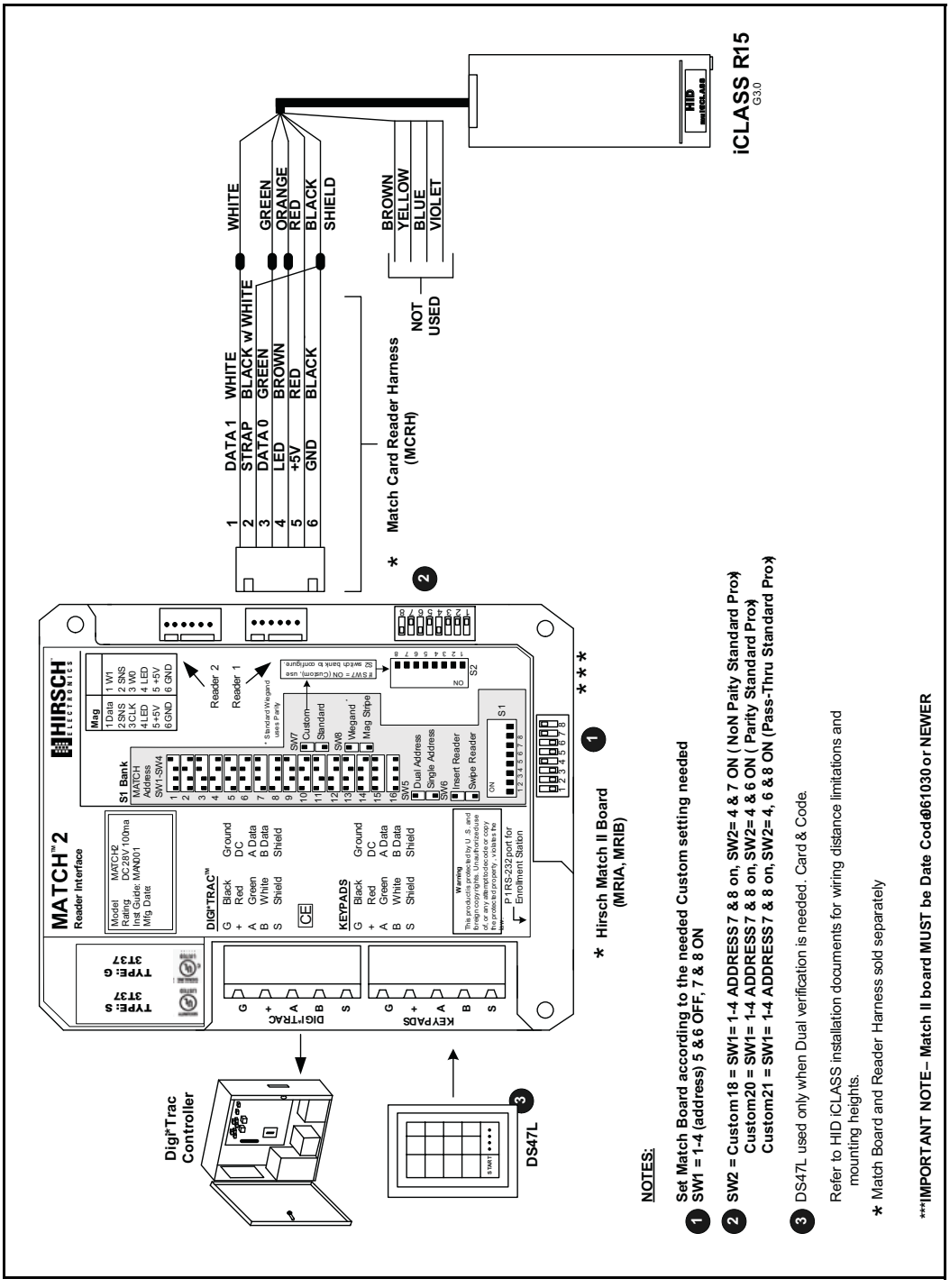
HID iClass R15 Contactless Smart Card Reader

This diagram shows wiring and settings for the HID iClass R15 Contactless Smart Card Reader, model CR-ICR15.



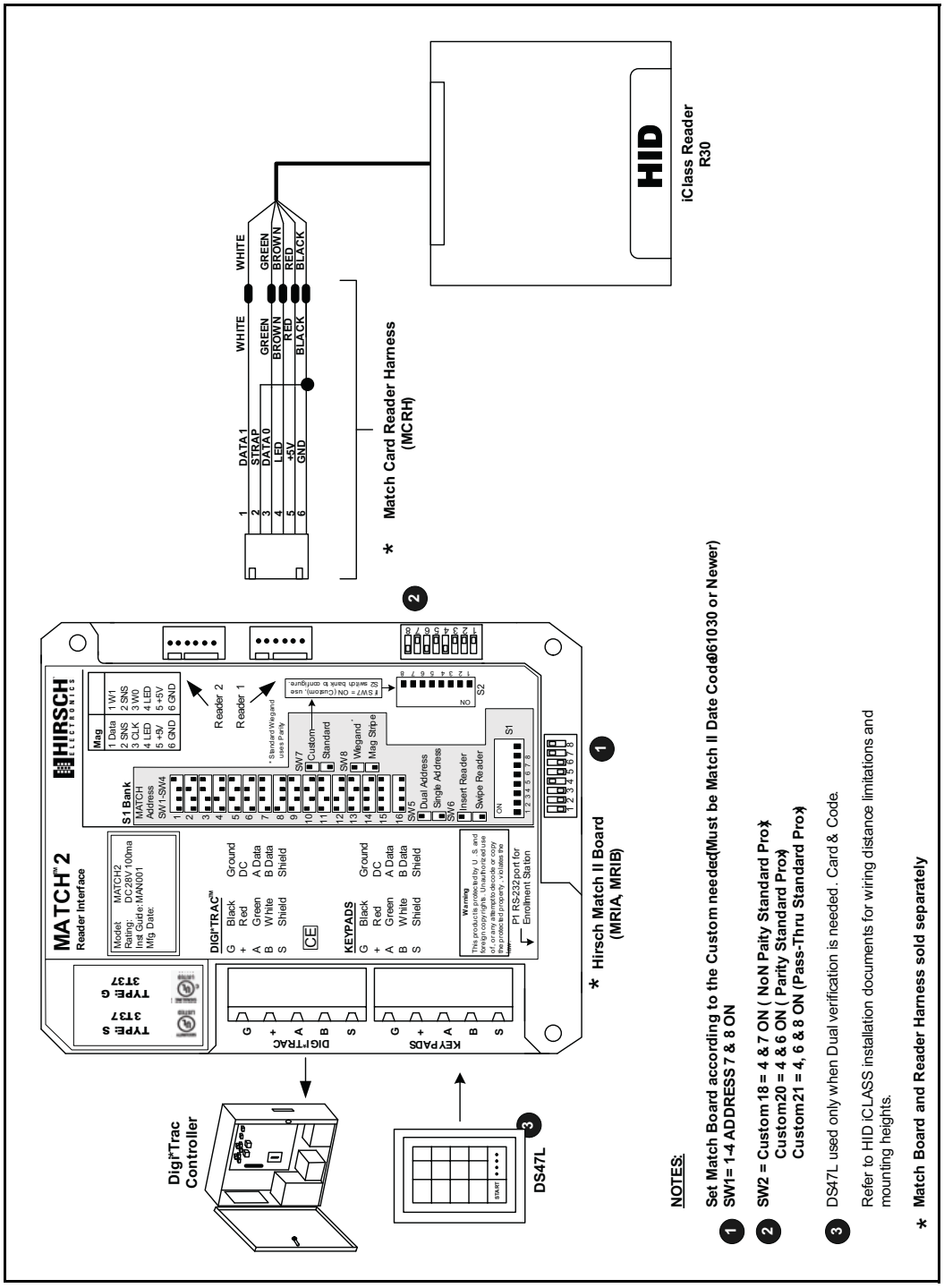
HID iClass/PIV R15 Contactless Smart Card Reader

This diagram shows wiring and settings for the HID iClass/PIV R15 Contactless Smart Card Reader, model CR-ICR15-PIV.



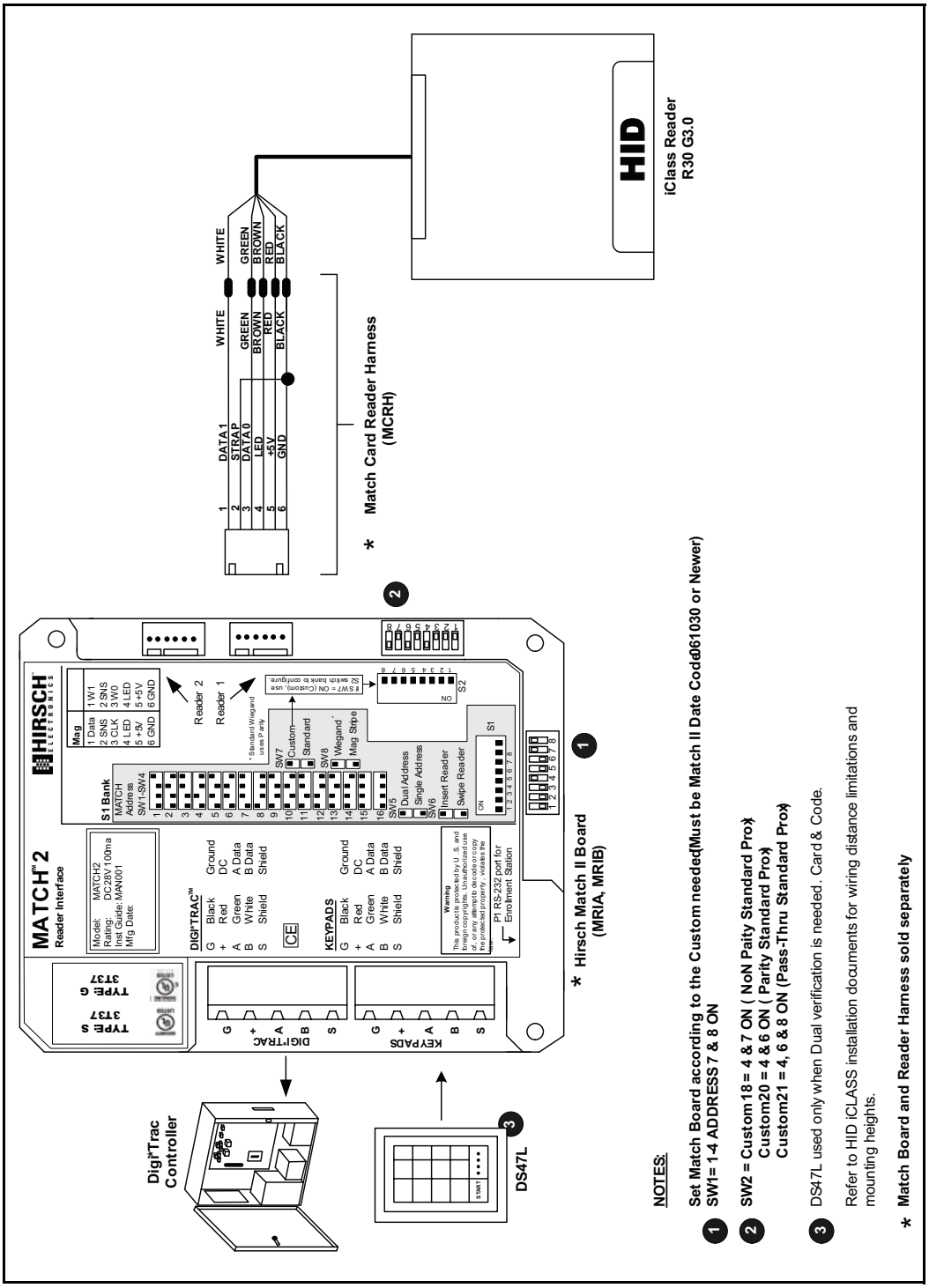
HID iClass R30 Contactless Smart Card Reader

This diagram shows wiring and settings for the HID iClass R30 Contactless Smart Card Reader, model CR-ICR30.



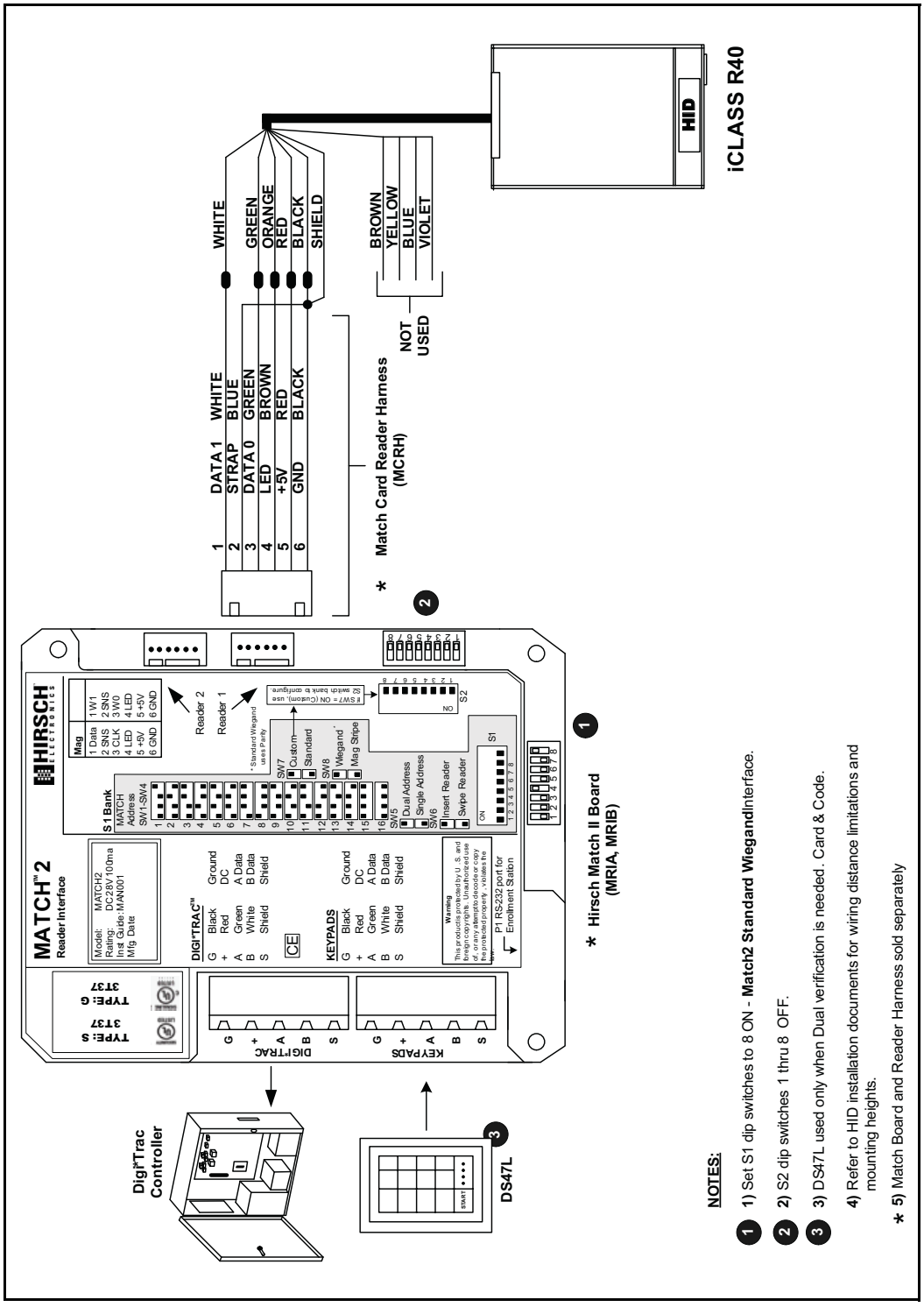
HID iClass/PIV R30 Contactless Smart Card Reader

This diagram shows wiring and settings for the HID iClass/PIV R30 Contactless Smart Card Reader, model CR-ICR30PIV.



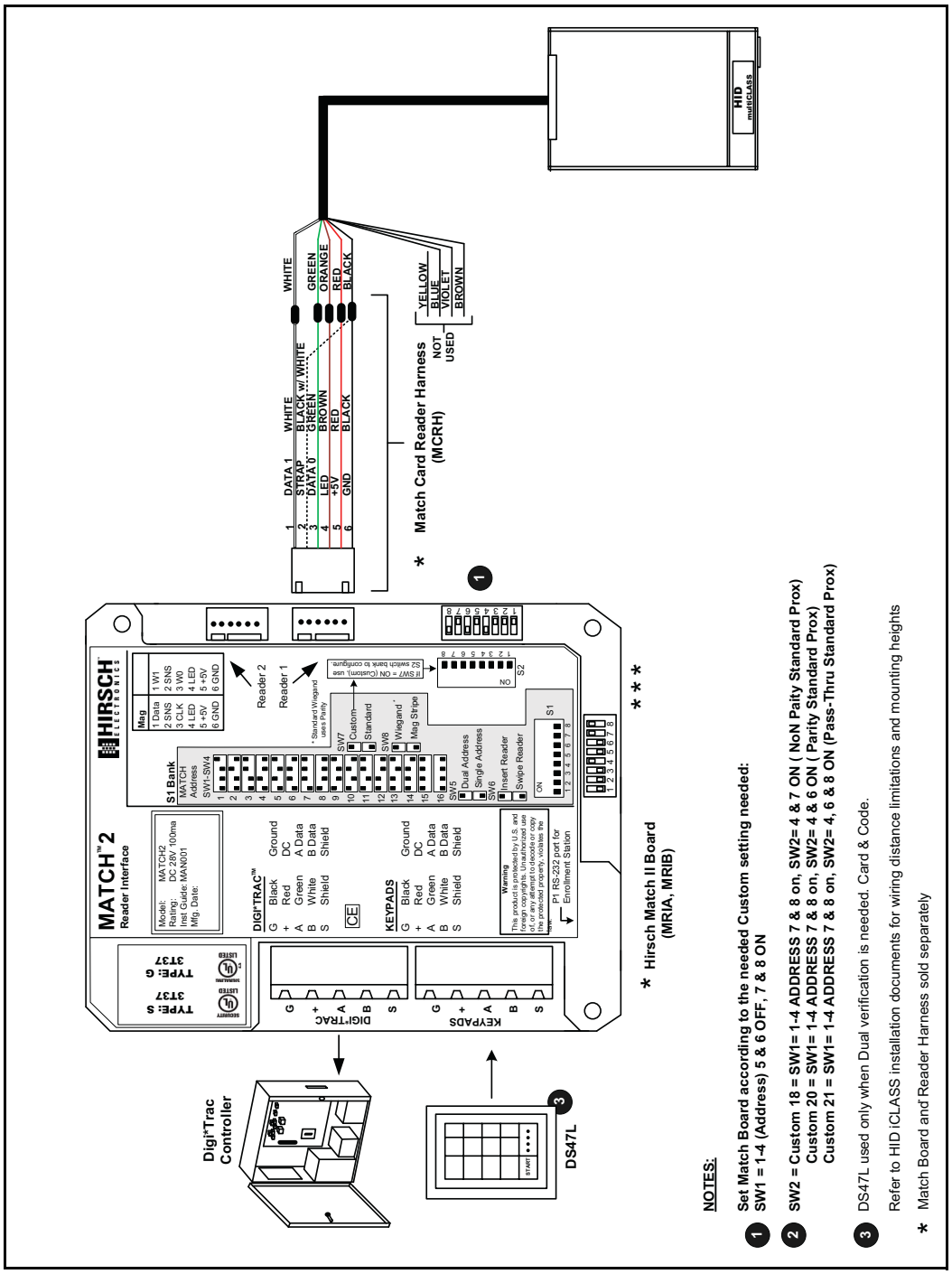
HID iClass R40 Contactless Smart Card Readers

This diagram shows wiring and settings for the HID iClass R40 Contactless Smart Card Readers, model CR-ICR40.



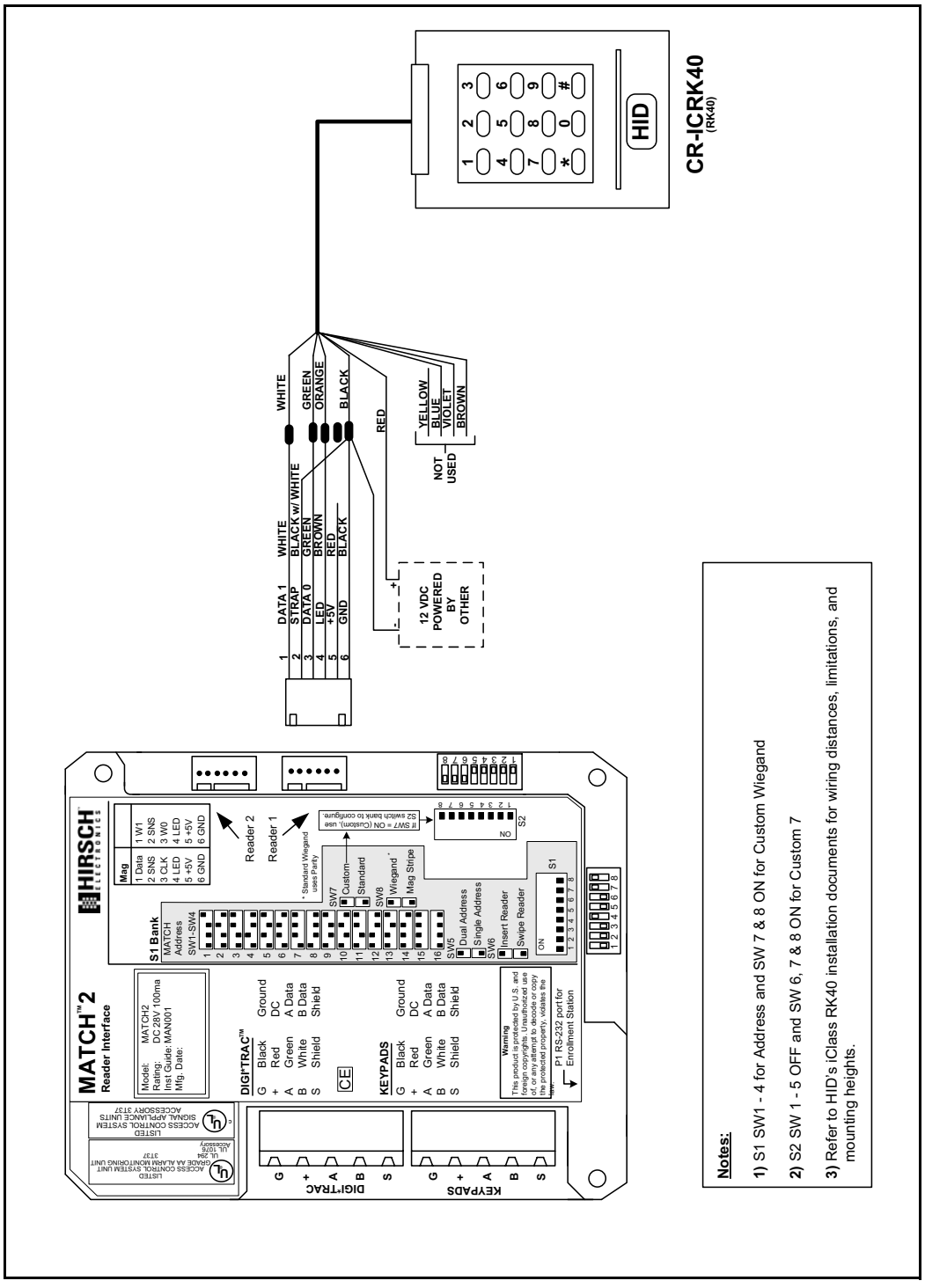
HID iClass/PIV R40 Contactless SmartCard Readers

This diagram shows wiring and settings for the HID iClass/PIV R40 Contactless Smart Card Readers, model CR-ICR40PIV.



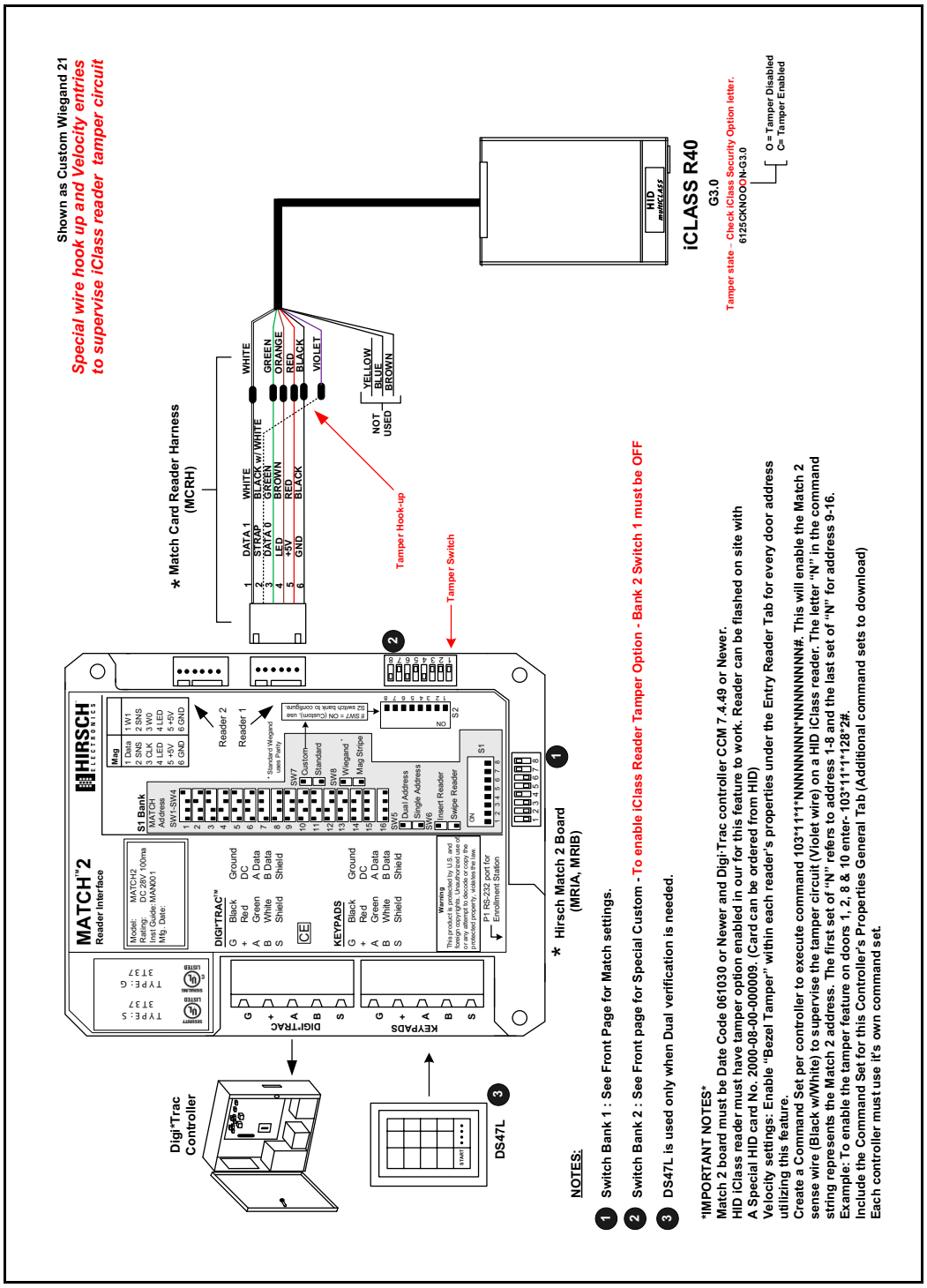
CR-ICRK40 HID RK40 iClass Prox SmartCard Reader with Keypad

This diagram shows wiring and settings for the BQT SmartCard Biometric Reader, model CR-BT910X.



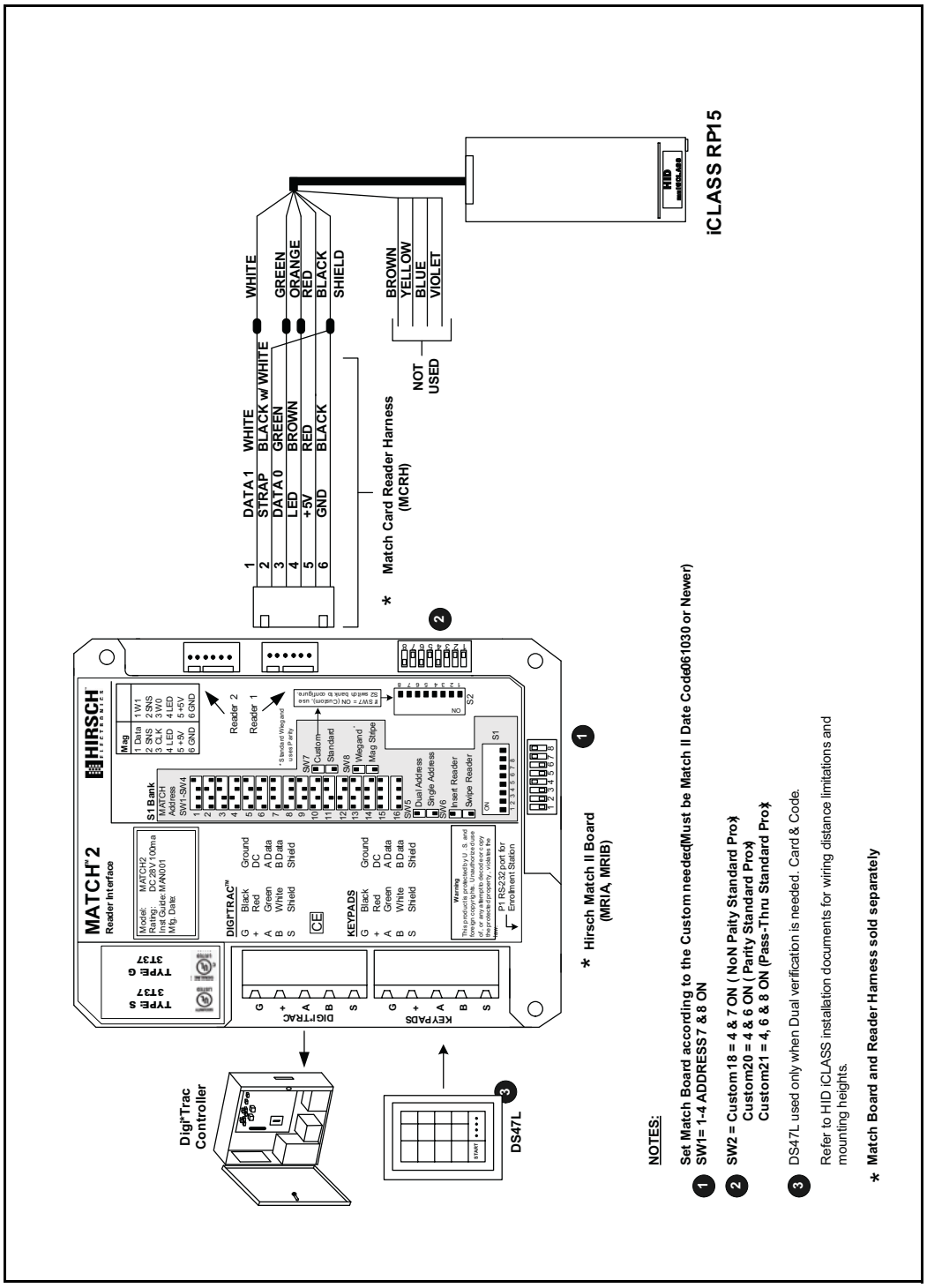
CR-ICRK40 HID PIV iClass Prox SmartCard Reader with Keypad and Special Tamper Hookup

This diagram shows wiring and settings for the CR-ICR40 with a special tamper hookup.



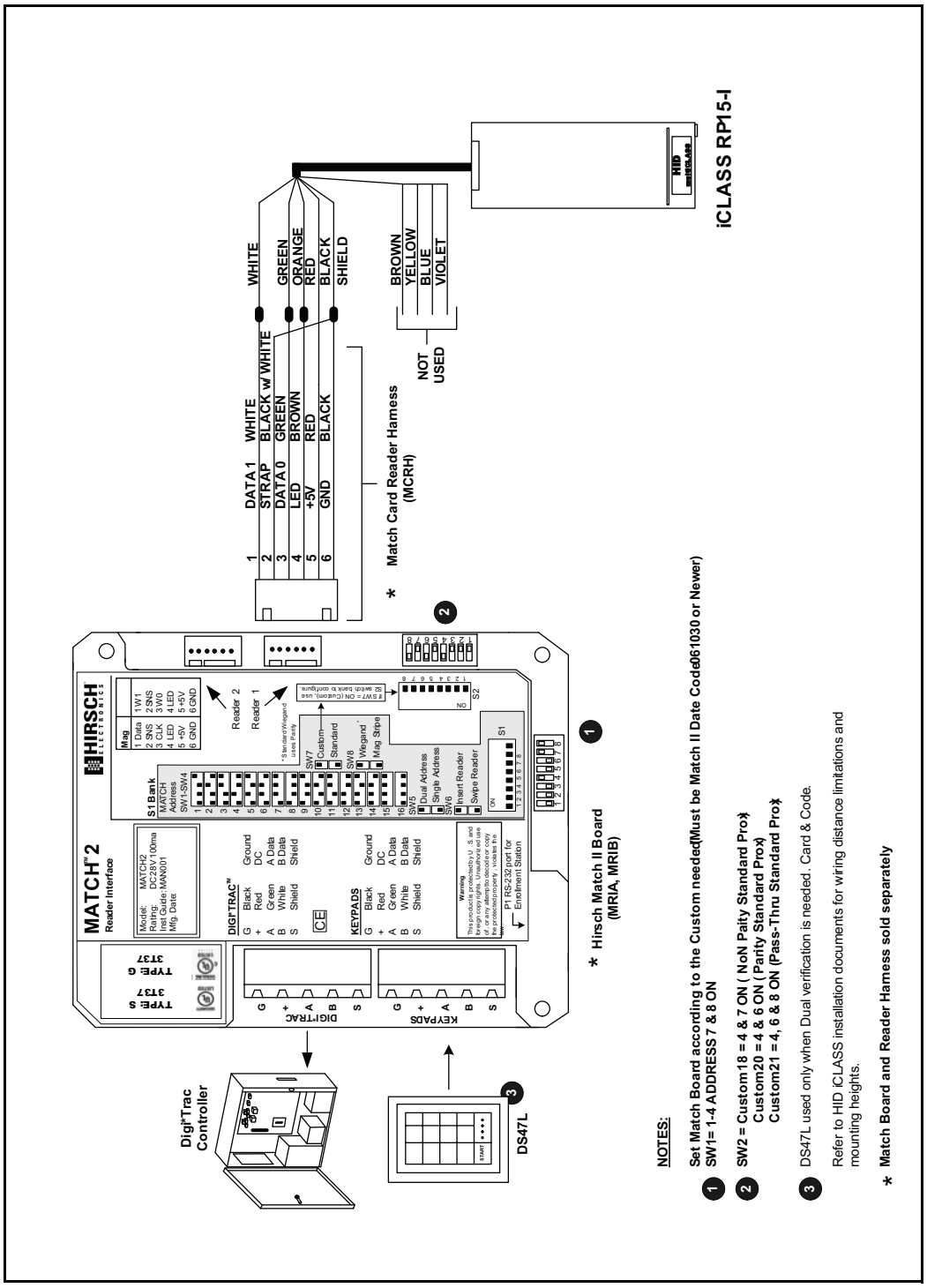
CR-ICRP15 HID RP15 iClass Prox Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



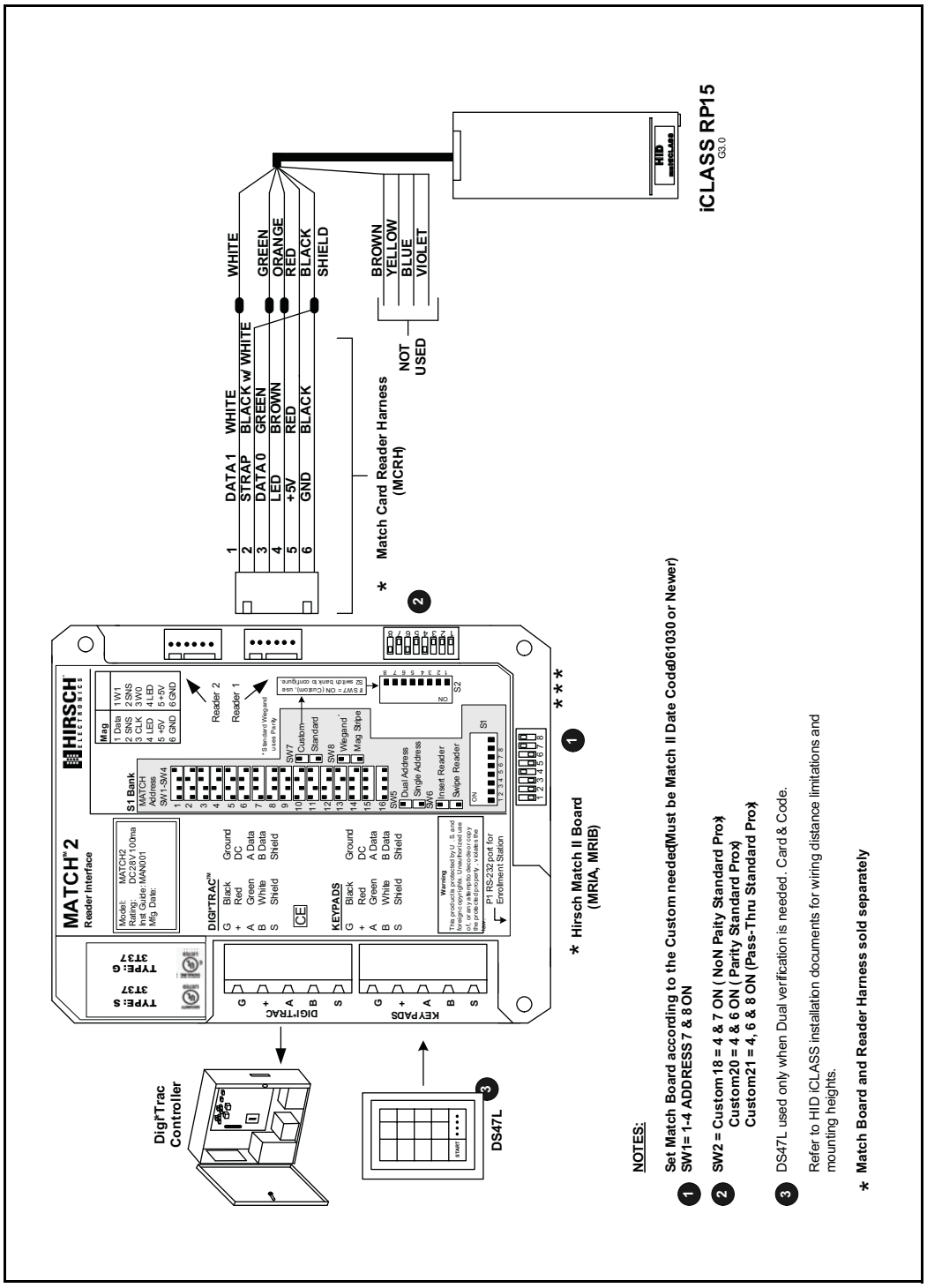
CR-ICRP15-I HID RP15 iClass Indala Prox Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



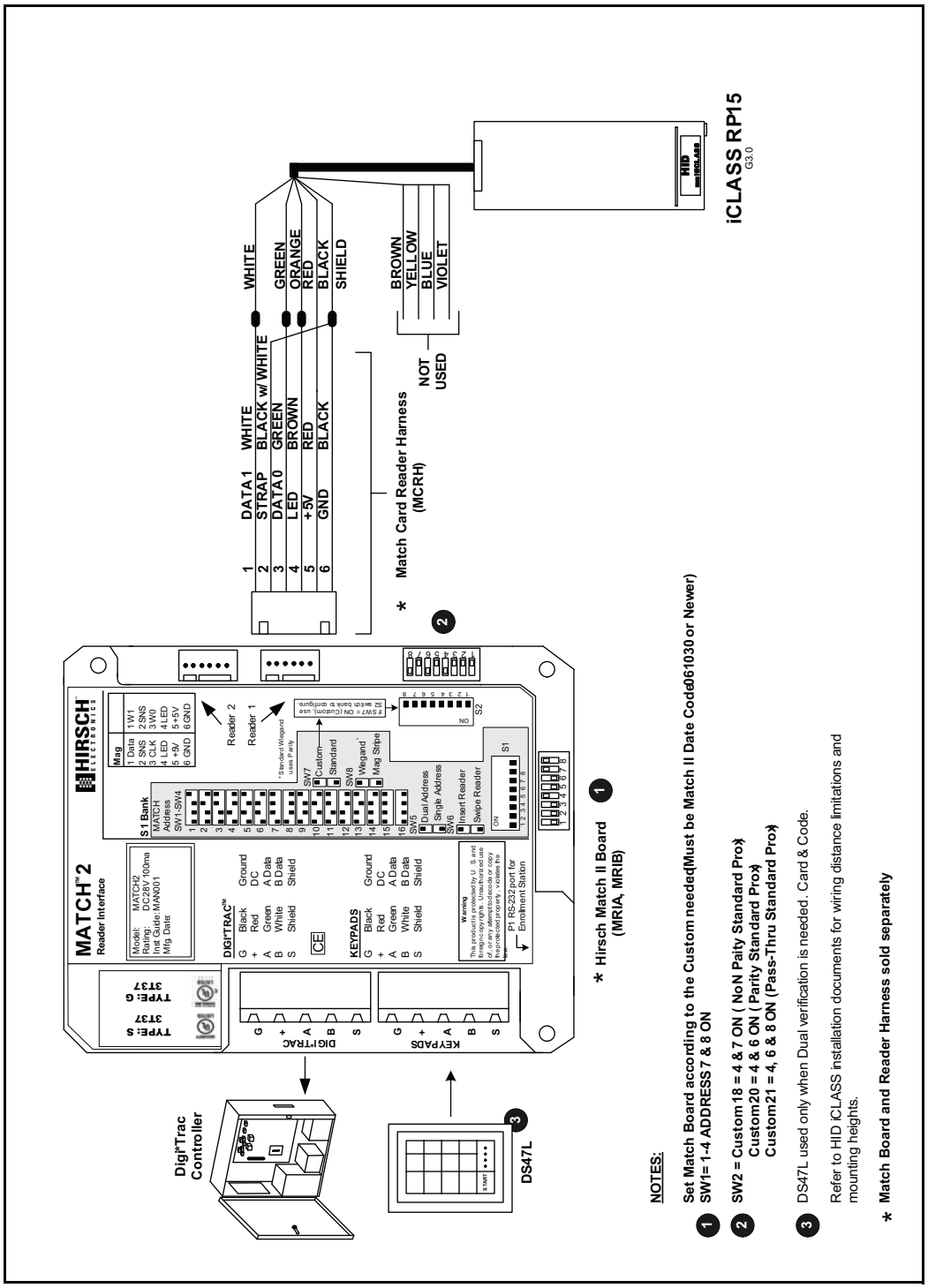
CR-ICRP15-PIV HID RP15 iClass Prox PIV Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



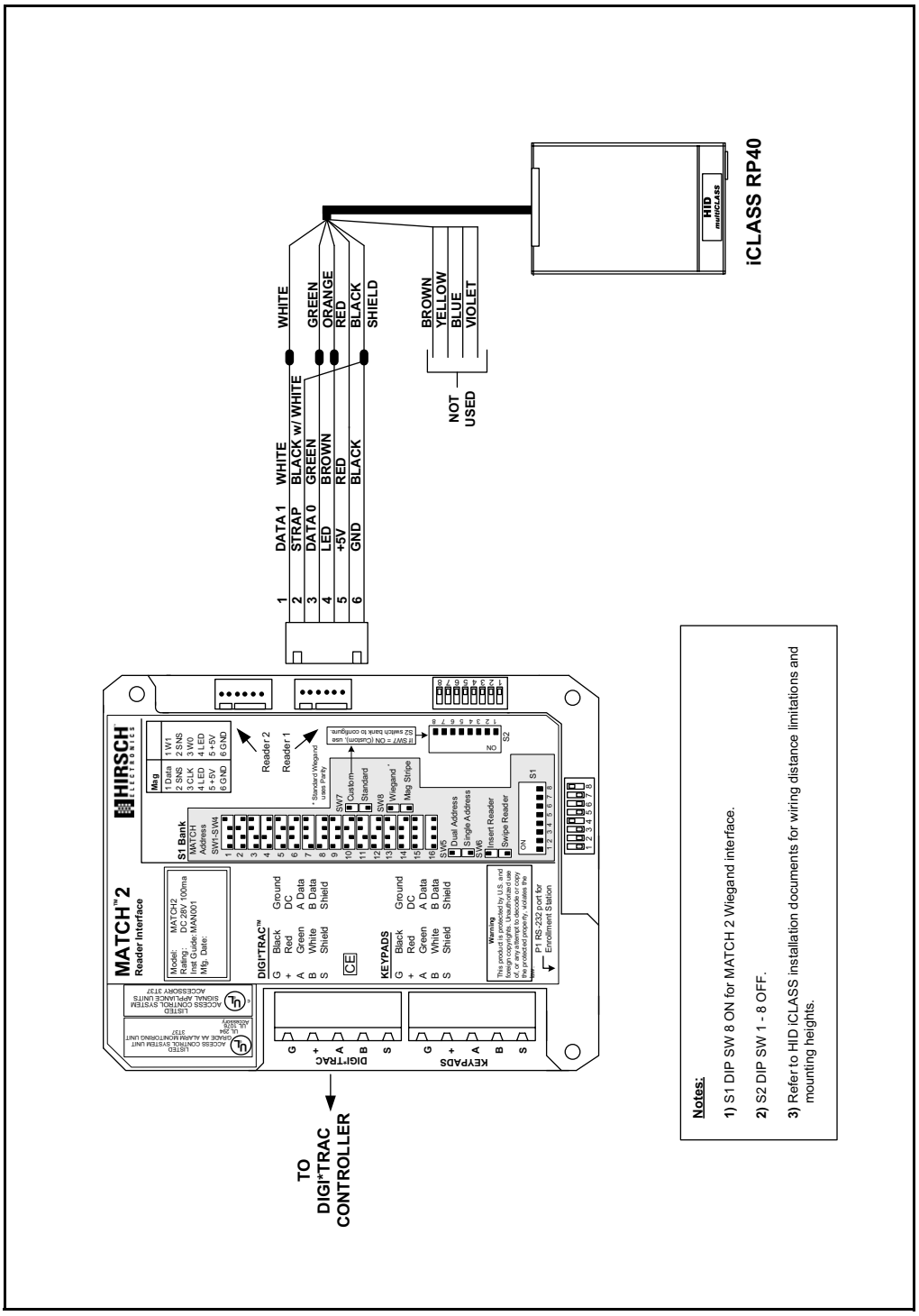
CR-ICRP15-PIV-I HID RP15 iClass Indala Prox PIV Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



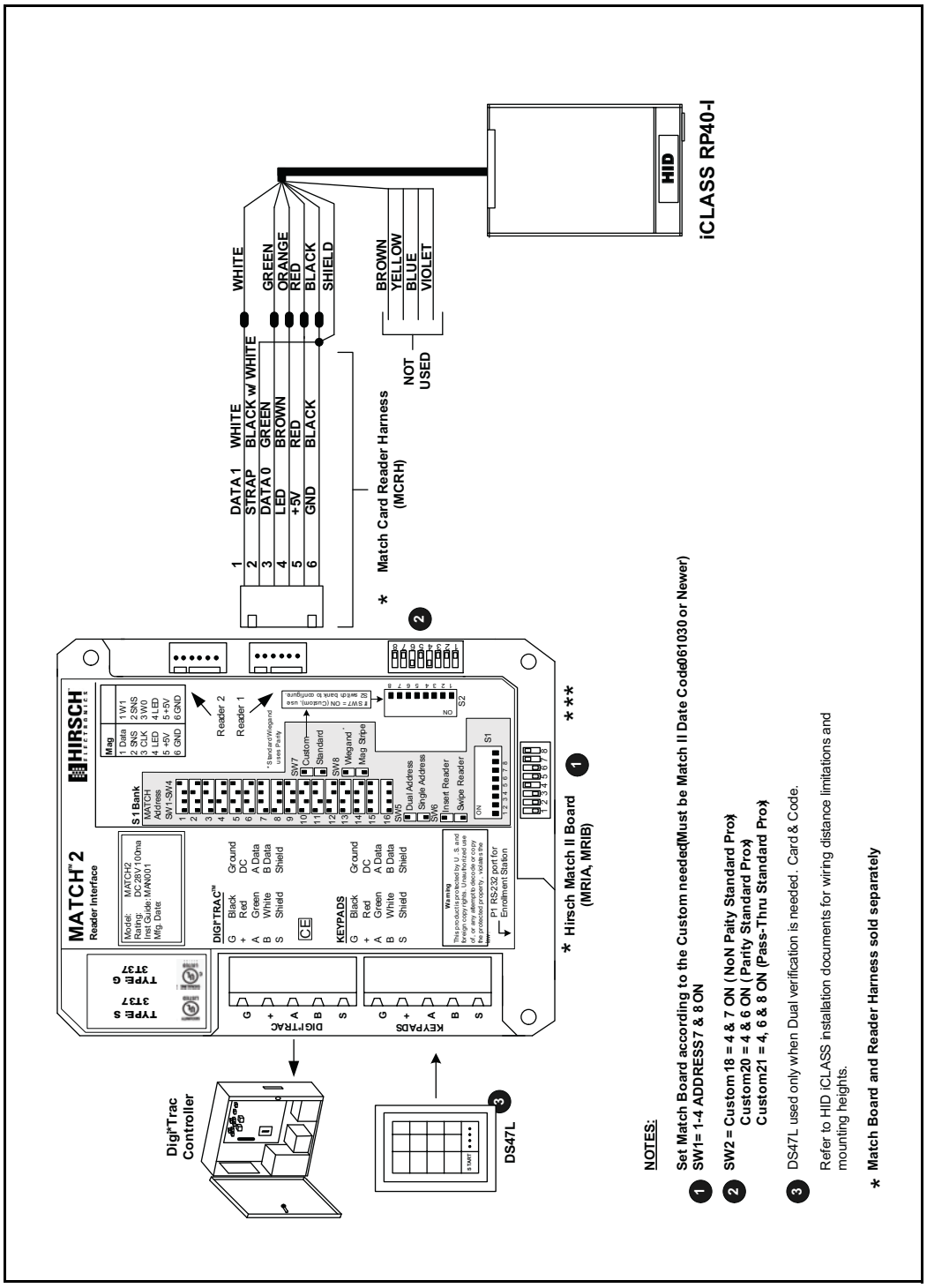
CR-ICRP40 HID RP40 iClass Contactless Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



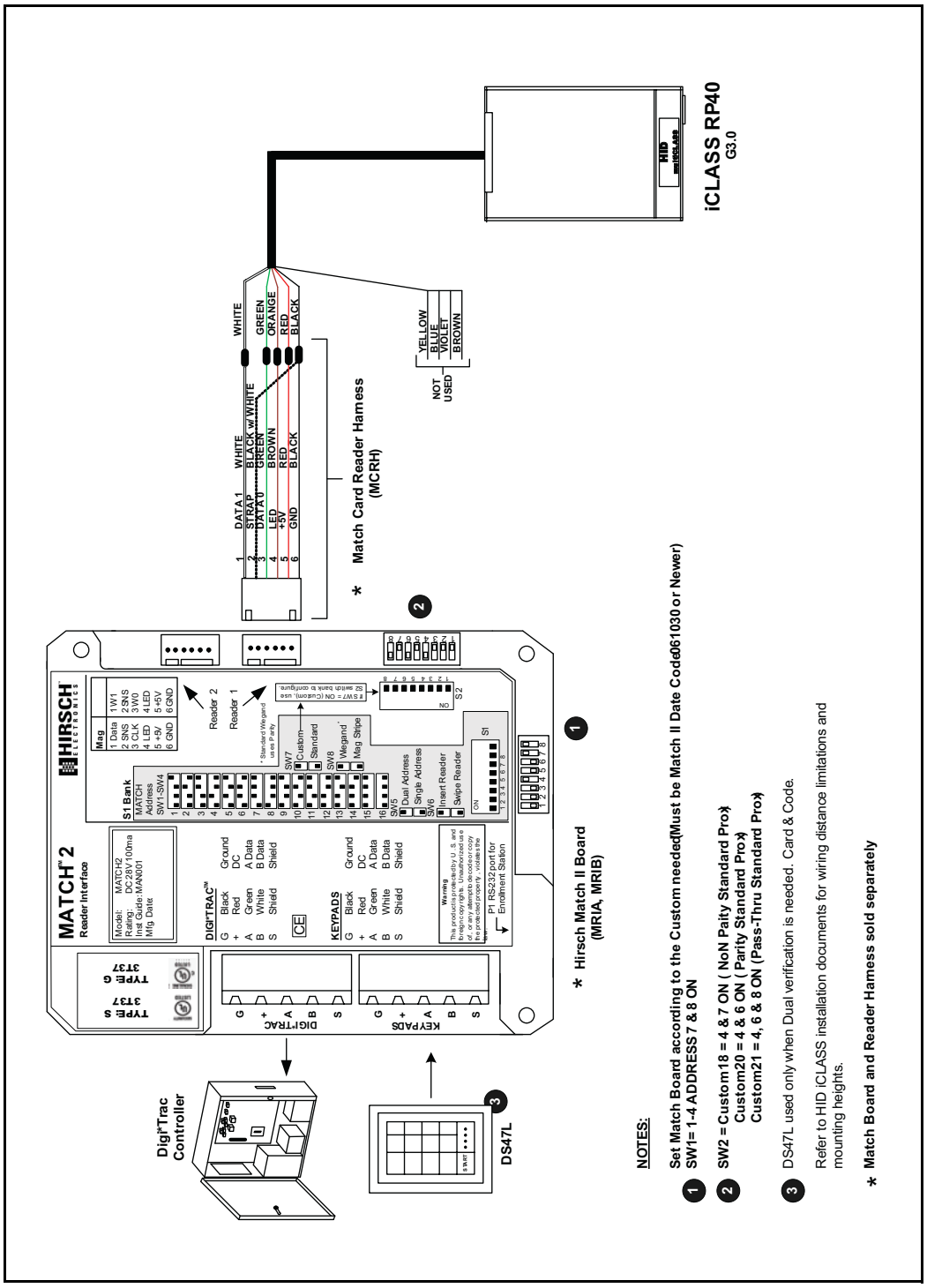
CR-ICRP40-I HID RP40 iClass Indala Prox Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



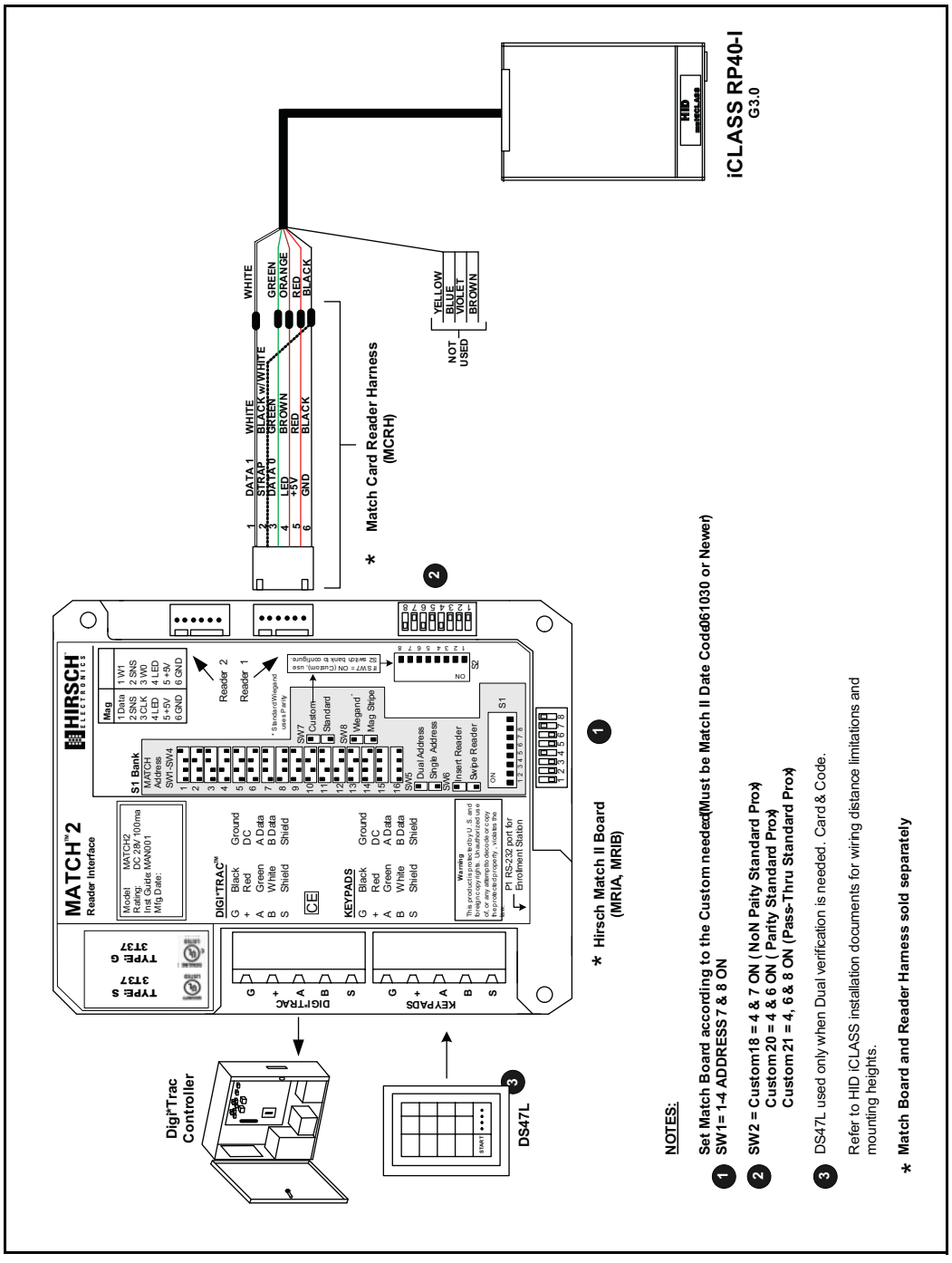
CR-ICRP40-PIV HID RP40 iClass PIV Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



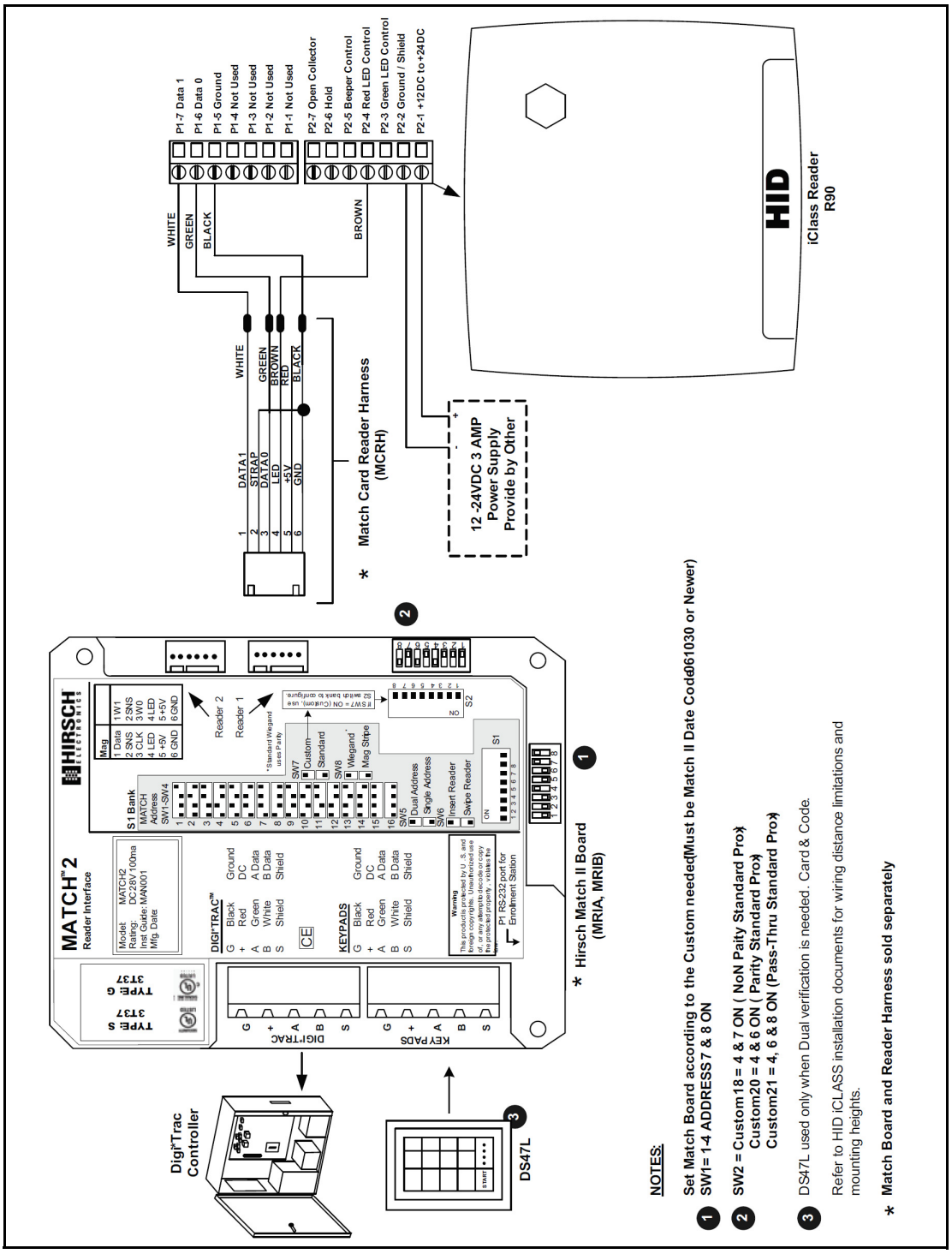
CR-ICRP40-PIV-I HID RP40 iClass Indala Prox PIV Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



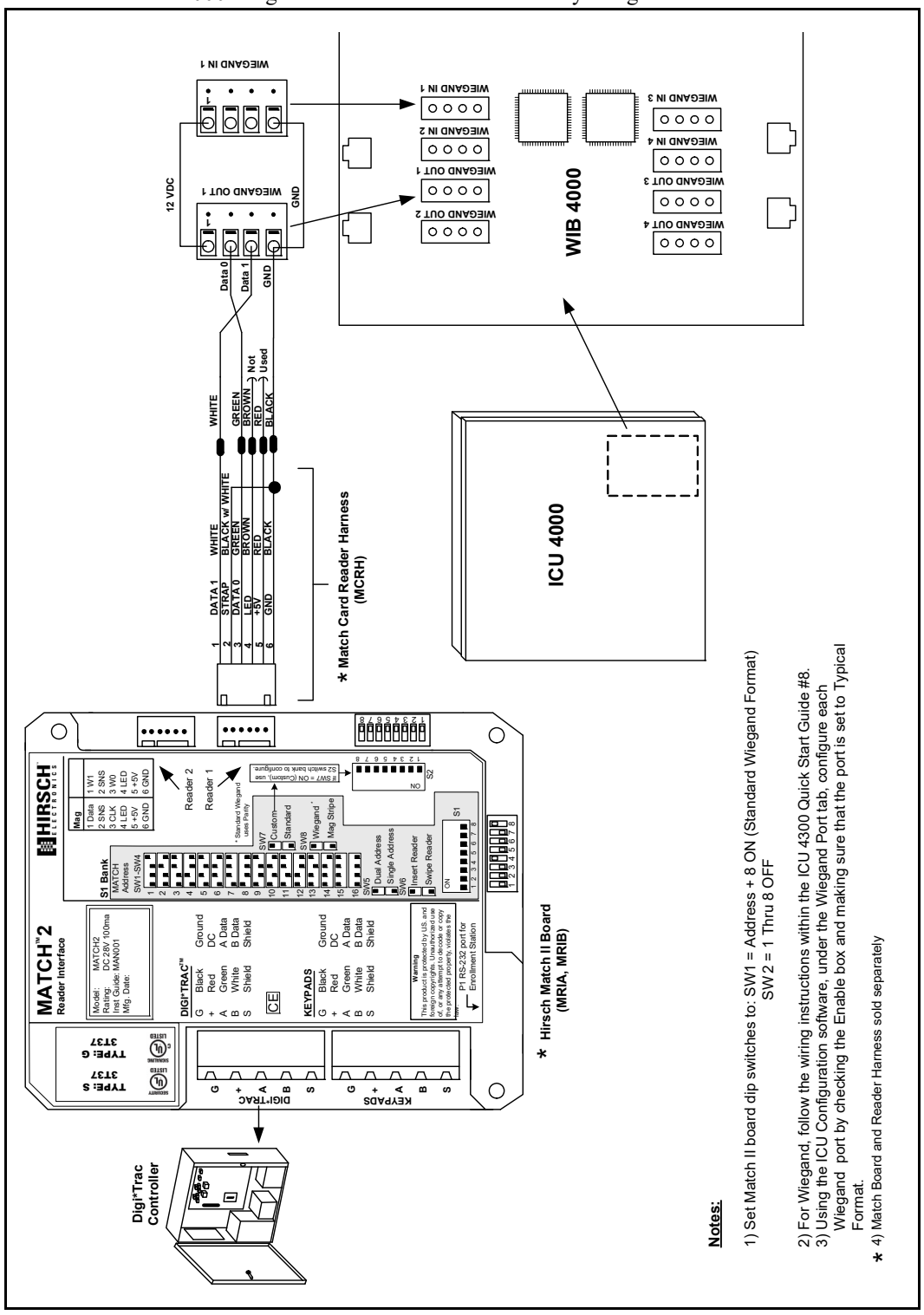
CR-ICR90 HID R90 iClass Long-Range Smart Card Reader

This diagram shows wiring and settings for the BQT Smart Card Biometric Reader, model CR-BT910X.



CR-BIO-ICU4000-W LG ICU-4000 Wiegand Smart Card Reader

The WIB 4000 daughter board contains the necessary Wiegand connectors.



Notes:

1) Set Match II board dip switches to: SW1 = Address + 8 ON (Standard Wiegand Format)
SW 2 = 1 Thru 8 OFF

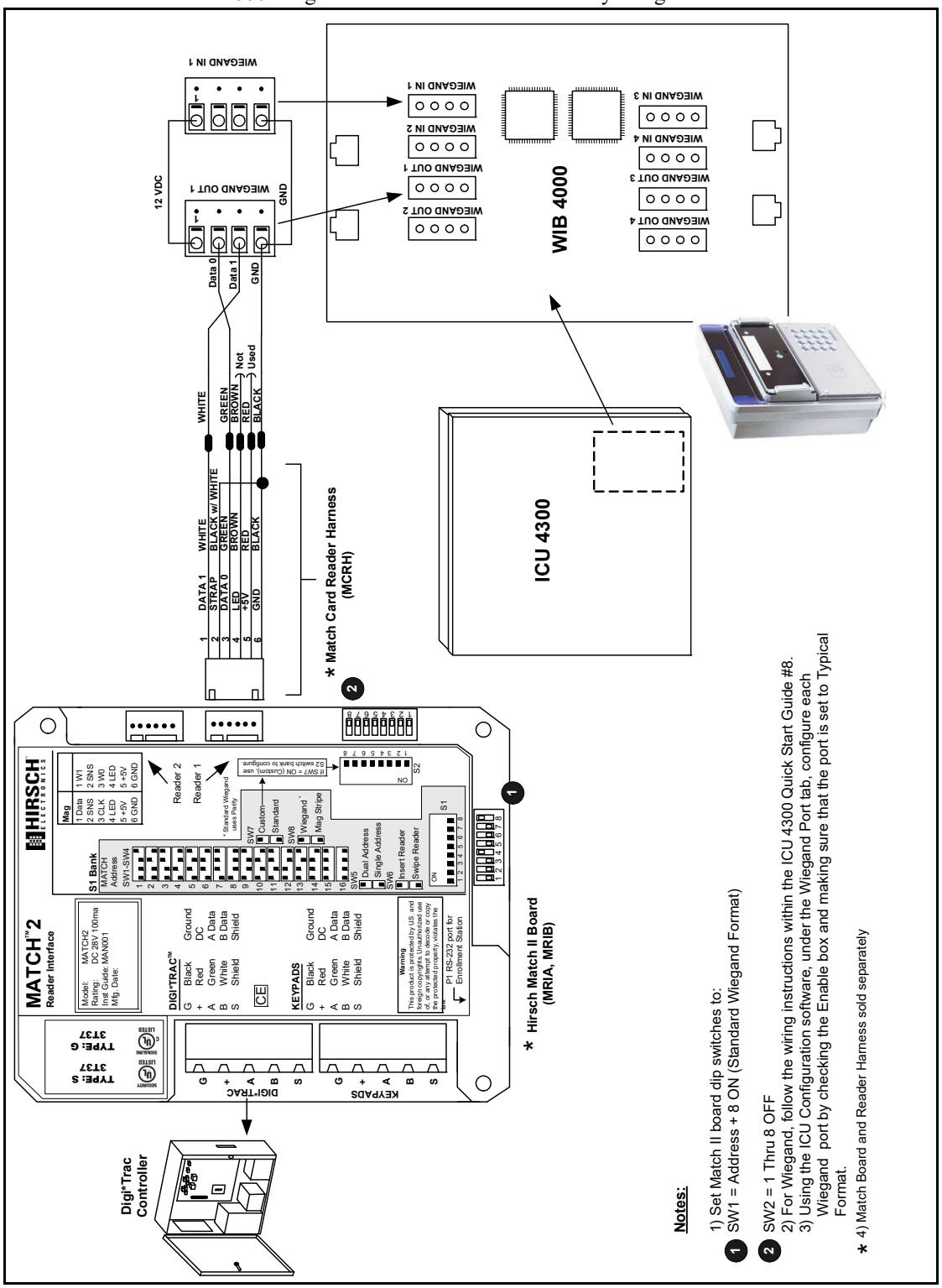
2) For Wiegand, follow the wiring instructions within the ICU 4300 Quick Start Guide #8.

3) Using the ICU Configuration software, under the Wiegand Port tab, configure each Wiegand port by checking the Enable box and making sure that the port is set to Typical Format.

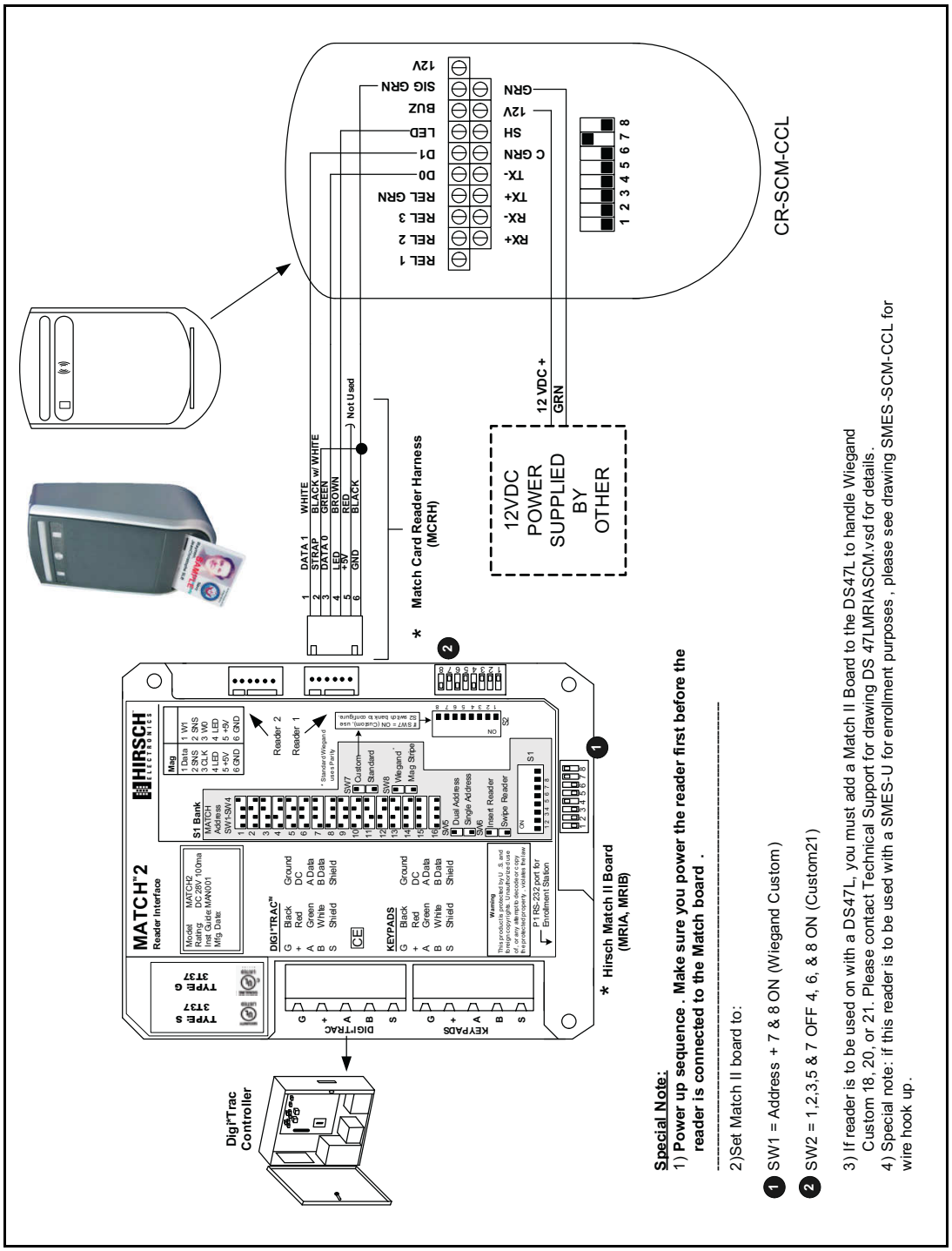
* 4) Match Board and Reader Harness sold separately

CR-BIO-ICU4300-W LG ICU-4300 Wiegand Smart Card Reader

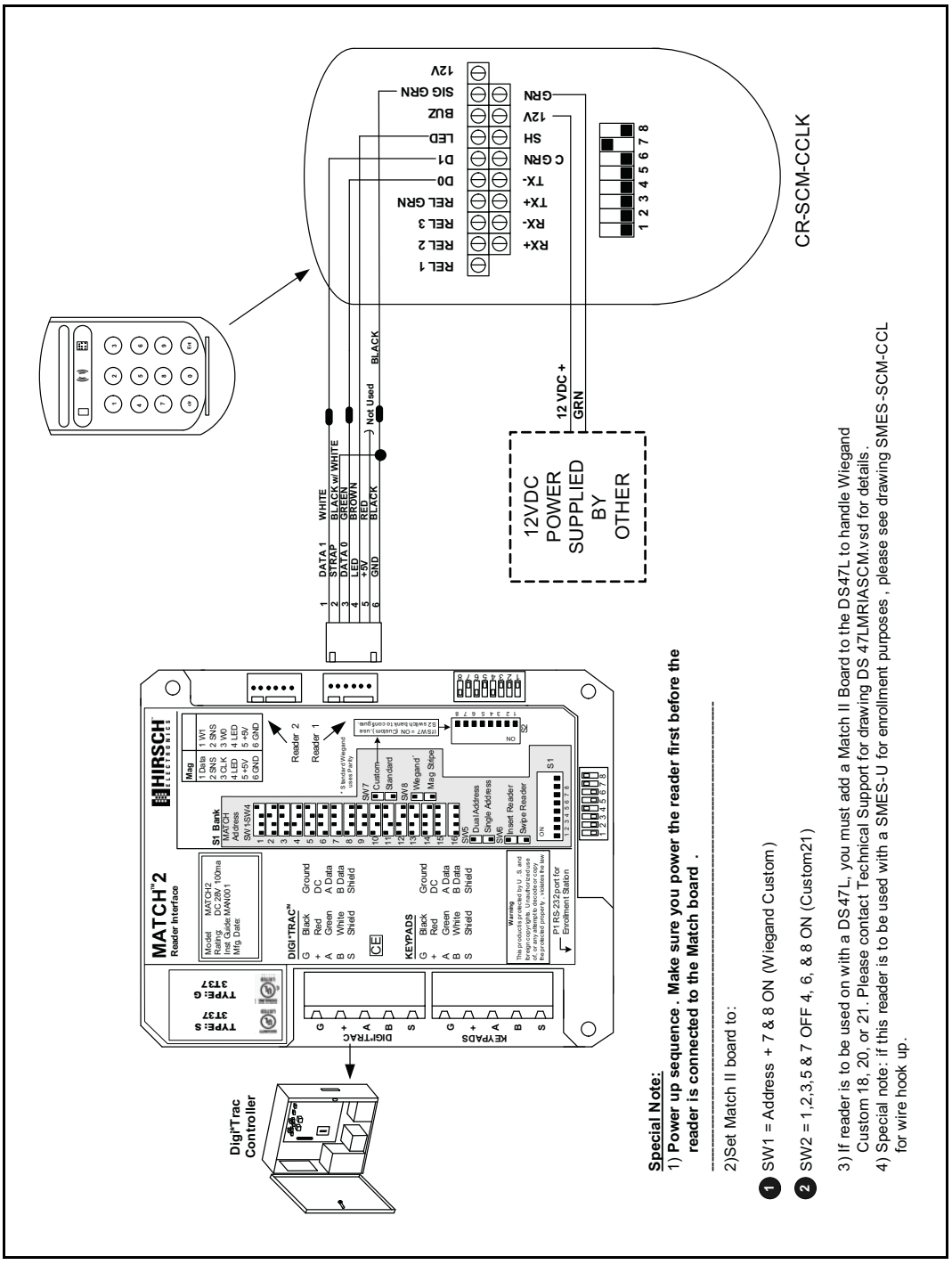
The WIB 4000 daughter board contains the necessary Wiegand connectors.



CR-SCM-CCL SCM SmartCard Reader (Custom 21)



CR-SCM-CCLK SCM SmartCard Reader with Keypad (Custom 21)



Special Note:

1) **Power up sequence . Make sure you power the reader first before the reader is connected to the Match board .**

---

2)Set Match II board to:

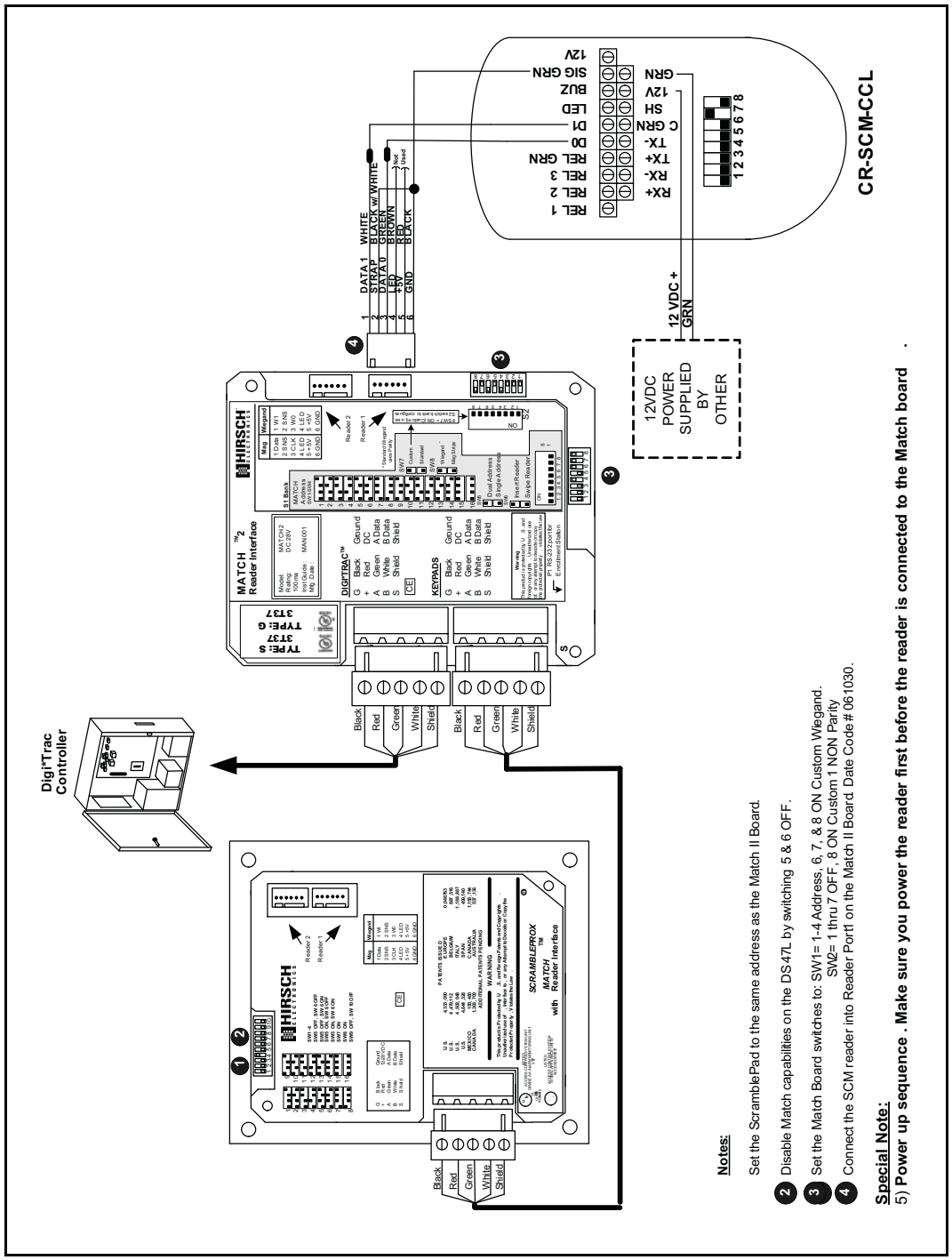
1. SW1 = Address + 7 & 8 ON (Wiegand Custom)
2. SW2 = 1,2,3,5 & 7 OFF 4, 6, & 8 ON (Custom21)

3) If reader is to be used on with a DS47L, you must add a Match II Board to the DS47L to handle Wiegand Custom 18, 20, or 21. Please contact Technical Support for drawing DS 47LMRIASCM.vsd for details .

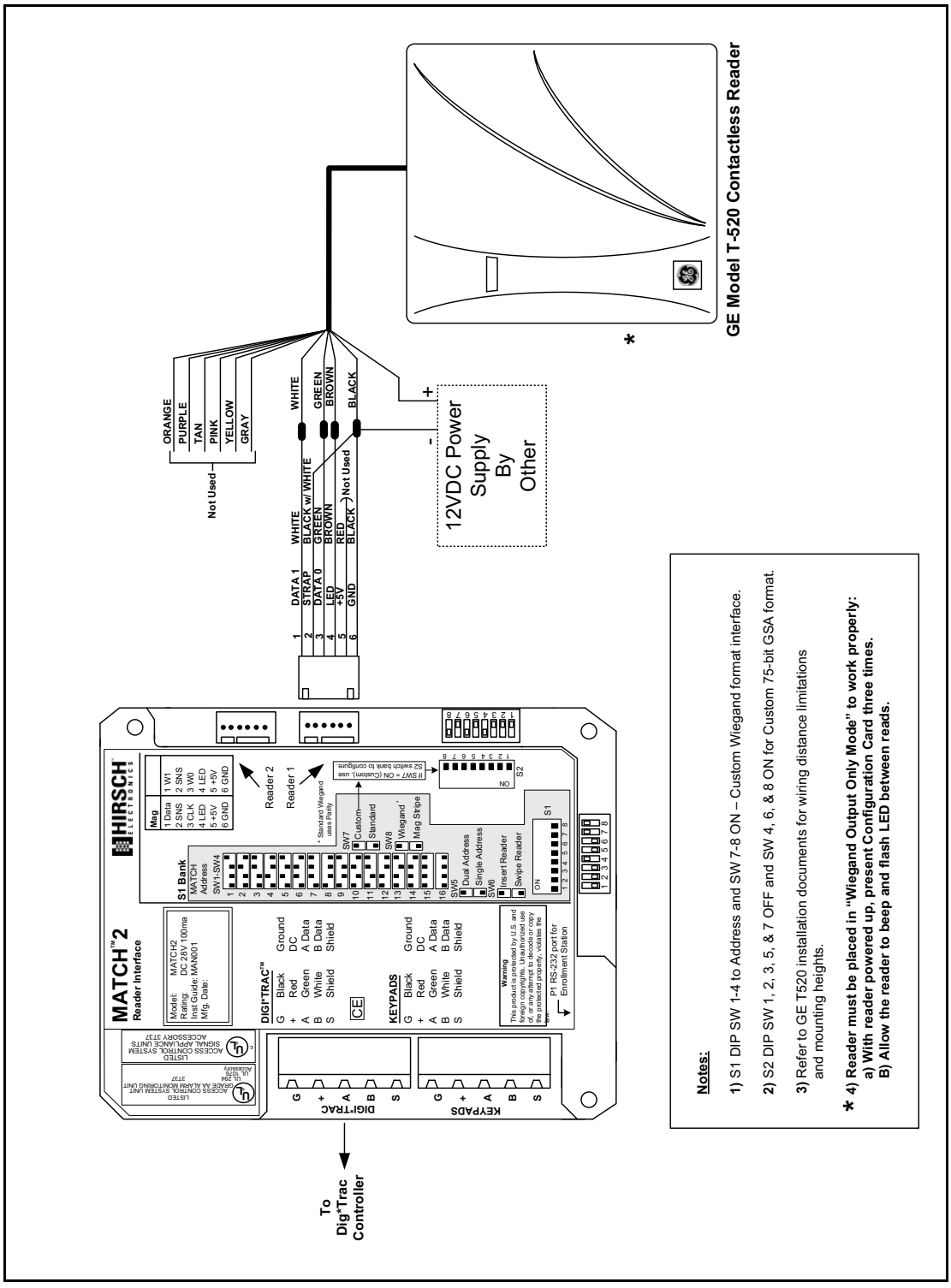
4) Special note: if this reader is to be used with a SMES-U for enrollment purposes , please see drawing SMES-SCM-CCL for wire hook up.

DS47L-MRIA-SCM-CCL (SCM SmartCard Reader with MRIA)

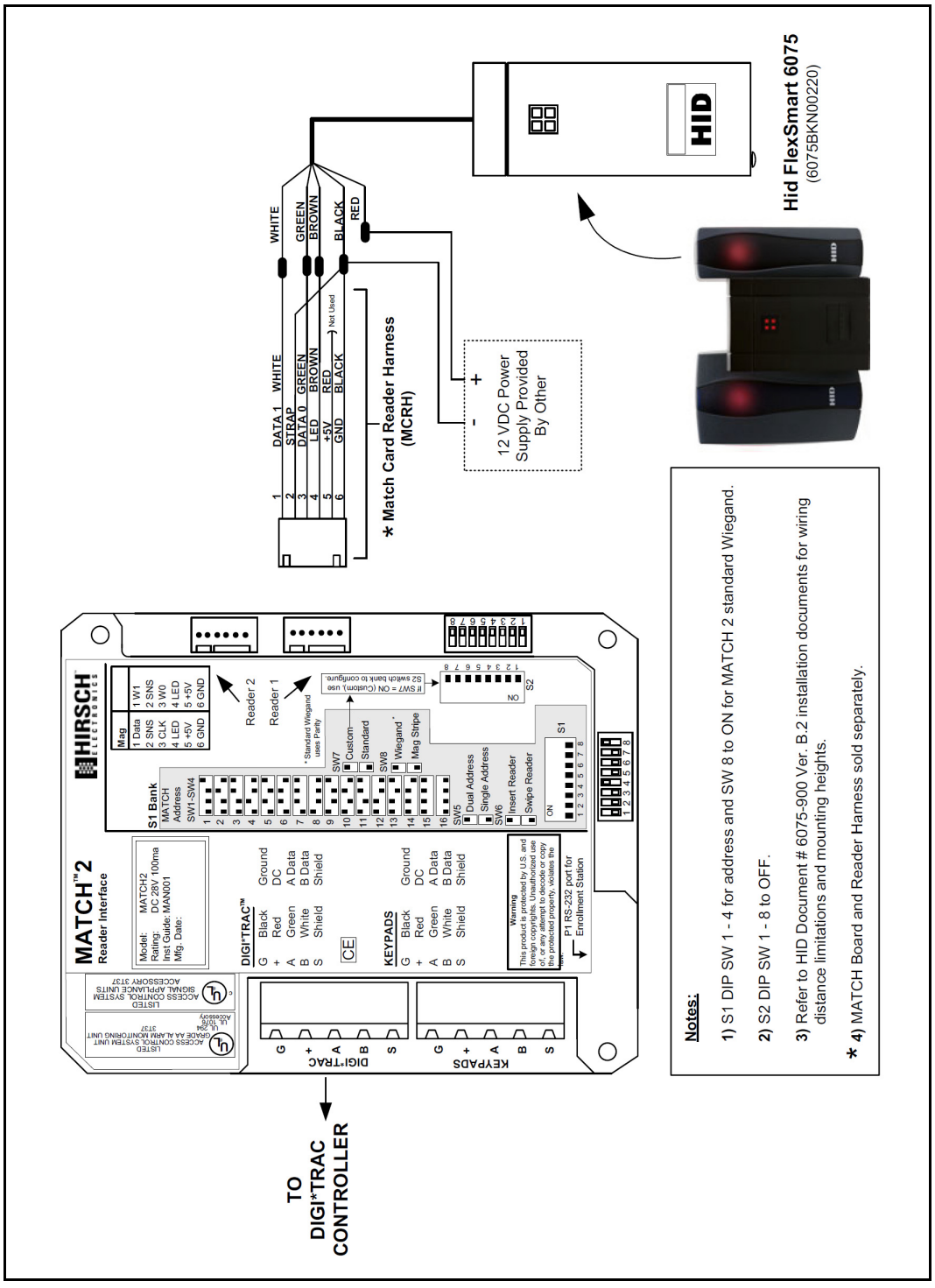
This combines the ScramblePrOx with the MRIA to controller connection.



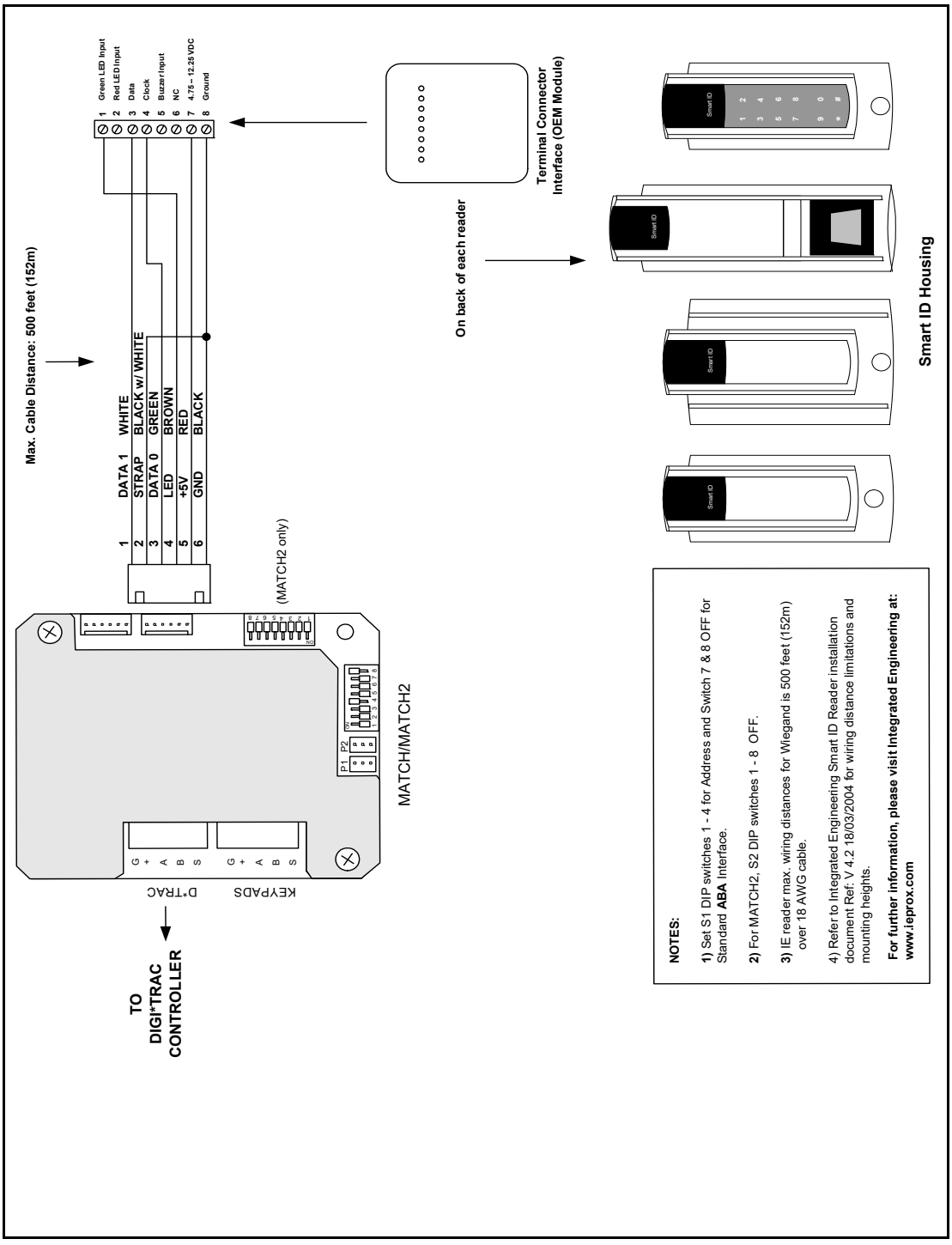
GE T-520 Multi-Technology Contactless Reader



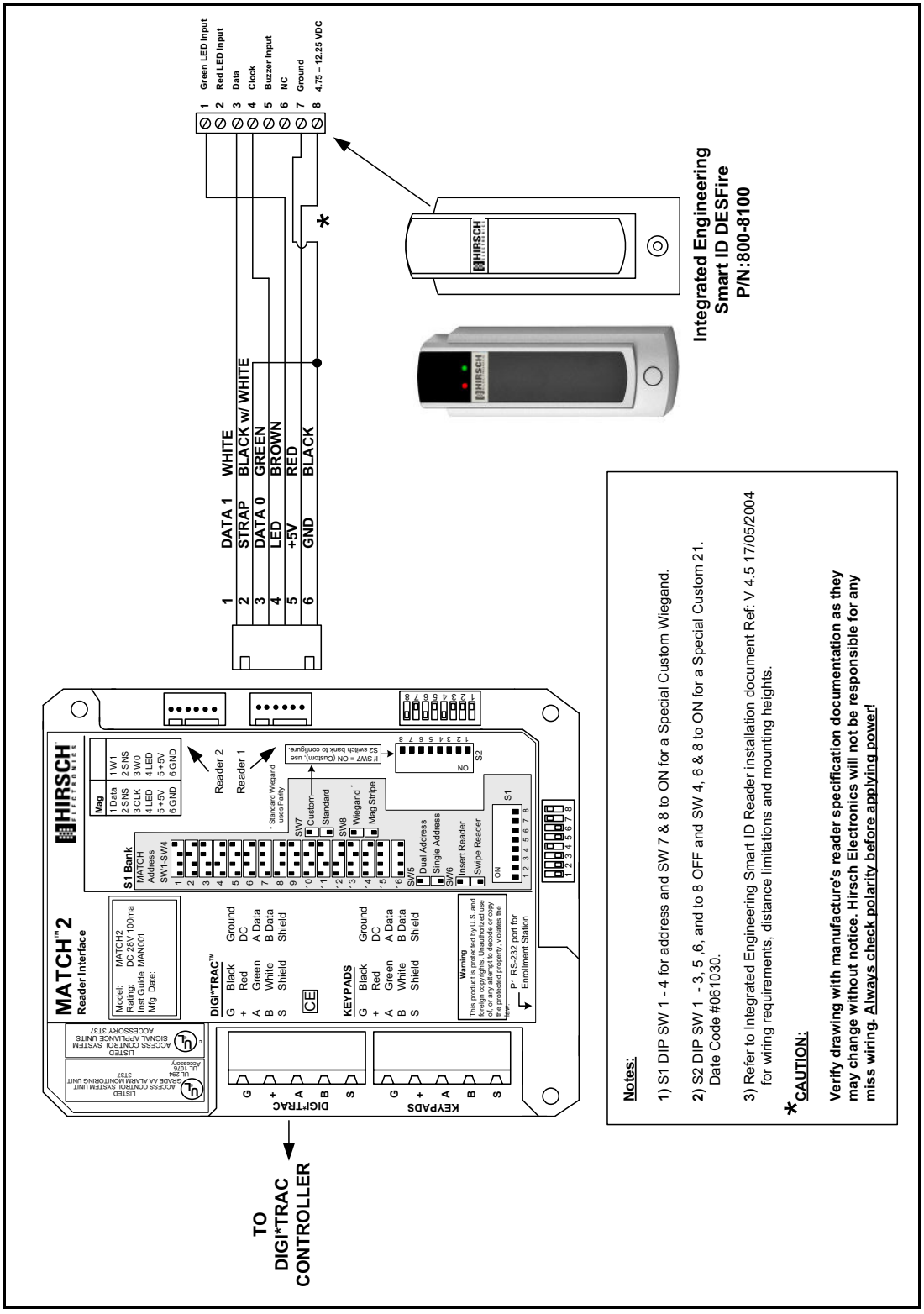
HID FlexSmart Series 6075



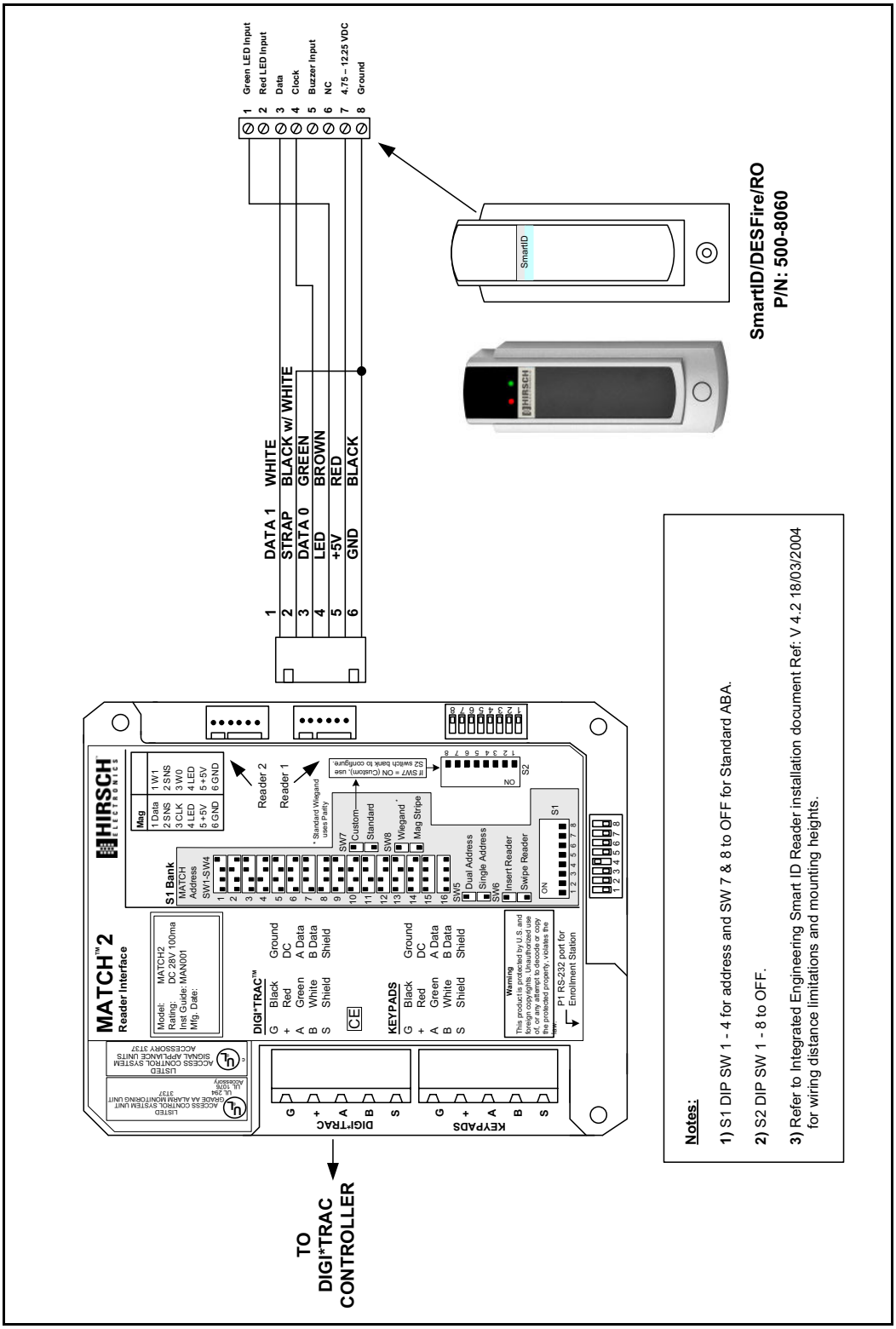
Integrated Engineering Smart Card Readers



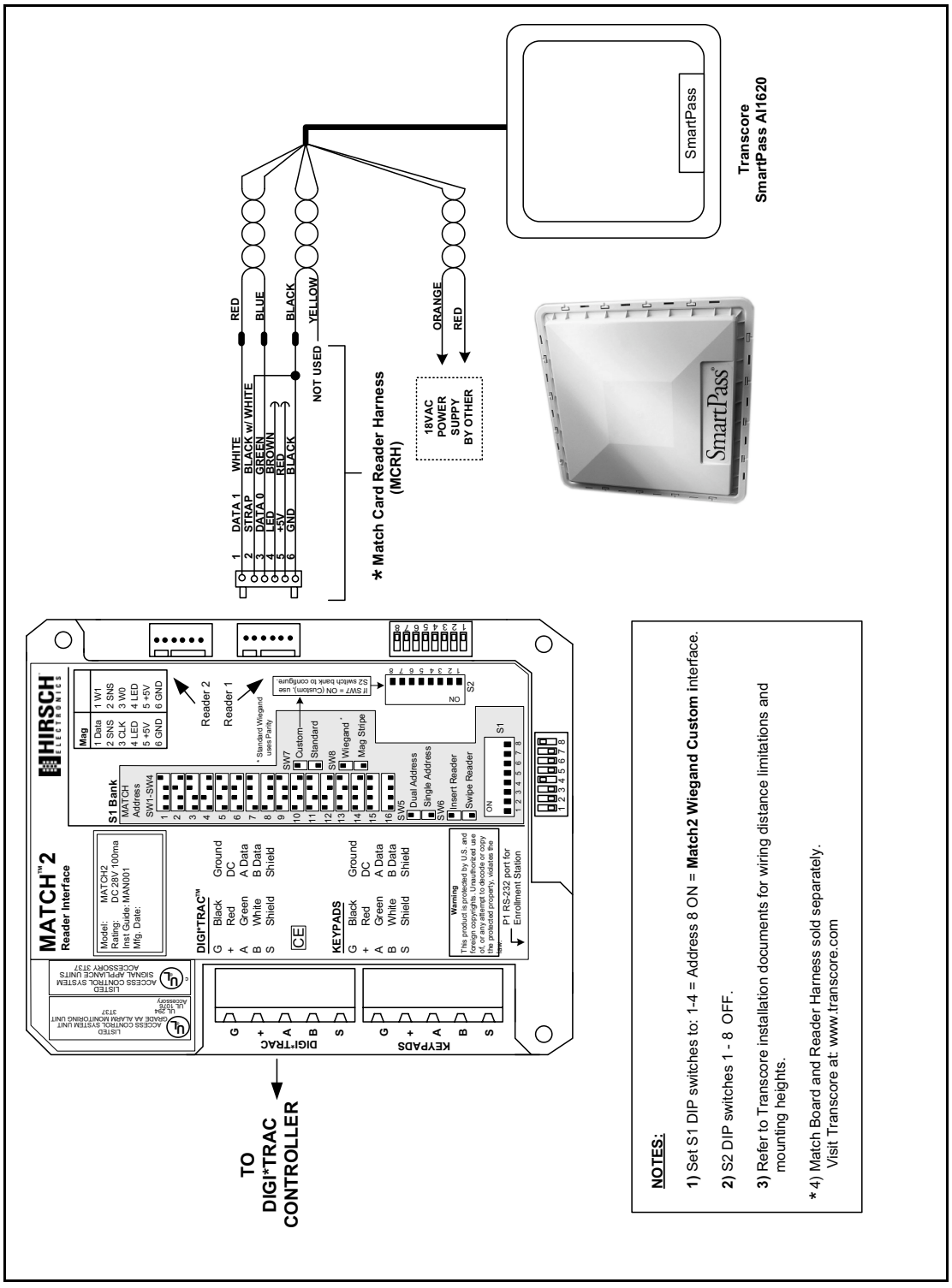
CR-IEM-DF75 Integrated Engineering SmartID DESFire Card Reader (Custom 21)



Integrated Engineering SmartID DESFire Smart Card Reader (Standard ABA)



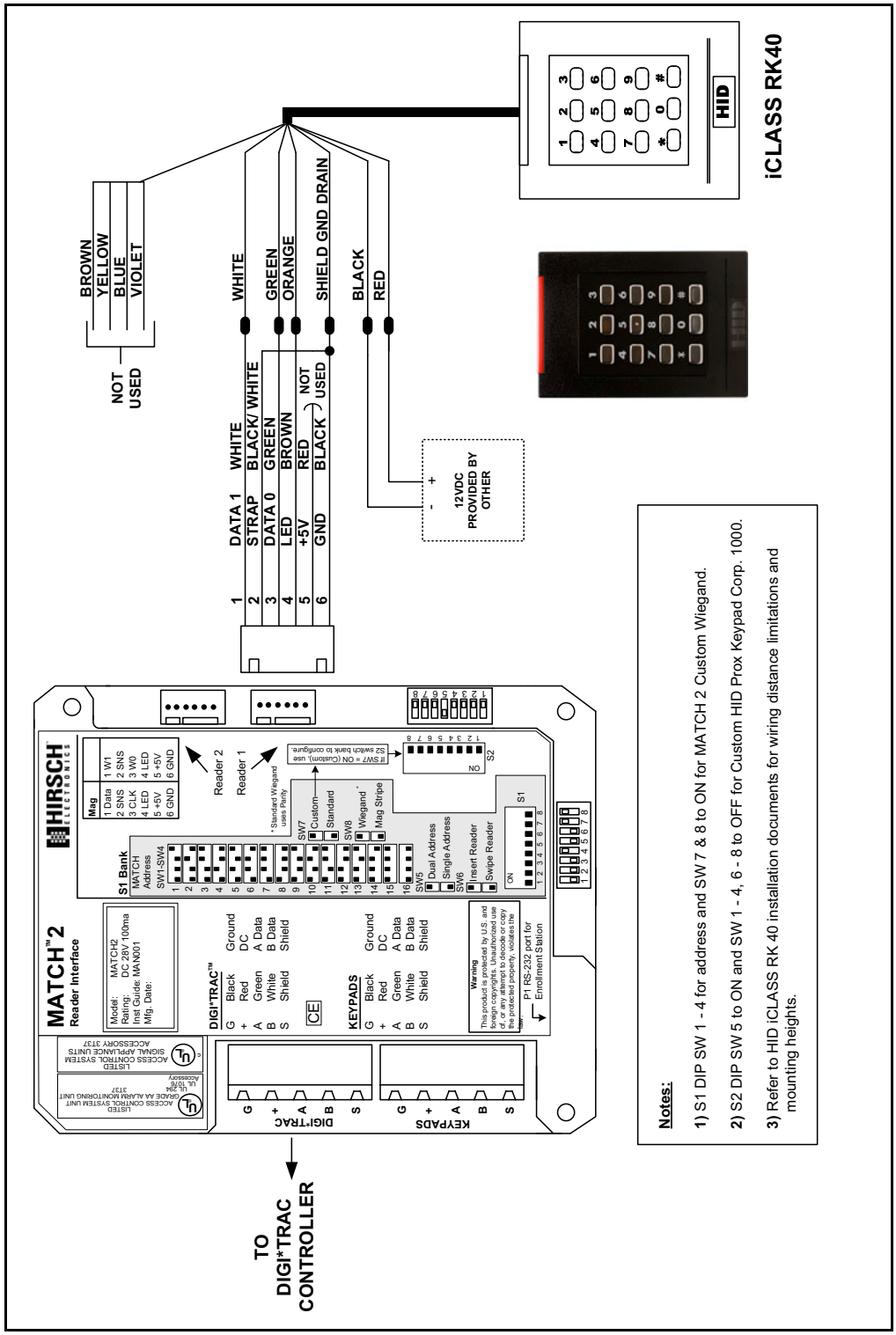
Transcore SmartPass AI1620



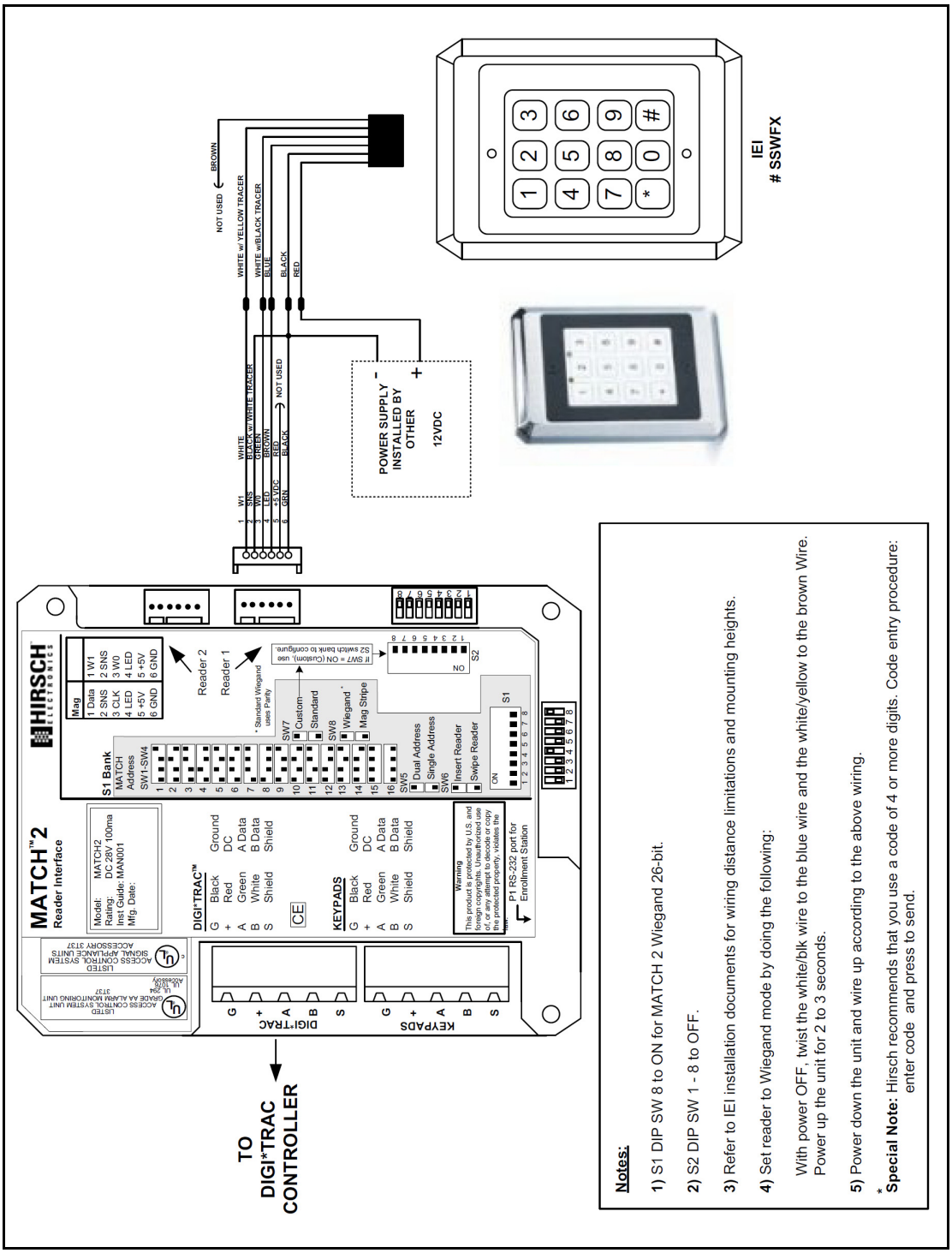
MATCH-Compliant Keypads

This section describes the MATCH wiring and settings information required to connect Hirsch-supported keypads.

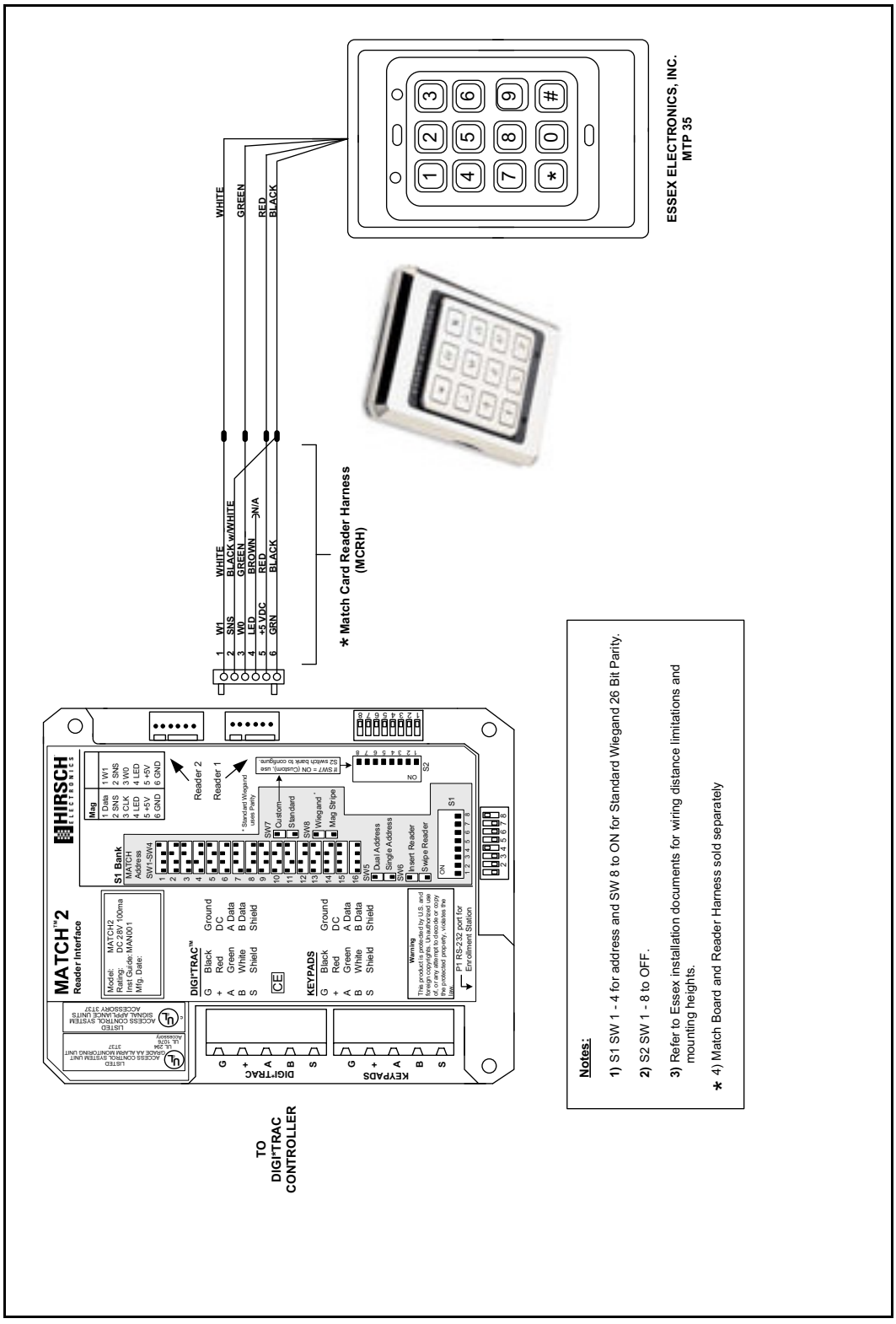
HID iCLASS RK40 WallSwitch Keypad Smart Card Reader (Corporate 1000)



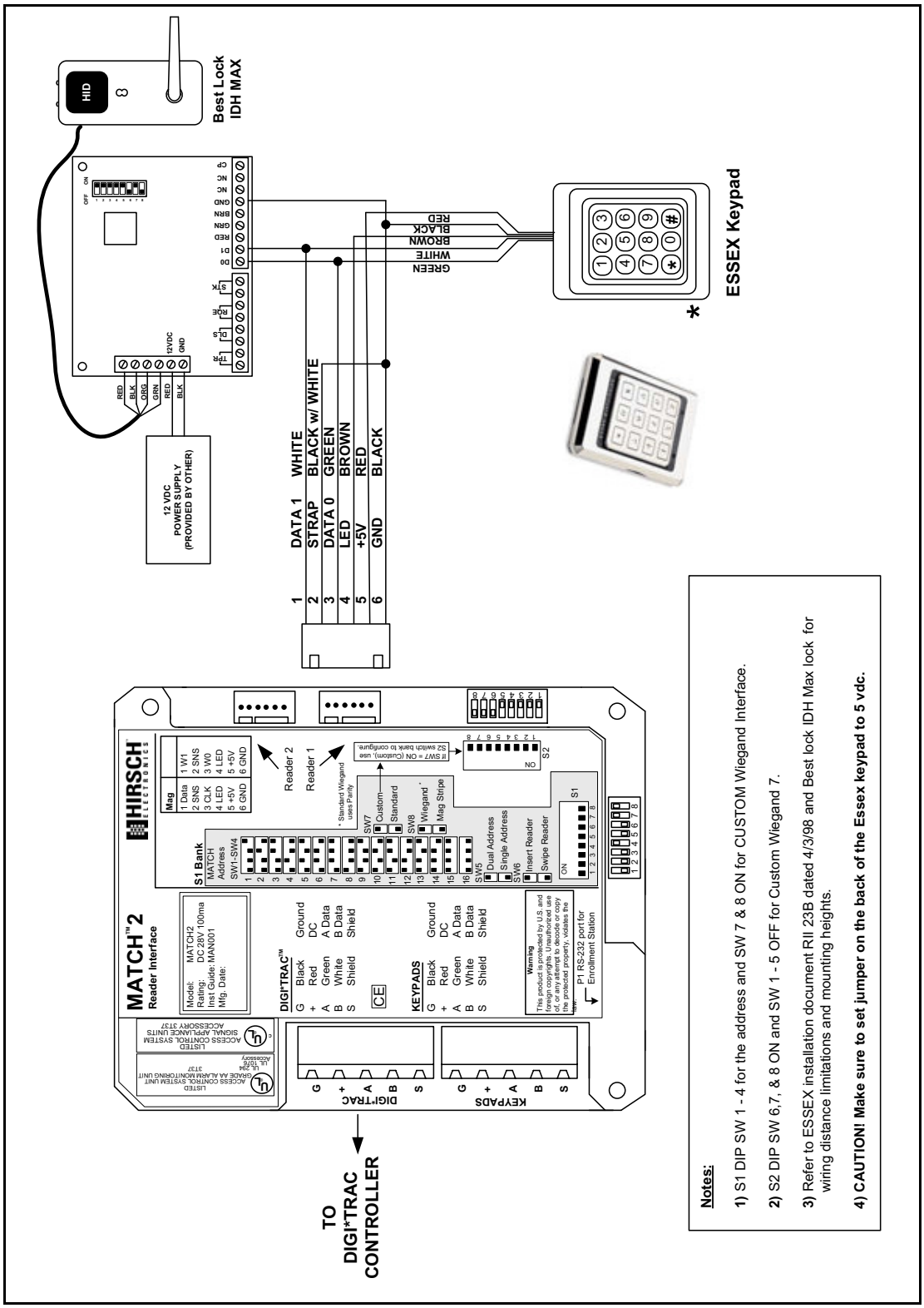
IEI SSWFX Wiegand Keypad



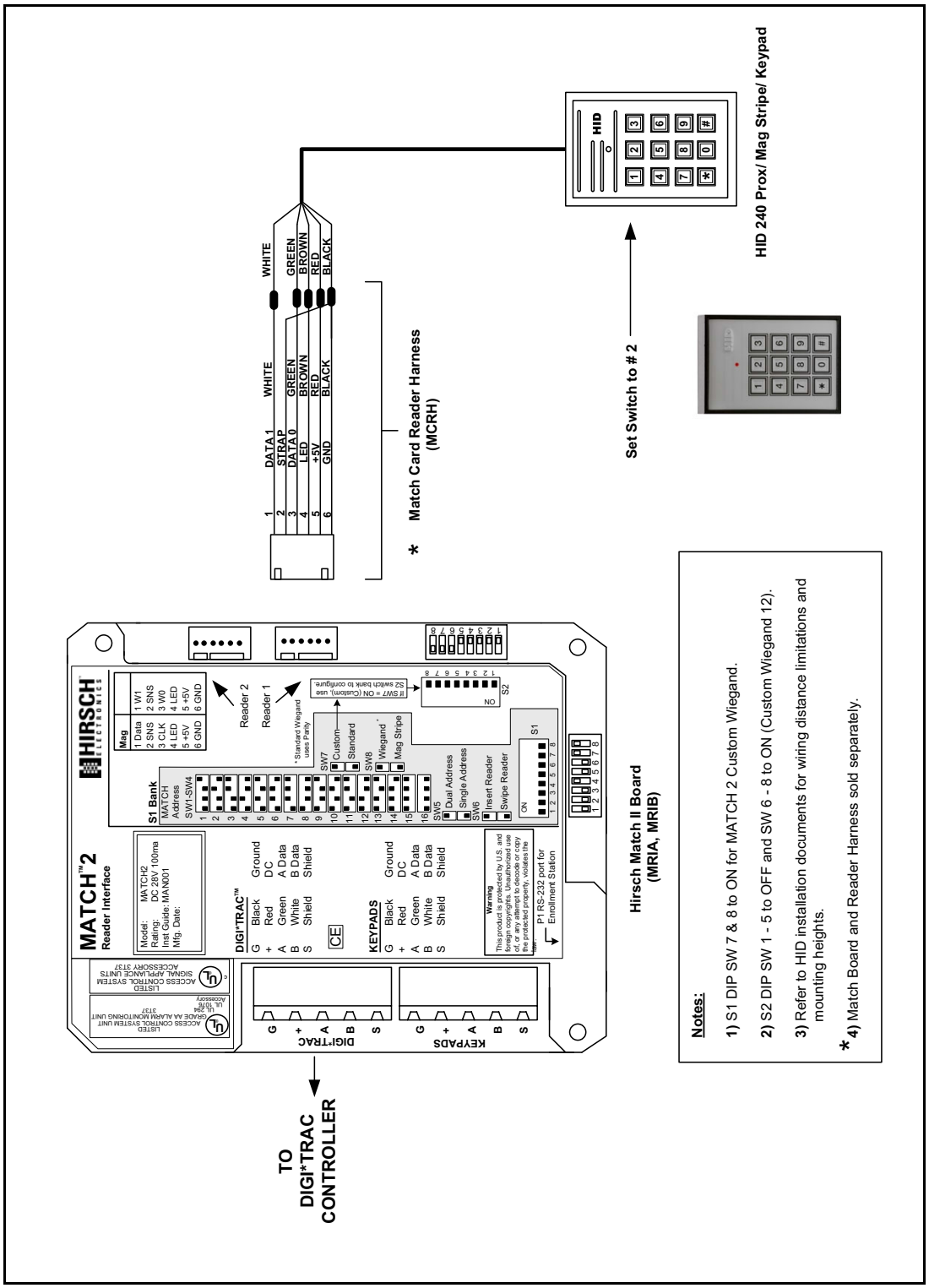
Essex MTP 35 Keypad



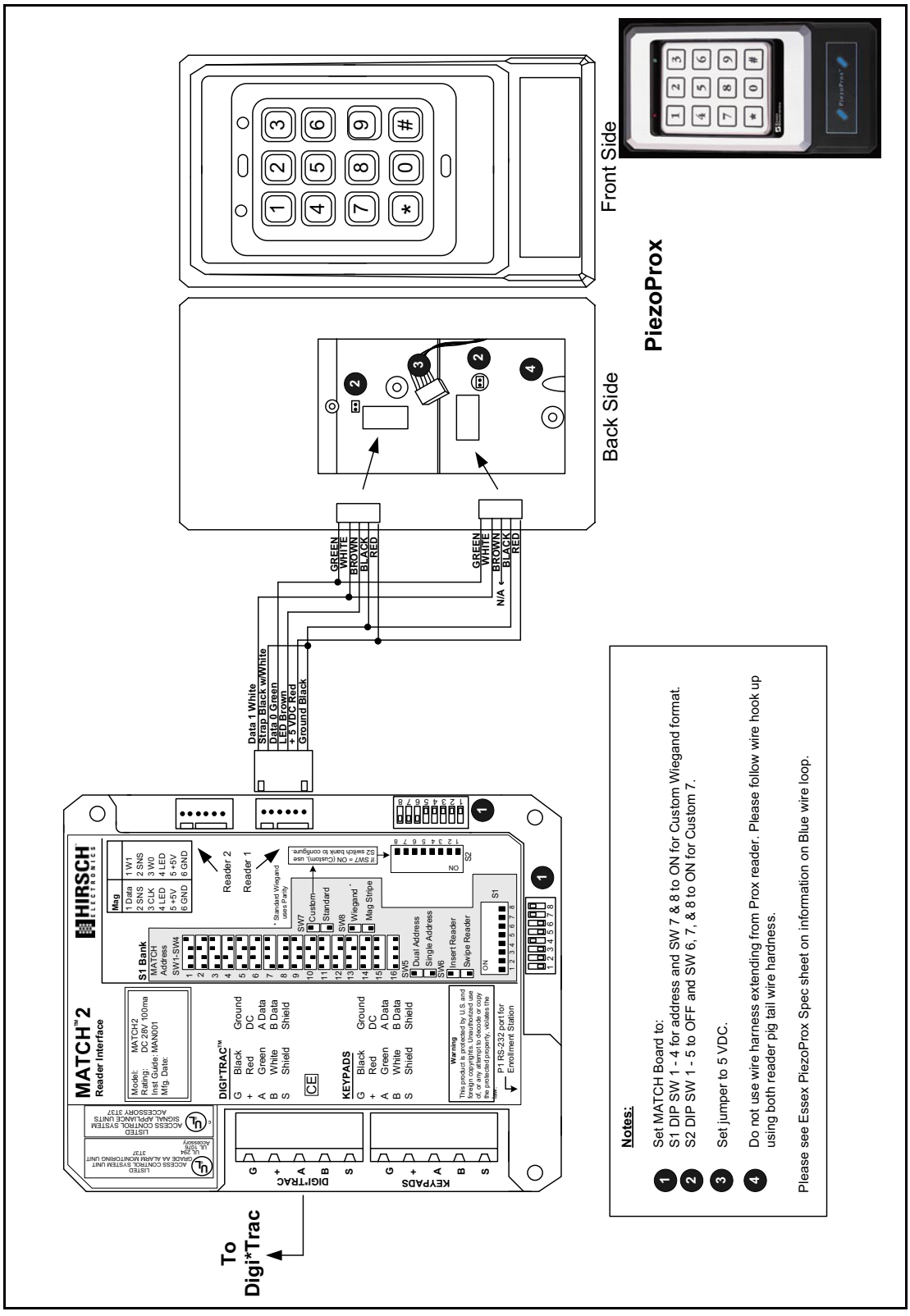
ESSEX Keypad and BEST LOCK IDH Max Lock



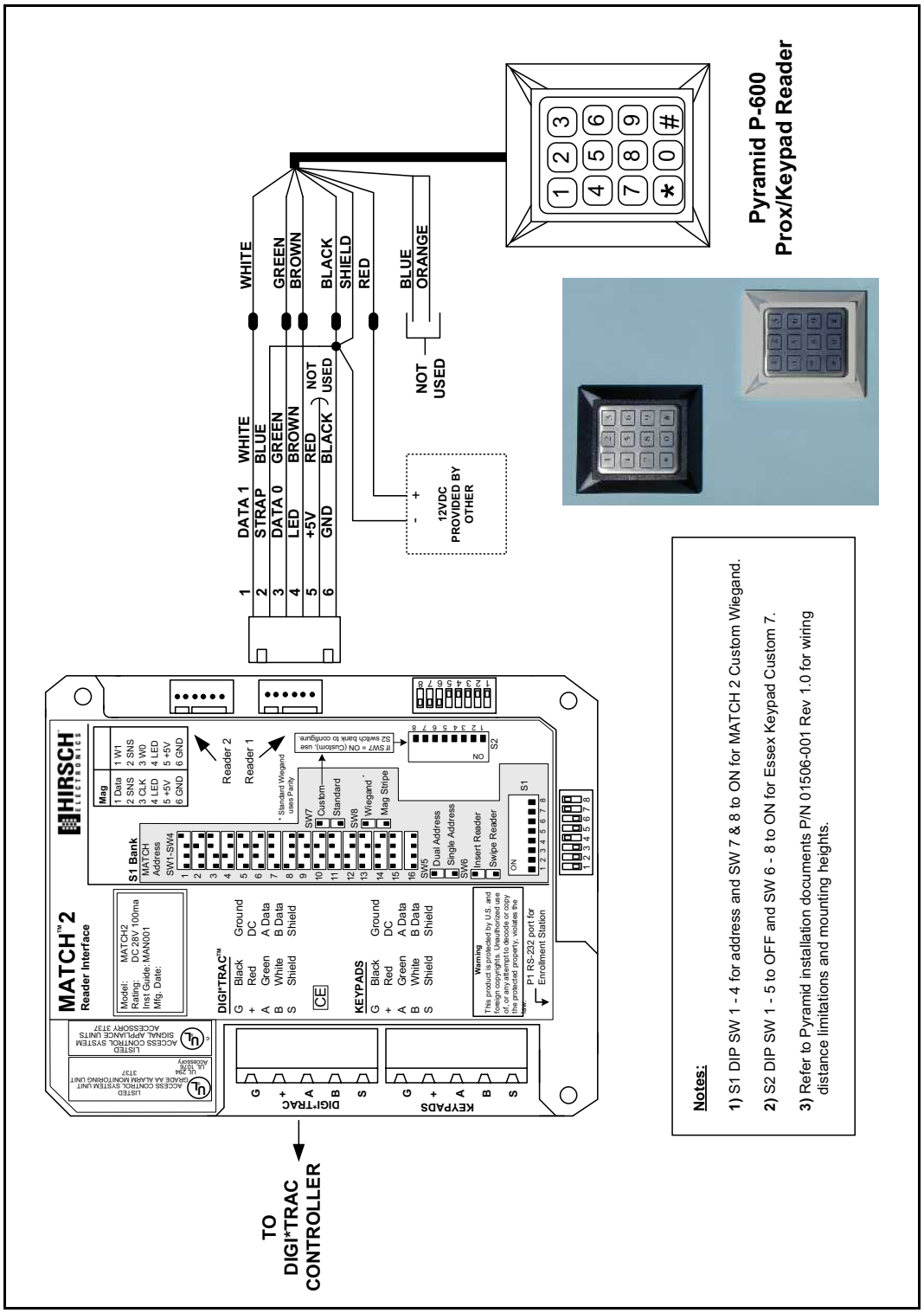
HID 240 Prox/Mag Stripe Reader and Keypad



PiezoProx Keypad/Prox Reader



Pyramid P-600 Prox/Keypad Reader

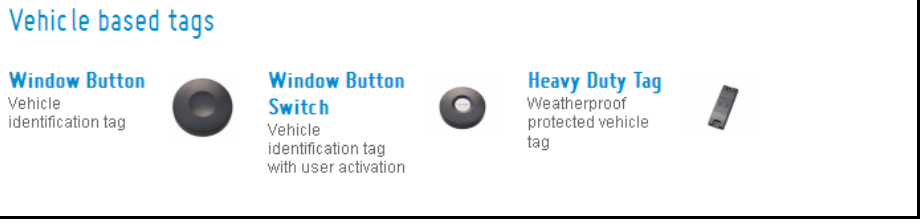


Miscellaneous Readers and Devices

This section includes miscellaneous readers (such as barium ferrite touch), boosters, and those devices which serve as intermediaries between Hirsch controllers and various readers.

CR-NCB Nedap Transit AVI Tag Combi-Booster

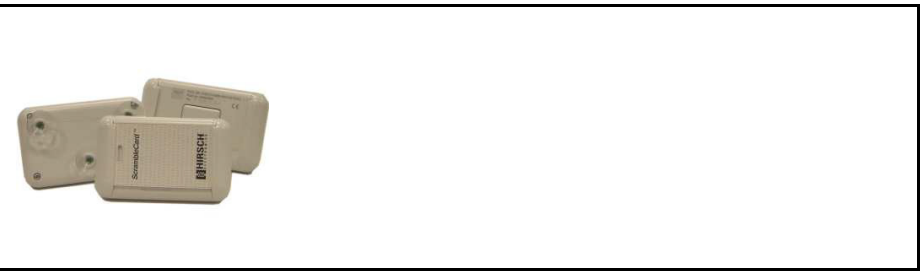
The CR-NCB is a button- or tag-shaped reader that boosts the signal for MIFARE, iClass or HID readers.



Passive 2.45 GHz Microwave Tag for the vehicle with integral 120KHz RFID reader for HID cards. Windshield mounting on inside of a vehicle via suction cups.

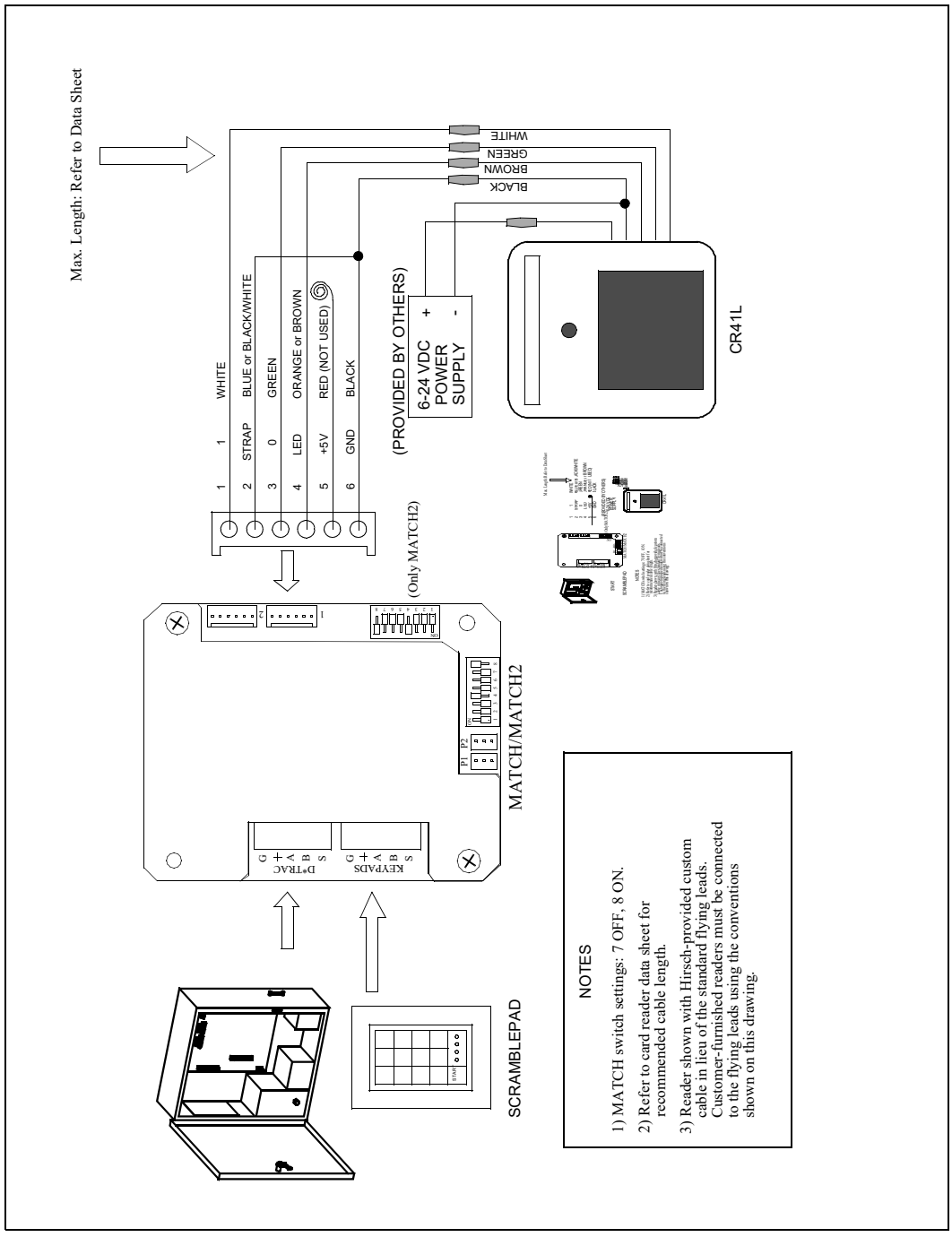
CR-NPB Nedap Transit AVI Tag HID Prox Booster

The CR-NPB is a tag-shaped reader that boosts the signal for MIFARE, iClass or HID readers.



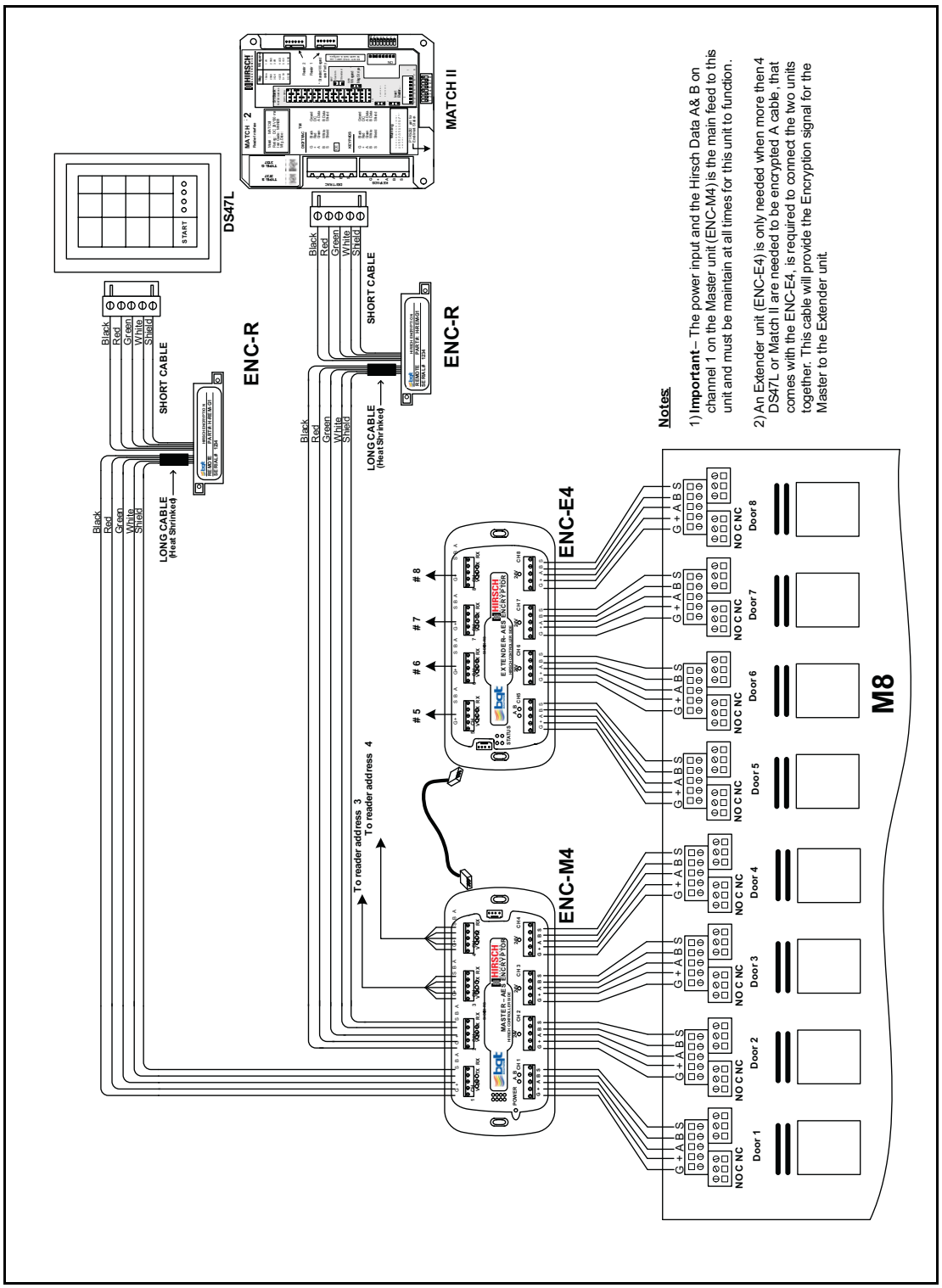
This booster is a passive 2.45 GHz Microwave Carrier/Transmitter with embedded 120KHz RFID reader for HID cards. Includes HID RFID card holder and ability to transmit the RFID card ID number over microwave to the CR-NMR microwave reader for greater distances than normally available for a Prox reader, allowing the window to remain rolled up. The Booster acts as an in vehicle Prox card reader. Windshield mounting on inside of a vehicle via suction cups. Lithium battery with lifetime of 8 to 10 years.

CR41L Barium Ferrite Touch Reader



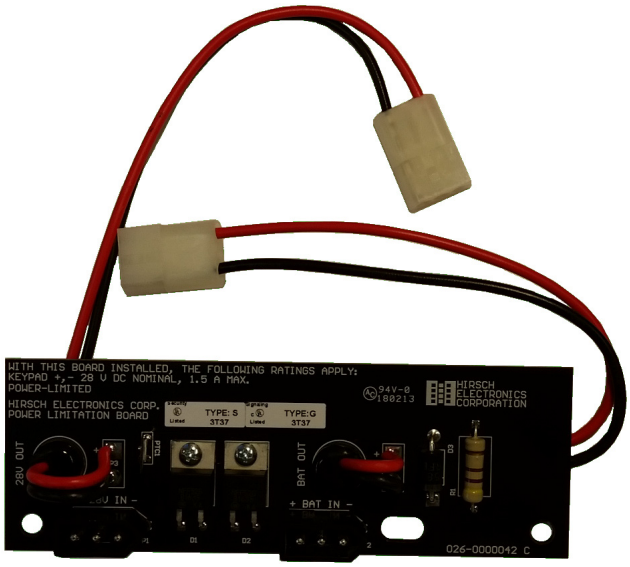
ENC-M4 AEB Encryption Extenders

An extender unit (ENC-E4) is only needed when more then four DS47Ls or MATCH 2s need to be encrypted. A cable that comes with the ENC-E4 is required to connect the two units. This cable will provide the encryption signal for the master to the extender unit.



Power Limitation Board Installation

To improve the safety of an M2, M8, or M16 DIGI*TRAC controller, you can install a Power Limitation Board.



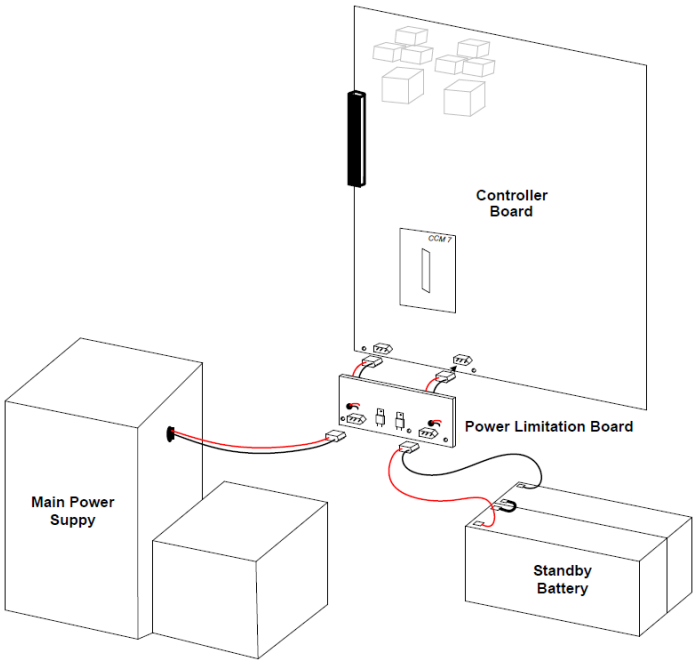
This board acts as a surge protector to ensure that the controller's keypad/MATCH terminal blocks (with a maximum of 1.5 Amps at 28 VDC) maintain their Class 2 power-limited level of safety. This board can also be used to ensure that a PS2 power supply's POWER 1 and POWER 2 terminal blocks maintain their Class 2 power-limited level of safety.

To Install the Power Limitation Board for a DIGI*TRAC Controller:

1. Unplug the Standby Battery's Molex power connector from the Controller's main board.
2. Unplug the Main Power Supply's Molex power connector from the Controller's main board.
3. Remove the two bottom left screws that attach the Controller's main board to the back panel of its metal enclosure.
4. Replace each of the removed screws by a connected pair of the supplied standoffs.

   Note: The standoffs for an M8 controller have a larger thread size.

5. As shown in the following illustration, plug the Power Limitation Board's **28V Out** and **BAT OUT** Molex power connectors into their receptacles on the Controller's main board.



6. Using the provided screws, mount the Power Limitation Board onto the standoffs.
7. Plug the Main Power Supply's Molex power connector into the **28V IN** receptacle on the Power Limitation Board.
8. Plug the Standby Battery's Molex power connector into the **BAT IN** receptacle on the Power Limitation Board.

To Install the Power Limitation Board for a PS2 Power Supply:

1. Unplug the Lock Standby / Inrush Battery pack's Molex power connector from the **LOCK BAT** connector on the PS2's main board.
2. Unplug the System Standby Battery pack's Molex power connector from the **SYS BAT** connector on the PS2's main board.
3. Unplug the Main Power Supply's Molex power connector from the **24 VAC** connector on the PS2's main board.
4. Remove the two bottom left screws that attach the PS2's main board to the back panel of its metal enclosure.
5. Replace each of the removed screws by a connected pair of the supplied standoffs.
6. Plug the Power Limitation Board's 28V Out Molex power connector into the **24 VAC** receptacle on the PS2's main board.
7. Plug the Power Limitation Board's **BAT OUT** Molex power connector into the **LOCK BAT** receptacle on the PS2's main board.
8. Using the provided screws, mount the Power Limitation Board onto the standoffs.
9. Plug the Internal Power Supply's Molex power connector into the **28V IN** receptacle on the Power Limitation Board.

10. Plug the System Standby Battery pack's Molex power connector into the **SYS BAT** connector on the PS2's main board.
11. Plug the Lock Standby / Inrush Battery pack's Molex power connector into the **BAT IN** receptacle on the Power Limitation Board.

PS2 Power Supply Installation

The PS2 Power Supply can power one or two heavy-duty locks/strikes or other powered devices. Power to these devices is triggered by outputs from the controller, connected to inputs on the PS2. The PS2 also includes a power connector for locally powering one or two ScramblePads at the door being controlled.

Mounting the PS2

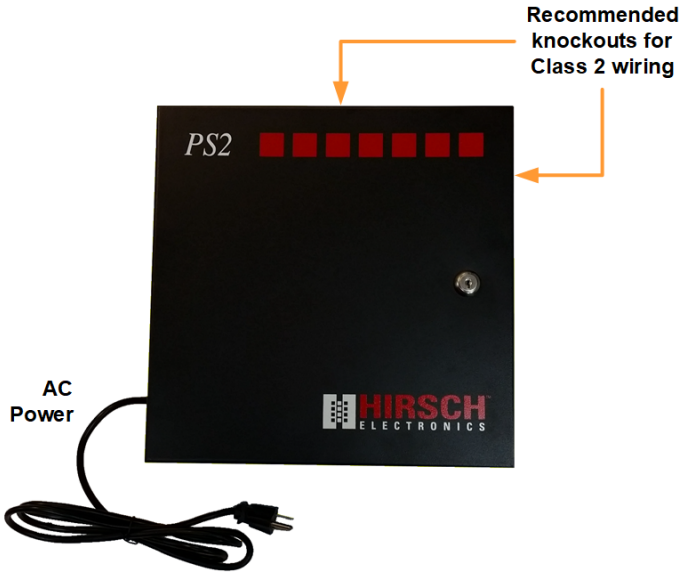
When connecting the PS2 to one or two ScramblePads, consider the maximum cable length allowed between the ScramblePads and the PS2. Refer to Table 2-15 on page 2-46 and the formula found in the next section for allowable lengths between these devices.

Mount the PS2 above the ceiling or on the secure side of the wall near the device(s) it is powering. Run either a 110 VAC power source to the PS2 or, if needed, a 220 VAC power source.

Note: If your facility uses a 220 VAC power source, make sure to specify this fact when ordering from Hirsch.

To Mount the PS2:

1. Locate a stud in the wall where the PS2 will be hung.
2. Punch the knockouts needed for AC input power and for the entry and exit of other conduits and cables in the PS cabinet. The following illustration of the 110V model shows the AC power cord installed by the factory through the knockout located on the lower left side, and the recommended knockouts for Class 2 wiring located on the top middle and the upper right side.



3. Use one of the three keyhole mounting holes along the top of the cabinet to hang the PS2. Since the PS2 cabinet is too narrow to mount on a pair of wall studs, use the center keyhole to catch a stud.
4. Use molly bolts or similar hardware in the other two keyholes to secure the cabinet to the wall. Use the bottom mounting holes to secure the cabinet further.

The PS2 power supply can be installed anywhere within the accepted range. It is normally installed as close to the devices it powers as possible. The maximum distance allowed between the PS2 and its attached devices depends on the wire gauge being used.

To calculate the allowed distance, refer to “Wiring the PS2” starting on page 7-308.

Wiring the PS2

Figure 7-71 provides an illustration of the PS2 connectors and the devices to which it can connect.

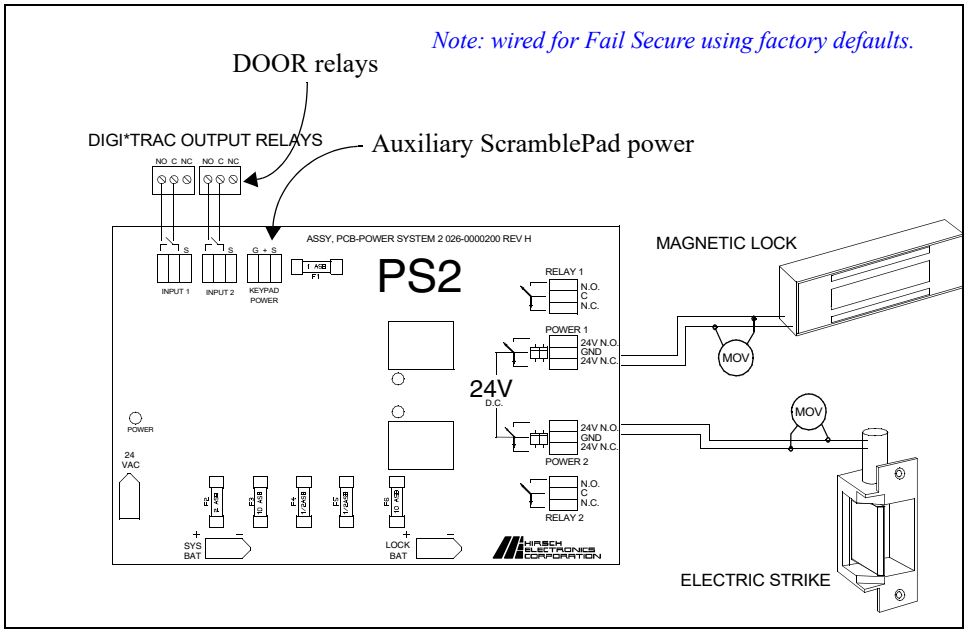


Figure 7-71: PS2 Connections

When routing the wires for the Class 2 limited-power circuits, make sure that you maintain a safe separation of at least 0.25 inches from the wires for the AC input power and the standby battery packs.

To Connect the PS2 to an AC Source:

The 120V version of the PS2 comes with a power cord and plug. You can:

- ❑ Connect the PS2 to an electrical outlet, or
- ❑ Remove the PS2 plug and rewire the power cord directly into the electrical wiring system of the facility.

For 100V and 240V versions, wire the PS2 directly into a transformer.

To Connect the PS2 to a Powered Device:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.

2. Run the cable from the device to the PS2. Do not run lock cable in the same conduit as other cable unless the lock cable is a twisted pair.
3. Connect the Common and NO or NC terminal of PS2's powered relays to the device you need to power. These are clearly marked as POWER 1 and POWER 2. Make sure you connect to the correct terminals. There is normally only one pair of connectors on the device.

Note: Only connect two of the three terminals. A device cannot be both NO and NC at the same time.

A Magnetic Lock is normally energized and must therefore be connected to the PS2 at the NC and C terminals while an Electric Strike is normally de-energized and is therefore connected to the PS2 at the NO and C terminals.

4. Install MOV suppression at the lock end. Use Hirsch Part# MOV35, Thomson VE09M00250K, GE #V39ZA1, or equivalent. If this is a DC lock, you can use a diode instead. Use a 1A, 400V diode (available as Hirsch Part# DIODE).

Note: Many locks come with suppression included. Make sure your lock does not have built-in suppression before adding an MOV or diode to the circuit.

To Connect Controller to the PS2:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Install the cable between the PS2 and the controller.
3. Connect one end of the twisted pair cable to two of the three terminals on a relay output terminal block at the Controller. One wire will connect to the C terminal. The other connects to the N.O. or N.C. terminal as shown in Figure 7-72.
4. Connect the cable to either INPUT 1 or INPUT 2 on the PS2 board. The input connectors (marked with the open switch symbol and a right angle symbol) are located at the upper left hand side of the board. INPUT 1 is tied to POWER 1 and INPUT 2 is linked to POWER 2 as shown in Figure 7-72.

For example, in Figure 7-71 the DIGI*TRAC controller output which will control the Magnetic Lock is wired into terminal block INPUT 1 because the lock is connected to POWER 1. Notice that the NC and C terminals are used, since the Magnetic Lock is designed as a normally energized device. The cable connected to INPUT 2 will trigger the device connected to POWER 2, the normally de-energized Electric Strike, so the NO and C terminals are used.

To Power ScramblePads/MATCH from the PS2:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Route the cable from the ScramblePad or MATCH to the KEYPAD POWER terminal block on the PS2. This terminal block is located at the upper center of the board.
3. Connect one end of the cable to the ScramblePad terminal block as shown in Figure 7-72. Use a three-wire cable to connect the wires in this manner:
   - Connect terminal G to the Black wire.
   - Connect terminal + to the Red wire.
   - Connect terminal S to the Shield wire.
4. Connect the wires to the PS2 in this order:
   - Connect the Black wire to the G terminal.

- Connect the Red wire to the + terminal.
- Connect Shield wire to the S terminal.

5. Connect one end of a twisted pair cable to the A and B terminals on the back of the ScramblePad. The G and S wires must be connected to the controller and the PS2.
6. Connect the other end of the twisted pair cable to the A and B terminals on the appropriate Controller ScramblePad/MATCH terminal block.

Each PS2 board also includes unpowered output for both Door 1 and Door 2. Use these outputs to trigger other operations associated with power maintenance or alarms.

To Connect To Unpowered Output:

1. Route the cable from the output device to the PS2. Each device must supply its own power, if power is required.
2. Connect one end of the cable to the output device (N.O. or N.C. and C).
3. Connect the other end of the cable to the Relay 1 or Relay 2 terminal block, located on the right side of the PS2 board.

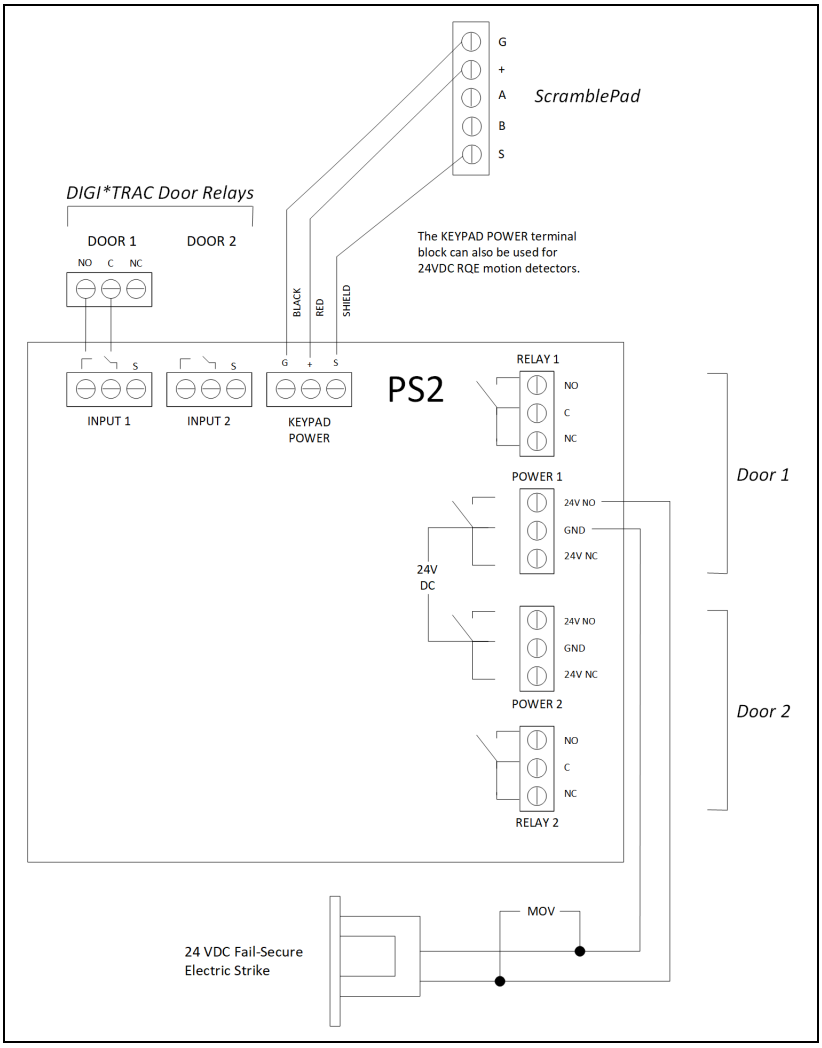


Figure 7-72: Connecting to the PS2

PS2 Versus Simple Power Supply Circuits

The PS2 is not just a power supply: it incorporates relays and inputs. Because of this, it is connected differently than normal power supplies.

In a normal power supply, the purpose is merely to power a lock or strike, therefore power is added to the circuit using a single line as shown in Figure 7-73:

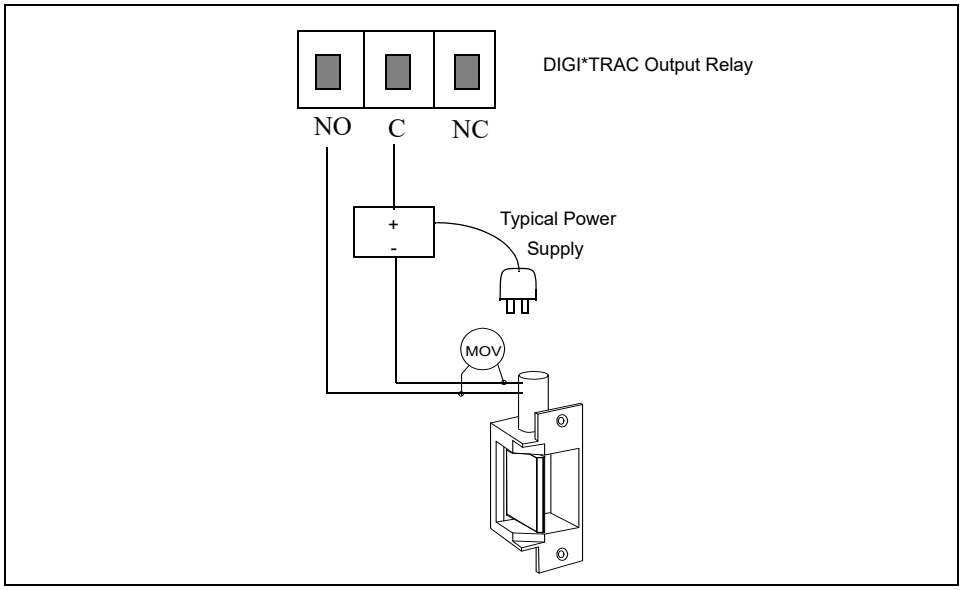


Figure 7-73: Typical Power Supply Circuit

As shown above, the Common line is connected through the power supply and this one wire is sufficient. However, when installing the PS2, both the Common and the NO or NC wires are connected as shown in the following figure.

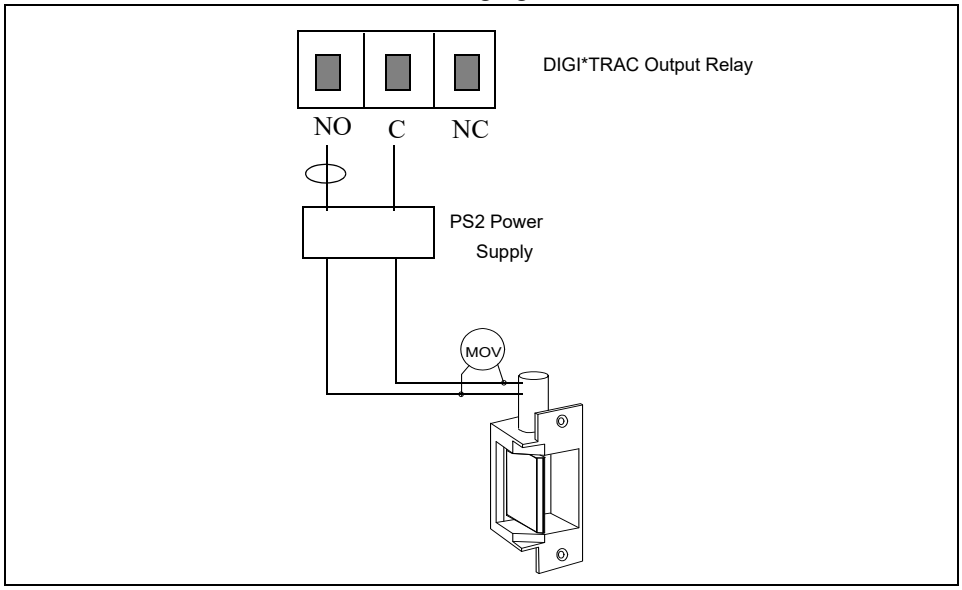


Figure 7-74: Typical PS2 Circuit

If a diode rather than an MOV is used, then this circuit should be included in the design:

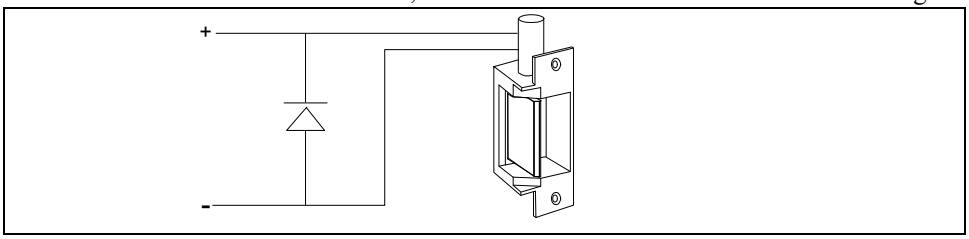


Figure 7-75: Diode Installation

Line Module Installation

The number of line module input functions depends on the DTLM or MELM selected. Choose the Line Module appropriate for the inputs being connected. Table 7-17 shows which Line Modules accommodate which inputs.

DTLM/MELM	INPUT 1	INPUT 2	INPUT 3
1	Door/Alarm	—	—
2	Door/Alarm	RQE	—
3	Door/Alarm	RQE	Tamper

Table 7-17: DTLM/MELM chart

The DTLM1/MELM1 has only one input for a dedicated Door/Line module input while the DTLM2/MELM2 has two inputs, accommodating both a dedicated Door/Line module input and RQE. The DTLM3/MELM3 has three inputs, enabling it to accept a Door/Line module input on INPUT 1, an RQE on INPUT 2, and a Tamper Detection on INPUT 3.

This section also explains how to install an SBMS3 balanced magnetic switch (refer to “Mounting and Wiring the SBMS3” on page 7-320).

Mounting the Line Module

The Line Module is usually located above the ceiling, on the wall, or in a J-Box (recommended), next to the door or accessway it is monitoring. A J-box or some other container is often used to protect the module from dust and debris; however, install the line module without a cover if so desired. An example of a DTLM connection is shown in Figure 7-76:

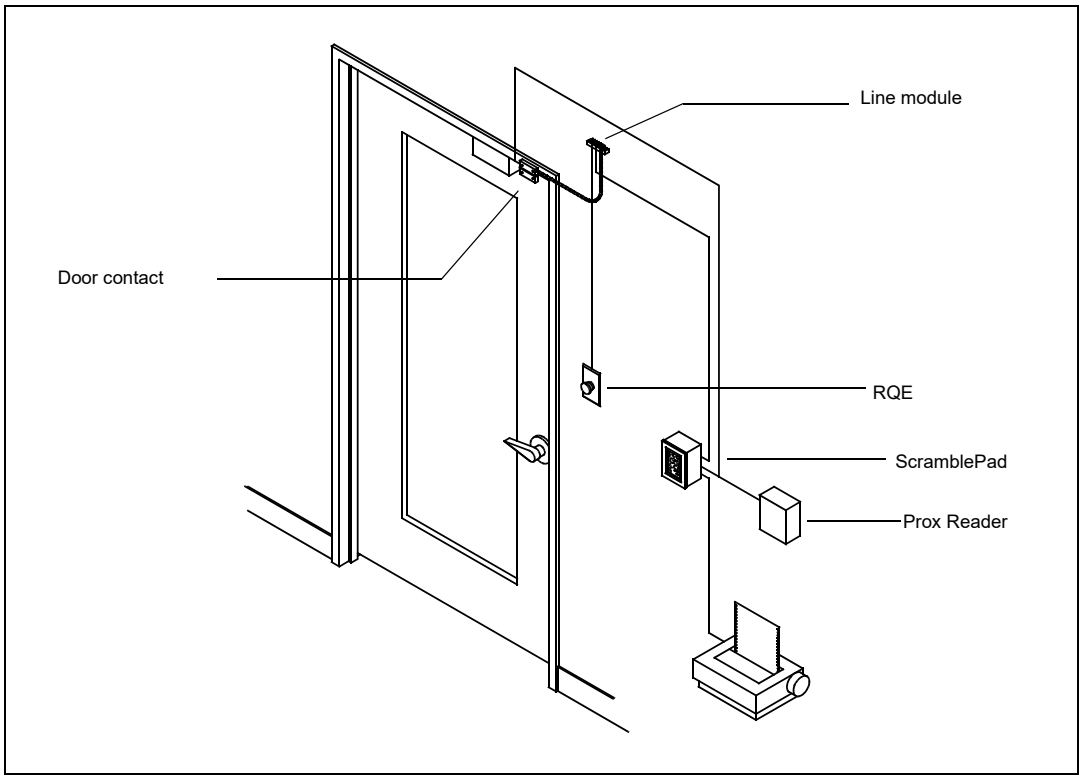


Figure 7-76: Line Module Example

A closer look at the example in Figure 7-76 reveals how connections and mountings are achieved for this DTLM:

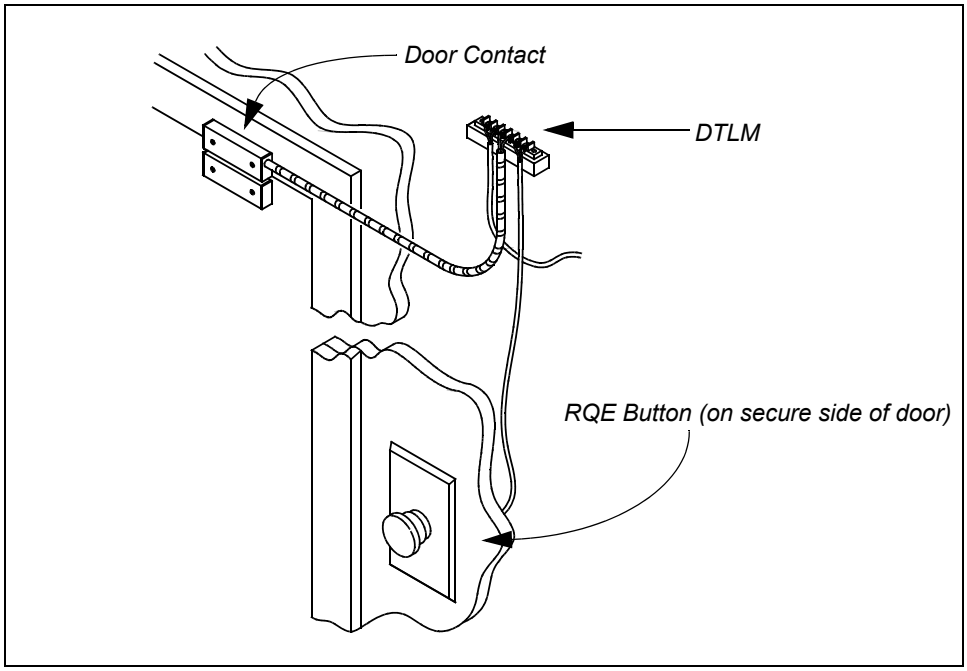


Figure 7-77: DTLM Example: Closer Look

The dimensions for each module are provided in Table 2-23 on page 2-77 and Table 2-25 on page 2-78.

In general, you should:

- ❑ Use the DTLM line module type where space is sufficient to place a small object and a screw terminal connection is needed.
- ❑ Use the MELM line module type – which is shaped like a short length of cable – where space is minimal and a flying lead connection is needed. MELMs can be used when mounting the module inside the monitored device.

Wiring the DTLM Line Module

Each DTLM input connector is designed for a specific input device. DTLM inputs are labeled 1, 2, and 3 for simplicity in which 1 normally connects to the door contact or alarm sensor, 2 connects to the RQE, and 3 monitors a Tamper switch. Don't try wiring an input device into an input connector for which it isn't designed. For example, don't try wiring an RQE to INPUT 1 or a Tamper Detection to INPUT 1 or 2.

DTLM line module connections are shown in Figure 7-80 on page 7-319. Their terminal assignments are described in Table 2-22 on page 2-75.

For maximum cable lengths between the controller and each DTLM/MELM module, see Table 2-2 on page 2-13.

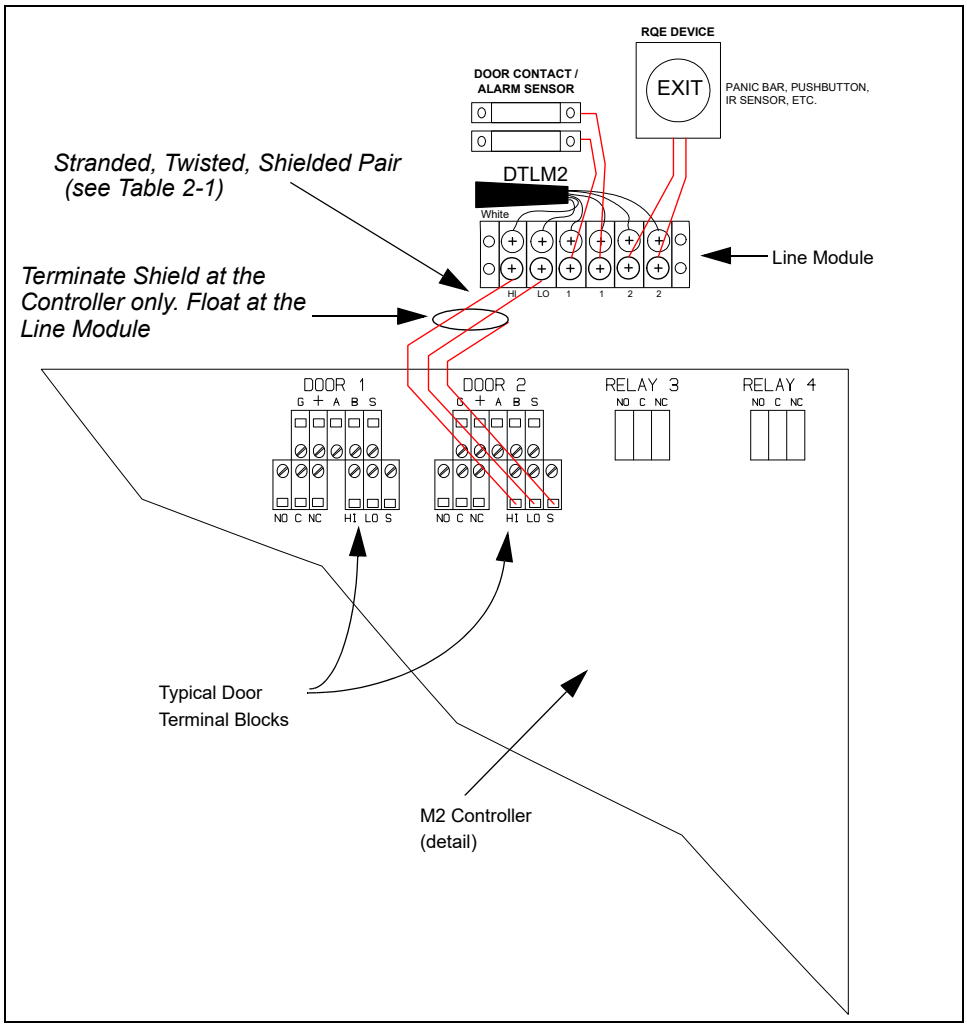


Figure 7-78: Typical Line Module Input Connection

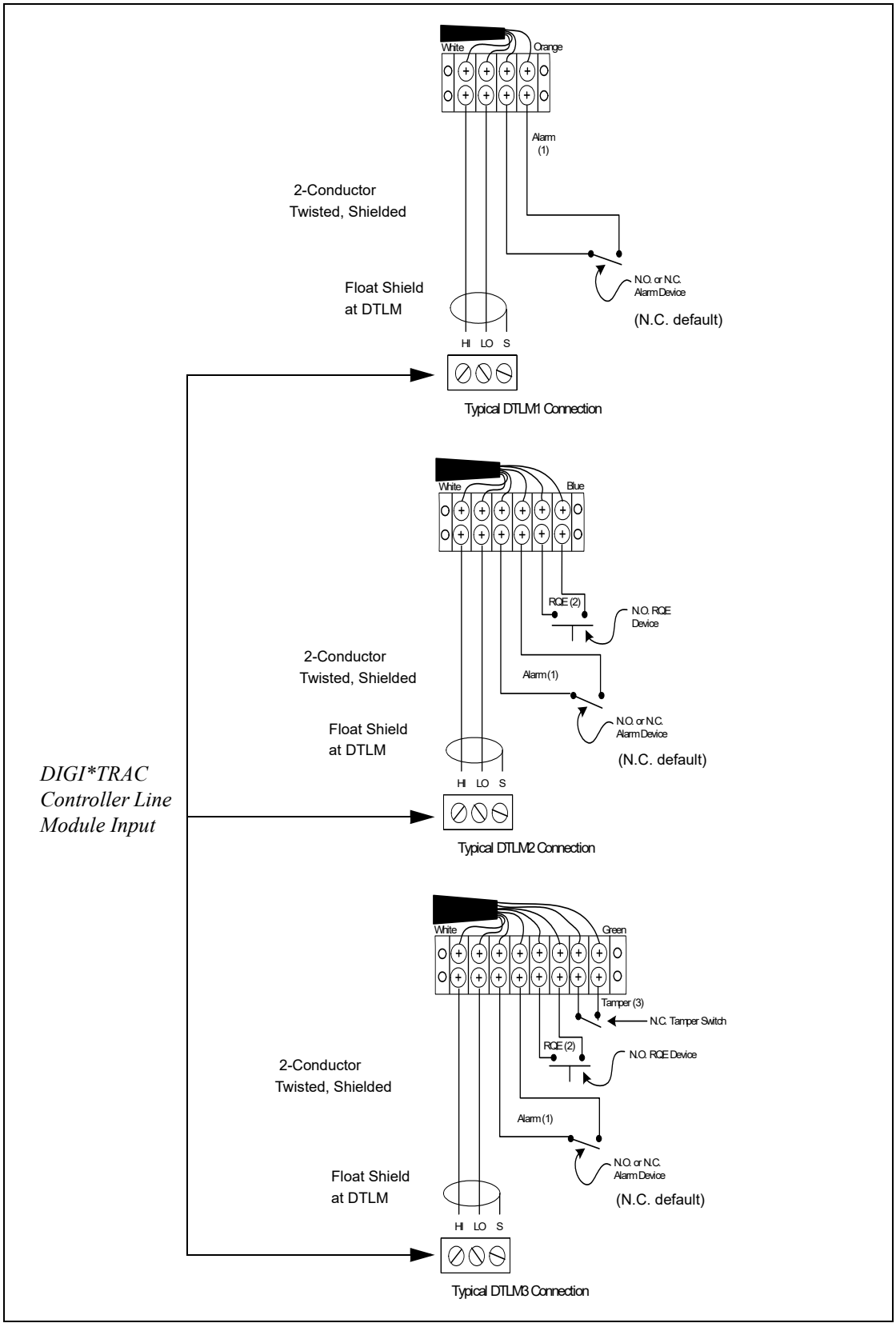


Figure 7-79: DTLM Wiring

To Connect Inputs to the DTLM Line Module:

1. Connect the door position or alarm sensor to INPUT 1. This connects to either an NO or NC alarm device.

DTLM2/3

2. Connect the RQE switch to INPUT 2. This always connects to an NO RQE device.

DTLM3

3. Connect tamper switch, if required, to INPUT 3. This always connects to an NC tamper device.
4. Run a twisted, shielded pair cable from the Line Module to the Controller.
5. Connect the shield at the controller terminal and let it float (do not connect it) at the DTLM/MELM.
6. Connect one end of the cable to the DTLM/MELM:
   - Connect one wire at the DTLM's HI terminal.
   - Connect the second wire at the DTLM's LO terminal.
7. Connect the other end of the cable to the Controller:
   - Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
   - Connect the HI wire from the DTLM to the Controller's HI terminal.
   - Connect the LO wire from the DTLM to the Controller's LO terminal.
   - Connect the Shield to the S terminal.

Wiring the MELM Line Module

Each Line Module input connector is designed for a specific input device. Don't try wiring an input device into an input connector for which it isn't designed. For example, don't try wiring an RQE to INPUT 1 or a Tamper Detection to INPUT 1 or 2.

MELM line modules are miniaturized versions of the DTLMs. As such they require a different wiring plan, as shown in Figure 7-80.

For maximum cable lengths between the controller and each DTLM/MELM module, see Table 2-2 on page 2-13.

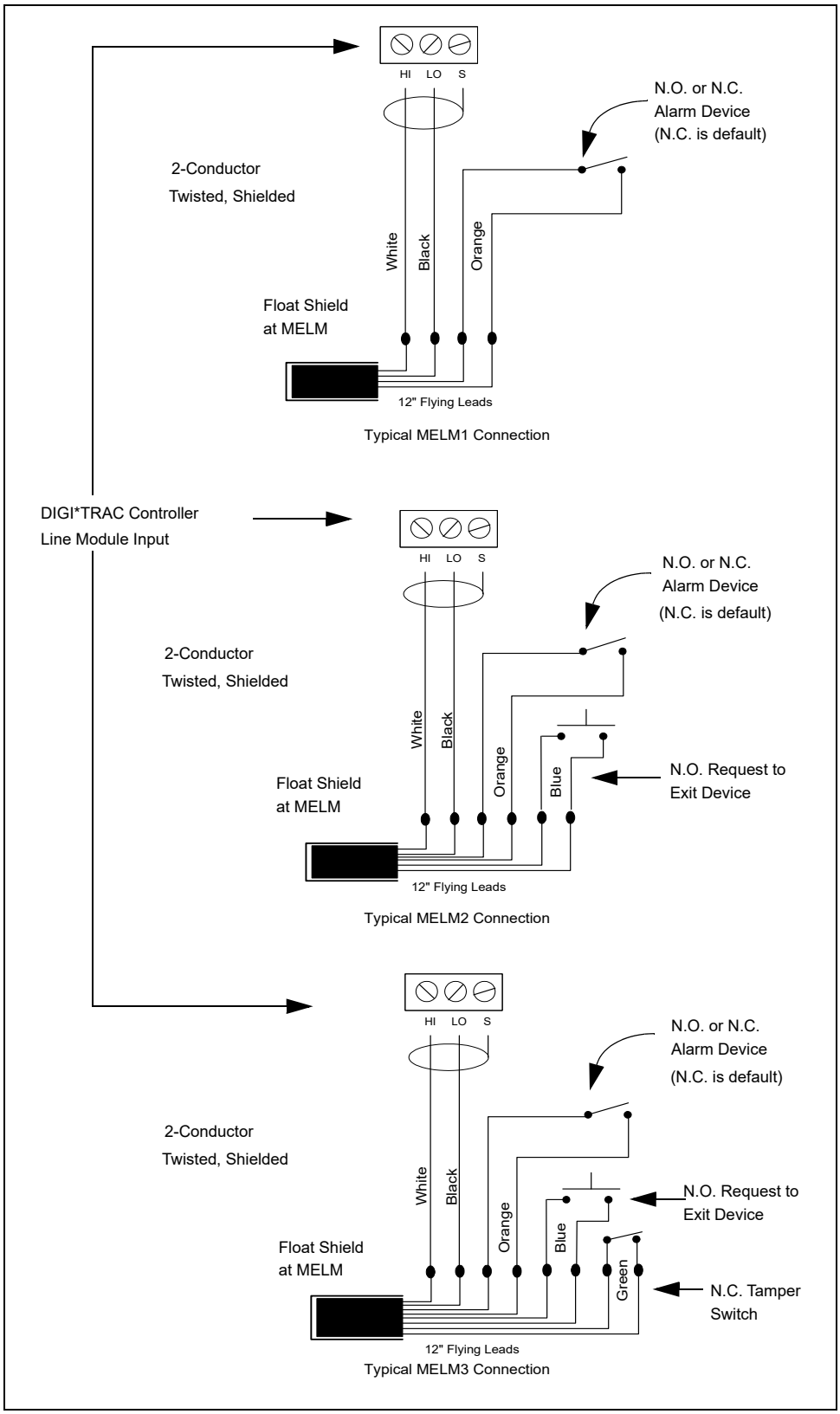


Figure 7-80: MELM Wiring

To Connect Inputs to the MELM Line Module:

1. Connect the door position or alarm sensor to Orange wire pair. This connects to either an NO or NC alarm device.

MELM2/3

2. Connect the RQE switch to Blue wire pair. This always connects to an NO RQE device.

MELM3

3. Connect tamper switch to Green wire pair. This always connects to an NC tamper device.
4. Run the Black and White wire pair to the Controller.
5. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
6. Connect the shield at the controller terminal and let it float at the MELM.
7. Connect the other end of the cable to the Controller:
   - Connect the White wire from the MELM to the Controller's HI terminal.
   - Connect the Black wire from the MELM to the Controller's LO terminal.

Mounting and Wiring the SBMS3

The SBMS3-2707A is a balanced magnetic switch with an MELM3 installed.

To Mount and Connect Inputs to the SBMS3:

1. Install the SBMS3 switch on the required door.
2. Connect the RQE switch to the Blue wire pair. This always connects to an N.O. RQE device.
3. Run the Black and White wire pair to the Controller.
4. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
5. Connect the shield at the controller terminal and let it float at the MELM.
6. Connect the other end of the cable to the Controller:
   - Connect the White wire from the SBMS3 to the Controller's HI terminal.
   - Connect the Black wire from the SBMS3 to the Controller's LO terminal.

Note: Tamper is built into the device. Follow the manufacturer's mounting instructions.

Door Relay Installation: Strikes and Locks

A number of door relays including locks and strikes can be wired to a DIGI*TRAC controller. A typical door relay connection between a lock and a controller would look like Figure 7-81.

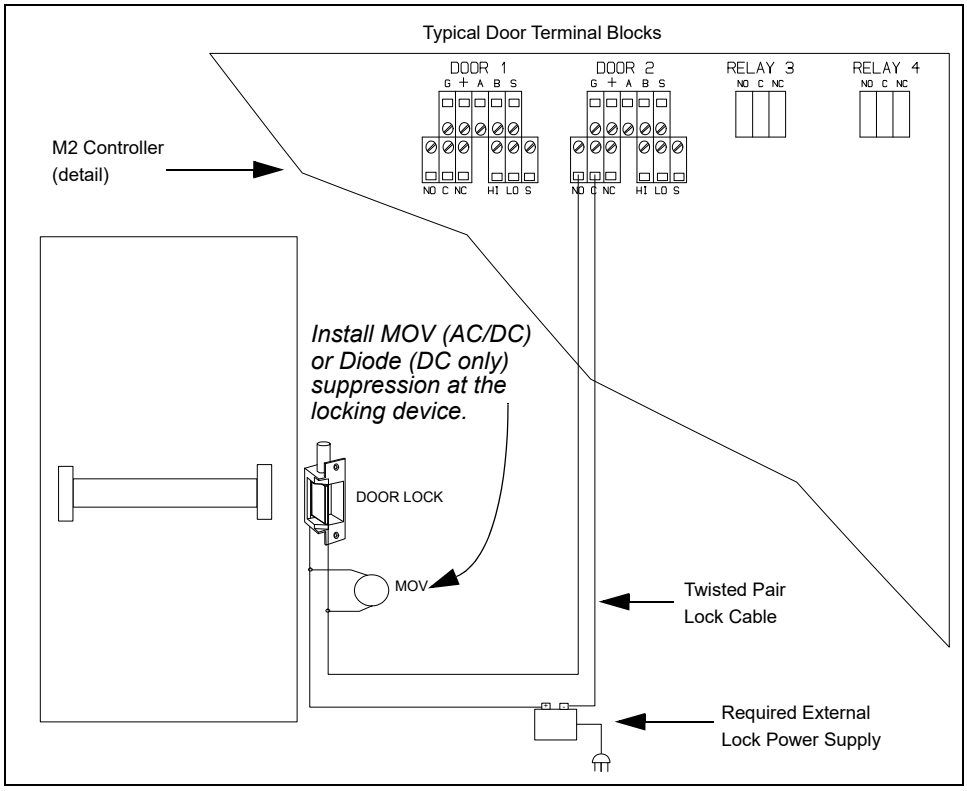


Figure 7-81: Typical Door Relay Connection

If you are using a PS2 power supply, DIGI*TRAC door relays don't switch lock power through their contacts. Only a pilot signal is run between the controller relay and the PS2 input. This configuration allows wiring from the controller to be run in a common conduit since ScramblePad/MATCH and line module circuits are protected from the induction of electrical interference – such as surges, spikes, or noise – which are commonly experienced by electric lock cables.

HVAC, Lighting, and Elevator Control

Heating, ventilation, air conditioning, lighting and elevator control are generally handled by the smaller 24 VDC, 2A relays found on expansion boards and MSP-8R or M64 controllers. The MSP-8R and M64, are specifically designed for this kind of control switching. One of the chief uses for the M64 is elevator control while the MSP-8R is used for many management and control applications, including HVAC, lighting, prison door control, interlock, and CCTV.

An example of both lighting control and elevator control are shown in Figure 7-82:

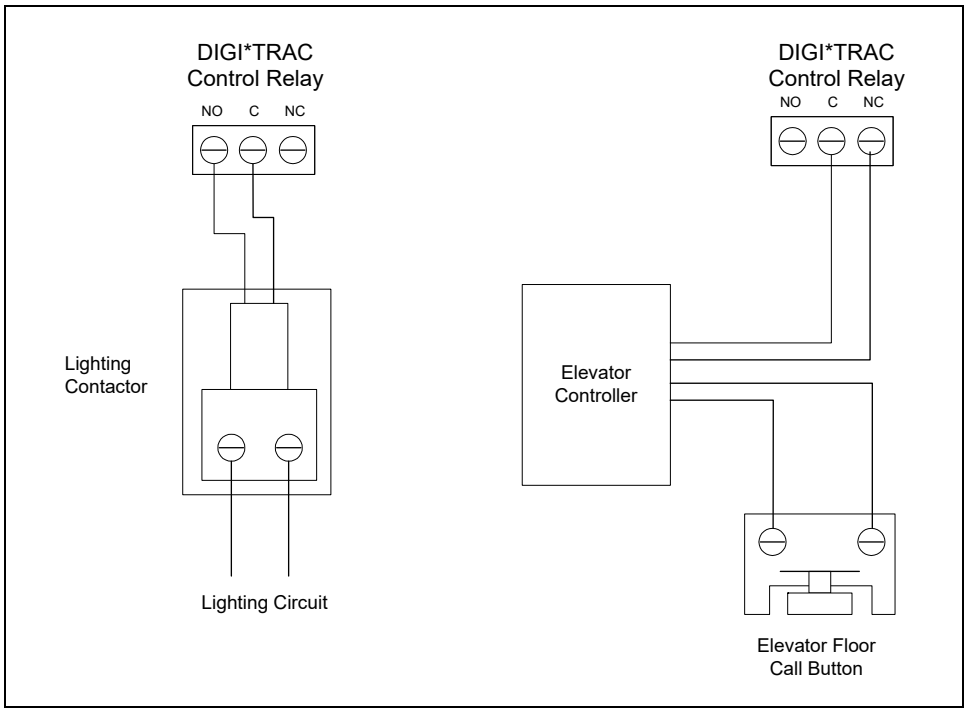


Figure 7-82: Lighting/Elevator Control

HVAC and lighting circuits are normally connected to the N.O. and C terminals on the control relay terminal block. They are generally turned off until they are activated by the relay. Lighting contractors can use split coil solenoids which require a separate DIGI*TRAC control relay for ON and another for OFF.

Elevator control circuits can utilize the N.C. and C terminals if the wiring passes through the floor call button. Modern elevators, however, have separate inputs for access control, and provide dedicated circuits from the floor call button to the elevator control panel.

There are no hard-and-fast rules for HVAC, lighting, and elevator control circuits: different devices call for different circuit states and the designing engineer must determine the best arrangement for each application.

Printer Installation for Standalone Controller

To install a standard parallel printer for a standalone controller, do the following:

1. Connect the cable to the controller's parallel printer port.
2. Tighten the screws.
3. Plug the other end into a dot matrix printer. (Do not use a laser or inkjet printer for this purpose.)
4. Load paper in the printer and align the printer head with the top of page before turning on the printer. Aligning the top of page prevents transactions and reports from printing beyond the end of a page.

   Hirsch Systems print a page/sequence number at the top right hand edge of every page. This number will indicate to you if a page is missing or a multiple page report is out of sequence. The numbering starts with the first page printed when the system is started for the first time or cold started.
5. Allow for a clear paper path. One of the most common problems associated with printers is paper jams. A good printer stand with a clear feed for the paper is essential for reliable printing.
6. Turn the printer on to verify it is working properly.

Printing in Programming Mode

DIGI*TRAC systems include a unique Operator Help capability. If an error is made when entering a programming command on a ScramblePad, the Controller will detect it and print an error message, such as "value too big", then print the correct syntax. If you know the command number but not the correct syntax, enter the command followed by two asterisks and the # key. For example:

```
START 10 * * #
```

The correct syntax will be printed out for Command 10. In addition, the complete set of programming commands can be printed by category or in numerical order by using the Command 00. In order to use this capability, you must have a ScramblePad connected to your controller.

Using Printing to Troubleshoot

If your system isn't operating properly, you can usually diagnose the problem using Command 88 – System Setup and Status. Of particular use is the syntax for Detailed Relay Status. The most frequent problem is caused by improper programming or set up conflicts. It is possible to program events so that they prevent other events from occurring, or prevent otherwise valid codes from working. These conditions can be observed in print outs. Use this command syntax:

```
88 * 0 #
```

Normal Printing

DIGI*TRAC controllers are shipped with the default setting to print everything. This includes all code transactions, all alarm events, all relay state changes, daily status reports and weekly system status reports. During initial system configuration, all this data is useful in order to verify the initial system operation. However, after a certain amount of time – 3 to 6 months – you can reduce the quantity of information printed by using Commands

05 and 06. Command 05 lets you turn off printing by category of events, such as relay state changes. Command 06 lets you turn off printing of granted but not denied code transactions and granted RQE events on a door-by-door basis. Whenever an alarm occurs – such as code tampering, duress, or tagged user code – the alarm is printed by time, date, and location.

Figure 7-83 illustrates the parallel port connection between the DIGI*TRAC controller and a printer, such as the PR1. For a serial printer connection, refer to “Serial Communications Interface Board (SCIB) Installation” on page 7-39.

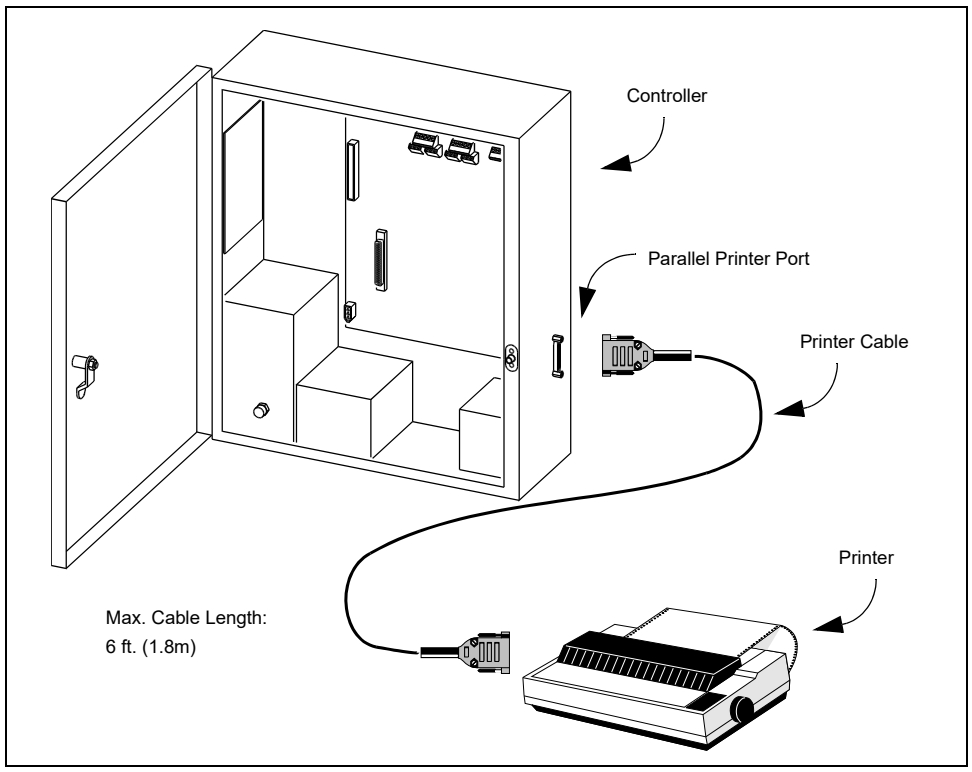


Figure 7-83: Controller to Printer Connection

Enrollment Station Installation

Hirsch offers several choices for enrollment stations:

- ❑ DMES
- ❑ SMES
- ❑ nedap enrollment station
- ❑ RUU Verification Stations

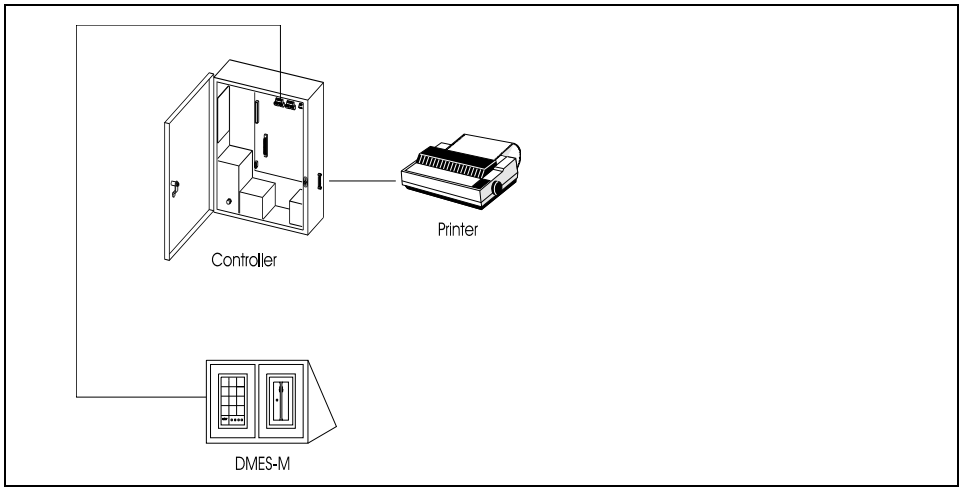


Figure 2-84: DMES Station

Both stations require correct connection of the MATCH on the back of the station to the appropriate device (Controller for the DMES or Host PC for the SMES). Figure 7-85 shows possible connection arrangements.

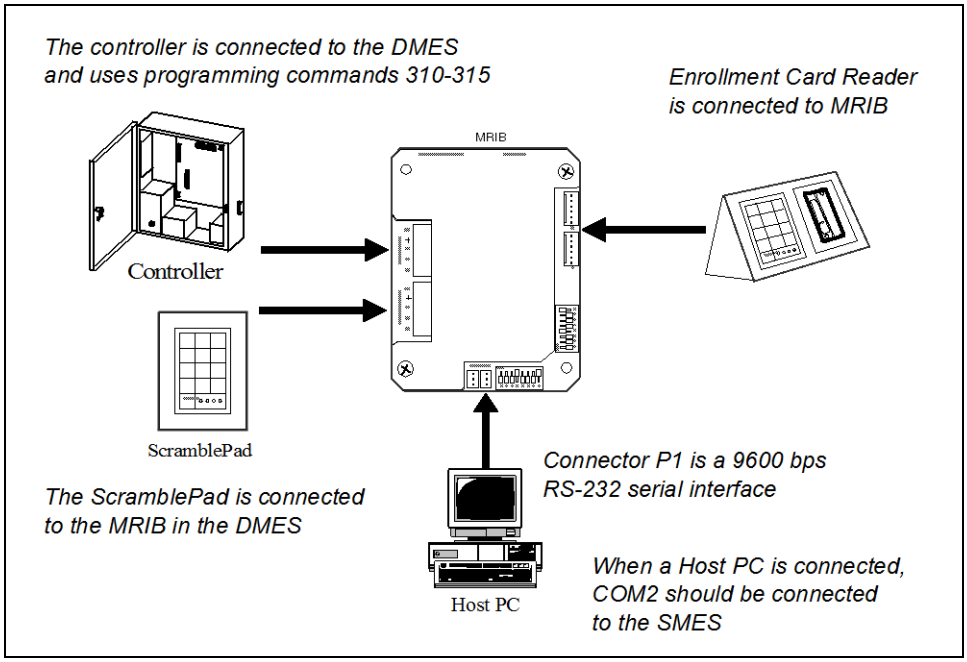


Figure 7-85: Possible Enrollment Station Connections

To install the DMES:

1. Turn the DMES over to expose the MRIB on the underside of the DS47L. Make sure the DS47L is correctly connected to the KEYPAD port on the MRIB.

   If you have purchased a DMES-U, you must connect your selected reader to the MRIB reader port on the back of the DMES.

2. Using a 2-pair shielded, twisted, stranded cable, connect one end to the D*TRAC port on the MRIB as shown in Figure 7-86.

   If this station will be independently powered, only connect the A, B, G, and S wires. If the controller will power this station, connect all five wires.

3. Connect the other end of the cable to an available ScramblePad/MATCH terminal on the controller as shown in Figure 7-86.

4. If not already done, connect a printer to the controller. Refer to "Printer Installation for Standalone Controller" on page 7-323 for more information.

5. To connect the DMES to a host PC:

   a. Purchase an ESC1 cable from Hirsch.

   b. Connect the 3-pin connector of the cable to the P1 port on the bottom of the MATCH board as shown in Figure 7-85.

   c. Connect the cable's DB25 connector to the COM2 serial port on the host PC.

Note: This uses the newer MATCH2 port designations. The older MATCH used the P2 port designation as the connector to the host PC.

6. Use commands, like CMDs 310 through 315, on the DMES ScramblePad to enroll cards and assign user numbers to them.

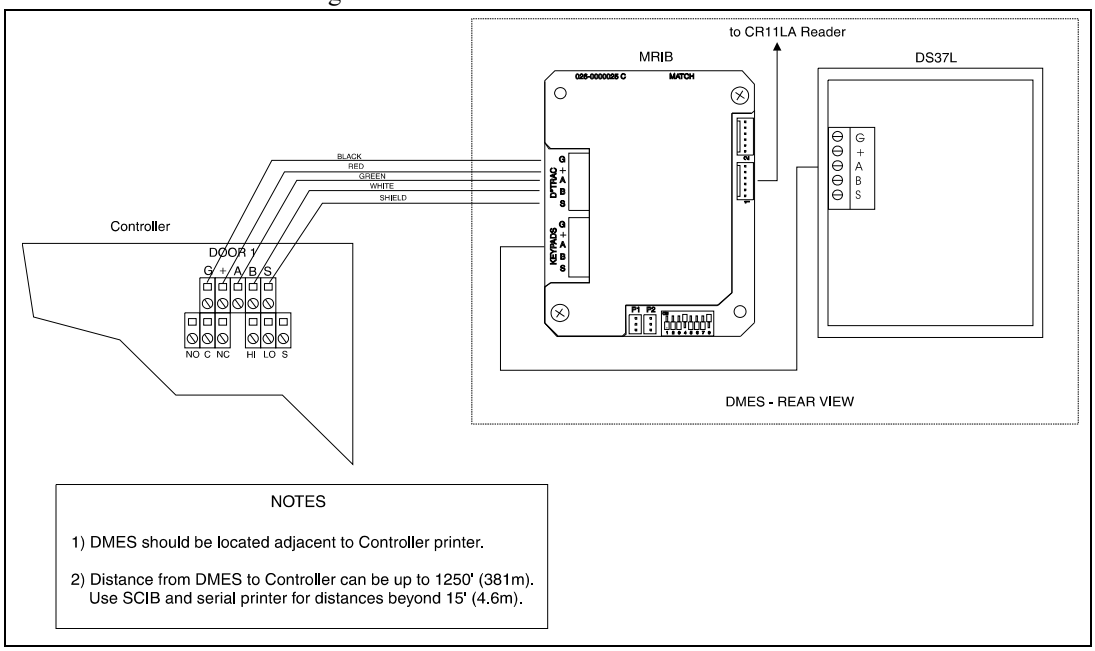


Figure 7-86: DMES Installation

For more on applicable commands, refer to Chapter 4, "Command Reference."

To install the SMES:

1. Turn the SMES over to expose the MRIB on the underside of the ES2 stand.

Make sure the reader is correctly connected to the reader port on the MATCH2.

2. If you have purchased a SMES-U, you must connect your selected reader to the MATCH2 reader port on the back of the SMES.
3. Connect the 3-pin connector end of the ESC1 cable (included with the SMES package) to the 3-pin P1 port on the bottom of the MATCH2 board as shown in Figure 7-87.
4. Connect the ESC1's DB25 connector to the COM2 serial port on the host PC.

Note: This uses the newer MATCH2 port designations. The older MATCH used the P2 port designation as the connector to the host PC.

5. Connect the terminal block end of the ESPT power adaptor (included with the SMES package) to the D*TRAC connector on the MATCH2 board.
6. Plug the ESPT power block into a convenient socket.

An example of the SMES-M wiring is shown in Figure 7-87:

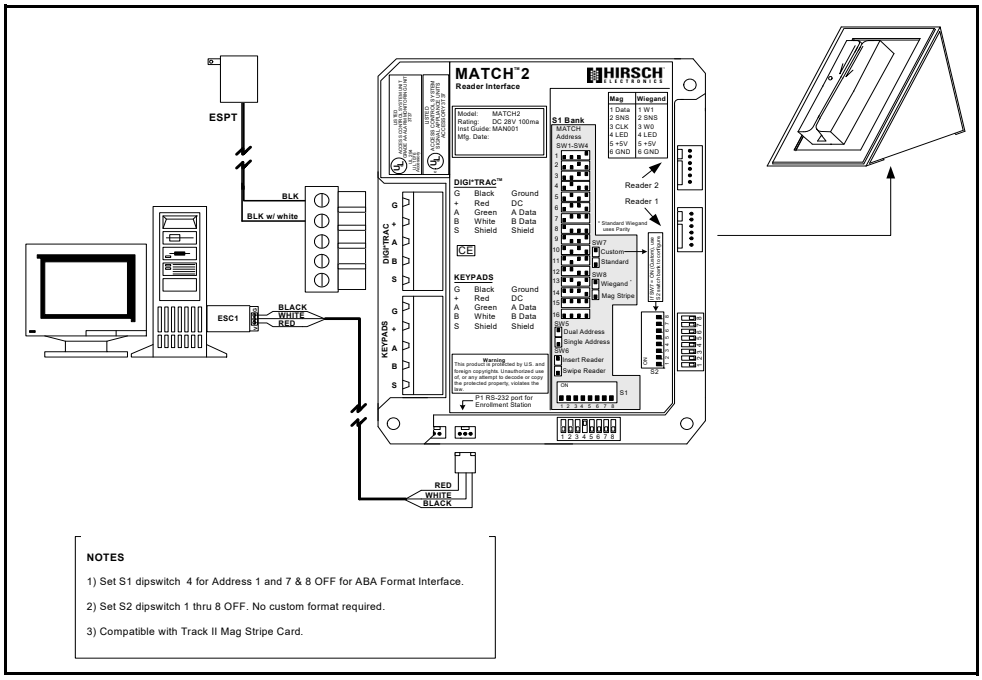


Figure 7-87: SMES Wiring

Hirsch nedap Enrollment Station Installation

Use the following procedure to connect the Hirsch nedap® Enrollment Station (Hirsch # CR-NES) to the DIGI*TRAC system:

1. Fabricate a cable using the specifications shown in Figure 7-88.

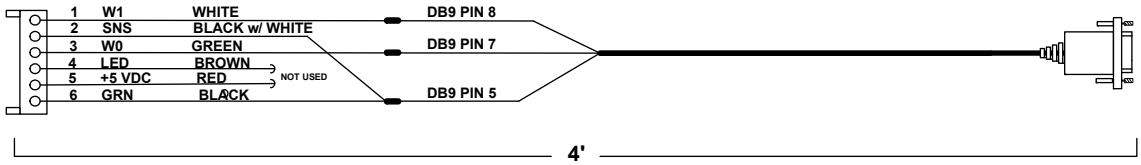


Figure 7-88: nedap Enrollment Station Cable Fabrication

2. Connect the terminal block end of the fabricated cable to one of the two Reader ports on the MATCH 2.

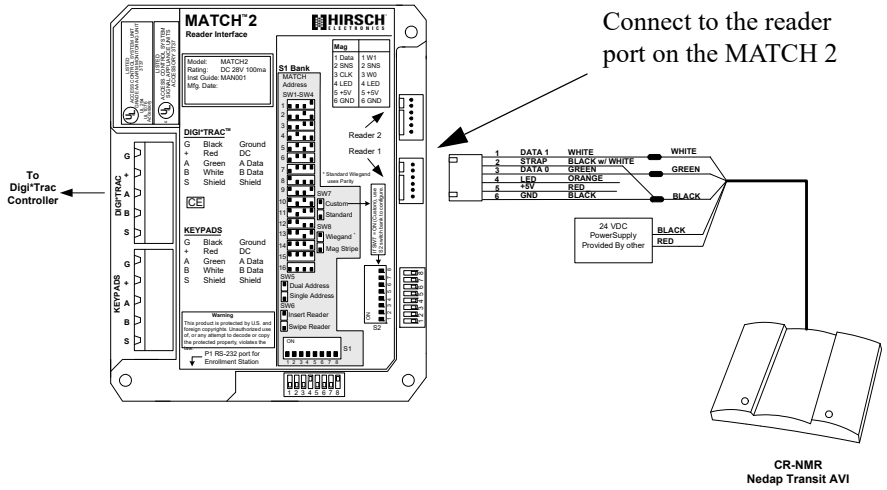


Figure 7-89: nedap to MATCH Connection

3. Connect the serial connector end of the cable to the nedap serial port.

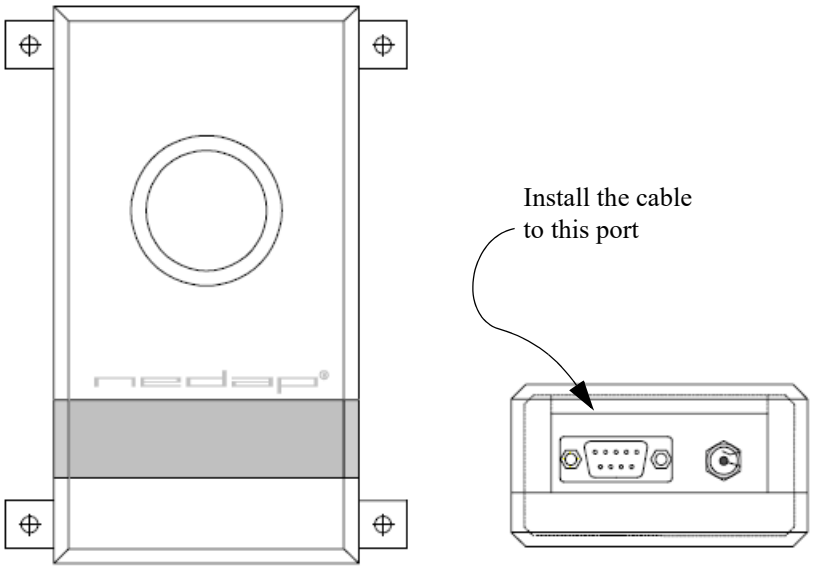


Figure 7-90: nedap Port Connector

4. Using an ESC1 cable, connect the MATCH to the workstation.

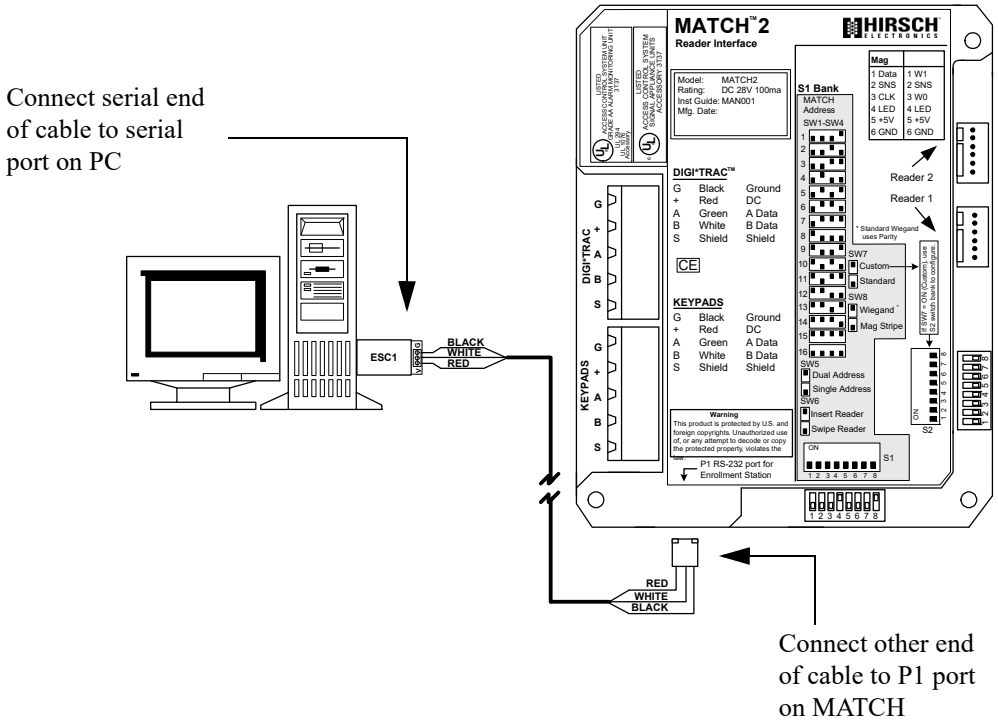


Figure 7-91: Connecting Workstation to MATCH

Purchase the ESC1 cable through Hirsch.

RUU Verification Station

The RUU can be used as either a smart card entry/exit reader or an enrollment station for a variety of smart cards.

For details on setting up and configuring this system, refer to “RUU Verification Station” on page 7-329.

For a complete explanation of the set up and configuration of the RUU, refer to the *Verification Station Configuration Guide*.

DIGI*TRAC Annunciator Installation

The DIGI*TRAC Annunciator (DTA) is integrated with its own MATCH2 so that most of the installation and configuration requirements for the Annunciator are identical to those you would make for the MATCH2 board (refer to “MATCH Interface Installation” on page 7-134).

In general, the DTA connects to the reader or ScramblePad which activates it in this way:

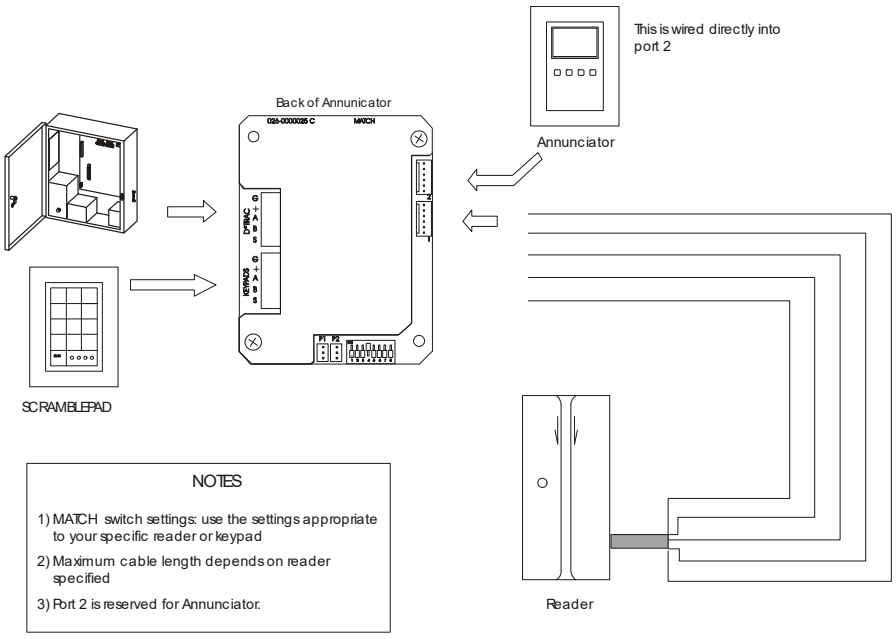


*Figure 7-92: DIGI*TRAC Annunciator Installation*

This is almost exactly the same way the MATCH attaches to the controller and reader/keypad.

If a local power supply is required, refer to “Powering the ScramblePad Locally” on page 7-125 for the technique to use.

If you need to attach a ScrambleProx to the Annunciator, you must first disconnect the ScrambleProx data cable from its connection to its local MATCH2 board. Once disconnected, reconnect it to the keypad port on the back of the DTA.

For more specific instructions on installing and using the DTA, please refer to the *DIGI*TRAC Annunciator User’s Guide*.

Network Component Installation

This section explains the setup and installation of these network components:

- ❑ Secure Network Interface Board (SNIB)
- ❑ NET*MUX4 Network Multiplexor
- ❑ Adaptors and Connectors
  - NET*ADAPT Communications Adaptor (NA1) (External)
  - NET*ADAPT-PC Communications Adaptor (NAPC) (Internal)
  - MODEM*CONNECT Network Connector (MC1/MC2)
  - MODEM*ADAPT Communications Adaptor (MA1/MA2)
  - MODEM Cable (MC-PC)
  - AT ADAPTOR Cable (AT-AC)
  - PC*CONNECT Network Connector (PC1)
- ❑ Telecommunications: Modems/Transceivers
  - Dial-Up Modems
  - Leased-Line Modems or Short-Haul Modems
  - Fiber Optic Transceivers
- ❑ SCRAMBLE*NET Gateway (XBox)

Secure Network Interface Board Installation

For complete SNIB installation instructions, refer to “Secure Network Interface Board (SNIB, SNIB2, or SNIB3) Installation” on page 7-42.

For information on the SNIB’s use within the SCRAMBLE*NET, see “Secure Network Interface Board (SNIB, SNIB2, or SNIB3)” on page 2-33.

NET*MUX4 Network Multiplexor Installation

The NET*MUX4 is used to expand the Hirsch SCRAMBLE*NET system to:

- ❑ 63 controllers on a multi-drop RS-485 network (wired in a star configuration)
- ❑ Multiple single-ended devices, such as leased-line modems. Additional NET*MUX4s can be cascaded for more than four single-ended devices and/or RS-485 multi-drop cable runs

*Note: Installation of other equipment or devices within the NET*MUX4, or powering of non-approved equipment or devices from the NET*MUX4, can cause system failure or damage, and can void the warranty.*

Each NET*MUX4 S*NET channel provides 1500V of magnetic and optical isolation, to eliminate the ground potential problems that are often associated with widely dispersed networks.

RS-485 ports are designed to withstand circuit transients as described in UL294. This is of particular importance when a network is dispersed among several buildings.

NET*MUX4 Mounting and Connection

There are several steps involved in installing the NET*MUX4:

- ❑ Mounting the NET*MUX4 in an appropriate location.
- ❑ Connecting the NET*MUX4 to the Host PC.
- ❑ Connecting the NET*MUX4 to its Controllers.

Each procedure is described in the following section.

To mount the NET*MUX4:

1. Install the NET*MUX4 in a convenient location.
2. Connect the NET*MUX4 to the PC as described in the following procedure.
3. Connect the NET*MUX4 to modem(s) and/or Controller(s) as described.

To connect the NET*MUX4 to the Host PC:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power on the NET*MUX4. Power off the PC.
2. Obtain the required serial (RS-232) cable or RS-485 cable (NA1, which comes with SAM).
3. Wire into either the RS-232 or RS-485 terminal block of the appropriate S*NET MASTER port on the NET*MUX4. The wires are arranged in this way:

   For RS-485 Cabling:

Connector Block	5	4	3	2	1
Wire	G	-RX	+RX	-TX	+TX

   For RS-232 Cabling:

Connector Block	4	3	2	1
Wire	G	TX	RX	V

4. Connect the other end of the cable to the PC's RS-485 or RS-232 serial port.

   To connect the PC using the RS-232 interface, the cable will use one of two connectors: DB25 or DB9.

   Depending on which connector it is, make sure the wiring conforms to this pinout:

S*NET MASTER (RS-232)	**PC COM Port**	
	DB25	**DB9**
G	7 G	5 G
TX	3 RX	2 RX
RX	2 TX	3 TX

Table 7-18: RS-232 to PC COM Port Pinout

To connect the NET*MUX4 to a Leased-Line Modem:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Obtain the serial (RS-232) cable you require.
3. Wire one end of the cable into the RS-232 terminal block on the appropriate S*NET (S*NET1, 2, 3, or 4) port on the NET*MUX4. The wires are arranged as shown in the previous tables.
4. Connect the other end of the cable to the modem.

   If this is an RS-232 cable, make sure your modem has a DB25 connector with these wiring specifications:

S*NET RS-232	G	TX	RX
Modem DB25 Pins	7	2	3

Make sure this is a leased-line modem.

To connect the NET*MUX4 to one or more Controllers:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power on both the NET*MUX4 and controller.
2. Wire one end of the cable to either the RS-232 or RS-485 terminal block from the appropriate S*NET port on the NET*MUX4.
3. Connect the other end of the cable to the SNIB board installed in the Controller.

   If this is an RS-485 cable, make sure it connects to the appropriate S*NET connector on the SNIB board. Make sure the wiring conforms to this specification:

NET*MUX4 RS-485	G	-TX	+TX	-RX	+RX
SNIB S*NET Pins	G	-RX	+RX	-TX	+TX

   If this is an RS-232 cable, make sure it connects to the appropriate RS-232 connector on the SNIB board.
4. To multi-drop additional SNIB-installed Controllers (up to 16 for each NET*MUX4 S*NET port):

   d. Run an RS-485 cable from the first Controller to the second. The total distance from the NET*MUX4 to the last controller can be up to 4000 feet (1220 meters) for RS-485.

   e. Insert a second set of wires from the new cable into the appropriate SNIB terminal block on the first controller. See Figure 7-93 for an example.

      To facilitate wiring, remove the terminal block from the SNIB, insert second set of wires, then reinsert the block.

   f. Remove the SNIB terminal block on the second Controller and wire the other end of the cable to that block as shown in Figure 7-93.

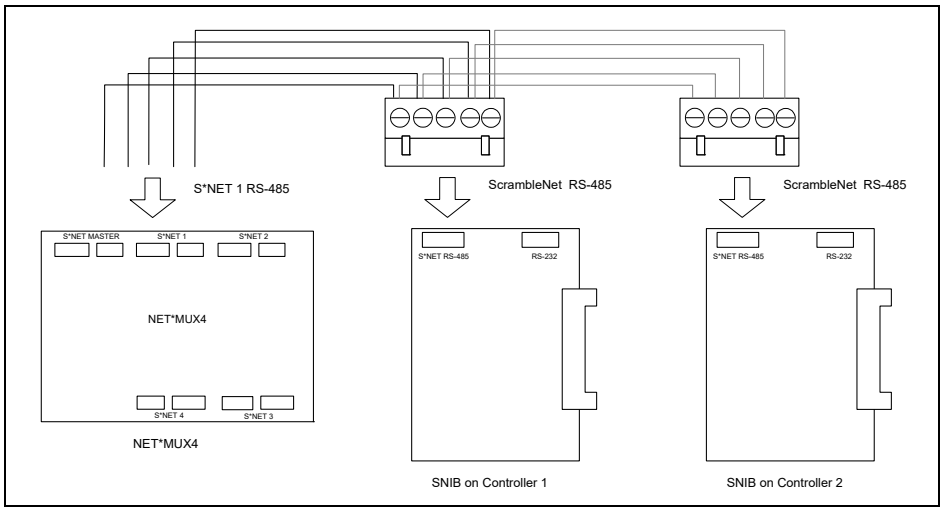


Figure 7-93: Multi-Dropping Controllers

g. Reinsert the terminal block into the second Controller.

h. Repeat steps a - d for each Controller you want to add to the link.

i. At the last SNIB in the multi-drop sequence, turn ON DIP switches SW1 and SW2.

*Note: Make sure that you don't mix RS-232 or RS-485.Figure 7-94 illustrates possible NET*MUX4 connections. For more on SNIB installation, refer to "Secure Network Interface Board (SNIB, SNIB2, or SNIB3) Installation" on page 7-42.*

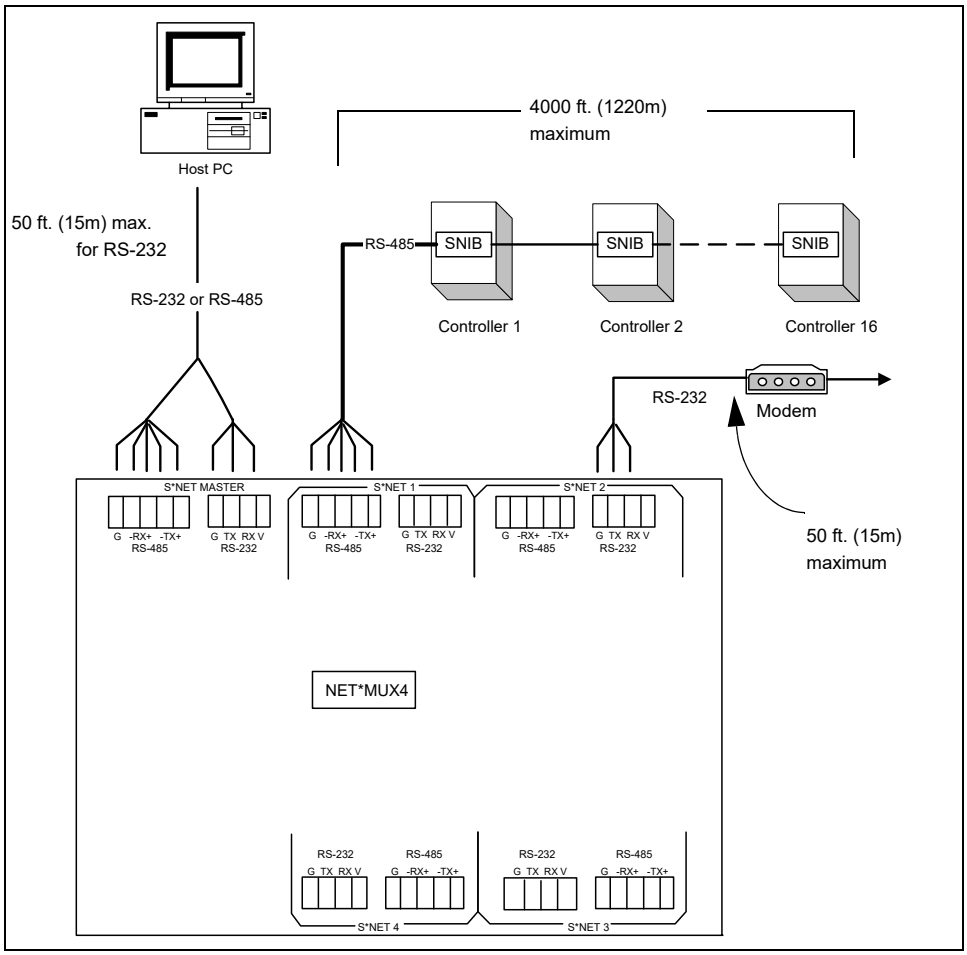


*Figure 7-94: NET*MUX4 Installation*

NET*MUX4 Status LEDs

The NET*MUX4 board possesses several LEDs for status.

POWER	AC or DC power is on.
S*NET MASTER IN	Data Input: Polls from Host Computer
S*NET MASTER OUT	Data Output: Poll responses to Host Computer.
S*NET 1,2,3,4 OUT	Data Output: Polls to DIGI*TRAC Controllers
S*NET 1,2,3,4 IN	Data Input: Poll responses from DIGI*TRAC Controllers
OUTMUX	Host-to-DIGI*TRAC Controllers Polls
INMUX	DIGI*TRAC Controllers-to-Host Responses

*Table 7-19: NET*MUX4 Status LEDs*

Cables and Adaptors

There are a variety of cables and adaptors Hirsch supplies to link various parts of the DIGI*TRAC system. These are:

- ❑ NET*ADAPT Communications Adaptor (NA1)
- ❑ NET*ADAPT-PC Communicators Adaptor (NAPC)
- ❑ Modem Connect Cable (MC1/MC2)
- ❑ Modem Adapt Cable (MA1/MA2)
- ❑ Modem-to-PC Cable (MC-PC)
- ❑ AT Adaptor Cable (AT-AC)
- ❑ PC1 Adaptor

NET*ADAPT Communications (NA1) Installation

Use the NET*ADAPT Communications Adaptor (NA1) to connect the Host PC to a SNIB or NET*MUX4 when the wire between the two devices is longer than 50 feet, or when more than one controller is connected. It also serves one controller for short distances.

The NA1 converter is a small module with a DB-25 connector on one end and a terminal block connector on the other. The NA1 has transmit and receive LEDs to verify both the RS-232 and RS-485 port communications. It includes a 6-foot (2m) cable pre-wired to the NET*ADAPT on one end and to a 5-pin SNIB terminal plug on the other, a 9-inch (23 cm) AT-AC (DB9-to-DB25) adaptor cable, and a wall-mounted transformer. For continuous operation during a power outage, connect this transformer to a UPS power source.

RS-485 allows cable runs up to 4000 feet (1220m) from the host PC to the NET*MUX4 or last controller.

To connect the NET*ADAPT:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Plug the NET*ADAPT's DB-25 connector into an available COM (serial) port on the back of the Host PC. Use the AT-AC adaptor cable if the PC has a DB9 connector.
3. Wire the other end of the NA1, the terminal block connector, into either the:
   a. S*NET MASTER RS-485 port on the NET*MUX4, or
   b. RS-485 port on the SNIB

   The pin-out for connecting the NA1 to a NET*MUX4 or SNIB is shown in Figure 7-97 on page 7-338.
4. Plug the NET*ADAPT's plug-in transformer into an available electrical outlet.
5. Tighten all connections.

These connections are shown in Figure 7-95 on page 7-337 and Figure 7-96 on page 7-338.

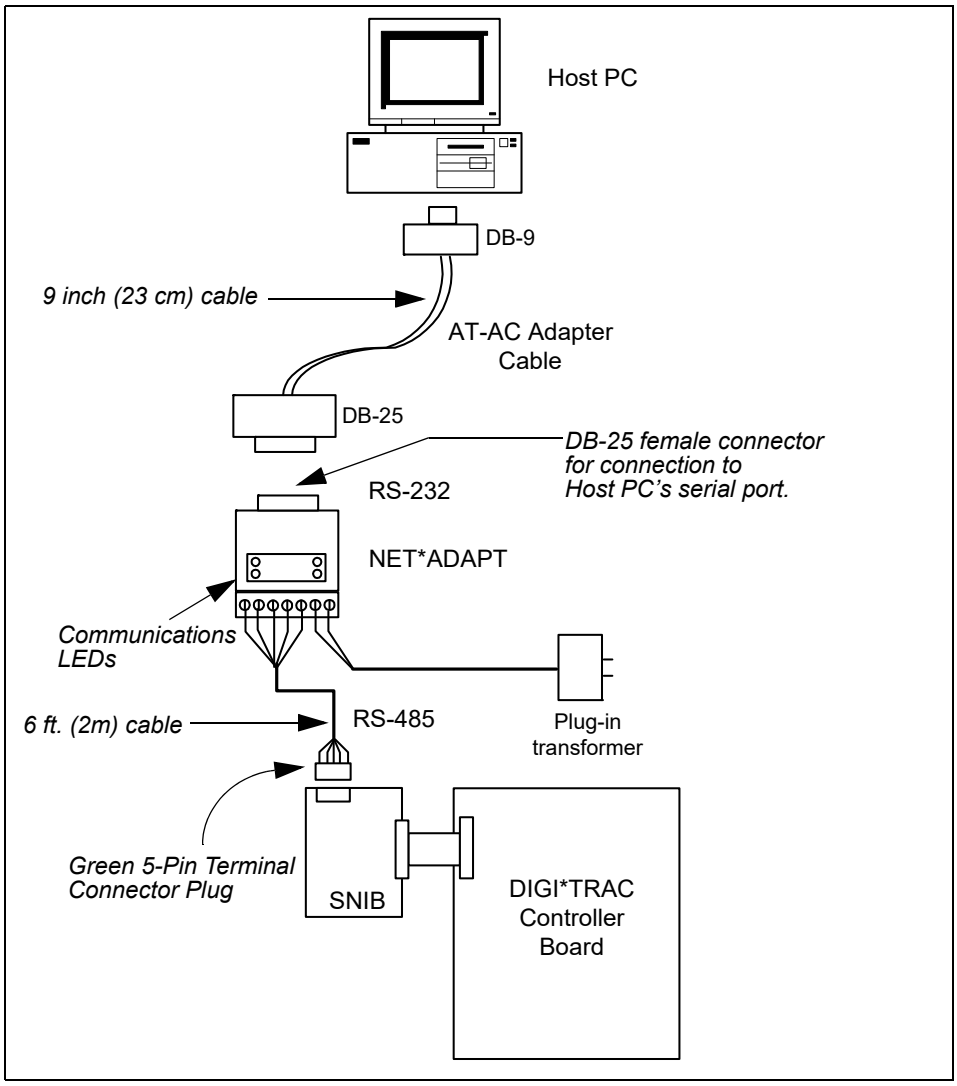


*Figure 7-95: NET*ADAPT to the Controller's SNIB*

Note: Since most PC COM ports are 9-pin ports, a 9-25 adaptor cable, the AT-AC, is included with the NA1.

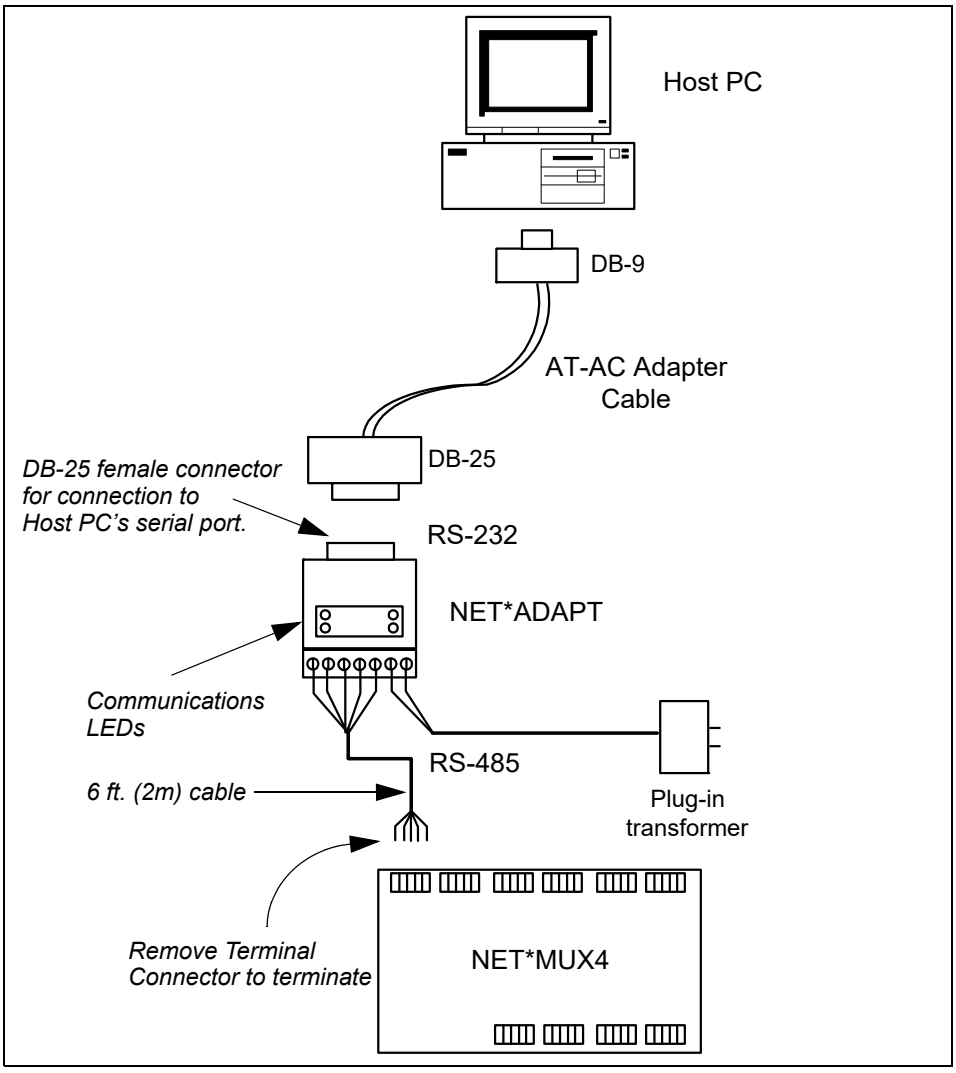


*Figure 7-96: NET*ADAPT to the NET*MUX4*

Wiring for the NET*ADAPT is shown in Figure 7-97.

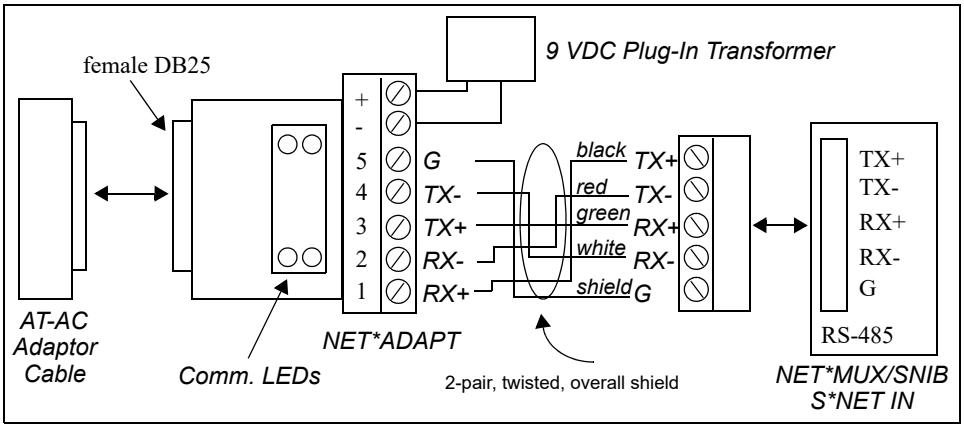


*Figure 7-97: NET*ADAPT Wiring*

NET*ADAPT-PC Communications Adaptor (NAPC) Installation

The NAPC provides two serial ports on a host PC for connection to a DIGI*TRAC system through the NET*MUX4 or a SNIB. Each port has an optically-isolated, individually-selectable RS-232/RS-485 output. In addition, each port has a DB9 (male) connector with transmit and receive LEDs to verify communications.

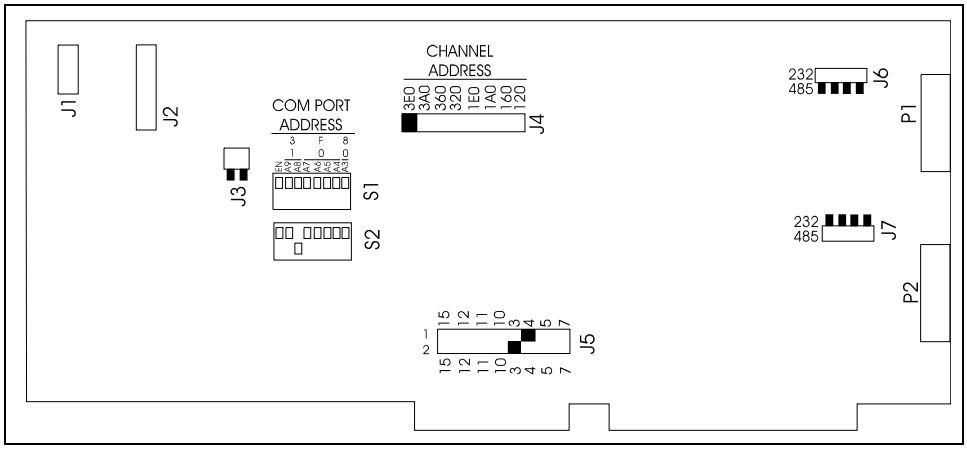


Figure 7-98: NAPC Board

Insert this board into the host PC to enable quick connections between the computer and a SNIB or NET*MUX4 via a normal serial cable using either RS-232 or RS-485. The RS-232 cable cannot exceed 50 feet (15m). RS-485 allows cable runs up to 4000 feet (1220m) from the host PC to the NET*MUX4 or last controller.

Before installing the NAPC in the host PC, first configure it using the 7 jumpers and 2 DIP switch banks, then mount it into the host PC. Configure the jumpers in this manner:

J1	Watchdog Connector	Unused at this time.
J2	DES Module Header	Unused at this time.
J3	Handshake Adaptor	Factory set for no handshake (to J3 side).
J4	Channel Address	Factory set for address 3E0. Unused at this time.
J5	Interrupt	Factory set at IRQ4 for port 1 (COM1), IRQ3 for port 2 (COM2)
J6	Port P1 RS-232/RS-485	Factory set to RS-485 (SCRAMBLE*NET)
J7	Port P2 RS-232/RS-485	Factory set to RS-232

Table 7-20: NAPC Jumper Settings

Set the COM1 and COM2 address by setting S1 and S2 DIP switches in this fashion:

S1	Port P1 Address	Factory set for 3F8 (COM1).
S2	Port P2 Address	Factory set for 2F8 (COM2).

Table 7-21: NAPC Port Address Settings

Standard IBM PC serial port settings are shown in the table below:

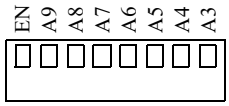
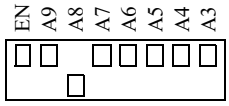
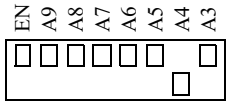
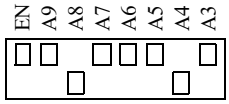
Port	Address	DIP Switch (S1/S2)	IRQ (J5)
COM1	3F8		4
COM2	2F8		3
COM3	3E8		5
COM4	2E8		10

Table 7-22: NAPC Serial Port Settings

The P1 or P2 port pinouts are provided in the following table in case you need to build your own connector for either RS-232 or RS-485:

Pin	RS-232	RS-485
1		+RX
2	RX	-RX
3	TX	+TX
4		-TX
5	G	G

MODEM*CONNECT Network Connector (MC1/MC2) Installation

Use the MODEM*CONNECT Connector for connecting the modem's RS-232 connector directly to a SNIB RS-232 terminal block on a controller. The MC1 cable consists of a DB25 male connector on one end and a 3-terminal block plug connector on the other end. The MC2 cable consists of a DB9 male connector on one end and a 3-terminal block plug connector on the other end.

To connect the MODEM*CONNECT Cable:

1. If the modem accepts a DB-25 connector, plug the MC1 DB-25 connector into the RS-232 port on the back of the modem (such as the Hirsch EM9600).

   If the modem accepts a DB9 connector, plug the MC2 DB-9 connector into the RS-232 port on the back of the modem.

2. Plug the other end of the Modem Connect cable—the green terminal block connector—into the S*NET input RS-232 port on the SNIB, or remove the connector and wire to the NET*MUX4's Master RS-232 terminal block.

3. Tighten all connections.

Figure 7-99 shows the pin-outs for the MC1/MC2:

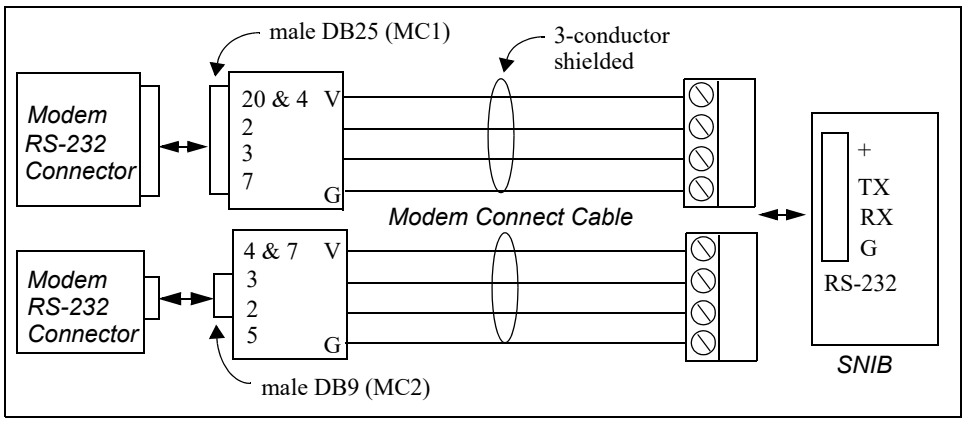


*Figure 7-99: MODEM*CONNECT Network Connector*

For more information on the MC1 and MC2, see "MODEM*CONNECT Network Connector (MC1/MC2)" on page 2-110.

MODEM*ADAPT Communication Adaptor (MA1/MA2) Installation

The MA1/MA2 enables the connections shown in Figure 7-100 and Figure 7-101:

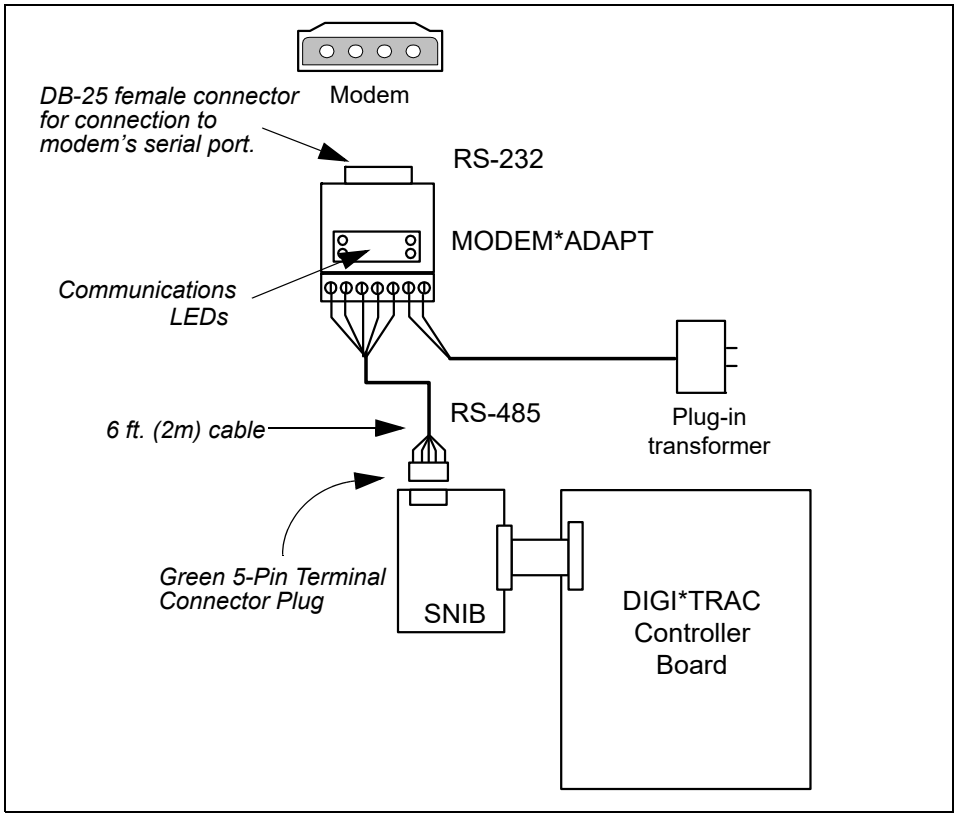


*Figure 7-100: MODEM*ADAPT to the Controller's SNIB*

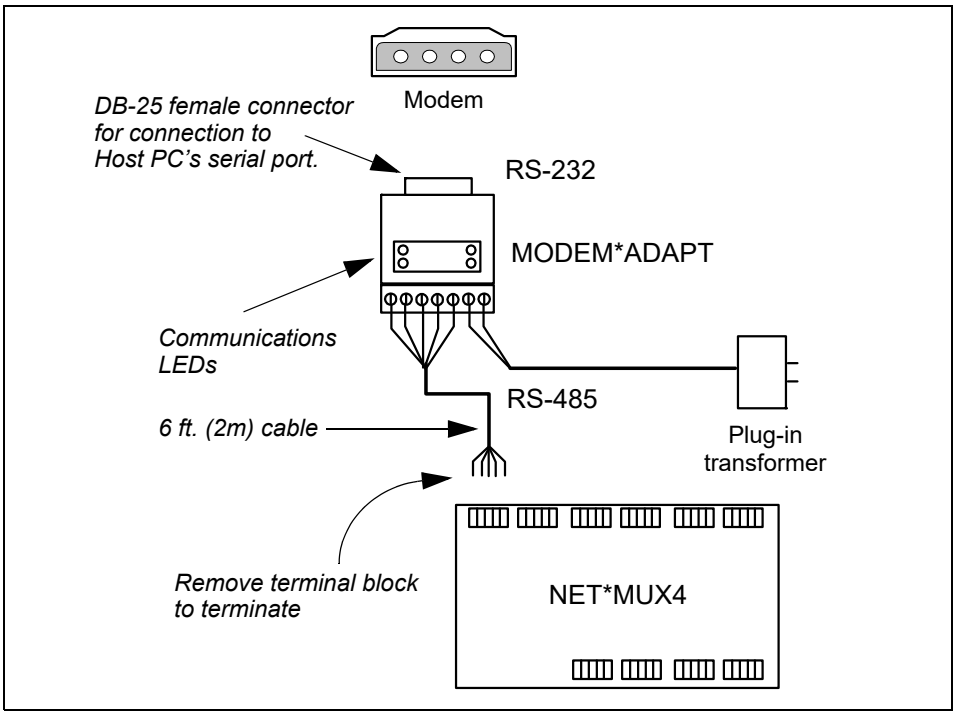


*Figure 7-101: MODEM*ADAPT to the NET*MUX4*

The MA1/MA2 includes a 6-foot (2m) cable pre-wired to the MODEM*ADAPT on one end and to a 5-pin SNIB terminal plug on the other.

To connect the MODEM*ADAPT:

1. Plug the MA1/MA2 DB-25 connector into the RS-232 port on the back of the modem (such as the Hirsch EM9600)
2. Plug the other end of the MA1/MA2 – the green terminal block connector – into the S*NET input RS-485 port on the SNIB, or remove the connector and wire to the NET*MUX's Master RS-485 terminal block.
3. Tighten all connections.

The pin-out for wiring the MA1/MA2 to either the NET*MUX4 or SNIB is shown in Figure 7-102.

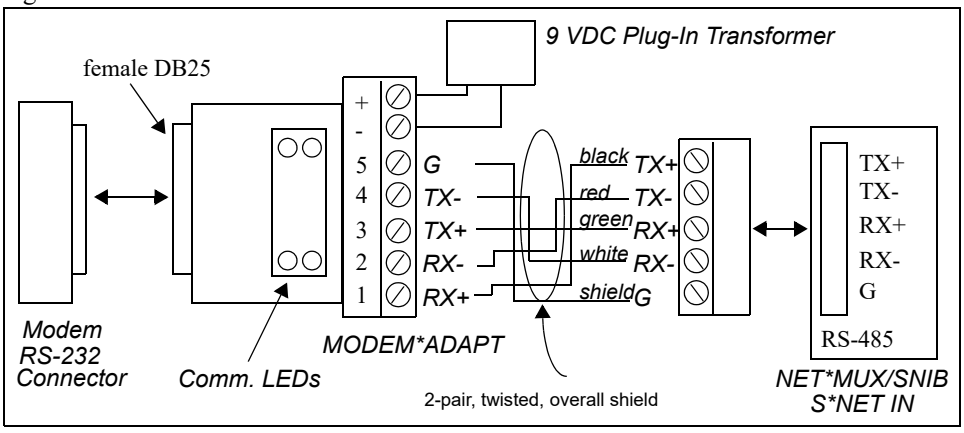


Figure 7-102: MA1/MA2 Wiring

MODEM Cable (MC-PC) Installation

To connect the MC-PC:

1. Connect one end of the cable to the DB-25 connector on the COM port of the PC.
2. Connect the other end to the modem's RS-232 port.

The MC-PC's cable length is three feet (1m).

AT Adaptor (AT-AC) Installation

Since most PC COM ports are DB9 9-pin ports, use an AT-AC to adapt an NA1 or any DB25 to the PC. The AT-AC includes a short 9-inch (23cm) cable with a connector at each end.

To connect the AT-AC:

1. Connect the 9-pin end of the AT-AC to the selected COM port on the back of the PC. The AT-AC's DB9 is female.
2. Connect the NA1's female 25-pin connector (or other DB25 converter or cable) to the other end of the AT-AC. The AT-AC's DB25 connector is male.

PC*CONNECT Network Connector (PC1) Installation

To Connect the PC1 to a SNIB:

1. Connect the DB-25 connector on the PC1 to the Host PC RS-232 connector.
2. Connect the other end of the PC1 to the RS-232 port on the SNIB.
3. Tighten all connections.

The wiring for the PC1 Adaptor is shown here.

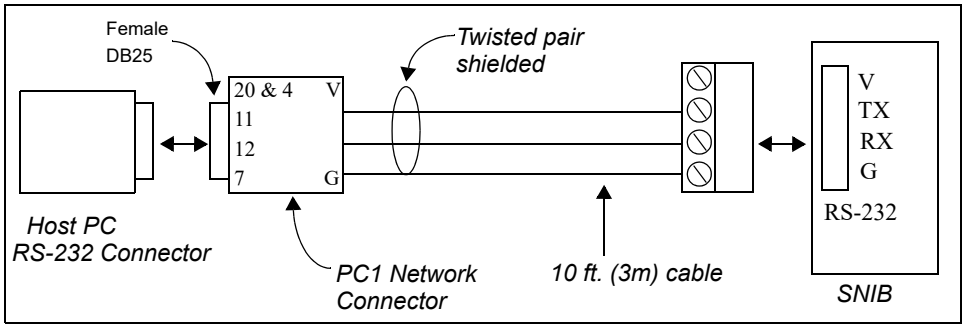


Figure 7-103: PC1 Adaptor

The PC1 includes a 10-foot (3m) pre-wired cable with a terminal plug on one end and the PC1 connector on the other.

To Connect the PC1 to a NET*MUX4:

If you are connecting the PC1 to a NET*MUX4:

1. Connect the DB-25 connector on the PC1 to the Host PC RS-232 connector.
2. Remove the PC1's terminal plug.
3. Wire the other end of the PC1 into one of the NET*MUX4's RS-232 terminal blocks.
4. Tighten all connections.

The wiring for the PC1 Adaptor is shown in Figure 7-104.

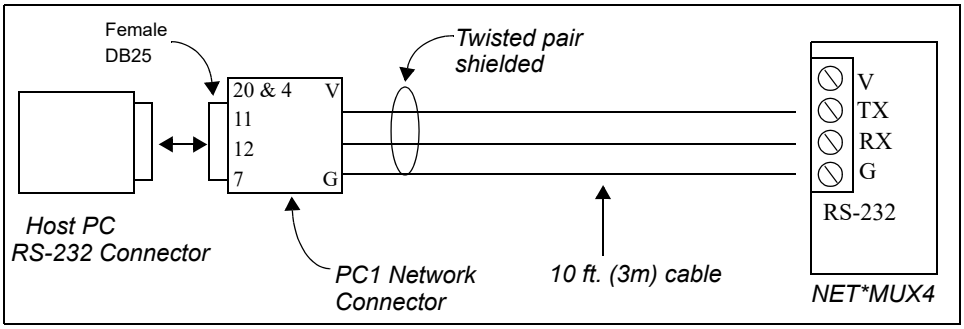


*Figure 7-104: PC1 to NET*MUX4*

Serial Printer Adaptor (SPA) Installation

The Serial Printer Adaptor (SPA) converts RS-485 to RS-232 for connections between the Serial Communications Interface Board (SCIB) in a DIGI*TRAC controller and a serial printer (or terminal).

The SCIB and SPA allow cable runs up to 4000 feet (1220m) from the controller to the serial printer.

The SPA has transmit and receive LEDs for verification of both RS-232 and RS-485 port communications. It includes a 10-foot (3m) cable pre-wired to the SPA on one end and to a 5-pin SCIB terminal plug on the other, and an external plug-in power transformer.

To Connect the SPA:

1. Install the SCIB as described in "Serial Communications Interface Board (SCIB) Installation" starting on page 7-39.
2. Connect the SPA's female DB25 connector to the printer's serial port.
3. Connect the SPA's terminal block connector plug into the RS-485 port on the SCIB.
4. Connect the SPA's plug-in transformer to the most convenient AC outlet.

The pin-out for wiring the SPA to the SCIB is shown below.

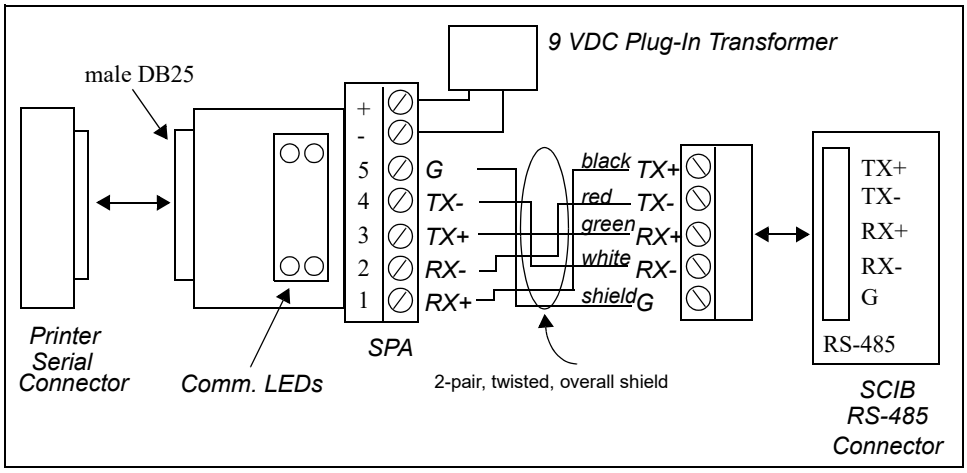


Figure 7-105: SPA Wiring

Telecommunications: Modems/Transceivers

Hirsch supplies three different types of modems/transceivers for three different types of communications:

- ❑ Dial-Up Modem
- ❑ Leased-Line Modem
- ❑ Fiber Optic Transceivers

The installation for each is discussed in the following sections.

Dial-Up Modem Installation

In order to work, there must be two modems of the same sort at each end of the connection. Other setup and installation instructions apply to the specific modem.

EM9600-DL External Modem

EM9600-DL modems must be configured alike. This means setting both EM9600-DL modems to dial-up and setting their switches to common asynchronous operation values. To set both EM9600-DL modems to Dial-Up Mode, select the DIP switch on the side of the modem as shown in Figure 7-106:

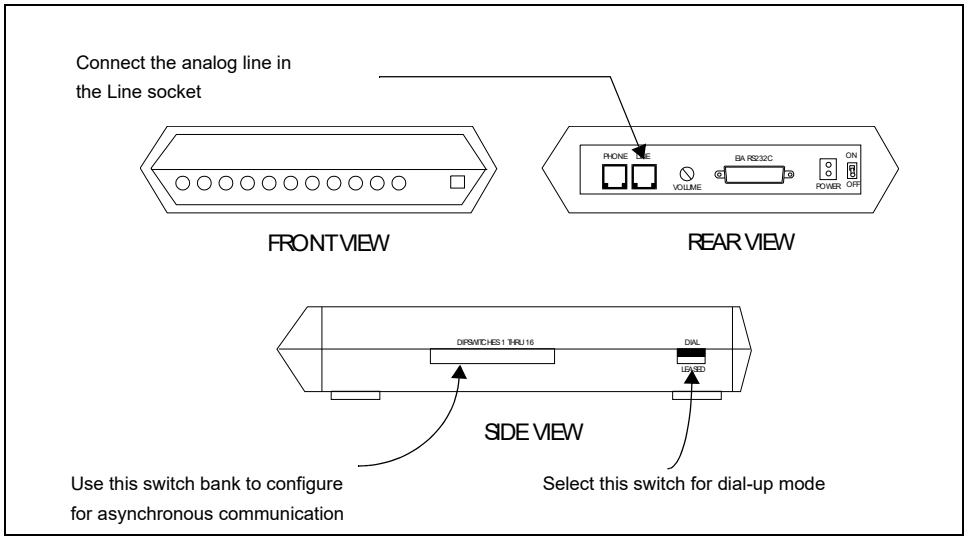


Figure 7-106: EM9600-DL Dial-Up Modem

Note: If you purchased the modem from Hirsch, no changes are necessary.

Use the DIP switch bank on the EM9600-DL's side to configure both modems with the same values:

Switch	EM9600-DL		Switch	EM9600-DL	
	PC End	Remote End		PC End	Remote End
1	DOWN	DOWN	9	DOWN	DOWN
2	UP	UP	10	UP	UP
3	DOWN	DOWN	11	UP	UP

Switch	EM9600-DL		Switch	EM9600-DL	
	PC End	Remote End		PC End	Remote End
4	DOWN	DOWN	12	DOWN	DOWN
5	DOWN	DOWN	13	UP	UP
6	UP	UP	14	UP	UP
7	DOWN	DOWN	15	DOWN	DOWN
8	DOWN	DOWN	16	DOWN	DOWN

Table 7-23: Dial-Up Modem Switch Settings

Once the modem is configured, it can be connected to either a controller or a Host PC. Both installations are explained here.

To install the EM9600-DL Modem to a Host PC:

1. Purchase an MC-PC cable, or make your own cable using the instructions in “MODEM Cable (MC-PC)” starting on page 2-111.
2. Power down the PC.
3. Connect one end of the MC-PC cable to an available COM port in the back of the Host PC.
4. Connect the other end of the MC-PC cable to the RS-232 port on the back of the modem.
5. Connect the telephone line to the ‘Line’ jack.

Note: PBX phone lines are not supported for dial-up modem connections.

6. Set the modem’s DIP switch settings to emulate the PC end as shown in Table 7-23: SW2, SW4, SW6, SW7, SW8, SW13, SW14, SW15, and SW16 UP; all other switches DOWN.
7. Plug the Modem transformer into the nearest power outlet.
8. Check that the modem power switch is on.
9. Power up the PC.

A diagram of this operation is shown in Figure 7-107.

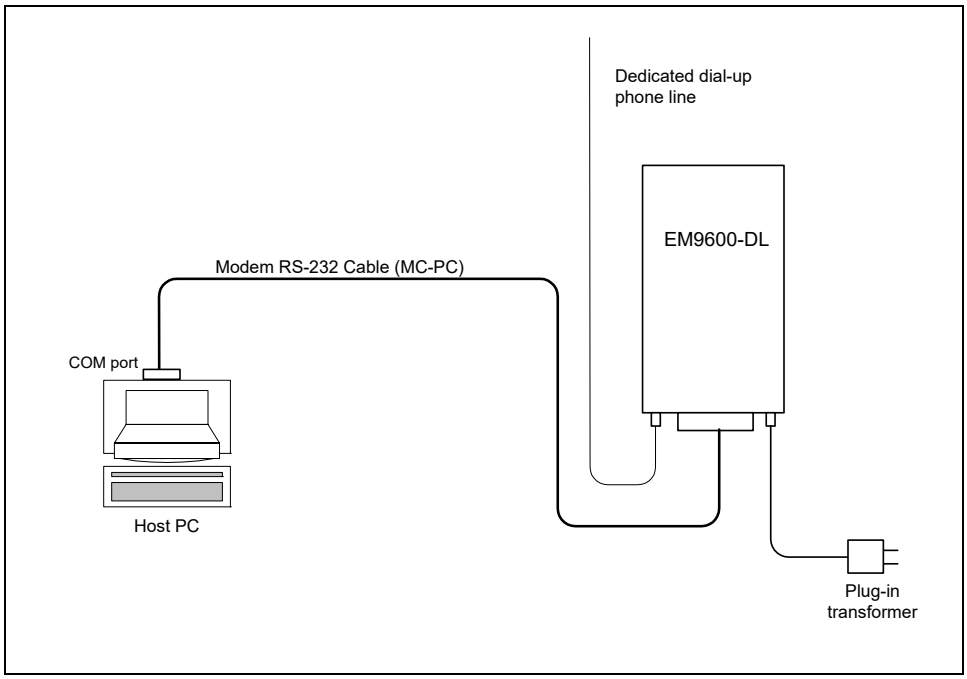


Figure 7-107: EM9600-DL Dial-Up Modem Connections (PC)

To install the EM9600-DL Modem to a Controller:

1. Purchase a Hirsch MC1 cable, or build your own equivalent cable using the wiring instructions provided in "MODEM*CONNECT Network Connector (MC1/MC2)" starting on page 2-110.
2. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
3. Connect the 4-pin RS-232 plug on the MC1 cable to the SNIB's RS-232 connector.
4. Connect the other end of the MC1 cable to the RS-232 port on the back of the modem.
5. Connect the telephone line to the 'Line' jack.

Note: PBX phone lines are not supported for dial-up modem connections.

6. Set the modem's DIP switches to emulate the remote end.
7. Set the SNIB's SW3 ON. For other switch settings, see "SNIB Setup" on page 7-43.
8. Connect the modem's plug-in transformer to the nearest AC outlet.
9. Check that the modem power switch is on.
10. Power up the controller.

Note: If more than one controller at a remote site is configured to dial out on alarm conditions, but they share a single dial-up modem, wire an output relay (for the alarm) on each controller to an input on the controller which has the modem.

A diagram of this operation is shown in Figure 7-108.

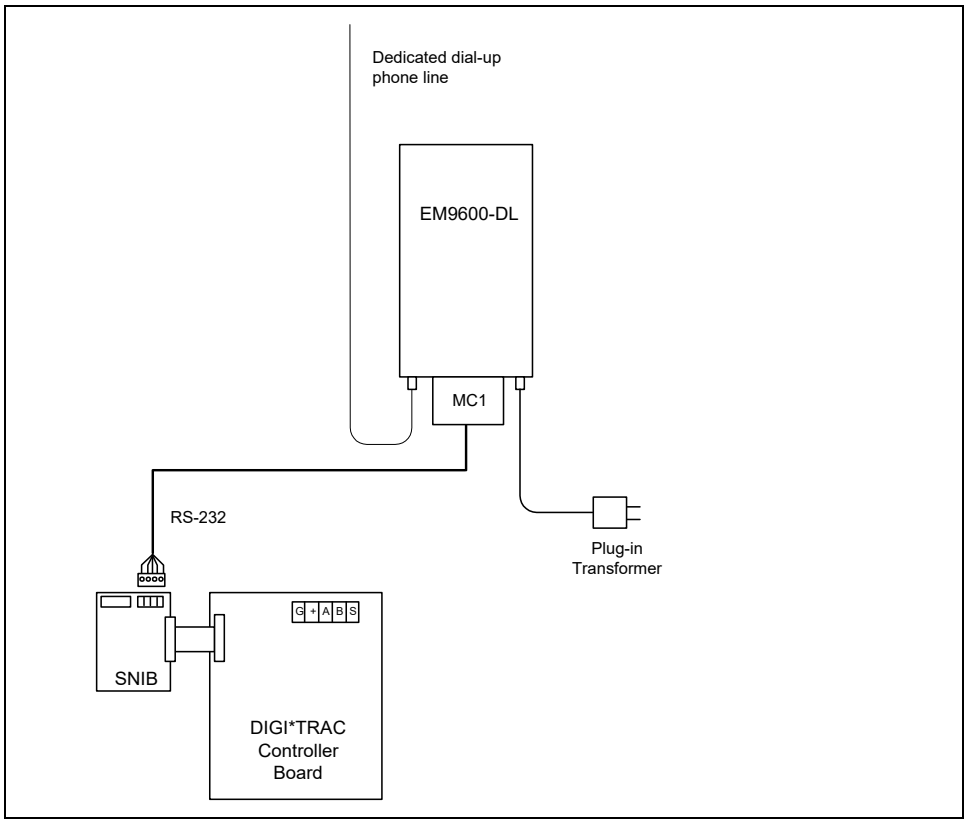


Figure 7-108: EM9600-DL Dial-Up Connections (Controller)

Configuring the EM9600-DL

After physical connections are completed, the EM9600-DL must be properly configured:

1. If you are using Windows 95/NT without SAM loaded, use this procedure:
   a. At the connected host PC, bring up a terminal emulation program. HyperTerminal is used in here, but most programs require the same steps.
   b. Type the name for this connection and press **OK**. The Phone Number dialog box appears.
   c. At the Connect Using field, specify one of the Direct Connect to COM options. Normally this will be Direct Connect to COM1 if there is only one modem or one XBox connected to the PC. Press **OK**.

      The COM Properties dialog box appears.
   d. Specify the communications parameters supported by this modem. These are:

Baud	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

      Press **OK**. The Terminal screen appears with a blinking cursor.

e. Proceed to Step 3.

2. If your are using a host PC with SAM loaded, use this procedure:
   a. Bring up SAM and access the Setups Option list.
   b. Select Configure Dial-Up Systems. The Select Remote System to Dial Up dialog box appears.
   c. Select the modem to dial up.
   d. Proceed to the next step.
3. Check to see if the modem is responding by typing this:

   ```
   at
   ```

   Press Enter. If the modem responds with OK, you are connected.
4. If this is an S*NET connection, configure the modem using these AT commands:

   ```
   at&f&w0
   at$sb9600
   at&w0
   ```

   If this is an X*NET connection (connecting to one or more modems through an XBox), configure the modem using these AT commands:

   ```
   at&f&w0
   at$sb9600
   at&q0
   at&w0
   ```

If any problems occur, contact your Hirsch representative or Hirsch Technical Support.

DM9600A-DL DIGI*TRAC Modem Assembly

The DM9600A-DL requires no configuring. The modem senses its partner on the other end of the line and negotiates the link automatically.

To install the DM9600A-DL Modem:

1. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
2. Using the Velcro strips provided with the DM9600A-DL, attach the modem to the top of the right side wall inside the controller's enclosure, so that the telephone jack faces the front of the enclosure.
3. Connect the DB9 end of the RS-232 cable to the serial port on the DM9600A-DL.
4. Connect the DB25 end of the cable to the DB25 connector on the Modem Power Supply Harness (MPSH). The MPSH comes with the DM9600A-DL.
5. Connect the 4-pin RS-232 plug on the MPSH to the SNIB's RS-232 connector.
6. Connect the MPSH's power cord into the power port on the DM9600A-DL.
7. Connect the black and red wires from the MPSH into the Controller Board in this way:
   a. Connect the black wire from the MPSH into the G terminal on the selected ScramblePad/MATCH terminal block on the controller board.
   b. Connect the red wire from the MPSH into the + terminal on the selected ScramblePad/MATCH terminal block on the controller board.
8. Connect the telephone line to the 'Line' jack.

Note: PBX phone lines are not supported for dial-up modem connections.

9. Set the SNIB's SW3 ON. For other switch settings, see "SNIB Setup" on page 7-43.
10. Check that the modem power switch is on.
11. Power up the system.

A diagram of this procedure is shown in Figure 7-109.

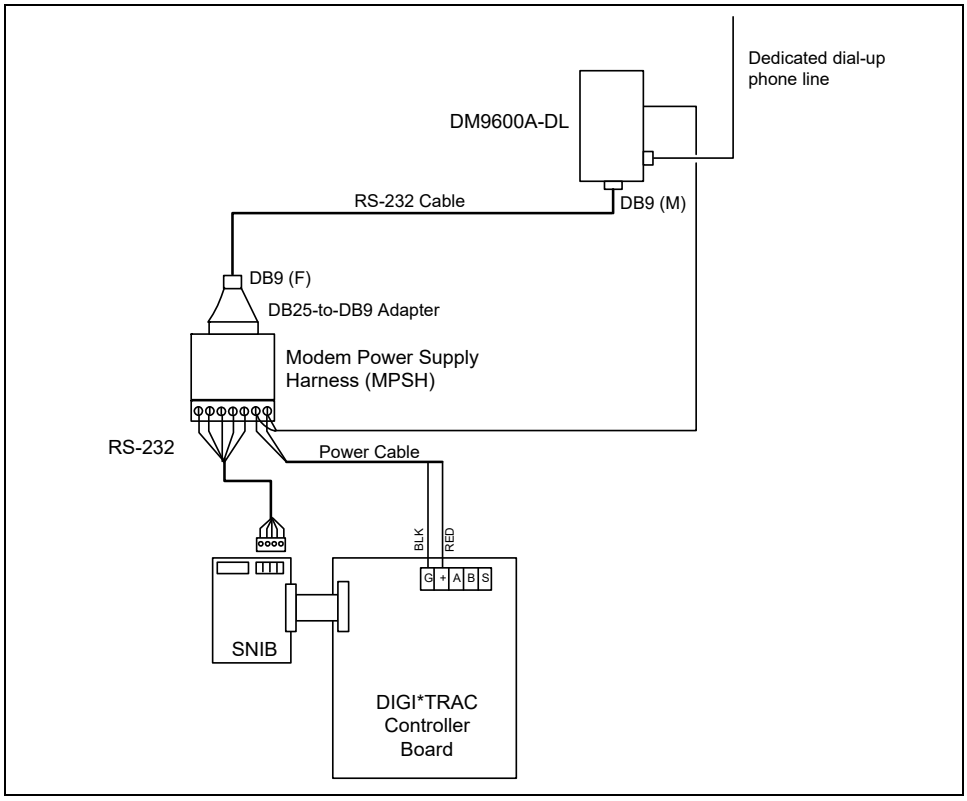


Figure 7-109: DM9600A-DL Connection to a Controller

*Note: The DM9600A-DL modem can be ordered preconfigured and pre-installed in the DIGI*TRAC controller when ordered with a DIGI*TRAC controller.*

Configuring the DM9600-DL

Once physical connections are completed, the DM9600-DL must be properly configured:

1. At the connected host PC, bring up a terminal emulation program. HyperTerminal is used in here, but most programs require the same steps.
2. Type the name for this connection and press **OK**.

   The Phone Number dialog box appears.
3. At the Connect Using field, specify one of the Direct Connect to COM options. Normally this will be Direct Connect to COM1 if there is only one modem or one XBox connected to the PC.
4. Press **OK**.

   The COM Properties dialog box appears.

5. Specify the communications parameters supported by this modem. These are:

Baud	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

   Press **OK**.

   The Terminal screen appears with a blinking cursor.

6. Check to see if the modem is responding by typing this:

```
at
```

   Press **Enter**. If the modem responds with OK, you are connected.

7. Configure the modem using these AT commands:

```
at&f&w0
atn0
at%c0
at&k0
at&w0
```

   Use this set of AT commands whether the connection is straight S*NET or uses an XBox intermediary.

Leased-Line Modem Installation

In order to work, there must be two modems of the same sort at each end of the connection. They must also be configured alike. This means setting both modems to leased-line and setting their switches to complementary asynchronous operation values. To set both modems to leased-line mode, select the DIP switch on the side of the modem as shown in Figure 7-110:

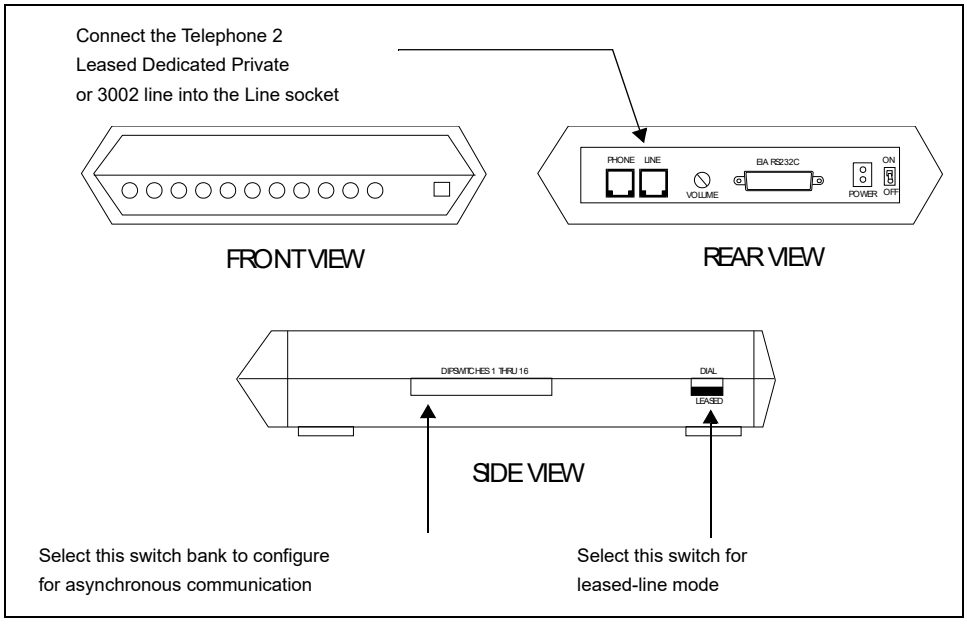


Figure 7-110: EM9600-LL Leased-Line Modem

Note: If you purchased the modems from Hirsch, no configuration changes are necessary.

Use the DIP switch bank on the modem's side to configure both modems with these values:

Switch	EM9600-LL		Switch	EM9600-LL	
	PC End	Remote End		PC End	Remote End
1	DOWN	DOWN	9	DOWN	DOWN
2	UP	UP	10	DOWN	DOWN
3	DOWN	DOWN	11	DOWN	DOWN
4	UP	UP	12	DOWN	DOWN
5	DOWN	UP	13	UP	UP
6	UP	UP	14	UP	UP
7	UP	UP	15	UP	UP
8	UP	UP	16	UP	UP

Table 7-24: Leased-Line Modem Switch Settings

Once the modem is configured, it can be connected to either a controller or a Host PC. Both installations are explained here.

To install the EM9600-LL Modem to a Host PC:

1. Purchase an MC-PC cable, or make your own cable using the instructions in "MODEM Cable (MC-PC)" starting on page 2-111.
2. Turn all system power off, remove connectors to the standby battery, then remove connectors to the AC power.
3. Connect one end of the MC-PC cable to an available COM port in the back of the Host PC.
4. Connect the other end of the MC-PC cable to the RS-232 port on the back of the modem.
5. Connect the telephone line to the 'Line' jack.
6. Set the modem's DIP switch settings to emulate the PC end: SW2, SW6, SW10, SW11, SW12, and SW14 UP, all the rest DOWN.
7. Plug the Modem transformer into the nearest power outlet.
8. Check that the modem power switch is on.
9. Power up the system.

A diagram of this operation is shown in Figure 7-111.

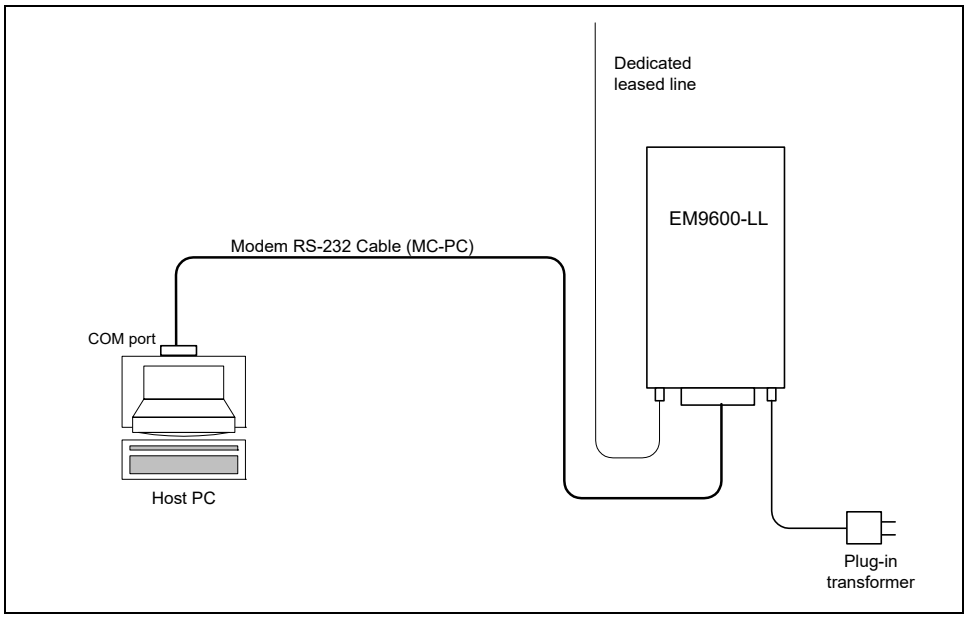


Figure 7-111: EM9600-LL Leased-Line Modem Connections (PC)

To install the EM9600-LL Modem to a Controller:

1. Purchase a Hirsch MC1 cable or build your own equivalent cable using wiring instructions provided in "MODEM*CONNECT Network Connector (MC1/MC2)" starting on page 2-110.
2. Power down the system.
3. Connect the 4-pin RS-232 plug on the MC1 cable to the SNIB's RS-232 connector.
4. Connect the other end of the MC1 cable to the RS-232 port on the back of the modem.
5. Connect the telephone line to the 'Line' jack.
6. Connect the modem's plug-in transformer to the nearest AC outlet.
7. Set the modem's DIP switches to emulate the remote end.
8. Set the SNIB's SW3 OFF. For other switch settings, see "SNIB Setup" on page 7-43.
9. Check that the modem power switch is on.
10. Power up the system.

A diagram of this operation is shown in Figure 7-112.

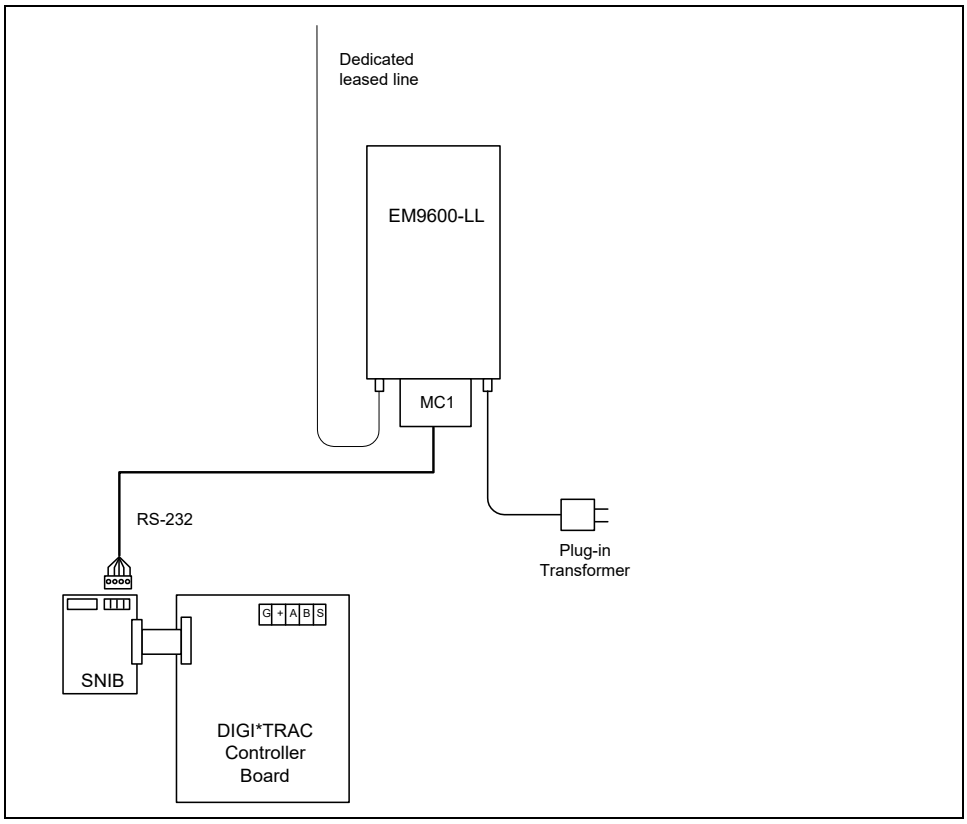


Figure 7-112: EM9600-LL Leased-Line Connections (Controller)

For connection between the leased-line modem and the NET*MUX4, do one of the following:

❑ Fabricate a cable per the following diagram:

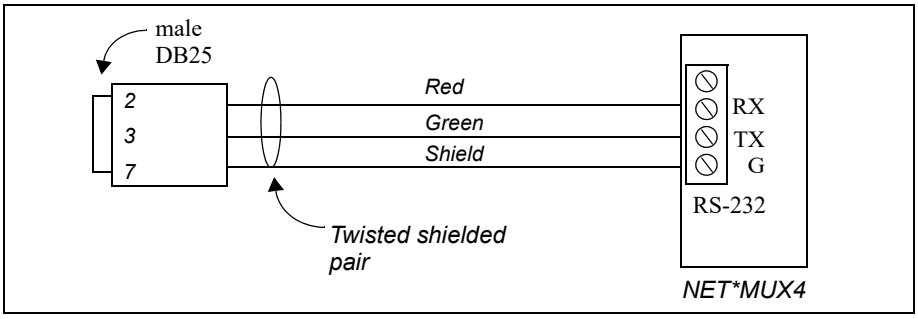


*Figure 7-113: Fabricating a Cable Between the NET*MUX4 and Leased-Line Modem (Option 1)*

❑ Order an MC1 and remove the green SNIB connector and connect it to the NET*MUX4 as follows:

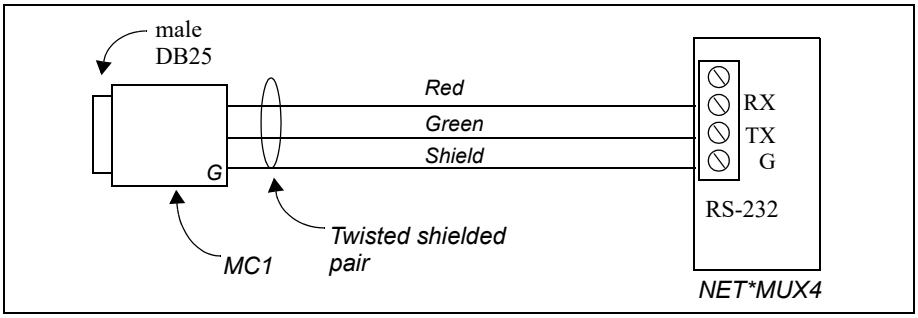


*Figure 7-114: Fabricating a Cable Between the NET*MUX4 and Leased-Line Modem (Option 2)*

While running these modems, the Auto-Answer feature must be disabled at both the Host PC and remote modems for all brands and types of modems used.

Once you've set the DIP switches and connected the modems, you should verify that the handshake is working properly by observing the Carrier Detect LED. This LED should illuminate on both modems if they are communicating with each other.

If any problems occur, contact your Hirsch representative or Hirsch Technical Support.

Fiber Optic Transceiver Installation

Installation procedures for the FiberLink fiber optic transceiver is described in this section.

Use Fiber Optic cable and FL fiberlink transceivers for SCRAMBLE*NET and ScramblePad/MATCH communications circuits. The FL transceivers come standard with SMA optical fiber connectors; however, ST connectors are also available upon request.

SMA connectors are plug-in type. ST connectors are bayonet type and offer less DB loss.

Two types of FL transceivers are provided:

❑ FLKM for keyboard/MATCH connections

❑ FLN for SNIB connections

To Run Fiber Between a Host PC to a SNIB-installed Controller:

1. Connect an NA1 adaptor to an available COM port on the back of the selected PC. For more about this, refer to "NET*ADAPT Communications (NA1) Installation" on page 7-336.
2. Wire the NA1 to the FLN as shown in Figure 7-115.
3. Connect the fiber optic cables to the SMA connectors on the other end of the FLN.
4. Connect the other end of the fiber optic cables to the SMA connectors on the other FLN transceiver.
5. Wire the terminal block on the other end of the transceiver to the RS-485 S*NET IN port of the SNIB board.

*Note: We recommend that you not exceed 100 feet (30.5 meters) of copper wire between the fiber optic transceiver and devices such as SNIB's and NET*MUX's.*

6. Plug the 12 VAC transformers for both FLNs into the nearest convenient AC outlets.

This procedure is shown in Figure 7-115.

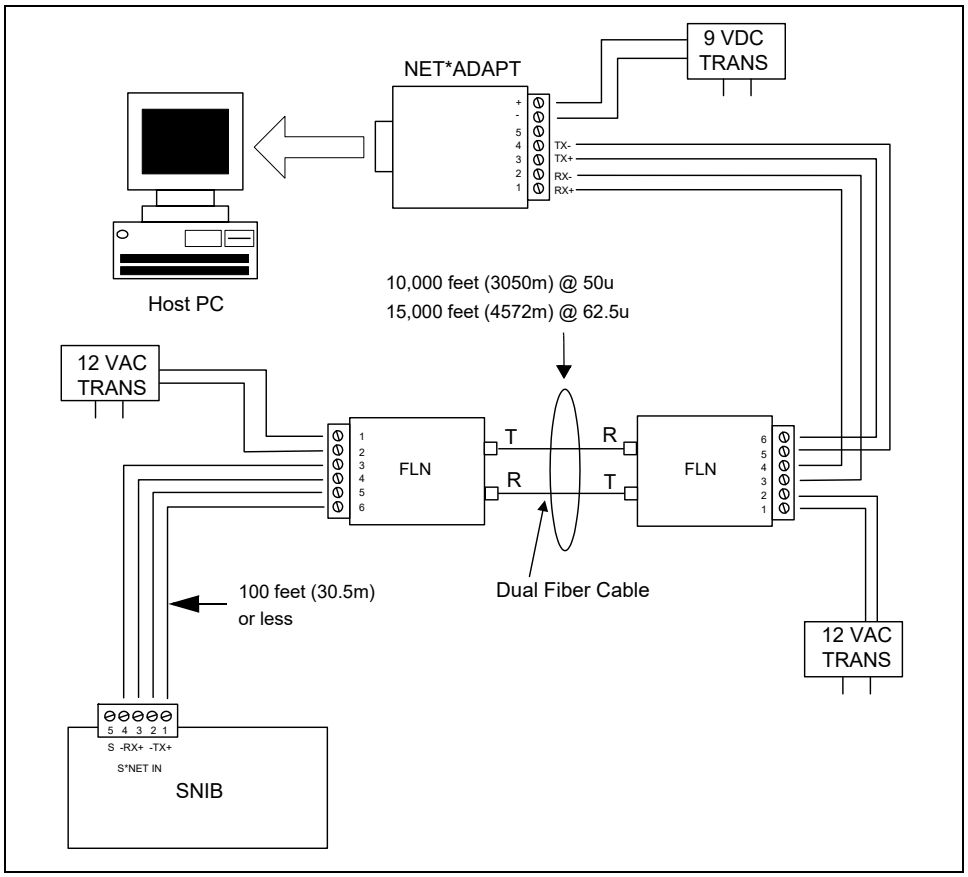


Figure 7-115: Host PC to Controller Using Fiber Optic Cable

Note: Do not place the FL adaptor inside the controller enclosure.

To Connect a ScramblePad/MATCH to a Controller via Fiber Optic Cable:

1. Connect one of the controller ScramblePad/MATCH terminal blocks to the FLKM adaptor as shown in Figure 7-116. Use two twisted, shielded, stranded pairs of 22 AWG wire and float the shield at the fiber optic transceiver.
2. Connect the fiber optic cables to the SMA connector on the FLKM.
3. Connect the other end of the fiber optic cable to the SMA connector on the other FLKM adaptor.
4. Wire the terminal block on the second FLKM adaptor to the D*TRAC port on the back of the ScramblePad or MATCH as shown in Figure 7-116.

   Float the shield at the transceiver end.
5. Connect a 1A/24VDC battery-backed power supply into the G and + lines. Observe polarity: G ties to the ground and the + to +.

A diagram of this procedure is shown in Figure 7-116.

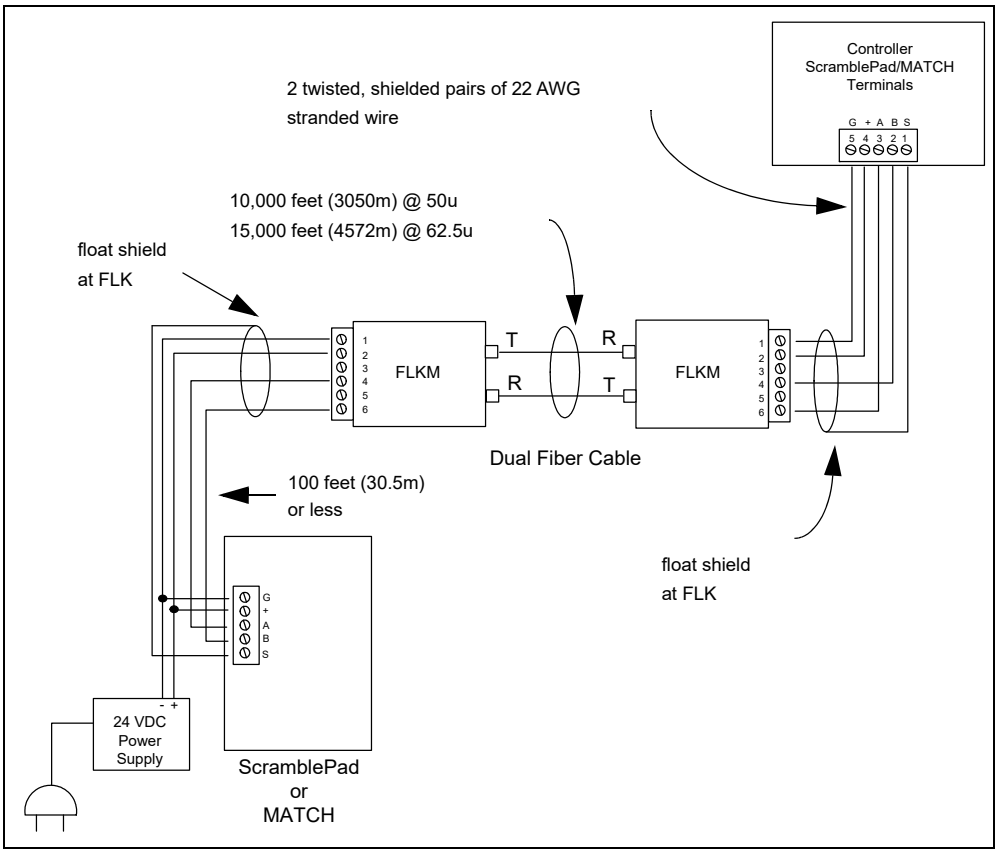


Figure 7-116: ScramblePad/MATCH to Controller Using Fiber Optic Cable

XBox Installation

The default XBox Host PC interface is configured to connect a single XBox to a standard PC COM port at speeds ranging from 2400 bps to 38,400 bps. The XBox Host interface can also be configured for RS-485 multidrop, enabling multiple XBoxes to reside on an RS-485 COM port using a NET*ADAPT (NA1) adaptor.

The S*NET interface connects to 1 – 63 Controllers. DIGI*TRAC Controllers use the proprietary S*NET protocol, a secure encrypted network protocol capable of sustaining a transaction rate of approximately 16 events per second. The S*NET interface offers a choice of either RS-232 or multidropped RS-485 (one or the other, but not both).

For local hardwired applications, the NET port connects 1 – 63 multidropped DIGI*TRAC controllers on the RS-485 connector.

*Note: A NET*MUX4 is still required whenever more than 16 controllers are on one electrical path.*

For remote applications, a modem may be connected to the NET RS-232 connector. Via the XBox, the host sends AT commands to the modem and receives the modem result codes. When the modem connects with a remote site, the XBox initiates Hirsch S*NET communications with the remote controllers, and the remote site then behaves the same as local hardwired controllers. LEDs mounted on the front and five connectors on the back.

Configuring the XBox

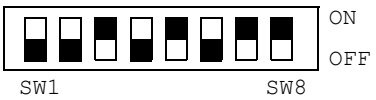
To Configure the XBox:

Set the address and speed on the XBox switches and power up the XBox. The red NET TX will flicker, indicating that it is searching for panels. Depending on options installed, the panel may require up to 20 seconds to complete its startup and become operational.

1. Use DIP Switch Bank 1 on the back of the XBox to designate an address the box will use to identify itself. Available addresses are 0 - 255.

   As shown in Figure 7-117 on page 7-359, this bank uses a standard 8-bit binary, where SW1 is the most significant bit – having a value of 128 when ON – and SW8 is the least significant bit – having a value of 1 when ON

   For example, if Switch Bank 1 is set like this,

   it designates Address 43.

2. Do one of these:

   - *If this is the version 1 XBox*, Switch Bank 2 designates the speed available for both Host PC and S*NET communication. SW1-2 indicates the Host-to-XBox speed and SW3 indicates the XBox-to-Controller speed as shown in Figure 7-117 on page 7-359. Make sure the S*NET speed you set here is the same as that set for the rest of the network. The other five switches in Bank 2 (SW4-8) are unused.
   - *If this is the version 2 or 3 XBox*, Switch Bank 2 designates a variety of host and net characteristics. SW1-2 indicates the Host-to-XBox speed and SW3-4 indicates the XBox-to-Controller speed. SW2-5 determines the net mode while SW2-6 determines software compatibility. SW2-7 determines the net mode and SW2-8 enables alarm annunciation. For an illustration of this, refer to Figure 7-118 on page 7-360.

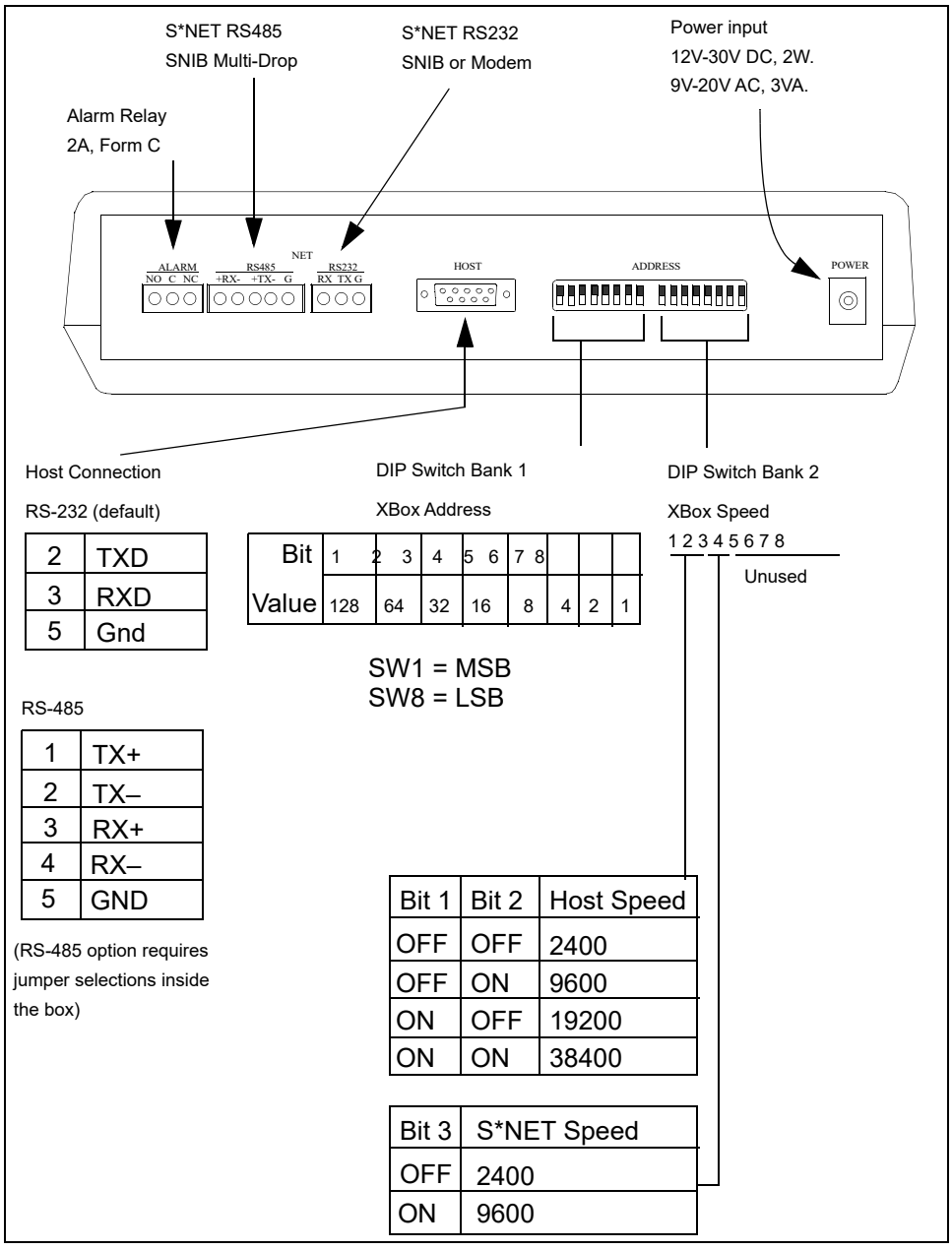


Figure 7-117: Back Panel Connectors and Switches for XBox Version 1

For UL installations:

- ❑ Connections are limited to equipment located within the same room or within 25 feet.
- ❑ S*NET RS-232 ports require shielded cable.
- ❑ Power input uses 12VDC, 300 mA.
- ❑ Alarm relays must be 2A *resistive* Form C.

This applies to Figure 7-117 and Figure 7-118.

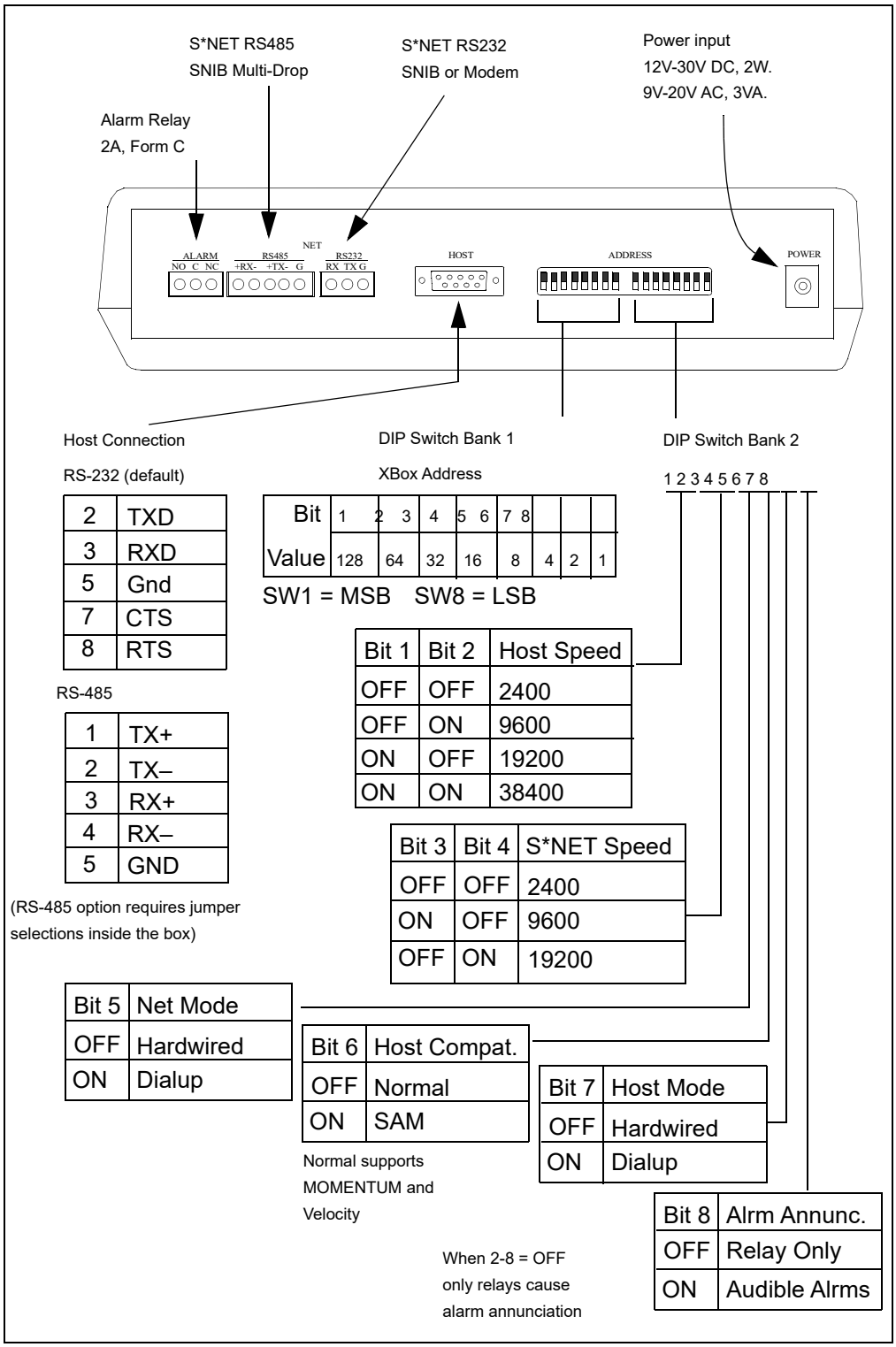


Figure 7-118: Back Panel Connectors and Switches for XBox Version 2 or 3

Connecting the XBox

Connection between the Host PC and one or two XBoxes is accomplished in several ways:

- ❑ RS-232 Serial Cable
- ❑ NA1 Adaptor
- ❑ NAPC Adaptor

For most connections between the Host PC and an XBox, you will use a normal RS-232 serial cable with DB9 connectors—female at one end, male at the other. If you are fabricating the RS-232 cable for an XBox 2, remember that pins 7 and 8 must be connected in order for the host port to use flow control. When multidropping XBoxes (see Figure 2-94 on page 2-123), also use an NA1 or NAPC to achieve RS-485 communication between the PC and the XBox.

When using an NA1, it is also necessary to connect the terminal block end to a Hirsch PC3 cable (or fabricate an equivalent—Figure 7-119 on page 7-362) which provides the proper DB9 male connection to one or two XBoxes.

If you use an NA1 or NAPC to make an RS-485 multidrop connection between the PC and the XBox (see Figure 2-95), you must also reconfigure the XBox by changing several jumpers inside the device.

Use one of these procedures to connect the XBox.

To connect the XBox to the Host PC:

1. Connect the transformer that comes with the XBox to the POWER INPUT port at the back of the XBox.
2. Do one of these:
   - If you are using the default serial RS-232, connect one end of the Host cable to the COM port on the back of Host PC. Use a standard serial cable with a DB-9 connector at both ends. A 10-foot (3m) cable is included with the XBox.
   - If you are using RS-485, first open the XBox and change the jumpers on the board from the default RS-232 to the RS-485. Then connect one end of the cable to the COM port on the host PC.
3. Connect the other end of the cable to the HOST port on the back of the XBox.
   - For RS-232 connections, use a DB-9 connector.
   - For RS-485 connections, use an RS-485 cable with DB-9 connectors configured as shown in Figure 7-117 on page 7-359. RS-485 connectors use a 5-pin configuration.

UL Ratings

For UL Purposes, the following conditions apply to XBox:

- For Host (P2) and RS-232 (P3) connections, cabling is limited to equipment located within the same room or no more than 25 feet.
- Use shielded wiring for connection to the RS-232 (P3) connector.
- Power input rating is 12VDC, 300 mA

When using an NA1, it is also necessary to connect the terminal block end to a Hirsch PC3 cable (or fabricate an equivalent) which provides the proper DB9 male connection to one or two XBoxes.

To fabricate a cable for this purpose, see Figure 7-119:

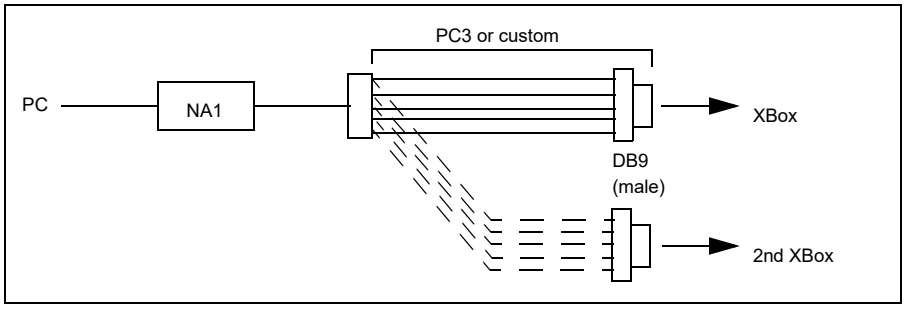


Figure 7-119: Fabricating Cable for Connection between Host PC and XBox Using An NA1

To connect the XBox to the Controller:

Wire the XBox to the controller's SNIB.

- ❑ If wiring to only one panel, you can choose either the RS-232 or RS-485 port.
- ❑ If wiring to multiple panels (multi-drop), use RS-485.

You must fabricate your own wiring between the XBox and SNIB. Figure 7-120 illustrates this wiring scheme:

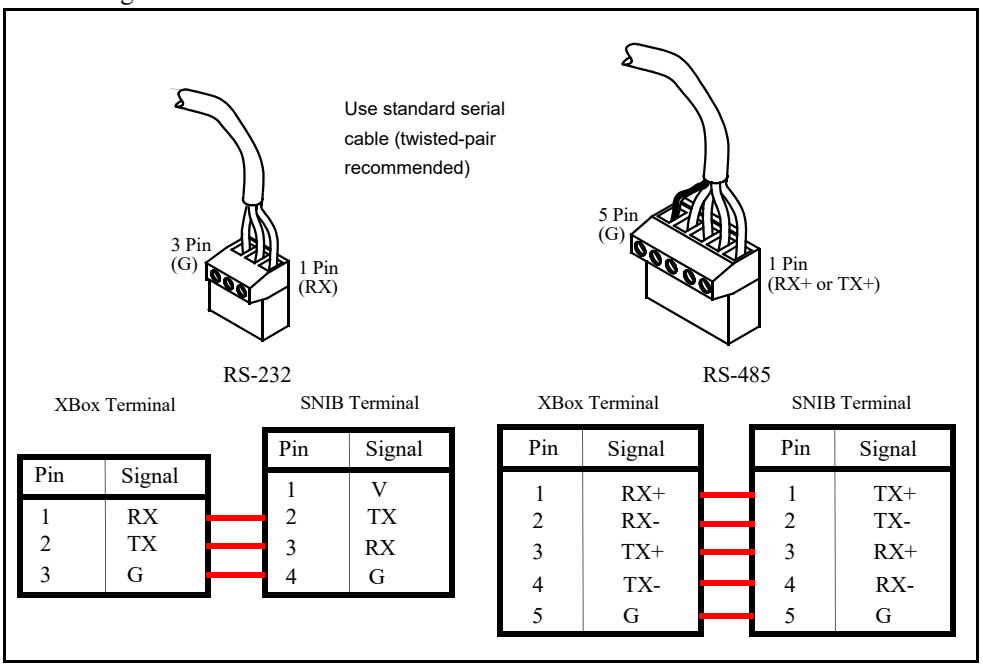


Figure 7-120: XBox to SNIB Wiring Plan

Use standard serial cable for both RS-232 or RS-485. Twisted-pair is recommended. The ground wire is often unnecessary if the cable is shielded.

It doesn't matter which color wire you use for each connection as long as you are consistent. For example, you might use green to connect one ground to another, red to connect RX+ to TX+, and so on.

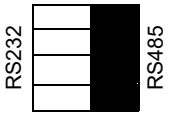
To power the XBox:

1. Connect the XBox transformer to the POWER connector on the back of the XBox.
2. Plug the transformer into the nearest electric outlet.

If required, you can choose to connect the XBox to a UPS or battery backup supply.

To reconfigure the XBox for RS-485 Host:

1. Open the XBox cover. Inside you'll see four shunts marked 'J1' on the board. One side of these shunts is marked 'RS232' and the other is marked 'RS485'. The RS-232 configuration is the default.
2. Switch all the shunts over to the RS-485 side like this:



3. Close and fasten the XBox cover.
4. Connect the XBox to the required devices with the proper cable(s).

XBox to UDS-10 Connection

The Lantronix UDS-10 device server can connect the XBox for TCP/IP communication between one or more controllers on one end and a remote host computer.

To connect an XBox to a UDS-10:

To purchase this cable from Hirsch, refer to the LIFUX cable.

1. Purchase or fabricate a serial cable for connection between the two devices. One end should be a DB9 male connector; the other should be a DB-25 male connector.
2. Connect the DB9 end of the cable into the XBox RS-232 serial port.
3. Connect the DB25 end of the cable into the UDS-10's RS-232 serial port.
4. Set the communication parameters for these devices as follows:

Parameter	Value
Baud	38400
Data Bits	7
Stop Bit	1
Parity	Even
Flow Control	RTS/CTS

If you need to fabricate a serial cable for this purpose, the pin-outs are:

UDS-10 DB25 Male	XBox DB9 Male	Signal
2	2	RXD
3	3	TXD
4	8	CTS
5	7	RTS
7	5	COM
Shield	Shield	Ground

XBox LEDs

The seven front panel LEDs provide this information:

This LED:	Lights when:
POWER	power is on.
CANCEL	Not yet implemented. (Alarm cancel push button.)
ALARM	alarm condition is active (not yet implemented)
HOST TX	the XBox responds to the host
HOST RX	the Host is transmitting polls or commands
NET TX	the XBox sends polls or commands to the controller(s)
NET RX	controller(s) respond to the XBox

Testing the XBox

Once the XBox is wired to a controller, the XBox red NET TX LED and the SNIB's two red IN LEDs will be lit, indicating that the XBox is polling panels, and the SNIB is receiving polls. If the SNIB's red IN LED isn't lit, recheck the wiring (XBox TX wired to SNIB RX, and XBox RX wired to SNIB TX).

If the controller is receiving polls and understands them, the SNIB's two green OUT LEDs and the XBox green NET RX LED will be lit. If the SNIB's two green OUT LEDs are not lit, recheck the XBox and SNIB speed settings.

A flicker will be evident on NET TX and NET RX pulsing once per second. This is the XBox hunt mode: the XBox hunts for SNIB addresses that aren't presently responding. With 64 possible SNIB addresses, it may take up to 63 seconds to recognize a newly connected panel.

Using a terminal program, any typing should light the XBox red HOST RX. Host polls and ACKs don't require checksums, so type a poll at the XBox. For example, if the XBox address is 1, then:

```
!10e [return]
```

The XBox will return either a message, or a no-message sync. If the XBox returns a message, then type an acknowledge:

```
!10a [return]
```

otherwise the XBox will resend the same message on the next poll.

Host commands to the XBox and panels require checksums, so manually typing commands gets somewhat laborious.

DIGI*TRAC panels require a logon password before they will transmit event messages or receive programming commands. Logon is a host responsibility. The XBox does not have the passwords, or store them.

Basic Programming Procedures

Once the DIGI*TRAC system is completely installed, basic programming and testing must be done to ensure that the system is running properly. In many cases, this is done from the connected Host PC through the installed security software (like Hirsch's SAM software). However, a procedure is also available which enables the installer/technician to setup and test the system from a standalone ScramblePad. To learn how to do this, read this section. For information on troubleshooting problems encountered, see the next section.

Programming with the ScramblePad is simply a matter of pressing the START button, entering a series of parameters, separated by an asterisk (*), and concluding with the pound key (#) to send the entire string of numbers to the controller. Figure 7-121 shows the face of a ScramblePad in its unscrambled state (the ScramblePad does not scramble while in Programming Mode):

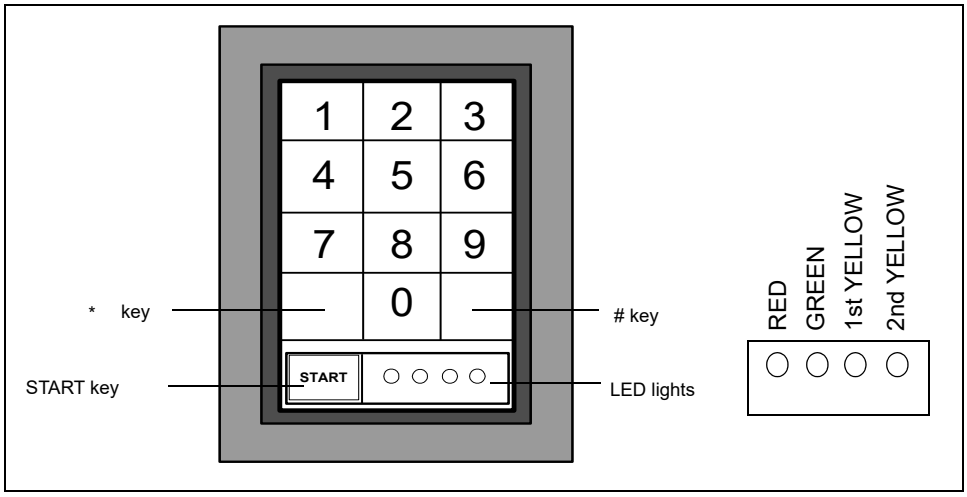


Figure 7-121: ScramblePad Setup For Programming

Note: The Asterisk and Pound keys are not labeled on the ScramblePad.

These keys are used in the following ways:

This Key:	Tells the Program That:
START	This is the beginning of the command sequence.
*	Another element of the command sequence follows, such as a variable or option. This is a *separator*.
#	This is the end of the command sequence. Send it to the controller.

There are also a series of four LEDs on the ScramblePad: Red, Green, and two Yellows. A great deal of information can be conveyed through these LEDs. There are three sets of LED displays:

- ❑ User Display
- ❑ Status Request Display
- ❑ Programming Display

Each is explained on the next pages.

Users will see the results of their entries on the ScramblePad LEDs like this:

This LED state:	Tells You That:
GREEN Steady	Granted Command
RED and Tone	Denied Command (Wrong Code, Wrong Door, Wrong Time, etc.)
RED Flashing & Tone, ScramblePad disabled	Code Tamper (continues for a configurable number of minutes)
2nd YELLOW Steady	Communications failure
RED & Tone & GREEN	Valid Code but overridden by higher priority

Table 7-25: ScramblePad LED User Responses

Note: RED, GREEN, and YELLOW LED 1 can be set to Always ON on the M1N, M2, and M8.

Technicians and users can see the results of their status request inquiries on the ScramblePad LEDs by entering a sequence following the general format:

```
START * Door/Alarm No. #
```

For more about this, refer to “Testing the ScramblePad” starting on page 7-126.

Programmers will see the results of their entries on the ScramblePad LEDs like this:

This LED state:	Tells You That:
1st & 2nd Yellow LED Flashing	System code still 123 (please change this), or using CMD 88.
2nd Yellow LED Flashing	In Programming Mode
Red LED and Tone	Denied Command
Green LED	Granted Command
1st Yellow solid, 2nd Yellow Flashing	Busy with long command

Table 7-26: ScramblePad LED Programming Responses

For an explanation of the basic command syntax, see Chapter 3, “Basic Programming.” For detailed instructions on commands, refer to Chapter 4, “Command Reference.”

The following pages contain information on using the DIGI*TRAC Control Language (DCL) to program some of the more common aspects of the system using the ScramblePad keypad.

Note: If you are using a PC and host software such as SAM, programming is transparent. SAM oversees the selection and proper formatting of commands and takes care of all error checking. This section and the following chapter (Chapter 4) are most useful for those users interested in acquiring proficiency with programming from the ScramblePad, or for using the diagnostic window in SAM.

How To Enter A User Code

To Enter Any Code:

1. Press the START key.
2. Enter the 3-8 digits of the user code.
3. Press the # key to send the code to the controller.

Entering a valid code causes the GREEN LED to flash once. If an invalid code is entered, the RED LED flashes once and the tone sounds once. Either of these operations causes the program to print out a transaction message (if a system printer is installed).

How To Request Status of Door Relays/Line Module Inputs

To Request Status for All Relays/Line Module Inputs:

If you wanted a report on the status of all Line Module Inputs and Relays that are at the same address as the ScramblePad you're currently using (such as, Alarm 1 and Relay 1 from ScramblePad 1), you would use this sequence:

1. Press the START key.
2. Press the * key.
3. Press the # key.

The controller indicates the current status of the input/relay specified by flashing the LEDs on the ScramblePad as shown in Table 7-27:

This LED state:	Tells You That:
Red LED ON Steady	Line Module Input Unmasked (armed)
Red LED Flashing and Tone ON	Alarm is Active
Red LED OFF	Alarm is Masked (disarmed)
2nd Yellow LED ON	Line Module Input is unsecured (door open, sensor active)
2nd Yellow LED OFF	Line Module Input is Secure (door closed, sensor inactive)
Green LED ON	Relay Active
Green LED OFF	Relay Inactive

Table 7-27: ScramblePad LED Test Responses

To Request Status for Specific Relays/Line Module Inputs:

If you need a report on the status of a specified Line Module Input and/or Relay, use the following sequence:

1. Press the START key.
2. Press the * key.
3. Press the required Line Module Input or Relay ID Number.
4. Press the # key.

The controller indicates the current status of the specified input/relay by flashing the LEDs on the ScramblePad. For more on the ScramblePad's LED status, refer to page 7-

126.

For instance, if you entered

```
START * 16 #
```

it means you are requesting the controller to display the status of Expansion Line Module Input 16 and Expansion Relay 16. If, for example, Expansion Line Module Input 16 is currently masked, the Red LED would turn off. If Expansion Relay 16 is currently inactive, the Green LED would turn off.

When designating a specific Line Module Input/Relay, the way in which you enter the number is important:

- ❑ To request the status of a base (on-board) Line Module Input/Relay, use single-digit numbers (e.g. 1, 2, 8).
- ❑ To request the status of an Expansion Line Module Input/Relay, use double digit numbers (e.g. 01, 02, 08).

How To Enter Programming Mode

To enter Programming Mode:

1. Press the START key.
2. Press **1 2 3**.
3. Press the # key to send the System Code to the Controller.

   The # key is the lower right unmarked key.

When in Programming Mode, the ScramblePad will not scramble its display for ease of command entry. While in Programming Mode, both Yellow LEDs will be flashing if the system code is set to 123, or the right most Yellow LED will be flashing if the system code has been changed from 123 to a new system code.

The system is shipped from the factory with a programming code of 123. To protect the system from unauthorized programming, change this code to a new system code of your choice.

How To Enter A Programming Command

To enter a command:

1. Enter Programming Mode as described above.
2. Press the START key.
3. Press the 2 or 3 digits of the Command Number.

   For a detailed explanation of each command number and its meaning, refer to Chapter 4, “Command Reference.”
4. Press the * key to enter additional command parameters and variables where required.

   The * key is the lower left unmarked key.

   The arrangement of command number and parameters is called *command syntax*, and is different for each command.

   For a complete list of all commands and the syntax they require, refer to Chapter 4, “Command Reference.”
5. Press the # key to send the Command to the Controller.

If you have entered a valid command with no errors, the green LED on the ScramblePad flashes once.

If you have entered an invalid command, or committed a syntax or data entry error, the red LED flashes once and a tone sounds. The printer will also print an error message followed by the correct syntax for the selected command. This makes it easy to program DIGI*TRAC correctly, since the program is usually there to guide you through the process.

The use of the printer to record programming commands is important. Always make sure the controller is connected to a printer (whether it is a local parallel printer or a remote serial printer) since this is one of the best ways of determining errors when they occur.

For more about this, refer to “Printing” starting on page 3-32.

How To Quit Programming Mode

To quit programming mode:

1. Press the START key.
2. Press **99**.
3. Press the # key to send the Command to the Controller.

The controller will quit Programming Mode on its own after a designated number of minutes (8 minutes is the default) if no Programming Commands are entered on the Reader.

Note: You don’t have to exit Program Mode after each command. Enter all the commands you need, then exit when you’re finished.

Changing System Codes

Use this procedure to change the number which allows you to enter Programming Mode. You should always replace the factory default code (123) with one of your own selection. If the system code is not changed, anyone with access to this manual can enter Programming Mode and change the controller’s setup values.

To change the System Code:

1. Press the START key.
2. Press **1 2 3** to enter Programming Mode. (1 2 3 is the factory default.)
3. Press the # key to send the system code to the Controller.
4. Press the START key.
5. Press **01** (the Change System Code command).
6. Press the * key.
7. Enter a new 3- to 8-digit code.

Note: Be sure to memorize this code. If necessary, write it down and put it in a safe place.

8. Press the # key to send the new system code to the Controller. The system code is now changed.

If the Code 123 is not changed, both Yellow LEDs will flash while in Programming Mode, the Printer will print a reminder Warning Message on entering Programming Mode, and the Controller will print a reminder Warning Message once every hour.

For more on CMD 01, see “CMD 01: CHANGE SYSTEM CODE” starting on page 4-31.

Set Time and Date

Use this command to set the initial time and date for the controller. This time and date will then be used by the controller as the reference point for all further time- and date-related information.

To set the date:

1. Enter Programming Mode.
2. Press the START key.
3. Enter 50 * *Month Day Year* * *Day of the Week*.

   where:

   Month is figured from January=01 to December=12

   Day of the Week is figured from Monday=1 through Sunday=7.
4. Press #.

For example, if you wanted to set the date as Sunday, June 7, 1998, you would do this:

```
START 50 * 060798 * 2 #
```

To set the time:

1. Enter Programming Mode.
2. Press the START key.
3. Enter 51 * *HHMM*.

   where *HHMM* is figured from midnight=0000 through 11:59 p.m.=2359.
4. Press #.

For example, if you wanted to set the time as 4:32 p.m., you would do this:

```
START 51 * 1632 #
```

For more on CMD 50, refer to “CMD 50: SET DATE & DAY OF THE WEEK” starting on page 4-82. For more on CMD 51, refer to “CMD 51: SET TIME” starting on page 4-83.

Define Time Zone

This command (52) allows the programmer to assign start/stop times for an action in hours, minutes, and days. Each set of start/stop times is a Time Zone. You can have up to 64 standard time zones.

To define a Time Zone:

1. Enter Programming Mode
2. Press the START key.
3. Enter 52 * *Time Zone* * *HHMM* * *HHMM* * *Days*

   where:

   Time Zone is the number from 1 - 64 you wish to define.

   The first group of *HHMM* are the hours and minutes (in 24-hour clock) to START the Time Zone period

The second group of *HHMM* are the hours and minutes to END the period.

Days are the preassigned number of days in the week where 1 = Monday, 7 = Sunday, and 8 = holiday.

4. Press #.

For example, if you entered this command sequence:

```
START 52 * 6 * 0830 * 1800 * 12345 #
```

it indicates that Time Zone 6 has been defined as the time from 8:30 AM to 6:00 PM on Monday, Tuesday, Wednesday, Thursday, and Friday. Time Zones are associated with doors to define Access Zones as shown in the next example, or automatic events like unlocking/relocking a door.

For more about CMD 52, refer to “CMD 52: DEFINE STANDARD TIME ZONE 1-64” on page 4-84.

Define Access Zone

The command (CMD 17) assigns a specific Time Zone to one or more doors. This combination is defined as an *Access Zone*. It is one of the most important commands you will use, since at least one access zone must be assigned to every access user.

To define a standard Access Zone:

1. Enter Programming Mode
2. Press the START key.
3. Enter 17 * *Access Zone* * *Time Zone* * *Doors*

   where:

   Access Zone is a number from 0 - 65 you want to associate with this combination of Time Zone and doors. (Two values are predefined: 0 = never at any doors and 65 = always at all doors; all other values are available.)

   Time Zone is a number from 0 - 149 describing start and stop times. For more about defining time zones, see “Define Time Zone” on page 7-370, or “CMD 52: DEFINE STANDARD TIME ZONE 1-64” on page 4-84.

   Doors are the door relay number for each door you assign to this Access Zone.
4. Press #.

For example, if you entered this command sequence:

```
START 17 * 1 * 1 * 123 #
```

it indicates that Access Zone 1 has been defined as Time Zone 1 used at doors 1, 2, and 3. For more on CMD 17,refer to “CMD 17: DEFINE STANDARD ACCESS ZONE (1-64)” starting on page 4-51.

Another command, CMD 24, is used to define a different Time Zone for each door. For more on CMD 24, refer to “CMD 24: DEFINE STANDARD ACCESS ZONE 1-64 (One Time Zone Per Door/Reader)” starting on page 4-60.

Define Control Zone

This command (45) defines a Control Zone. Control Zones are used to link selected users with a variety of relay or alarm functions, such as lights, power, and elevator functions, or define inputs used to trigger a group of outputs.

To define a Control Zone:

1. Enter Programming Mode
2. Press the START key.
3. Enter 45 * *Control Zone* * *Time Zone* * *Relays or Inputs*

   where:

   Control Zone is a number from 0 - 191 you want to associate with this combination of Time Zone and relays/inputs. (One value is predefined: 0 = never at any relay; all other values are available.)

   Time Zone is a number from 0 - 149 describing start and stop times. For more about defining time zones, see “Define Time Zone” on page 7-370, or “CMD 52: DEFINE STANDARD TIME ZONE 1-64” on page 4-84.

   Relays or Inputs are the relay or input numbers for each device you assign to this Control Zone.
4. Press #.

For example, if you entered this command sequence:

```
START 45 * 3 * 1 * 367 #
```

it indicates that Control Zone 3 has been defined as Time Zone 1 which is being used at relays/inputs 3, 6, and 7.

For more on CMD 45, refer to “CMD 45: DEFINE STANDARD CONTROL ZONE” on page 4-77.

Assigning A ScramblePad Code To A New User

To enroll a new user with a ScramblePad code:

1. Enter Programming Mode (START *System Code #*).
2. Press the START key.
3. Enter 10 * *User Number* * *Code* * *Access Zone*

   where:

   User Number is the unique number in the Controller’s database that has been assigned to the user

   Code is the 3 - 8 digit number the user enters on the ScramblePad.

   Access Zone defines the doors to which this user can have access and the times at which this access is allowed.

   With a base controller, the code range is 1- 999. If one of the optional MEB/CE code expansion boards is installed in this Controller, code ranges expand to 1 - 4,000 (for the MEB/CE4) or 1 - 16,000 (for the MEB/CE16).
4. Press #.

Once the new user has been assigned a code, he/she can use it to enter/exit from any secure door defined within the specified access zone.

For more about assigning codes to new or existing users, refer to “Assigning a Card to a New User” on page 7-373. For more about CMD 10, refer to “CMD 10: ADD KEYPAD ACCESS USER (IDF 1)” on page 4-43.

Changing a User's Code and/or Access Zone

This command (11) can be used to reprogram not only the user's code, but also the Access Zone to which he/she is assigned.

To change a user's code/access zone:

1. Enter Programming Mode
2. Press the START key.
3. Enter 11 * *User Number* * *Code* * *Access Zone*

   where:

   User Number is the unique number in the Controller's database that has been assigned to the user.

   Code is the 3 - 8 digit number the user enters on the ScramblePad.

   Access Zone defines the doors to which this user can have access and the times at which this access is allowed.
4. Press #.

Once the user has been reassigned a code and/or access zone, he/she can use it to enter/exit from any secure door defined within the specified access zone.

For more about assigning codes to new or existing users, refer to "Passback Zones (Physical Zones)" starting on page 3-26. For more about CMD 11, refer to "CMD 11: REDEFINE KEYPAD ACCESS USER (IDF 1 & 6)" starting on page 4-44.

Assigning a Card to a New User

To enroll a new user with a card:

1. Enter Programming Mode.
2. Press START
3. Enter 310 * *User Number* * *Access Zone* * *Card Number*

   where:

   User Number is the number assigned to the user who will possess this card.

   Access Zone defines the doors/times this user/card has access.

   Card Number is the number assigned to the specific card.
4. Swipe the card through the card reader or at the enrollment station. This automatically reads the raw code, converts it to Hirsch format, assigns the card code to the specified User Number, and records the information in the connected Controller.

   An *enrollment station* is a device (such as Hirsch's DMES series) dedicated to the enrollment process. This device is recommended when there are many cards to be enrolled, since it leaves card readers free to handle the task of access control. A ScramblePad and MATCH Reader combination is required to enroll cards into a stand-alone DIGI*TRAC System. Contact Hirsch for information on pre-configured Enrollment Stations.
5. Press #.

Enrolling a valid Card will cause the Green MATCH Reader LED to flash once. Reading a Card with invalid formatting, or with damaged or conflicting data, will cause the Green LED to flicker and cause the red LED on the ScramblePad to light and sound a tone.

For more about assigning codes to new or existing users, refer to "User Numbers" on

page 3-23. For more about enrolling users, refer to “Card Enrollment” starting on page 3-31. For more about CMD 310, refer to “CMD 310: ADD ACCESS USER CARD ONLY (IDF 2)” starting on page 4-210.

Delete a User

To delete any user:

1. Enter Programming Mode.
2. Press the START key.
3. Enter 16 * *User Number*

   where *User Number* is the number assigned to the user who will be deleted.
4. Press #.

The user is deleted from the database and will not be able to enter any secure areas.

For more about CMD 16, refer to “CMD 16: DELETE ANY USER (All IDFs)” starting on page 4-50.

Printing the List of Commands

To print a list of commands:

1. Make sure the page fed in the printer is positioned at the top.
2. From the ScramblePad, enter Programming Mode.
3. Press the START key.
4. Enter 00 * 0 #

The attached printer prints out a complete list of all programming commands. Refer to Chapter 4, “Command Reference,” for a complete list of all variables and meanings. For a complete explanation of the Command 88 printouts, refer to Chapter 5.

Testing a System

Use this command sequence to verify the system is operating properly. First, add a Test Code. Adding a Test Code enables an installer to test the operation of the door relays, automatic relock, and door status monitoring immediately upon completion of the initial System installation. For programming and testing to go smoothly, you should connect a printer to the controller.

Hirsch controllers are factory configured so that a test code will trigger a relay for the Factory Set Time Up time of 6 seconds. If changes are required from the Factory Set Ups, review Command 88 in Chapter 5. For more on Factory Setups, refer to Chapter 5.

For convenient testing you may want to temporarily connect a ScramblePad at the Controller (if one isn’t already installed there) to program, test, and observe the controller’s operation. Also, turn on all disabled RQEs so you can observe their response (as required).

To Add A Test ScramblePad Code:

1. Enter Programming Mode.
2. Press START 10 * 1 * 100 * 65 #
3. Press START 100 #

The relay associated with the ScramblePad address which just entered the test code should be triggered.

4. Complete the testing by entering the test code from each permanently installed ScramblePad.

The controller's printer will show the results.

To Delete the Test Code once testing is completed:

1. Enter Programming Mode.
2. Press START 16 * 1 #
3. Press START 99 # to quit programming mode upon completion of testing.

If the controller is monitoring alarms, be sure to completely test each circuit by tripping the alarm sensor, whether it's a door switch or a motion sensor. If you have Time Zone masking of alarms programmed, be sure you change the controller clock to a few minutes before the masking is activated and try the alarms. Try the same tests for any Time Zone with automatic controls, such as door unlocking and relocking.

*Note: It takes the controller clock up to one minute to update the internal system controls. Don't get impatient when changing the controller time to force Time Zone controls for testing. Wait a minute. To verify that a Time Zone is active, print the Time Zone Status Report with Command 88 * 3 and check the Zone's status in the right column.*

Printing Setups

Once your setups are complete and you have finished system testing, make a printout of the exact setups for your records. To do this, enter:

```
START 88 * 0 #
```

Make sure you have enough paper in the printer and that it's properly aligned at the top of the page before you use this command.

This testing process also represents the final checkout of the installation for the customer. Give a copy of the system setups to the customer for their acceptance before handing over the configured system to the customer/owner and the system operator.

Note: Do not cold start the controller after you've finished programming. If you do, all programming will be lost from memory and you'll have to reprogram the system. If SAM is installed, use SAM's Backup procedure to back up programming.

Printing in Programming Mode

Programming becomes simpler and easier when a printer is installed on a standalone system. Having a printer installed when programming provides a wide array of benefits, some of which are listed below.

- ❏ In a stand-alone system, results from programming can be printed as they are entered. Having results print as you are programming is very helpful, especially when the system detects an error. When the system detects a programming error, it prints the correct command syntax for your verification.
- ❏ When you're in a situation where you don't have your programming guide and you remember the command number but not the syntax, printing capability becomes extremely helpful. Entering the command number followed by two asterisks (**) and the pound (#) key prints the proper command syntax.

- A complete set of programming commands can be printed by category, or in total, by using Command 00.
- Printouts are the best way to verify changes in system setups.
- Printing is the *only* way the system can automatically generate codes. As codes are generated, the system must be able to print them so they can be issued and associated with a user.

Printing in Day-to-Day Operation

Once your facility is in full operation you can reduce the quantity of printed information by using Commands 05 and 06:

- Command 05 – provides selective printing by category of events, such as relay state changes.
- Command 06 – provides selective printing of granted (not denied) code transactions and RQE events on a door by door basis.

Troubleshooting

When troubleshooting a controller, do things in a methodical manner and take careful notes regarding status of ScramblePad LEDs, controller board LEDs, voltage levels, and so on. In DIGI*TRAC controllers, a printer is essential for troubleshooting. The only way to determine how the controller and system it controls is working is to review the printouts. Also, the only way in which a programmer can tell how the system is responding to instructions is to view the responses on the printer. Hirsch provides a comprehensive set of commands that can print out the setups and status of the entire DIGI*TRAC system.

Common Problems

Problems fall into two broad categories:

- ❑ Hardware
- ❑ Programming

Common hardware-related problems on initial system installation include:

- ❑ Wiring not connected properly
- ❑ ScramblePads not addressed correctly
- ❑ Electric locks and power supplies not installed or wired properly
- ❑ Door contacts not aligned or wired properly
- ❑ RQE motion detectors not aligned, balanced, or wired properly
- ❑ Wiring gauge or length is inappropriate
- ❑ MOVs are not installed at electric locks

Common hardware problems encountered after a system has been up and running for a while are:

- ❑ Loose wire connections or damaged splices
- ❑ Spikes, surges, brownouts causing electrical damage
- ❑ Noise on the primary AC input circuit

Common programming-related problems on initial system installation include:

- ❑ System clock not accurately set so codes and automatic events do not work as expected
- ❑ RQE inputs not programmed to unlock doors
- ❑ User codes assigned to the wrong Access Zones

Common programming problems encountered after the system has been up and running for a while are:

- ❑ Wrong user deleted from the system
- ❑ Access Zones changed
- ❑ New user added and is given the wrong code or Access Zone
- ❑ Time Zones, Alarms, or Control codes affecting relays are in an unexpected or conflicting mode
- ❑ System administrator forgets system code to get into programming

General Troubleshooting Procedures

The following things should always be checked in any system this is not operating properly:

1. Verify that the system is powered properly. Check AC input voltage and all fuses.
2. Verify that all wiring is terminated properly and that there is line continuity (no breaks or shorts).
3. Look for any visible signs of damage at the ScramblePad and controller.
4. Confirm system programming. Verify system clock is set accurately. Verify that all Time Zones, Access Zones, Access Codes, Control Codes, and so on are properly entered.

DIGI*TRAC Troubleshooting Guide

Problem	Possible Cause	Possible Solution
System doesn't operate or only operates for a short period of time when 110VAC fails.	Battery disconnected.	Connect battery. Allow time to recharge, then test.
	Battery was not fully charged when AC failed.	Allow adequate time for battery to recharge, then test.
	Battery is defective.	If battery will not hold charge, replace.
	System battery fuse blown.	Replace system battery fuse.
	Battery charger fuse blown.	Replay battery charger fuse.
Cannot enter Programming Mode	System code was changed from factory default, forgot new code.	Hold blue reset button on controller for 5 seconds then release. System code reset back to factory default of 123. Sets all ScramblePads to allow programming.
	Command 03 was used to make ScramblePad non-programming.	Use ScramblePad authorized for programming.
Yellow LED 2 on ScramblePad steady. ScramblePad not communicating with system.	Voltage spike, surge, noise on primary AC input.	Power system down by disconnecting battery then AC, then reverse procedure to power up.
	Inductive kickback from lock to system.	Same as above. Verify MOV installed at lock according to this guide. Replace MOV if needed.
	ScramblePad not wired correctly.	Check Data A and B lines.
After inserting a new CCM and powering the controller back up, the lights freeze in a fixed pattern and the test light remains ON.	This indicates that either the CCM has not been inserted correctly, the controller received an electric shock during the procedure, or the CCM is damaged.	Power down the controller, make sure the CCM is securely seated in its socket, then power the controller back up. If the problem persists, power the controller down, reinstall the previous CCM and power it back up again. (WARNING: The controller will cold start if you go back an entire version.) If the controller comes out of its startup and runs, the new CCM is damaged and you need to replace it. If it doesn't come out of its startup, the controller board is suspect. Contact your Hirsch supplier or Hirsch Technical Support for assistance.

*Table 7-28: DIGI*TRAC Troubleshooting Guide*

Problem	Possible Cause	Possible Solution
Valid access code is entered at ScramblePad. Red and Green LEDs flash and door does not unlock.	Access code is being overridden by higher level Time Zone event or control code.	Request CMD 88*7 (Relay Setups and Status) and CMD 88*17 (Detailed Relay Status) printouts to determine what is the causing override.
The controller appears to be functioning, but not as expected.	There may be some errors in programming.	Refer to the printouts and the section on reprogramming and updating in "Upgrading the CCM" starting on page 7-27. Make sure the controller is programmed with the same values as the previous CCM. If the pre- and post-CCM update printouts are considerably different, the controller's memory is corrupted. Perform a cold start on the controller and reprogram it using your previous printouts as a guide.
What are compatible modems for Hirsch Products?		At this time, there are only three manufacturers: MultiTech MT932BA, Zoom 14.4 Model 516, and US Robotics (any 28.8 baud modem). However, most 14.4 and 28.8 modems should work with Hirsch products: just disable both the Flow Control and Auto-Answer features and see if they work.
Can't get my enrollment station to read a card.	The enrollment station is not properly configured by software. The enrollment station's MATCH/ScramblePad is incorrectly configured.	See your software manual for instructions. Make sure the MATCH/ScramblePad on the enrollment station is correctly configured. For example, if you are using Prox cards, make sure DIP switch 8 is ON. Bring up HyperTerminal and test the enrollment station by addressing the correct port. If it responds, you are connected. For more information on this problem, refer to Hirsch Technical Support.

*Table 7-28: DIGI*TRAC Troubleshooting Guide (Continued)*

Problem	Possible Cause	Possible Solution
What are the steps or considerations in adding to my system down the road?		This depends on the additions being made: to the controller or to the components connected to the controller. If you are adding a board or CCM to the controller, make sure to turn off the controller's power before adding or replacing a component. However, make sure not to remove a memory expansion board; if you do, all information stored in that board will be lost and you'll have to reprogram the system. If you are adding components to the system, follow these suggestions: 1. As a general rule, it's easier to program the system first before connecting the new component. If done the other way around, the system may make assumptions about the new component which are based on the default and can result in alarm conditions. For example, the controller assumes the connected line module is a DTLM2 unless it has been programmed in advance to recognize a DTLM3. 2. If you are adding a NET*MUX, your one consideration is how long your remote site can afford to be out-of-touch with the host site. 3. If you are adding a new door, you should set up Access Zones including the door. 4. If you are adding an XBox, there is a problem with switching from S*NET to X*NET. See the SAM Manual for more on this.

*Table 7-28: DIGI*TRAC Troubleshooting Guide (Continued)*

Troubleshooting the Controller Using Status LEDs

You can troubleshoot the controller board using the LED status lights on the right side of the controller board.

Table 7-29 describes what each of the LEDs mean:

LED	Status	Condition
BOX TAMPER	Yellow ON Red ON	Box Tamper Multiple Box Tamper
AC	Green ON Red ON	AC OK AC Fail
BAT	Green ON No lights Red ON	Battery OK (24V-28V) Battery Low (21V-23V) Battery Failure
SYS	Green ON Red ON	Controller OK Controller Failure
KPD	Red Flash Green Flash	Controller polling all attached ScramblePads/MATCH ScramblePad/MATCH poll response
NET	Red Flash Green Flash	Network polling all attached controllers Controller poll response
TEST	Yellow ON	Controller in Self Test Mode
ALARM	Yellow ON	Alarm events in the buffer

Table 7-29: LED Status Chart

The Controller board's power circuits are all fused. The location of each fuse is clearly marked on the board and provides surge protection. If a fuse blows, replace it immediately.

On power-up, the system performs a series of tests. A failure is indicated by a steady red from SYS. A quick LED diagnostic is shown below.

LED Configuration	Meaning/Solution
● ○ AC ○ ○ BAT ○ ● SYS ○ ○ KPD ○ ○ NET	RAM test failure. Check the memory on the controller board. If you have recently replaced the CCM 6.x with a new CCM 7.x, you may have forgotten to remove the underlying RAM chip. For more on this, refer to Step 5 of "Upgrading the CCM" on page 7-27.
○ ○ AC ● ○ BAT ○ ● SYS ○ ○ KPD ○ ○ NET	Clock failure. The MC146818 chip could be at fault. Contact Hirsch Technical Support. You may need a new controller board.

Table 7-30: Status LED Configurations

LED Configuration	Meaning/Solution
● ○ AC ● ○ BAT ○ ● SYS ○ ○ KPD ○ ○ NET	ROM failure. Check/replace the CCM on the controller board. For more about this, refer to “Upgrading the CCM” starting on page 7-27.
○ ○ AC ○ ○ BAT ● ● SYS ○ ○ KPD ○ ○ NET	A-to-D converter failure. The ADC0844 chip on your controller board could be at fault. Contact Hirsch Technical Support. You may need a new controller board.
● ○ AC ○ ○ BAT ● ● SYS ○ ○ KPD ○ ○ NET	Power to the controller board is inadequate. Check power supply.
○ ○ AC ● ○ BAT ● ● SYS ○ ○ KPD ○ ○ NET	Timing failure. The 14.7 MHz and 32.7 KHz clock on the controller board may be at fault. Contact Hirsch Technical Support.
○ ○ AC ○ ○ BAT ○ ● SYS ● ○ KPD ○ ○ NET	ROM page register failure. Check/replace CCM.

Table 7-30: Status LED Configurations (Continued)

Note: In black and white, grey indicates steady green and black indicates steady red.

For more about troubleshooting the controller, refer to “DIGI*TRAC Troubleshooting Guide” on page 7-379.

ScramblePad Troubleshooting Guide

Problem	Possible Cause	Possible Solution
Red LED is flashing on 2 or more ScramblePads.	ScramblePads have been given the same address.	Address each ScramblePad uniquely (refer to "ScramblePad Installation" on page 7-97).
All four LEDs are flashing and periodic beep from ScramblePad.	ScramblePad is in Physical Tamper. Bezel is removed or tab is broken.	Install bezel. If tab is broken, replace bezel. Turn OFF DIP switch 6 (for DS37L) or switch 8 (for DS47L) on ScramblePad to disable Physical Tamper.
Yellow LED 2 is on steady.	ScramblePad Data line A is not properly terminated. AC surge or lock inductive kickback caused ScramblePad to go off-line.	Check terminations and line continuity. Power system down (battery first, then AC), then power back up. Cold start as last resort.
Press the START key and nothing happens.	Controller not powered. ScramblePad not wired properly. ScramblePad power fuse blown. Controller board power fuse blown.	Verify primary AC power source is good. Check internal power supply fuse. Verify wiring and line continuity (refer to "ScramblePad Installation" on page 7-97). Replace ScramblePad power fuse (refer to "Controller Installation" on page 7-17). Replace circuit board power fuse (refer to "Controller Installation" on page 7-17).
ScramblePad keys work intermittently	Membrane switch is faulty	Replace membrane switch or return to factory for repair.
Yellow LED 1 on steady.	DIGI*TRAC has a serious problem.	Check AC source, fuse. Power system down, then back up. Cold start as last resort.
ScramblePad is beeping and Red LED is flashing.	ScramblePad is in Code Tamper.	Device automatically times out after one minute and returns to normal operation. It is not configurable.

Table 7-31: ScramblePad Troubleshooting Guide

Hardware Cold Start Procedure

There are rare occasions when you will have to perform the hardware cold start procedure. Normally, if you just want to reassign or relocate the panel or erase all codes and setups, use the 30-second RESET button procedure defined in “Resetting the Controller” on page 7-26.

Note: This procedure only works for pre-CE CCM Version 6.X.X. boards manufactured more than three or four years ago. Newer CCM7 boards cannot use this procedure. The difference between these boards is shown in Figure 7-122.

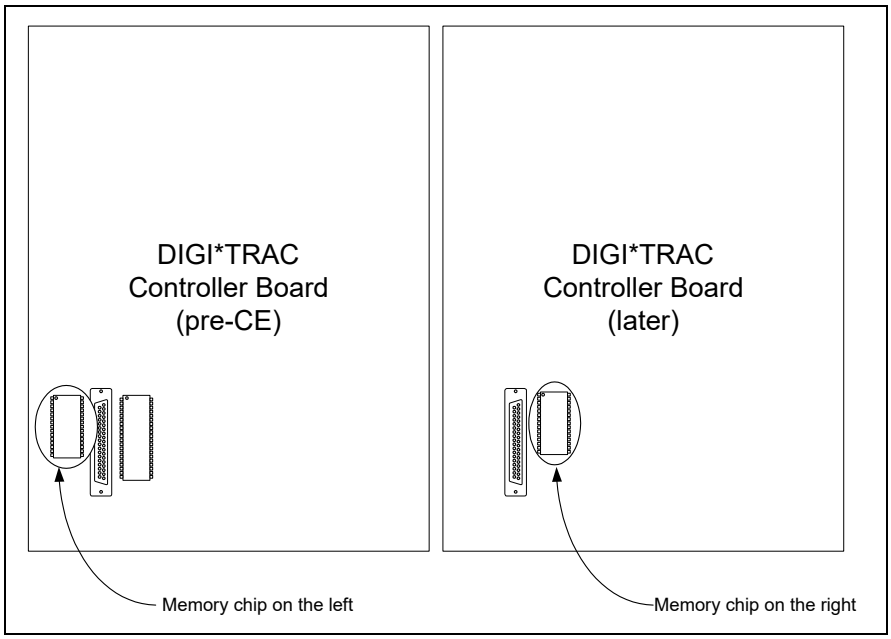


Figure 7-122: CCM Version Comparisons

This procedure should only be performed when the red SYS LED on the controller board is lit and no action you take seems to affect this condition. This usually means that the controller is locked up and only a cold start will work. Performing this procedure under any other circumstances is highly discouraged.

Warning: Using this procedure deletes all setups and configurations.

To perform a cold start:

1. Ground yourself by touching the controller enclosure or power supply to remove any potential static electricity.
2. Turn all controller system power off by removing connectors for both AC power and the standby battery.
   a. Disconnect the DC battery. To locate the DC battery, see Figure 1-3 on page 1-7.
   b. Disconnect the main power to the controller.
   c. Remove the AC fuse located on the power supply in the lower left corner of the enclosure.

   This procedure can only be performed with the power off.
3. Remove the CCM module.

4. Use a wire jumper, such as Radio Shack #278-016, to do this:
   a. Attach the jumper to the pins 14 and 28 as shown in Figure 7-123.

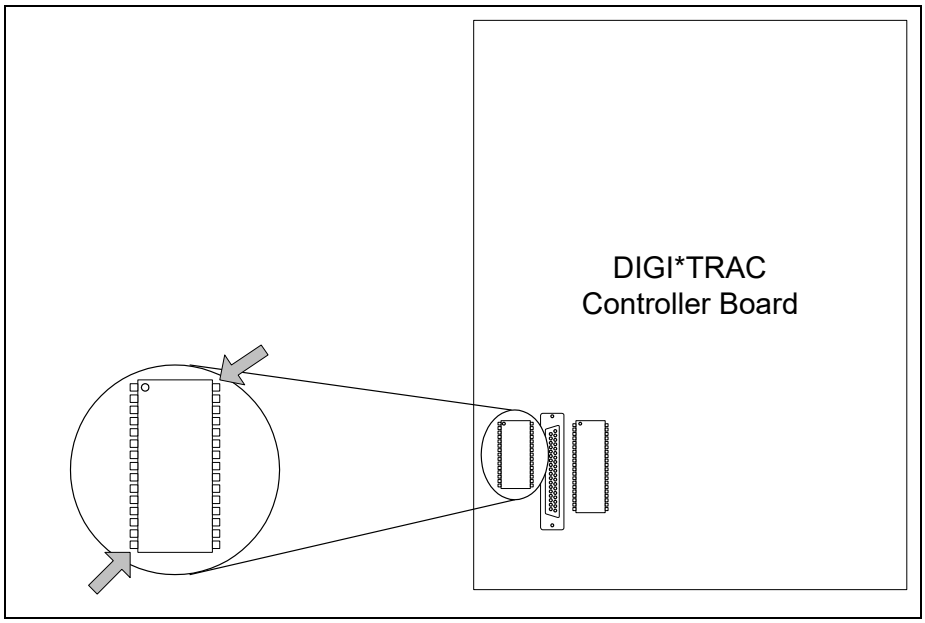


Figure 7-123: Hardware Cold Start Jumper Setting

   b. Wait 3 seconds.
   c. Remove the jumper.
5. Plug the CCM module back into the controller.
6. Power up the controller.

Use this procedure only once or twice to see if the panel resumes normal operation after power-up. If the red SYS LED remains lit, it means there is a real hardware failure and the panel must be replaced and repaired.

Before You Call

If you are unable to diagnose a problem and take the necessary corrective action, contact your local dealer. The following steps should be performed to gather useful information:

1. Make a detailed description of the problem.
2. Make a detailed description of the system, including:
   - Controller type
   - Firmware version numbers (see “Getting Help” on page v)
   - Type and number of readers
   - Other system components (locks, door contacts, RQEs, and so on)
3. Specify how long the system has been installed and list any previous problems with the system.
4. Approximate the distance between system components, such as the distance between the controller and all readers.
   - Identiv recommends that all physical installations and cabling meet the specifications published in the appropriate electrical standard to ensure proper operation of all Identiv devices connected. When determining the required power delivery for connected devices, Installers should calculate cabling needs based on the power specifications of each connected device, the operational output of the power source and the voltage drop relative to the length of the cable. Identiv does not specify cable types or gauges due to the wide variance of available cable configurations, and similar wide variance in installation types and environmental conditions. All examples provided throughout this installation document are designed to provide guidance only and should be verified by a certified low voltage electrician or contractor on a per site basis.
5. For older DIGI*TRAC systems:
   - Use CMD 88*0 to print out a complete set of system setups and status.
   - Use CMD 38 to print out a complete list of all users.
   - Use CMD 260*0 to printout the Alarm Condition Block.

If your dealer is not available, contact Technical Support directly. This can be done in a number of ways:

Internet: https://support.identiv.com/contact/

Email: support@identiv.com

Phone: 877-447-7249 toll-free

Mail: Identiv
1900-B Carnegie Avenue
Santa Ana, CA 92705-5520

Attn: Technical Support

Mx Controller

8

This Page Intentionally Left Blank

Introduction

This chapter provides information about the Hirsch Mx controller, including:

- ❑ Advantages of the Mx controller
- ❑ A summary of the different Mx controller configurations
- ❑ An overview of the Mx controller's main components
- ❑ Design considerations, including battery capacity and power limitations
- ❑ Typical connections, such as the wiring for a door
- ❑ Setup and installation, including wiring distance limits, and configuration of the integrated SNIB2 capability and the integrated Ethernet port
- ❑ A worksheet for an Mx Controller, to help you plan your security system. (Worksheets for other system components are provided in Appendix A.)
- ❑ Performing periodic maintenance

When a characteristic of the Mx Controller is essentially identical to that of a DIGI*TRAC Controller, a cross-reference is provided to an existing topic in this guide.

Advantages of the Mx Controller

Although the Mx controller is similar to a DIGI*TRAC controller in many ways, it does provide some distinct advantages:

- ❑ The Mx controller is designed to operate in a networked environment, so it has an integrated Ethernet connection and integrated SNIB2 capability. This frees up a slot for another optional expansion board, and saves you the time it would have taken to install a SNIB2 expansion board. (If you want to use a SNIB3 expansion board, see "Preparing an Mx Controller to Use a SNIB3" on page 7-75.)
- ❑ The Mx controller's main board includes a 5-pin MATCH terminal and a 6-pin Wiegand terminal for each door. Before the Velocity 3.6 SP2.1 release and the CCM firmware 7.5.70.12 release:
  - For basic access control applications that only need an entry reader on a door, the Wiegand terminal enables you to directly connect the Mx controller to a reader or keypad with a Wiegand interface, without a separate MATCH2 board.
  - For wire runs longer than 500 feet, or more advanced access control applications that need an exit reader on a door, the MATCH terminal had to be used to connect the Mx controller to a MATCH2 interface board or ScramblePad reader.

  Now on an Mx-2 or Mx-4 controller where Wiegand terminals are available from unused doors, some of those available terminals can easily be used for exit readers. For details, see "Connecting Exit Readers to Unused Wiegand Terminals on Mx-2 or Mx-4 Controllers" on page 8-22.
- ❑ The glass fuses for the reader circuits have been replaced by resettable fuses which automatically restore circuit integrity after the overcurrent has been removed. (Only two 5 Amp glass fuses remain, which are located by the power supply connector and the standby battery connector.)

❑ The Mx controller can be configured to control either 2, 4, or 8 doors, depending on which model of the Command and Control Module (CCMx) is installed. This enables a controller to be easily expanded in the field, by replacing the CCMx and wiring the additional doors.

NOTE: Because the Mx-2 controller now ships with just a 1.3 Ah standby battery, you will probably also need to either upgrade to a larger capacity standby battery or add a front-end UPS when upgrading an Mx-2 controller to an Mx-4 or Mx-8.

Mx Controller Configurations

There are three Mx Controller configurations, which differ only in the number of supervised doors (including alarm inputs) and the capacity of the factory-equipped standby battery.

❑ The Mx-2 can control up to two doors, and has a 1.3 Ah standby battery.

❑ The Mx-4 can control up to four doors, and has a 7.2 Ah standby battery.

❑ The Mx-8 can control up to eight doors, and has a 7.2 Ah standby battery.

The configuration is determined by the model of CCMx that is installed. This enables you to easily upgrade an Mx controller after its initial installation, without affecting the existing wiring. The number of readers and ScramblePads the controller can support is determined by:

- The number of addresses available (16 maximum) for ScramblePads and MATCH2 interfaces
- The total power required by ScramblePads and MATCH2 interfaces attached to the controller. This cannot exceed the power capacity of the controller. To calculate this capacity, see Table 8-5 on page 8-17.

Note: When the available controller power is insufficient, an external power supply can be used to power a ScramblePad or MATCH2 interface. For more information, see "UL Requirements" starting on page vii.

Components of the Mx Controller

Like the DIGI*TRAC Controllers, a Hirsch Mx Controller consists of several components in a secure enclosure, as shown in the following figure.

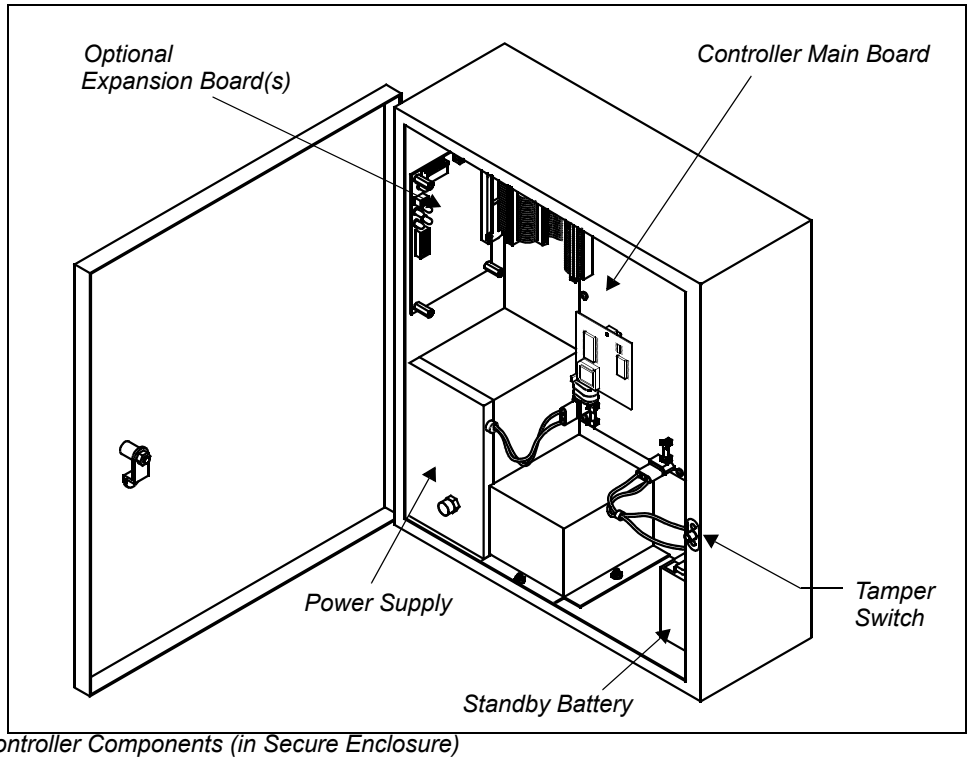


Figure 8-1: Mx Controller Components (in Secure Enclosure)

The Controller enclosure contains the following major components:

- ❑ Controller main board
- ❑ Power supply
- ❑ Standby battery
- ❑ Tamper switch
- ❑ Optional expansion boards

Each of these components is explained briefly.

Mx Controller Main Board

The Mx Controller Main Board contains the main connectors to the surrounding system. Through it, you can connect to ScramblePads, MATCH, and Wiegand reader interfaces, input devices, output devices, an Ethernet network, other controllers, and power sources.

The following figure shows the connectors (and other key components) of an Mx Controller's main board.

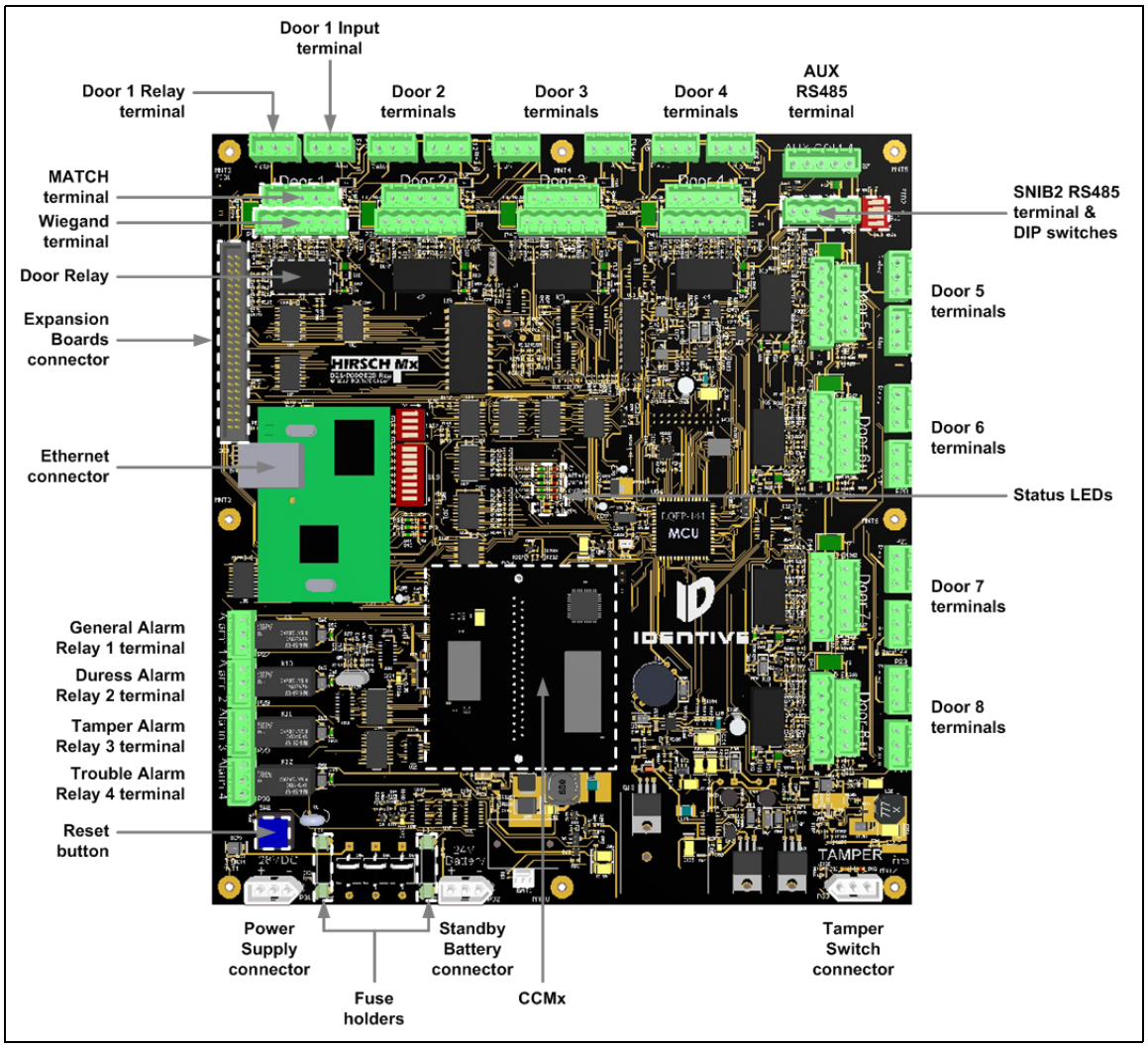


Figure 8-2: Mx Controller Main Board Connectors and Components

Relays come in two sizes:

- ❑ Larger (5 amp, Form C) relays for controlling door access devices, such as magnetic locks and electric strikes, and
- ❑ Smaller (2 amp, Form C) relays for executing various types of alarm events.

Terminal Blocks are the green plastic components into which wires are inserted from input/output devices. An Mx Controller provides a certain number of terminal blocks — and through them connections to input/output devices — which you can increase by adding optional expansion boards.

- ❑ The 3-wire (Door Input, Door Relay, and dedicated Alarm Relay) terminal blocks are used for *analog* inputs, such as multi-state alarm inputs through the line modules, and two-state outputs such as magnetic locks and electric strikes.
- ❑ The 5-wire MATCH terminal blocks are used for connecting the wiring from ScramblePad keypads or readers (through the MATCH2 Reader Interface). These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit.

- ❑ The 6-wire terminal blocks are used for connecting the wiring from a 12VDC keypad or reader with a Wiegand interface. These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.

AUX RS485 Terminal is initially unused, but is planned to later enable you to communicate with RS485 serial devices (such as readers and other interfaces), using protocols such as the Open Supervised Device Protocol (OSDP).

SNIB2 RS485 Terminal (and DIP switches) enables you to securely communicate with downstream Mx or DIGI*TRAC controllers (managed by the same computer).

Ethernet Connector (and DIP switches) enables you to connect to a LAN/WAN and communicate with a computer running Velocity.

Fuses are mounted by the power supply connector and the standby battery connector. (All reader terminals are protected with resettable fuses.)

Expansion Board Connector links any expansion boards mounted in the Controller enclosure to the Controller Main Board.

Status LEDs provide quick visual diagnostics on the current operation of the Controller.

Reset Button performs three types of reset depending on how long you hold down the button, as shown in Table 7-3 on page 7-26.

Command and Control Module (CCMx) contains the firmware that embodies the logic and control functions of the controller, including the DIGI*TRAC Control Language. Firmware can be downloaded from Velocity, or the CCMx can be reprogrammed on a Flashmaster device. For more information, refer to Chapters 3 and 4 which deal with the DIGI*TRAC Control Language and programming.

Note: Different models of the CCMx are available, which determine whether the Mx Controller is configured to control up to 2, 4, or 8 doors (and an equivalent number of alarm inputs).

Power Supply Connector provides cable connection to the Internal Power Supply.

Standby Battery Connector provides cable connection to the backup battery.

Enclosure Tamper Switch Connector provides a cable connection to the Tamper Switch on the Controller enclosure. Whenever the enclosure door is opened, the tamper switch alarm is activated.

Internal Power Supply

The Internal Power Supply can use either a 110 or 240 VAC supply (or 100 VAC for Japan) to provide DC power to the Controller Main Board and attached Expansion Boards. Depending on your controller, this means support for up to 16 ScramblePads or combination of ScramblePads and readers. For input and output devices requiring power – such as electric strikes and magnetic locks, motion detectors, retinal scanners, and surveillance cameras – auxiliary power supplies must be used.

Standby Battery

This component supplies 24 VDC of backup power to the Controller Board even if primary AC power fails. This battery is capable of supplying power to the Controller Board for several hours. The standby time is dependent on the connected devices and can be calculated by using the formula found in “Controller Battery Standby Capacity” starting on page 8-15.

The size of the 7.2 Ah battery pack provided with an Mx-4 or Mx-8 controller is approximately 3.69" H x 5.94" W x 5.13" D (94 mm H x 151 mm W x 130 mm D).

Under normal conditions, the standby battery has a life span of 4 to 5 years. Its status can be interrogated using Velocity's Diagnostic Window. For more information, see the topics in the section about "Performing Periodic Maintenance" starting on page 8-33.

Tamper Switch

The tamper switch is a contact switch that is normally closed while the door to the controller enclosure is closed. Opening the enclosure door opens a circuit, which generates a message that is sent to Velocity, enabling the event to be viewed in real-time and logged for later analysis.

Expansion Boards

Optional expansion boards increase the capabilities of Mx Controllers. For example, the Alarm Expansion Board increases the number of line module inputs that the controller can accept, and the Relay Expansion Board extends the number of control outputs that a controller can accommodate. The MEB series increases the controller's available memory, expanding the number of alarm and event buffers or codes the controller can hold.

Table 8-1 provides an overview of the available expansion boards. An Mx Controller can accommodate up to 5 expansion boards, subject to the restrictions explained in this table.

Model #	Description	Comments
AEB8	Alarm Expansion Board with 8 Inputs	Adds 8 additional high security alarm inputs, and features removable connectors. Each input requires an appropriate Line Module. An AEB8 draws 15 mA at 28 VDC. Velocity supports up to 4 of these boards in an Mx Controller.
REB8	Relay Expansion Board with 8 Relays	Adds 8 additional 2 Amp Form C dry mode relays. Features status LEDs and removable connectors. An REB8 draws 15 mA at 28 VDC when idle, and a maximum of 80 mA when all relays are active. Velocity supports up to 5 of these boards in an Mx Controller.
MEB/BE	Memory Expansion Board - Buffer Expansion	Expands the standard buffer from 1,560 events and 1,560 alarms to approximately 20,000 events and 2,000 alarms. Protected from data loss during power failures for up to 30 days by controller memory battery. An MEB draws 8 mA at 5 VDC. Velocity supports only 1 memory expansion board in an Mx Controller.

Table 8-1: Expansion Boards for the Mx Controller

Model #	Description	Comments
MEB/CB128	Memory Expansion Board - Code Expansion of 128,000 with Buffer Option	Expands Code Memory by approximately 128,000 (from 4,352 to 135,424) on Velocity. A portion of the Code Memory may be allocated to alarm and event Buffers, which will reduce the number of users. Protected from data loss during power failures for up to 30 days by controller memory battery. An MEB draws 8 mA at 5 VDC. Velocity supports only 1 memory expansion board in an Mx Controller.
SNIB	SCRAMBLE*NET Interface Board	Adds two optically isolated serial ports, one a multidrop RS-485 channel, the other a direct connect RS-232. Both can be active concurrently. When the RS-485 port is used for connection to other controllers, the RS-232 port can connect to a host PC locally or by modem. Velocity supports only 1 SNIB, SNIB2, or SNIB3 expansion board in an Mx Controller. The Mx Controller does not include an RS-232 port, so adding an original SNIB expansion board enables you to connect using a modem.
SNIB2	Secure Network Interface Board 2	Adds a 10/100 Ethernet (TCP/IP) port with an RJ45 connector, and two optically isolated serial ports, one a multidrop RS-485 channel, the other a direct connect RS-232. Uses the X*NET2 protocol, which supports AES (128 bit Rijndael) encryption between host PC and Master SNIB2, and between Master SNIB2 and downstream SNIB2. Master SNIB2 supports integral XBox functionality for globalization (no globalization between SNIB2 Masters). A SNIB2 draws 450 mA at 5 VDC during normal operation, and draws a maximum of 500 mA at 5 VDC when starting up. Velocity supports only 1 SNIB, SNIB2, or SNIB3 expansion board in an Mx Controller. Although the Mx Controller has integrated SNIB2 capability, it does not include an RS-232 port, so adding a SNIB2 expansion board enables you to connect using a modem, leased line module, or fibre optic converter.

Table 8-1: Expansion Boards for the Mx Controller (Continued)

Model #	Description	Comments
SNIB3	Secure Network Interface Board 3	Adds a 10/100/1000 Ethernet (TCP/IP) port with an RJ45 connector, and an optically isolated multidrop RS-485 serial port. Supports either IPv4 or IPv6 addressing. Can use either the X*NET2 protocol which supports 128-bit AES encryption (and a mixed network of SNIB2s and SNIB3s), or the X*NET3 protocol which supports 256-bit AES encryption (if every controller has a SNIB3). The SNIB3 is not compatible with the original SNIB, and cannot be used with the M1N controller (because it does not support any expansion boards). A SNIB3 draws 550 mA at 5 VDC during normal operation, and draws a maximum of 850 mA at 5 VDC when starting up. Velocity supports only 1 SNIB, SNIB2, or SNIB3 expansion board in an Mx Controller. If you want to use a SNIB3 expansion board, see “Preparing an Mx Controller to Use a SNIB3” on page 7-75.

Table 8-1: Expansion Boards for the Mx Controller (Continued)

Note: Although Velocity enables you to reconfigure an unused door so you can use its inputs and relay components for other purposes, the addition of alarm or relay expansion boards does not increase the supervised door capacity of an Mx Controller.

All expansion boards have the same dimensions and shipping weight:

Dimensions: 6”H x 4.25”W x 0.75”D (15.2cm x 10.8cm x 1.9cm)
Shipping Weight: 1 lb (0.5 kg)

The ribbon cable used to connect these boards to the Controller board is the EBIC5, which can link up to five expansion boards. For detailed information about the setup and installation of expansion boards, see “Expansion Board Installation” on page 7-31.

*Note: If you will be using the Ethernet connector to connect your Mx controller to a LAN/WAN so it can communicate with a computer running Velocity, **and** you plan to install multiple expansion boards, you should plug in the network cable before installing the expansion boards (while it is easier to access the Ethernet connector).*

Data Capacity of an Mx Controller

A DIGI*TRAC or Mx controller includes a base amount of memory which is dedicated to storing data about credentials, events, and alarms. (This memory enables a controller to continue performing its functions even when it is temporarily unable to communicate with the Velocity server.)

The data capacity of a controller can be increased by adding optional expansion boards. An expansion board can be configured so that its memory is dedicated either solely to additional credentials, or to a mixture of additional credentials, events, and alarms.

The following table shows the maximum data capacity of a controller in its base configuration and with various optional expansion boards configured either way.

Controller configuration	maximum Credentials	maximum Events	maximum Alarms
Base (no expansion boards)	4,352	1,560	1,560
With MEB/CB64 and 20% reduction Enabled	55,200	37,440	5,460
With MEB/CB64 and 20% reduction Disabled	69,888	1,560	1,560
With MEB/CB128 and 20% reduction Enabled	106,400	65,520	17,160
With MEB/CB128 and 20% reduction Disabled	135,424	1,560	1,560

Table 8-2: Data Capacity of an Mx Controller

Note that your system's actual capacity could be less, as explained in "Velocity Features that Reduce Available Memory" on page 2-24.

Replaceable Parts of the Mx Controller

The following table provides specifications for the replaceable parts of the different models of the Mx controller.

Part	Mx-2	Mx-4	Mx-8
Standby Battery	1.3 Ah 12V rechargeable sealed lead-acid; made by Prism, part# GH1213	7.2 Ah 12V rechargeable sealed lead-acid; made by Panasonic, part# LC-R127R2P (or LC-R127R2P1)	7.2 Ah 12V rechargeable sealed lead-acid; made by Panasonic, part# LC-R127R2P (or LC-R127R2P1)
Memory Battery	80 mAh 3.6V rechargeable nickel-metal hydride; made by House of Batteries, part# XVN-H80BC-L3C	80 mAh 3.6V rechargeable nickel-metal hydride; made by House of Batteries, part# XVN-H80BC-L3C	80 mAh 3.6V rechargeable nickel-metal hydride; made by House of Batteries, part# XVN-H80BC-L3C
Power Supply Input Fuse	5 A 250V 5 mm x 20 mm; made by Little Fuse Inc., part# 0218005.HXP	5 A 250V 5 mm x 20 mm; made by Little Fuse Inc., part# 0218005.HXP	5 A 250V 5 mm x 20 mm; made by Little Fuse Inc., part# 0218005.HXP

Table 8-3: Replaceable Parts for the Different Models of the Mx Controller

Design Considerations for the Mx Controller

This section documents the procedures for mounting, configuring, wiring, and powering an Mx Controller. Controllers are usually located in a safe and secure area, such as an electrical room, telephone equipment room, closet, or the security operations office. An environmentally managed room is not required as long as the temperature ranges don't exceed the Controller's specifications.

In addition to monitoring, reporting, and controlling a variety of devices, each controller can power a specific number of ScramblePads, MATCH2 interfaces, and attached readers. Other devices, such as interior motion sensors and some readers, may require power from a separate power supply.

Electrical Ratings

An Mx controller has the following electrical ratings:

- ❑ Input: 120 V, 1.25 A; Two batteries connected in series at 12 V DC, either 1.3 Ah provided with an Mx-2, or 7.2 Ah provided with an Mx-4 or Mx-8.
- ❑ Output: 5-pin MATCH terminal at 24 V DC - 28 V DC, 1 A; 6-pin Wiegand terminal at 12 V DC, 0.5 A.
- ❑ Door Relays (dry contact): 30 V DC, 5 A, 0.6 pF.

Mx Controller Design

Depending on its configuration, an Mx Controller provides for 2, 4, or 8 supervised doors: this includes 5Amp door relays with line module inputs. Each door is represented by a ScramblePad/MATCH terminal block, a Weigand terminal block, a relay terminal block, and an input terminal block (for connecting a line module). An Mx Controller can power ScramblePads and MATCH2 interfaces from the 5-pin MATCH terminal blocks, or it can power Weigand card readers from the 6-pin Weigand terminal blocks.

Starting with the Velocity 3.6 SP2.1 release and the CCM firmware 7.5.70.12 release, on an Mx-2 or Mx-4 controller where Wiegand terminals are available from unused doors, some of those available terminals can easily be used for exit readers. For details, see "Connecting Exit Readers to Unused Wiegand Terminals on Mx-2 or Mx-4 Controllers" on page 8-22.

An Mx Controller includes an integrated SNIB2 for direct connection via RS-485 to a SCRAMBLE*NET network, and an integrated Ethernet port for easy connection to a computer running Velocity. It also supports certain DIGI*TRAC expansion boards, as discussed in "Expansion Boards" on page 8-8.

Locate the controller near a dedicated AC power source. A 15Amp dedicated, unswitched circuit is required. If the power in the building is correctly grounded, there is no special grounding required for the controller. The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip.

Note: Do not install other equipment in the controller enclosure. Doing so may cause intermittent operation, product damage, and void the manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

Dimensions:	18"H x 15.25"W x 5.5"D (45.7cm x 38.7cm x 14cm)
Shipping Weight:	30 lbs (13.6 kg)

Separation of Circuits

As shown in the following figure, the Class 1 high-voltage AC input power for an Mx controller is routed through either one of the two knock-outs at the bottom of the enclosure, while the cables for the controller's Class 2 circuits (such as HI/LO inputs, MATCH reader terminals, and Wiegand reader terminals) are routed through several knock-outs located across the top and sides of the enclosure:

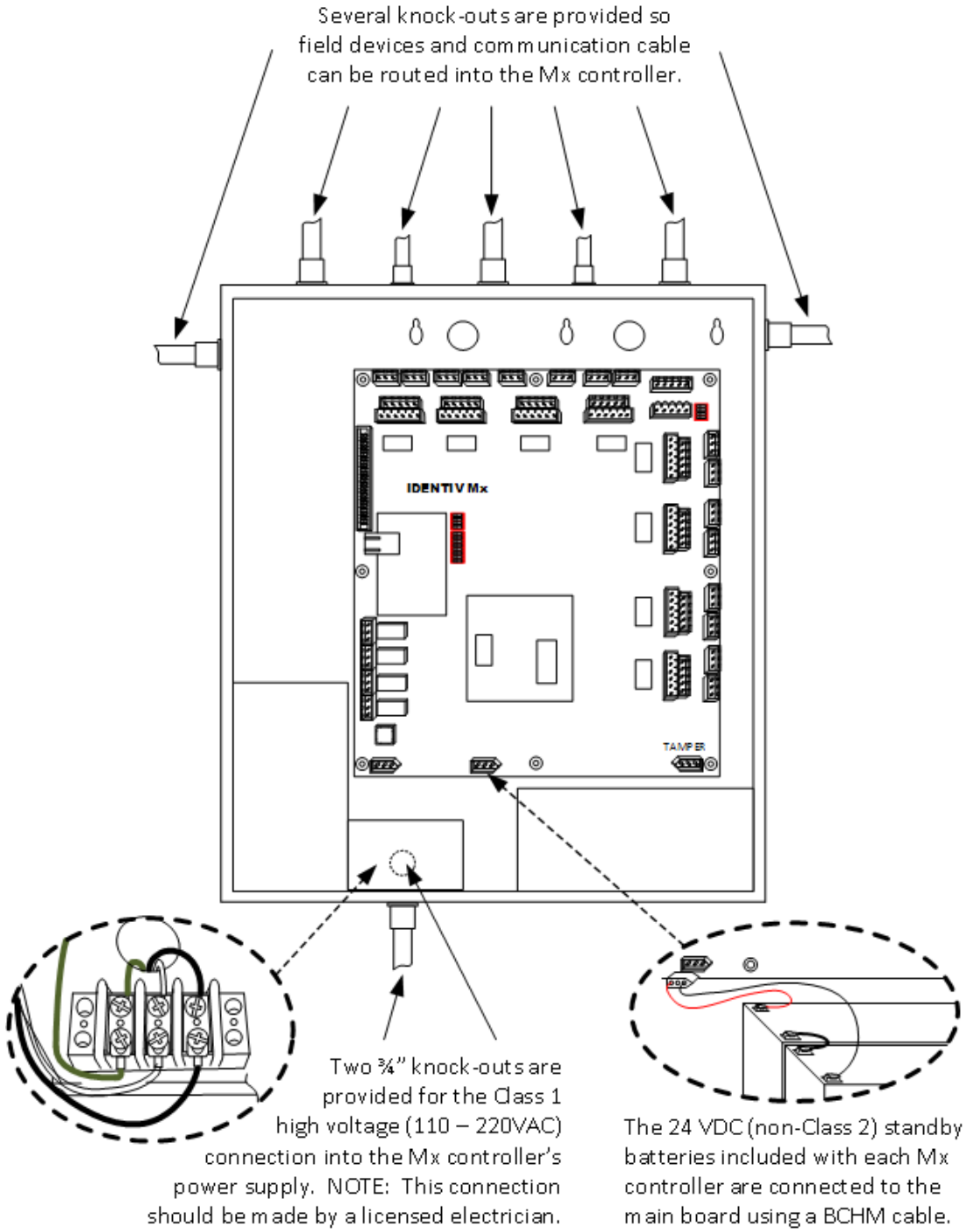


Figure 8-3: Cable Inlets of the Mx Controller's Enclosure

The Mx controller's Class 2 limited-power circuits include the following connections (as shown in Figure 8-2, "Mx Controller Main Board Connectors and Components", on page 8-6):

- ❑ 8 3-wire HI/LO analog input terminal blocks (for the line modules used to supervise doors, tamper circuits, and RQE devices).
- ❑ 8 5-wire MATCH terminal blocks (for connecting keypads or readers through the 28 VDC MATCH2 Reader Interface). These are *digital* circuits which support MATCH2 boards and DS47L series keypads.
- ❑ 8 6-wire Wiegand terminal blocks (for connecting the wiring from a 12VDC keypad or reader with a Wiegand interface). These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.
- ❑ The 5-wire SNIB2 RS485 terminal block (and its associated DIP switches) enables you to securely communicate with downstream controllers on a private network (which is managed by the same Velocity server).
- ❑ The Expansion Board Connector is used to link any expansion boards mounted in the controller's enclosure to the controller's main board (using a flexible EBIC5 ribbon cable).

All reader circuits are protected by resettable thermal fuses, which automatically restore circuit integrity after the overcurrent has been removed. When routing the wires for the Class 2 limited-power circuits, make sure that you maintain a safe separation of at least 0.25 inches from the wires for the AC input power and the standby battery pack.

A complete list of the Mx controller's Class 2 limited-power connectors is available in "ELECTRICAL SAFETY INFORMATION" which starts on page x.

Controller Battery Standby Capacity

The Mx-2 controller comes factory-equipped with a 24V 1.3 Ah battery. The Mx-4 and Mx-8 controllers come factory-equipped with a 24V 7.2 Ah battery, to comply with the standby power requirements of UL 1076 Section 40. Each battery kit consists of two 12-volt batteries connected in series for a full 24-volt standby unit.

If still more backup power is required, the provided internal standby battery can be replaced by larger-capacity external 24VDC batteries (up to a limit of 14 amp-hours), or by a charger and batteries (such as those made by AlarmSafe). A 120/240VAC UPS can also be tied into the main power, providing the controller with both surge protection and emergency power.

When using either external batteries or a charger and batteries, remember:

- ❑ When using an external battery pack, remove the controller's internal battery and connect the new power line into the unused standby battery input on the controller board. Remember: connecting two similar batteries in series doubles the voltage.
- ❑ When using a UPS, connect the UPS into the AC power line.

To determine how much backup battery power a particular controller requires, use this formula:

$$(I_{Devices} + I_{Controller}) \times \text{hours} = \text{Battery Life Required}$$

This is the sum of the load at 24VDC of all the attached devices plus the load at 24VDC of the controller itself, multiplied by the hours of battery operation required. Table 8-4 provides the extended standby battery requirements (current draw in amps) for the Mx

Controllers and typical DIGI*TRAC components, based on quiescent (idle) conditions:

Controller or Attached Device	Requirements @ 24VDC
Mx controller	0.53 A
DS47L (non-illuminated value)	0.04 A
DS47L-HI (non-illuminated value)	0.04 A
DS47L-SPX/DS47L-SPX-HI (non-illuminated value)	0.05 A
MATCH2 (readers powered separately)	0.07 A
MATCH2 (powering 1 or 2 readers)	0.20 A

*Table 8-4: Quiescent Current Draw for the Mx Controller and Various DIGI*TRAC Components*

For example, suppose an Mx controller is connected via MATCH2 Interfaces to four doors, each of which is using dual technology: 4 ScramblePads – 2 regular for interior and 2 high intensity for exterior – together with 4 CR11L mag stripe readers.

The installed example system's current draw is itemized:

1 Mx	x	0.53	= 0.53A
2 DS47L	x	0.04	= 0.08A
2 DS47L-HI	x	0.04	= 0.08A
4 MRIB	x	0.20	= 0.80A
Total			**= 1.49A**

A factory-installed 7.2 Ah battery pack (supplied with an Mx-4 or Mx-8 controller) could support this configuration for:

$$\frac{7.2 \text{ Amp-hours}}{1.49 \text{ A}} = \textbf{4.83} \text{ hours}$$

However, if you specify that the extended standby battery backup requirement must be at least 8 hours of operation without primary power:

1.49A x 8 hours = 11.92 Amp-hours

Obviously the included 7.2 Ah battery pack is not sufficient for this system. To operate this system without primary power for a full 8 hours, you will need to provide either an external battery or a front-end UPS, with at least a 12 Ah capacity.

Power Provided at the Terminal Blocks

An Mx Controller provides 12VDC power at the Wiegand terminal blocks, and 24VDC at the MATCH terminal blocks.

The following table shows the power provided for Wiegand and MATCH@ keypads/readers by an MX Controller.

Terminal Type	Max. Current Draw (Amps) per Controller	Max. Current Draw (Amps) per Channel
Wiegand	1.7	0.25
MATCH	2.9	1.0

Table 8-5: Maximum Current Draws for an Mx Controller's Terminals

ScramblePad/MATCH2 Power Requirements

Note: The following topic illustrates power calculations using ScramblePads and MATCH2 interfaces, because we know their power requirements. If you are using keypads/readers with a Wiegand interface (from another vendor), you can perform similar power calculations using the power requirements of your particular devices, and the information in the Wiegand row of Table 8-5.

To determine how many ScramblePads and MATCH2 interfaces an Mx controller can power, you must calculate the current draw of the ScramblePads and MATCH2 Interfaces and compare it to the maximum current draw available from the Mx controller (which is shown in the MATCH row of Table 8-5).

The controller powers ScramblePads and the MATCH2, then the MATCH2 powers one or two readers. The Mx controller has an integrated MATCH terminal and an integrated Wiegand terminal for each door, which can power the readers directly wired to those terminals.

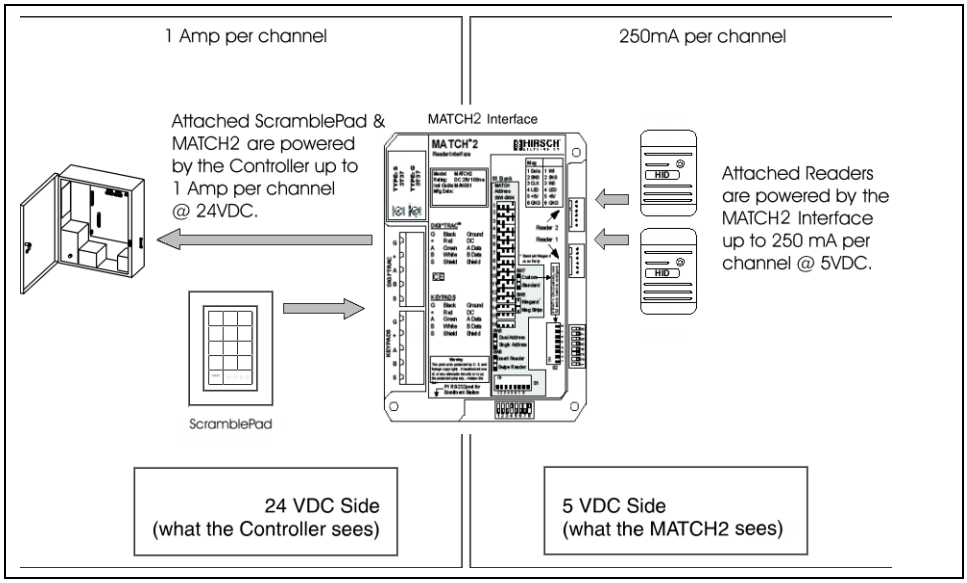


Figure 8-4: Current Draw Orientation for MATCH2 Interface

As shown in Figure 8-4, voltage from the Controller to the MATCH2 and ScramblePads is 24VDC, while voltage from the MATCH2 to its connected readers is 5VDC. (Although ScramblePads may be connected through the MATCH2 to the controller, the ScramblePads are powered by the controller, not the MATCH2.)

To determine how many ScramblePads and MATCH2 interfaces the controller can power, use the following procedure:

1. Determine what devices you will be using. For example, an Mx-4, DS47L ScrambleProx, an MRIB MATCH2 Interface, and MATCH-compatible readers.
2. Determine the quantity of each device you'll need. For example, 1 Mx-4, 1 DS47L-SPX and 1 DS47L-SPX-HI ScrambleProx, 1 MRIB, and 2 CR31L readers.
3. Determine whether the MATCH2 Interface will be able to power the connected readers. Make sure the readers' 5VDC draw does not exceed the MATCH2's 250mA at 5VDC limit. If the MATCH2 powers readers, it draws more current from the controller than if the readers were separately powered.
4. To determine the current draw of each attached device on the controller at 24VDC, multiply the number of devices by the current draw for each device, then add the total for each device to calculate the Total Current Draw required from the controller, using the values shown in Table 8-6:

Device	**Draw per Device (Amps) @ 24VDC**
DS47L ScramblePad (illuminated value)	0.125
DS47L-SPX ScrambleProx (illuminated value)	0.135
DS47L-SPX-HI ScrambleProx (illuminated value)	0.25
MATCH2 Interface (powering 1 or 2 readers)	0.20
MATCH2 Interface (readers powered separately)	0.07

Table 8-6: ScramblePad/MATCH2 Current Draw

Note: Do not include the reader's 5VDC current draw in the calculation.

As shown in Table 8-6, it doesn't matter to the controller whether a MATCH2 is powering one or two readers, because the MATCH2 is using a switching power supply. The MATCH2 can provide up to 250 mA @ 5VDC to each of two readers and present a load to the controller of only 200 mA @ 24VDC. If readers attached to a MATCH2 are self-powered, the MATCH2 presents a load to the controller of only 70 mA.

For this example, given both entry and exit dual technology – 1 DS47L-SPX-HI ScrambleProx and 1 CR31L Wiegand Swipe Reader on the entry side, and a DS47L-SPX ScrambleProx and 1 CR31L on the exit side – tied into a MATCH2 interface, the following calculations would result:

1 DS47L-SPX x 0.135A	=	0.135A
1 D437L-SPX-HI x 0.25A	=	0.250A
1 MRIB x 0.20A	=	0.200A
Total Current Draw	=	**0.535A**

5. Determine whether an Mx controller can power the ScramblePads/MATCH2s connected to it, by comparing the Total Current Draw required against the maximum current draw available from the controller (which is shown in the MATCH row of Table 8-5 on page 8-17).
6. Verify that current from any one ScramblePad/MATCH terminal block does not exceed 1.0 Amp.

The preceding total of 0.535A is well within an Mx Controller's 1.0A per channel limit and 2.9A total capacity limit. If the total current draw required exceeds an Mx controller's limits, use a remote power supply for one or more of the attached devices.

Typical Connections

Like DIGI*TRAC Controllers, the Mx controller can connect to a number of input and output devices. For details, see the following topics:

- ❑ "Typical Line Module Inputs" on page 2-12
- ❑ "Typical Door Relay Outputs" on page 2-13
- ❑ "ScramblePad/MATCH Inputs" on page 2-15

When referring to those topics, note that the layout of the terminal blocks of an Mx Controller (as shown in Figure 8-2 on page 8-6) is different from the layout of the terminal blocks of the DIGI*TRAC M2 or M8 Controller.

All interconnecting devices must be UL Listed, low-voltage Class 2 power limited.

Wiring for a Door

For each door, an Mx controller provides the following terminal blocks:

- ❑ A 3-pin Door Input terminal for analog inputs such as multi-state alarm inputs from the line modules.
- ❑ A 3-pin Door Relay terminal for two-state outputs such as magnetic locks and electric strikes.
- ❑ A 5-pin MATCH terminal for connecting ScramblePad keypads or readers through the MATCH2 Reader Interface. These are *digital* circuits which support daisy-chain connections to multiple devices on the same circuit.
- ❑ A 6-pin Wiegand terminal for directly connecting a reader or keypad which has a Wiegand interface.

Previously for each door, you had to use either the 5-pin MATCH terminal or the 6-pin Wiegand terminal, depending on your needs:

- ❑ For basic access control applications that only need an entry reader on a door, you could use the 6-pin Wiegand terminal to directly connect the Mx controller to a reader or keypad which has a Wiegand interface (without a separate MATCH2 board).
- ❑ For a more advanced access control application that needs both entry and exit readers on a door, you had to use the 5-pin MATCH terminal to connect the Mx controller to a MATCH2 interface board or ScramblePad reader.

Starting with the Velocity 3.6 SP2.1 release and the CCM firmware 7.5.70.12 release, on an Mx-2 or Mx-4 controller where Wiegand terminals are available from unused doors, some of those available terminals can easily be used for exit readers. For more information about this feature, see “Connecting Exit Readers to Unused Wiegand Terminals on Mx-2 or Mx-4 Controllers” on page 8-22. (For wire runs longer than 500 feet, you still must use the MATCH2 interface.)

CAUTION: To avoid possible damage to your Mx controller, make sure it is powered off before you add or remove a reader connected to a 6-pin Wiegand terminal.

The following diagram shows the logic of the typical wiring for a door supervised by an Mx controller, with a card reader wired to a MATCH2 board which is wired to the 5-pin MATCH terminal for a door.

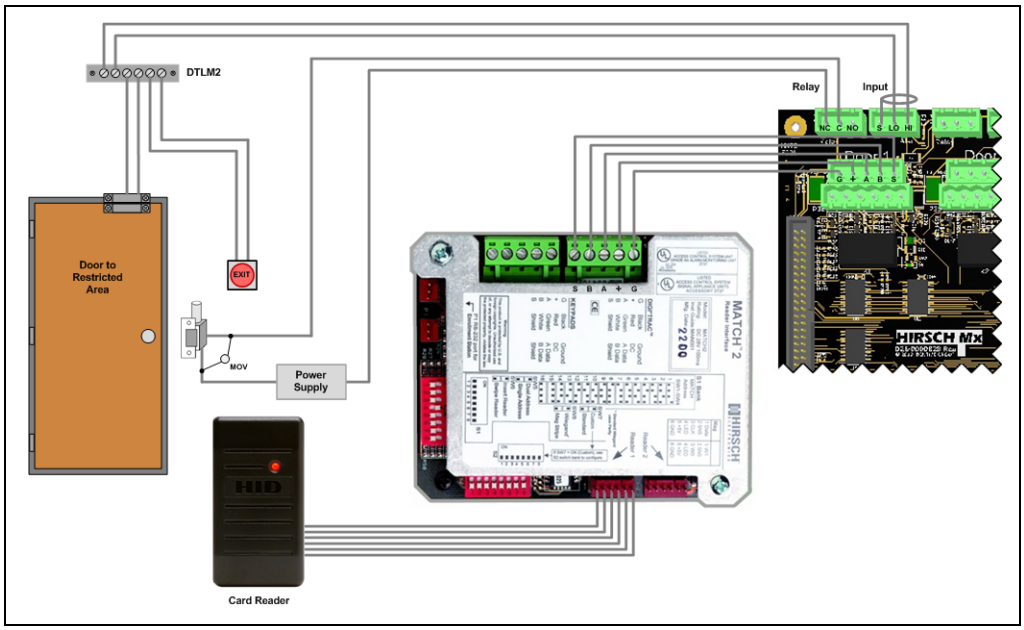


Figure 8-5: Typical Door Wiring Example for an Mx Controller

For information about setting up and installing Wiegand readers using a MATCH board, see “Wiegand Readers” on page 7-196.

If you are using a reader or keypad which has a Wiegand interface, you can use the 6-pin Wiegand terminal block instead of the 5-pin MATCH terminal block, as shown in the following diagram.

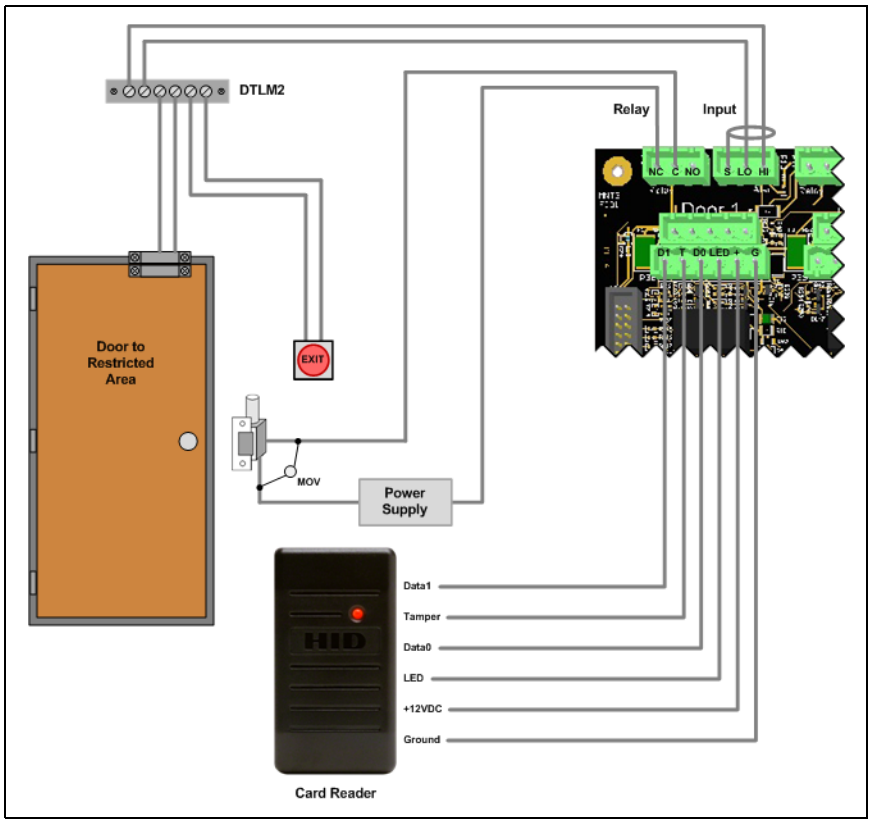


Figure 8-6: Wiegand Door Wiring Example for an Mx Controller

NOTE: Always refer to the actual wiring diagram provided with the specific reader that you are installing.

Connecting Exit Readers to Unused Wiegand Terminals on Mx-2 or Mx-4 Controllers

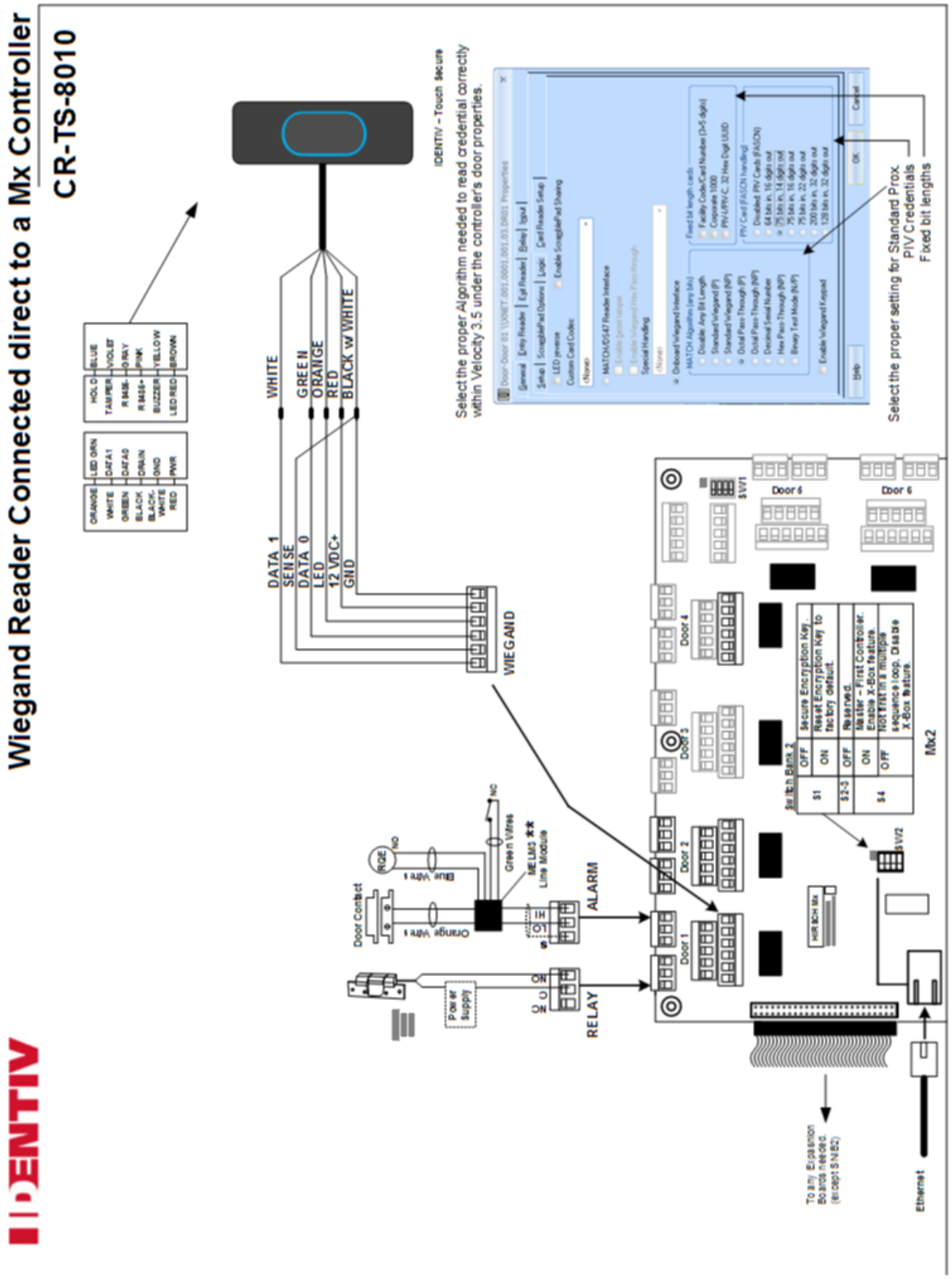
The Mx controller provides only one Wiegand terminal per door. Before the Velocity 3.6 SP2.1 release and the CCM firmware 7.5.70.12 release, if you wanted to have a door with a Wiegand exit reader, you had to connect that reader through a MATCH board. Now on an Mx-2 or Mx-4 controller where Wiegand terminals are available from unused doors, some of those available terminals can easily be used for exit readers. The following table shows the mapping of the 8 Wiegand terminals for the Mx-8, Mx-4, and Mx-2 models.

Terminal	Usage on Mx-8	Usage on Mx-4	Usage on Mx-2
Wiegand 1	Entry reader for Door 1	Entry reader for Door 1	Entry reader for Door 1
Wiegand 2	Entry reader for Door 2	Entry reader for Door 2	Entry reader for Door 2
Wiegand 3	Entry reader for Door 3	Entry reader for Door 3	(unavailable)
Wiegand 4	Entry reader for Door 4	Entry reader for Door 4	(unavailable)
Wiegand 5	Entry reader for Door 5	Exit reader for Door 1	Exit reader for Door 1
Wiegand 6	Entry reader for Door 6	Exit reader for Door 2	Exit reader for Door 2
Wiegand 7	Entry reader for Door 7	Exit reader for Door 3	(unavailable)
Wiegand 8	Entry reader for Door 8	Exit reader for Door 4	(unavailable)

NOTE: On an Mx-8 controller, the Wiegand terminals are all dedicated to entry readers. So when you use this feature to add Wiegand exit readers on an Mx-2 or Mx-4 controller, if you later decide to upgrade that controller to an Mx-8 model, you will need to rewire each Wiegand exit reader to use a MATCH board.

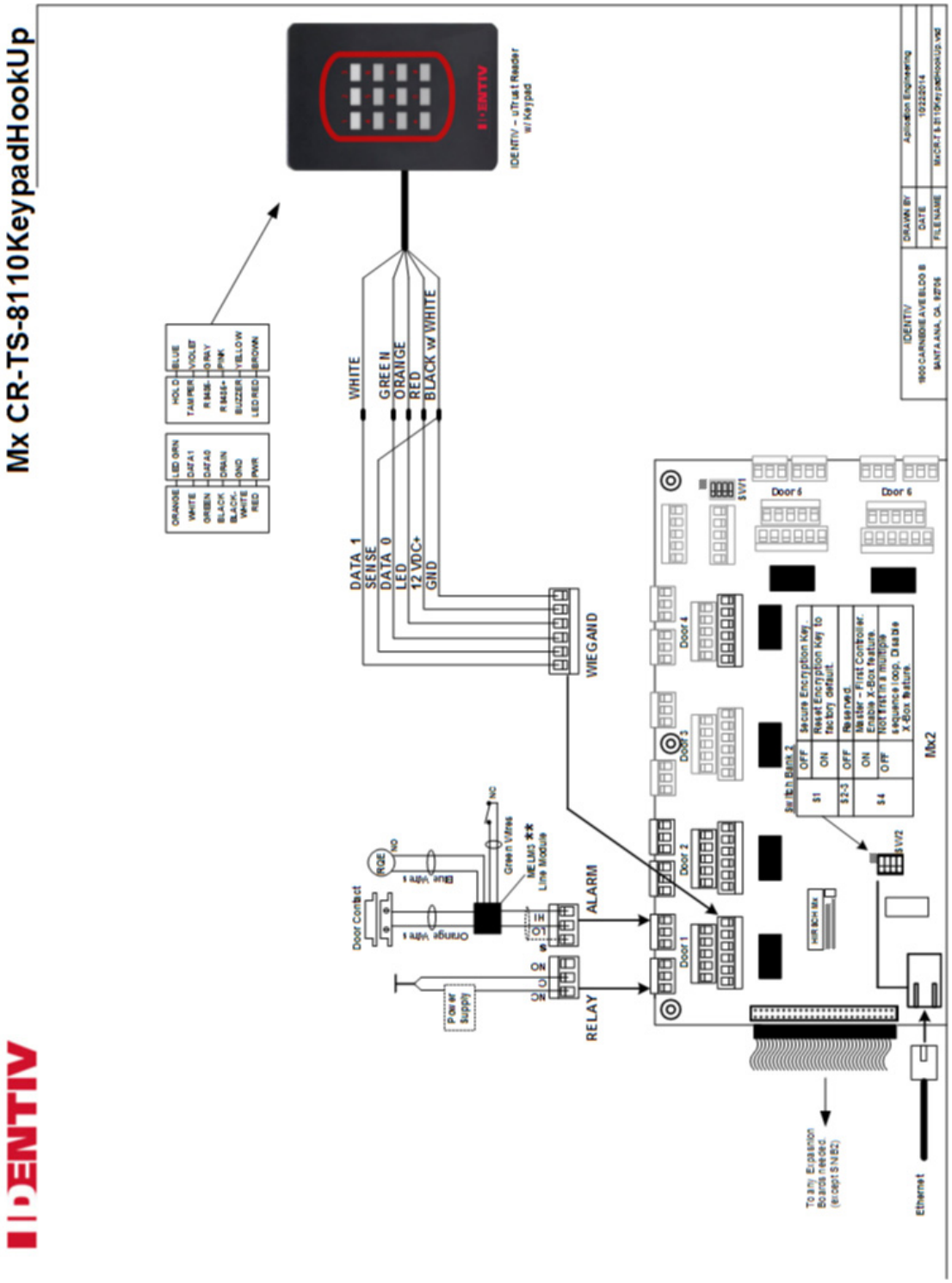
Wiring Diagram for the TS-8010 Reader

The following wiring diagram shows how to connect a TS-8010 reader to a Wiegand terminal on the main board of an Mx controller. It includes the connections for an electric lock and a door contact.



Wiring Diagram for the TS-8110 Reader

The following wiring diagram shows how to connect a TS-8110 reader to a Wiegand terminal on the main board of an Mx controller. It includes the connections for an electric lock and a door contact.



Setup and Installation of an Mx Controller

An Mx controller can be operated in ambient temperatures of 0 degrees Centigrade to 49 degrees Centigrade, with a maximum relative humidity of 93%. It must be installed indoors, within the protected premises.

Overall, the setup and installation of an Mx Controller is similar to that of most DIGI*TRAC Controllers. For example, all the information in "General Connection Rules and Procedures" starting on page 7-10 still applies, except that you don't have to worry about blocking the printer port (because an Mx Controller doesn't have one).

Most of the information in "Controller Installation" starting on page 7-17 also still applies, with the following differences:

- In "Controller Set Up" on page 7-17, note that an Mx Controller has integrated SNIB2 capability which must be configured using DIP switches. For information about setting those DIP switches, refer to "Configuring the Integrated SNIB2" on page 8-26.
- In "Mounting the Controller" on page 7-17, note that an Mx Controller has the same enclosure as an M2 DIGI*TRAC Controller.
- In "Wiring to the Controller" on page 7-18, note that an Mx Controller's status LEDs are much smaller and are located in the center of the main board. Also, refer to Figure 8-2 on page 8-6.

Wiring Distance Limits

The following table shows the wiring distance limits between the Mx Controller and various components, which is important information when you are designing a security system for a large facility.

Type of Wired Connection	Maximum Distance
RS-485 (between two controllers) using 22 gauge wires	4,000 feet (1,220 meters)
MATCH protocol (between controller and keypad, reader, or MATCH2 board) using 18 gauge wires	1,800 feet (550 meters)
MATCH protocol (between controller and keypad, reader, or MATCH2 board) using 22 gauge wires	750 feet (225 meters)
Wiegand protocol (direct wiring between controller and Wiegand device) using 18 gauge wires	500 feet (150 meters)

Table 8-7: Wiring Distance Limits Between the Mx Controller and Various Components

Note that the wires must be stranded and pair twisted, with an overall shield.

Configuring the Integrated SNIB2

An Mx Controller has integrated SNIB2 capability, with a 5-wire RS-485 connector that enables multi-drop or long hardwired serial connections, and an RJ-45 Ethernet connector for communication between the Velocity host and the master controller. For information about SNIB2 functionality (including multiple-controller configurations), see "SNIB2" on page 2-35.

Note: An Mx Controller does not include the 4-wire RS-232 connector which is provided on the separate SNIB2 expansion board.

To install a set of controllers connected using SNIB2s, perform the following procedure:

1. Run the required network cable to the controller(s) with the master SNIB2s.

   The Ethernet cable you are connecting to each master SNIB2 should be connected to the Velocity host through a hub or switch.

2. Run RS-485 cable downstream from the master SNIB2.

   The run between the master SNIB2 and the second SNIB2 must be wired according to the instructions in "Configuring a Master SNIB2 on the Same Subnet" on page 7-61.

3. Set the DIP switches on each SNIB2, which vary depending on whether it is the master, one in the middle, or the last one.

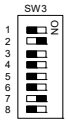
   The location of the three banks of DIP switches on a SNIB2 expansion board is shown in Figure 2-24 on page 2-35.

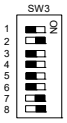
   On an Mx Controller's main board (shown in Figure 8-2 on page 8-6):

   - SW1 is located near the upper-right corner, by the SNIB2 terminal.
   - SW2 is located in the left middle, to the right of the Ethernet daughterboard.
   - SW3 is located below SW2.

   In general, set the DIP switches as shown in the following table.

Bank	Switch	Setting	Comments
Master SNIB2:			
SW1	S1-S4	all ON	Indicates this is the first/master SNIB2 (or the last one) in the run
SW2	S1	OFF	The SNIB2 communicates with the Velocity host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. Because this is the master SNIB2, you must also 'Reset Encryption' on the Velocity Port settings. All downstream units must have their encryption keys reset as well.
	S2-S3	OFF	Reserved
	S4	ON	This SNIB2 is first in the sequence (the master) and is connected to the host via Ethernet or direct RS-232 connection (not dial-up). This SNIB2 controls polling.
SW3	S1 S2	OFF ON	Set downstream RS-485 speed (38400 in this example)
	S3-S8	—	Address as required (Address 1 shown)

Bank	Switch	Setting	Comments
SNIB2s in the middle:			
SW1 	S1-S4	all OFF	Indicates this SNIB2 is in the middle of the run
SW2 	S1	OFF	The SNIB2 communicates with the Velocity host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. All downstream units must have their encryption keys reset as well. Because this is a downstream unit, the master SNIB2 automatically detects that the keys have been reset.
	S2-S3	OFF	Reserved
	S4	OFF	This SNIB2 is not the first/master (or you only have one controller)
SW3 	S1 S2	OFF ON	Set downstream RS-485 speed (38400 in this example)
	S3-S8	—	Address as required (Address 2 shown)

Bank	Switch	Setting	Comments
Last SNIB2 in run:			
 SW1	S1-S4	all ON	Indicates this is the last SNIB2 (or the first/master) in the run
 SW2	S1	OFF	The SNIB2 communicates with the Velocity host PC in XNET 2, using the encryption keys stored in memory
		ON	Return the encryption keys to their default settings. If this switch is set when the SNIB2 powers up or reboots after a firmware upgrade, the keys reset. This switch should be turned off after the LED patterns begin to light. All downstream units must have their encryption keys reset as well. Because this is a downstream unit, the master SNIB2 automatically detects that the keys have been reset.
	S2-S3	OFF	Reserved
	S4	OFF	This SNIB2 is not the first/master (or you only have one controller)
 SW3	S1 S2	OFF ON	Set downstream RS-485 speed (38400 in this example)
	S3-S8	—	Address as required (Address 3 shown)

Refer to “Setting Up the SNIB2” on page 7-54 for more configuration options.

4. Plug the RJ-45 connector from the cable into the Ethernet connector on the Mx Controller’s main board.
5. Connect the RS-485 cables to their respective SNIB2.
6. Reconnect and power up the controllers.
7. At the host, open Velocity and configure the new SNIB2s.

   For more about this, refer to the “DIGI*TRAC Hardware Configuration > Secure Network Interface Boards (SNIB2) > SNIB2 - Configuring” topic in the Velocity online help system.

SNIB2 Network Configuration Options

Most DIGI*TRAC controllers can be networked together and managed by a computer running Velocity, if they use an optional SNIB2 expansion board. For details, see "SNIB2 Network Configuration Options" starting on page 7-58.

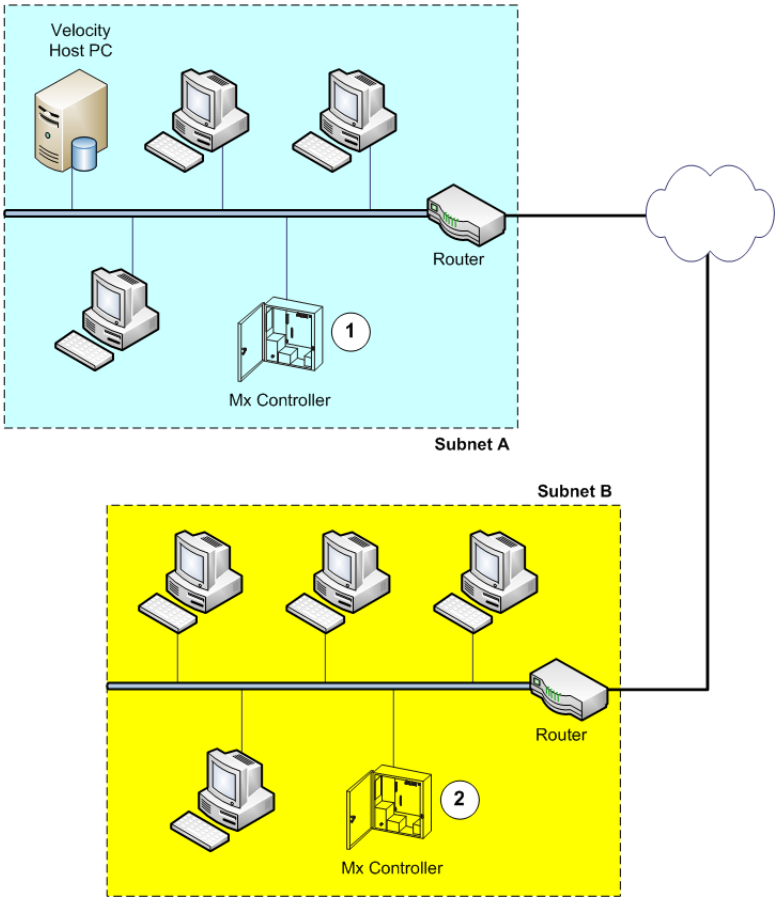
An Mx controller can be included in that network. The primary difference is that an Mx controller does not require a SNIB2 expansion board, because the Ethernet connector and the RS485 terminal are integrated onto the controller's main board, as shown in Figure 8-2 on page 8-6.

Deploying the SNIB2

Each master SNIB2 (Velocity port) must be assigned a unique IP address so it can communicate with Velocity on the host PC. Depending on the network location of the master SNIB2, this is accomplished in one of two ways:

- ❑ If the SNIB2 is located within the same subnet as the host PC, then you can use Velocity to assign the IP address. For more about this, refer to "Configuring a Master SNIB2 on the Same Subnet" on page 7-61.
- ❑ If the master SNIB2 is located outside the host PC's subnet, you must use the SNIB2 Configuration Utility. For more about this, refer to "Configuring a Master SNIB2 in a Different Subnet" on page 7-64.

What is a subnet? Put simply, it is any group of PCs and other devices, such as printers and scanners, connected by network cable to a network router. Anything behind the router is considered part of the subnet. Anything beyond this router is not part of the subnet.



In the preceding illustration, the master SNIB2 on the Mx controller labeled 1 is located in the same subnet as the host PC (Subnet A). This SNIB2 can therefore be configured using Velocity; however, the master SNIB2 on the Mx controller labeled 2 is located behind a different router, in a different subnet (Subnet B), and must be configured using the SNIB2 Configuration Utility.

Any number of computers and devices can be behind a single router, but for reasons of security and speed, a company network often incorporates many routers. It isn't uncommon to find that each department within a company has its own router. Routers not only find the quickest way to ferry packets of information between two points, but also could serve as a rudimentary firewall against potential intrusion.

Mx Controller Configuration Worksheet

The following figure provides a worksheet for an Mx Controller, to help you plan your security system. (The worksheet for the Mx-1 controller is provided in Figure 9-8 on page 9-48. Worksheets for other system components are provided in Appendix A.)

Velocity

IDENTIV

Mx Controller Configuration Worksheet

Controller Name: _____

Description: _____

Address: _____

Time Zone Location: _____

Port Type: ☐ S*NET ☐ X*NET

Port Name: _____

Expansion Boards

Board 1 =	
Board 2 =	
Board 3 =	
Board 4 =	
Board 5 =	

Doors / Readers / Outputs / Inputs

Door 1	1	9	
Door 2	2	10	
Door 3	3	11	
Door 4	4	12	
Door 5	5	13	
Door 6	6	14	
Door 7	7	15	
Door 8	8	16	

Expansion Inputs (Red Icons = Installed; Black Icons = not installed)

X11 -	X6 -	X111 -	X116 -	X21 -	X26 -	X31 -	
X12 -	X7 -	X112 -	X117 -	X22 -	X27 -	X32 -	
X13 -	X8 -	X113 -	X118 -	X23 -	X28 -	-	
X14 -	X9 -	X114 -	X119 -	X24 -	X29 -		
X15 -	X10 -	X115 -	X120 -	X25 -	X30 -		

Network Info:

☐ TCP/IP

IP Address: _____

IP Port: _____

Max Retry Attempts: _____

Expansion Relays\Virtual Relays (Red Icons = Installed; Black Icons = not installed)

XR1 -	XR12 -	XR23 -	XR34 -	XR45 -	XR56 -		
XR2 -	XR13 -	XR24 -	XR35 -	XR46 -	XR56 -		
XR3 -	XR14 -	XR25 -	XR36 -	XR47 -	XR57 -		
XR4 -	XR15 -	XR26 -	XR37 -	XR48 -	XR58 -		
XR5 -	XR16 -	XR27 -	XR38 -	XR49 -	XR59 -		
XR6 -	XR17 -	XR28 -	XR39 -	XR50 -	XR60 -		
XR7 -	XR18 -	XR29 -	XR40 -	XR51 -	XR61 -		
XR8 -	XR19 -	XR30 -	XR41 -	XR52 -	XR62 -		
XR9 -	XR20 -	XR31 -	XR42 -	XR53 -	XR63 -		
XR10 -	XR21 -	XR32 -	XR43 -	XR54 -	XR64 -		
XR11 -	XR22 -	XR33 -	XR44 -				

To Configure an Mx Controller:
From Velocity Configuration: Select DIGI*TRAC Configuration folder > Click Port > From Components pane, double-click Add New Controller. Fill out General page.

Figure 8-7: Mx Controller Worksheet

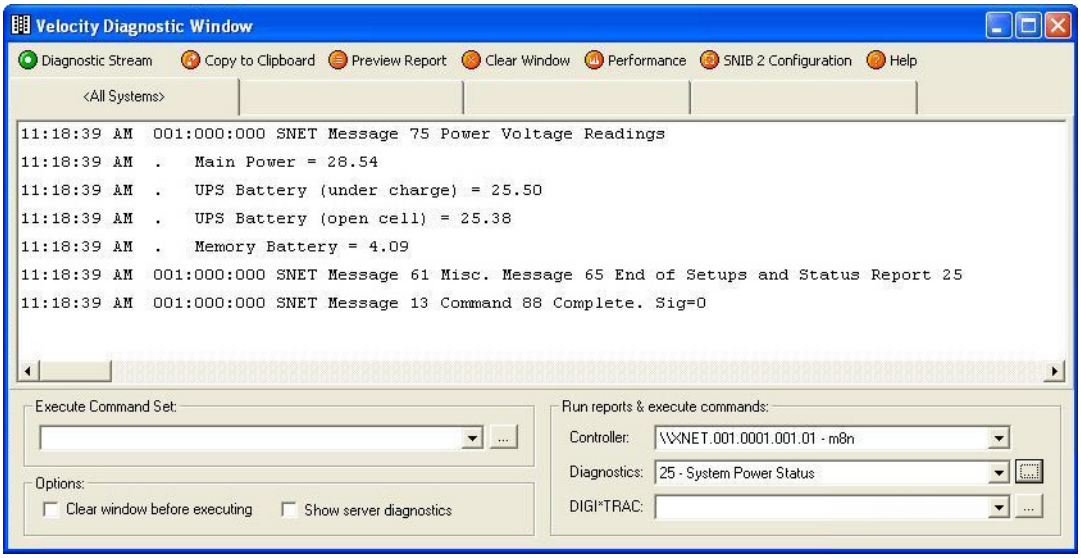
Performing Periodic Maintenance

The Mx controller was designed to be a reliable long-lasting product, with periodic maintenance consisting of:

- ❑ gathering diagnostic information (including the voltage status of the standby battery and the memory battery) once every 6 months
- ❑ visually inspecting the controller once every year for signs of:
  - corrosion around the battery terminals
  - damaged battery leads
  - exposed wires or loose connections
- ❑ replacing the standby battery or the memory battery when necessary (after several years)

Gathering Diagnostic Information

The Velocity software includes a Diagnostic Window which enables you to gather diagnostic information about a connected controller. To access this tool, click Velocity's menu button, and then select **Diagnostics/Reporting > DIGI*TRAC Diagnostic Window**.



To gather information about a controller:

1. Select the desired controller from the **Controller** drop-down list.
2. Select the appropriate diagnostic command from the **Diagnostics** drop-down list.

   This list includes all the basic 88 command options, such as 25 - System Power Status (of the AC input power, the standby battery, and the memory battery). For more information, see "CMD 88: PRINT SYSTEM SETUPS AND STATUS" starting on page 4-110.
3. Click the button located just to the right of the **Diagnostics** drop-down list.

The information generated by the selected command is displayed in the Results pane. To learn more about Velocity's Diagnostic Window, see the topics in the Diagnostic Window section of Velocity's help system.

Interpreting the System Power Status Information

The results of the 25 - System Power Status diagnostics command are somewhat cryptic. Here is what those results mean.

Main Power: This is the voltage of the main power after it has been transformed from AC to DC. The normal range is 28 - 29 VDC. AC Failure is reported if the voltage drops below 27.5 VDC.

UPS Battery: This is the DC voltage of the standby battery, which performs the function of an Uninterruptible Power Supply. The "under charge" number shows the voltage when the standby battery is being charged. The "open cell" number shows the voltage when the charging circuit is bypassed. The normal range is 24 - 28 VDC. The voltage is considered Low when it is 17 - 24 VDC. UPS Failure is reported if the voltage drops below 17 VDC. A weak battery will have a high "under charge" number and a low "open cell" number.

Memory Battery: This is the DC voltage of the memory protection battery, which provides up to 30 days protection of the controller's data. The normal range is 3.47 - 4.5 VDC. If the value remains below 3.47 VDC, the memory battery should be replaced.

Replacing the Memory Battery

The Mx controller's memory battery is a 3.6 V rechargeable nickel-metal hydride battery pack which can protect against data loss for up to 30 days. It should provide several years of reliable service, but will eventually have to be replaced when its voltage remains below 3.47 VDC. The location of this battery on the Mx controller's main board (within the enclosure) is shown in the following photograph:

When diagnostic information determines that there is a problem with the performance of the memory battery, you should replace it by performing the following procedure:

1. Contact Identiv (or your dealer) and order part number MPB1.
2. After the new memory battery arrives, take it and a small wire cutter to the Mx controller.
3. Open the Mx controller's enclosure, and locate the existing memory battery (as shown in the previous photograph).

   NOTE: The controller's power should remain on while you replace its memory battery.
4. Carefully unplug the memory battery connector from the controller's main board at location BAT1 (as shown in the following photograph).

5. Use a small wire cutter to cut through the existing cable tie (shown in the following photograph), and remove it.

6. Replace the old memory battery with the new one, and plug in its connector at location BAT1 on the controller's main board. Make sure the connector is aligned so that the red positive wire is on the left side.
7. Use a new cable tie to secure the new memory battery and its connecting wires to the plastic mount on the controller's main board.
8. Close the Mx controller's enclosure.

If the Mx controller is online and communicating with the Velocity software during this procedure, the Alarm Viewer will display a "Memory Battery Failure" alarm when the old memory battery is unplugged, and a "Memory Battery Restored" event when the new memory battery is plugged in.

If the Mx controller lost data because you replaced the memory battery while the main board was disconnected from both the main AC power and the standby battery power, you can easily download its data again using Velocity. In the Administration pane of Velocity's main window, locate the controller in the system tree, right-click on the controller, and select each of the following commands from the pop-up menu:

- ❑ **Download > Date/Time**
- ❑ **Download > Configuration**
- ❑ **Download > Credentials**

After these three downloads have completed successfully, the Mx controller is ready to use again.

Mx-1 Controller

9

This Page Intentionally Left Blank

Introduction

This chapter provides information about the Hirsch Mx-1 controller, including:

- ❑ Features of the Mx-1 controller
- ❑ A summary of the different Mx-1 controller configurations
- ❑ An overview of the Mx-1 controller's main components and connectors
- ❑ Design considerations, including battery capacity and power limitations
- ❑ Typical connections, such as the wiring for a door
- ❑ Setup and installation, including wiring distance limits, and configuration of the built-in SNIB3 capability and the integrated PoE+ Ethernet port
- ❑ A configuration worksheet for an Mx-1 controller, to help you plan its installation as part of your security system. (Worksheets for other system components are provided in Appendix A.)
- ❑ Performing periodic maintenance

Sometimes when a characteristic of the Mx-1 controller is essentially identical to that of a DIGI*TRAC controller, a cross-reference is provided to an existing topic in this guide.

NOTE: Revision 1 of the Mx-1 controller has the model number of "Mx-1 026-0000121-P", and is described in Chapter 9 of a previous version (Revision AH dated April 17, 2018) of this document. Revision 2 of the Mx-1 controller has the model number of "Mx-1 026-0000121-P-**2**", and is described in Chapter 9 of this version of this document. (The primary product change is a different set of Wet or Dry Mode jumpers for the power to the Door Relay and Aux Relay terminals, which are explained in Table 9-2.)

Features of the Mx-1 Controller

The Mx-1 controller has the following features.

- ❑ It manages one door (with an entry reader and an optional exit reader), and enables you to replace older models of DIGI*TRAC controllers (such as the M1N).
- ❑ Its built-in base memory can support up to 4,000 user credentials (depending on which features you are using; see "Velocity Features that Reduce Available Memory" on page 2-24).
- ❑ It is designed to operate in a networked environment, so it has an integrated Ethernet connection, and the functionality of the SNIB3 is built into the main board (instead of requiring an expansion board).
- ❑ Like previous Hirsch controllers, it also provides an RS-485 terminal so you can wire together a "chain" of controllers. (This feature was not evaluated by UL.)
- ❑ The functionality of the Command and Control Module (CCM) is built into the main board (instead of being on a separate removable module).
- ❑ It is packaged in a smaller plastic case, can receive its power as 24 V - 28 V DC from an external power supply (via the Power terminal) or as a nominal 25.5 Watts from POE+ (via the Ethernet jack), and can be installed either "at the edge" or stacked.
- ❑ Like previous Hirsch controllers, it is also available in a traditional metal enclosure with an AC power supply and a standby battery pack (Mx-1-ME), which has room for optional expansion boards.

- ❑ It does *not* support the traditional Hirsch MATCH interface, but it does support both an entry reader and an exit reader which can be wired using either the 8-pin Wiegand terminals or the 5-pin RS-485/OSDP terminal (where the optional exit reader is wired "through" the entry reader).

  NOTE: The door's entry reader and optional exit reader can use different protocols. (This feature was not evaluated by UL.)

- ❑ It includes special circuitry that helps protect the reader terminals and the relay terminals from excessive current draws.

The following table shows the features of the Mx-1 controller and some other currently available Hirsch controllers.

Table 9-1: Feature Comparison of the Mx-1 Controller to Other Hirsch Controllers

Feature	Mx-1	Mx2, Mx4, or Mx8	M2	M8
Doors, Inputs, and Relays				
Door Relays (supervised)[1]	1	2, 4, or 8	2	8
Door Relays (unsupervised)[1]	0	2, 4, or 8	2	0
Expansion Relays (base)[2]	0	0	0	0
Expansion Relays (max.)[3]	32	32	32	32
Line Module Inputs (base)[2]	2	2, 4, or 8	2	8
General Purpose Line Module Inputs (max.)[3]	32	32	32	32
Door or General Purpose Line Module Inputs (max.)[3]	34	40	34	40
Alarm/Aux. Relays (base)[2]	1	4	1	4
Reader Terminals (MATCH, Wiegand, or OSDP)				
5-pin MATCH Terminals[4]	0	2, 4, or 8	2	8
Wiegand Terminals	2 (8-pin)	2, 4, or 8 (6-pin)	0	0
RS485 OSDP Terminal[5]	1 (5-pin)	0 onboard; 8 (4-pin) on optional RREB	0 onboard; 8 (4-pin) on optional RREB	0 onboard; 8 (4-pin) on optional RREB
Expansion Boards (max.)[3]	0 standard in Mx-1 (plastic case); 5 in Mx-1-ME (metal enclosure)	5	5	5
User Credentials (base)[4]	4,000	4,000	4,000	4,000
User Credentials (max.)[3]	132,000	132,000	132,000	132,000

Table 9-1: Feature Comparison of the Mx-1 Controller to Other Hirsch Controllers (Continued)

Feature	Mx-1	Mx2, Mx4, or Mx8	M2	M8
Metal Enclosure				
Enclosure Height	14.25 inches 36.2 cm	15.25 inches 38.7 cm	15.25 inches 38.7 cm	20 inches 50.8 cm
Enclosure Width	14.25 inches 36.2 cm	18 inches 45.7 cm	18 inches 45.7 cm	22 inches 55.8 cm
Enclosure Depth	5.63 inches 14.3 cm	5.5 inches 14.0 cm	5.5 inches 14.0 cm	6 inches 15.2 cm
Shipping Weight	28 pounds 12.7 kilograms	30 pounds 13.6 kilograms	30 pounds 13.6 kilograms	60 pounds 27.2 kilograms
Plastic Enclosure (for the Mx-1 only; see above for the Mx-1-ME's Metal Enclosure)				
Plastic Enclosure (for Mx-1 only): Height by Width by Depth	1.25 x 8.0 x 8.0 in 3.18 x 20.3 x 20.3 cm	(not applicable)		
Mx-1 in Plastic Enclosure: Weight	1.5 pounds 0.69 kilograms			

Explanatory Notes for this table:

[1] Unused 'Door' relays may be reconfigured to serve as 'Control' relays.

[2] The term 'base' refers to how many of an item are included within a type of controller.

[3] The term 'max.' refers to the sum of what is included within the base model plus what is available in the relevant expansion boards. (The Mx-1 does not support any expansion boards; the Mx-1-ME supports up to 5 expansion boards.)

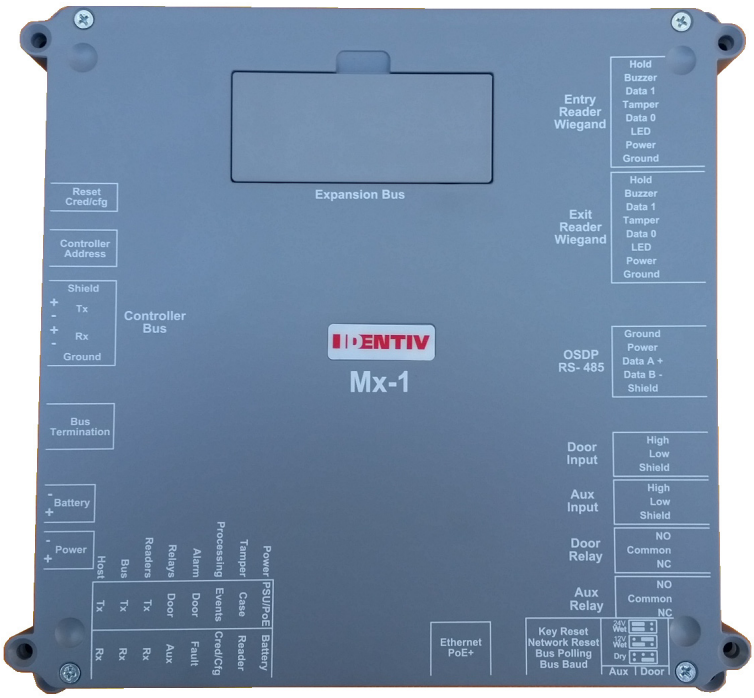
[4] An Mx-2, Mx-4, or Mx-8 controller provides both a 5-pin MATCH terminal and a 6-pin Wiegand terminal for each door, but only one of them can be used for a particular door. (The Mx-1 and Mx-1-ME controllers do *not* provide a MATCH terminal.)

[5] For the Open Secure Data Protocol (OSDP), an optional exit reader is wired "through" the entry reader. OSDP readers are required for FICAM, and they can be used with an older controller by adding a SNIB3 and an RREB, as part of Identiv's FICAM Solution. (For more information, see "RS-485 Readers Expansion Board (RREB)" starting on page 2-28.)

Mx-1 Controller Configurations

The Mx-1 controller is a 1-door controller designed to operate in a networked environment. The models in the Mx-1 product line are:

- The **Mx-1** controller, which is packaged in a compact plastic case, can be powered by either PoE+ (providing a nominal 25.5 Watts) or 24 V - 28 V of DC power from an external power supply. (Its light weight and small size provides more flexibility when deciding where to install it.)



NOTE: Revision 1 of the Mx-1 controller has the model number of "Mx-1 026-0000121-P", and is described in Chapter 9 of a previous version (Revision AH dated April 17, 2018) of this document. Revision 2 of the Mx-1 controller has the model number of "Mx-1 026-0000121-P-**2**", and is described in Chapter 9 of this version of this document. (The primary product change is a different set of Wet or Dry Mode jumpers for the power to the Door Relay and Aux Relay terminals, which are explained in Table 9-2.)

- The **Mx-1-ME** controller is packaged in a traditional metal enclosure (with a locking door, a tamper switch, a power supply, a standby battery, and room for up to five optional expansion boards).

- There is an **Mx-1-W** license for an Mx-1 or Mx-1-ME controller that is specifically configured to manage up to eight wireless locks. (These can be either ASSA-ABLOY's Aperio brand of wireless locks, or Allegion's Schlage brand of wireless locks.) For more information, see the DIGI*TRAC Hardware Configuration > Wireless Locks > **Wireless Locks – Overview** topic in the Velocity online help.

  NOTE: This functionality has not been evaluated by UL.

Components of the Mx-1 Controller

Both the Mx-1 and the Mx-1-ME models of the Mx-1 controller include a main board with various components and connectors, as shown in Figure 9-2 on page 9-8. The Mx-1-ME model's secure metal enclosure also includes a power supply, a standby battery, a locking door with a tamper switch, and room for optional expansion boards, as shown in the following figure.

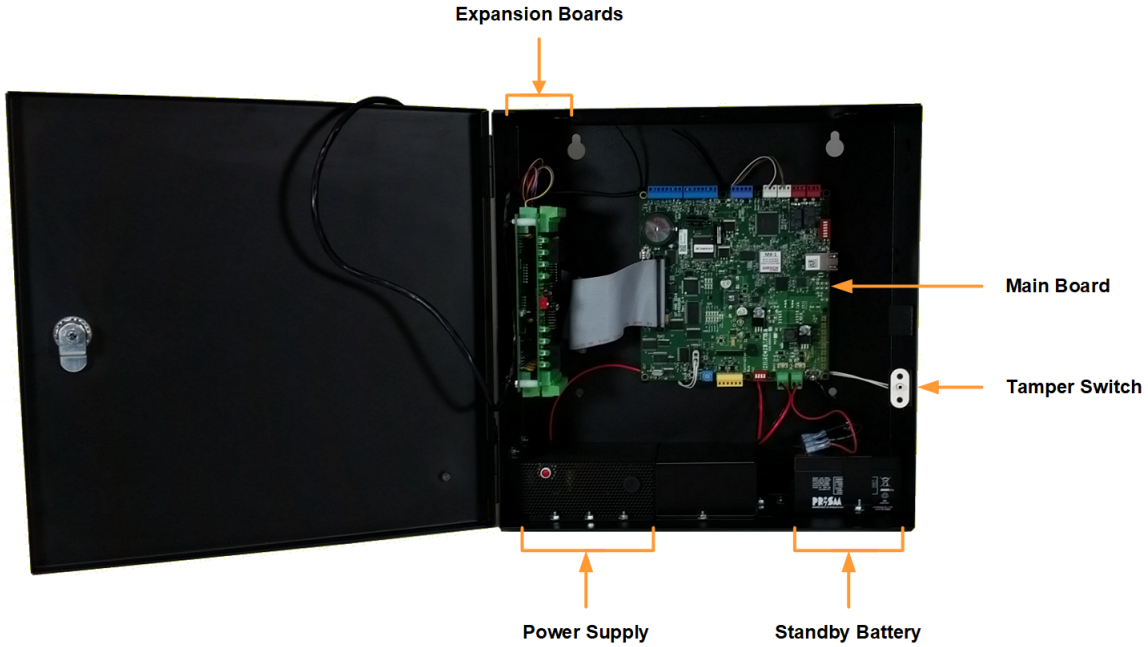


Figure 9-1: Components of the Mx-1-ME Controller

NOTE: Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet (PoE) functionality which is included on the standard Mx-1 model.

Mx-1 Controller Main Board

The Mx-1 controller's main board contains the main connectors to the surrounding system. Through it, you can connect to readers with Wiegand or OSDP interfaces, input devices, output devices, an Ethernet network (for communication with the Velocity server), other controllers (using RS-485 chaining), and power sources.

- For the Mx-1 model, all connectors, LEDs, DIP switches, and the RS-485 chaining address knob are right angled (facing outward) so they can be accessed while the plastic case is closed.
- For the Mx-1-ME model, all connectors, DIP switches, and the RS-485 chaining address knob are vertical, and the mini LEDs will be like those on the Mx-2/4/8 controller. Note that the new bank of 8 green and 8 yellow status LEDs (in the lower left corner) are not included on the Mx-1-ME's main board.

Figure 9-2 shows the connectors (and other key components) of an Mx-1 controller's main board which are for customer use. (Figure 9-3 on page 9-16 shows the connectors which are used by Identiv for testing, debugging, and programming.)

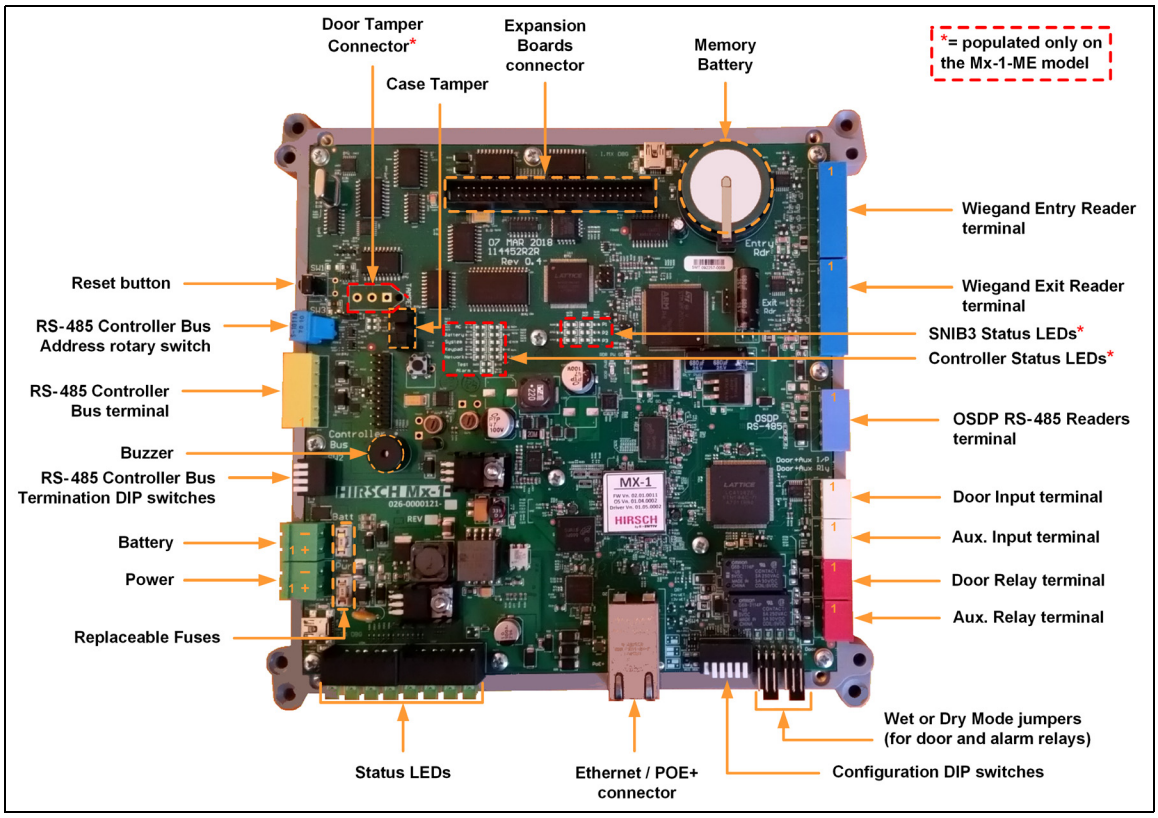


Figure 9-2: Mx-1 Controller Main Board Connectors and Components for Customer Use

The following table describes the connectors and components identified in Figure 9-2, starting at the lower left corner of the board and moving clockwise. (The detailed pin out information for the terminals is provided in Table 9-3 on page 9-14.)

Table 9-2: Description of the Mx-1 Controller's Connectors and Components for Customer Use

Connector or Component	Description
Replaceable Fuses	These small replaceable fuses (behind the Power and the Battery input terminals) protect the main board from power surges, and excessive current draw. They are 2 Amp 125 VAC/VDC fuses, part number 0451002.MRL, by Littelfuse, Inc.
Power	This 2-pin green connector is used to supply 24 V - 28 V of DC power to the Mx-1 controller, from a 2 Amps external power supply. • For the Mx-1-ME model, this connector is wired at the factory to the included power supply. (Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet functionality.) • For the Mx-1 model, you can either use this connector to supply DC power, or you can use the POE+ Ethernet connector to supply a nominal 25.5 Watts of power. NOTE: If the Mx-1 controller will be part of an access control system which must meet a particular UL standard, you must use a UL-listed power source which provides the required duration of standby power for that standard. For more information, see the table about "Standby Power Requirements for Various UL Standards:" on page ix. CAUTION: If you are using the POE+ Ethernet connector to supply power, you should not use this connector to supply additional power.
Battery	This 2-pin green connector is used to attach a 24V DC backup battery pack to the Mx-1 controller. • For the Mx-1-ME model, this connector is wired at the factory to the included 7.2 Ah backup battery pack. • For the Mx-1 model, you can use this connector for an external backup battery pack or an uninterruptible power supply. (This capability was not evaluated by UL.) NOTE: If the Mx-1 controller will be part of an access control system which must meet a particular UL standard, you must use a UL-listed backup battery which provides the required duration of standby power for that standard. For more information, see the table about "Standby Power Requirements for Various UL Standards:" on page ix. When using a 24V battery pack, the DC power source should be 28V at 2 Amps, in order to charge the batteries. (A PoE+ power source cannot be used to charge a 24V battery pack.)
RS-485 Controller Bus Termination DIP switches	If you are adding an Mx-1 controller (which has built-in SNIB3 functionality) to a chain of controllers connected by RS-485 wiring, this bank of four DIP switches is used to indicate whether the controller is located at the beginning, middle, or end of the chain. This is just like SW1 on the SNIB2, the Mx-2/4/8 controller's main board (with built-in SNIB2 functionality), and the SNIB3. • When the Mx-1 controller is in the middle of a chain, all 4 switches must be OFF. • When the Mx-1 controller is either the first (master) or last (termination) one in a chain, all 4 switches must be ON.
Buzzer	This component generates an audible alarm during certain conditions. NOTE: This buzzer's functionality has not yet been defined.

Connector or Component	Description
RS-485 Controller Bus terminal	This 6-pin yellow connector can be used to create a chain of controllers, where the first (master) controller communicates directly with the Velocity Server across a network using the POE+ Ethernet connector, and the other (downstream) controllers communicate along the chain using RS-485 wiring. Otherwise, an Mx-1 controller can communicate directly with the Velocity Server across a network using the POE+ Ethernet connector. For more information, see "Network Configuration Options for the Built-In SNIB3" starting on page 9-46. NOTE: The RS-485 cable linking the first (master) controller to the second (downstream) controller in the chain must cross over the RX± and TX± wires. The cable for each subsequent downstream controller is wired straight through. For details, see "RS-485 Cabling for SNIB3s" on page 7-80.
RS-485 Controller Bus Address rotary switch	This 16-position rotary switch is used to set the address of an Mx-1 controller when it is part of a chain of controllers connected using RS-485 wiring. The valid values are 1 through F (1-15).
Reset button	This recessed button performs three types of reset, depending on how long you hold down the button. (On previous DIGI*TRAC or Mx controllers, this was also known as the "blue button".) • Press the button for 1 second if you have a problem that won't clear within a few minutes. All alarm conditions in the alarm buffers will be deleted, and any alarm relays that are currently active will be turned off and reset. • Press the button for 5 seconds to reset the system code to the factory default of 123, and to reset ScramblePads to their original programming parameters. • Press the button for 30 seconds if a major and persistent problem occurs. This resets the entire controller, clears all controller memory, and returns all settings to the original factory default values. CAUTION: Only do this as a last resort. For more information, see "Resetting the Controller" on page 7-26.
Door Tamper connector	For the Mx-1-ME model only, this 5-sided 3-pin connector attaches to the corresponding connector for the wiring of the plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open. When the door is opened, the plunger is extended, and a "door tamper" alarm is generated in Velocity. (The Mx-1 model uses an optical tamper mechanism with its plastic case.)
Case Tamper	For the Mx-1 model only, this component provides an optical tamper mechanism that indicates whether the plastic case is closed or open. When the case is opened, the Case Tamper LED (in the group of large Status LEDs) is lit, and a "door tamper" alarm is generated in Velocity. (The Mx-1-ME model uses the Door Tamper connector to attach to a switch that is part of its enclosure.)
Expansion Boards connector	This connector is used to attach the EBIC5 flat ribbon cable that provides power to and communicates with any optional expansion boards installed in an Mx-1-ME. For more information, see "Connecting Expansion Boards" starting on page 7-13.

Connector or Component	Description
Memory Battery	This rechargeable Li-ion coin cell battery supplies backup power to the Mx-1 controller's memory, so critical information is not lost during a power outage of up to 10 days. That information includes user credentials, configuration, and date/time. This battery is model PD3048 by Route Jade (formerly Route JD or Korea Power Cell), which provides 3.7 VDC, and has a 300 mAh capacity. Its dimensions are 30.0 mm in diameter by 4.9 mm thick. For more information, see "Replacing the Memory Battery" on page 9-50.
Wiegand Entry Reader terminal	This 8-pin blue connector is used to attach the door's entry reader when it is one that uses the Wiegand protocol. For more information, see "Wiring Diagram for Wiegand Readers" on page 9-40. (If your readers use the Open Supervised Device Protocol (OSDP), then they will be attached using the OSDP RS-485 Readers terminal.) This terminal is fused and resettable, and provides 12V DC power for the entry reader. On the Mx-1, this terminal provides up to 0.5 Amps; on the Mx-1-ME, this terminal provides up to 0.355 Amps. (NOTE: The maximum simultaneous current draw for this Wiegand Entry Reader terminal and the Wiegand Exit Reader terminal is 0.75 Amps.)
Wiegand Exit Reader terminal	This 8-pin blue connector is used to attach the door's optional exit reader when it is one that uses the Wiegand protocol. For more information, see "Wiring Diagram for Wiegand Readers" on page 9-40. (If your readers use the Open Supervised Device Protocol (OSDP), then they will be attached using the OSDP RS-485 Readers terminal.) NOTE: The door's entry reader and optional exit reader can use different protocols. This terminal is fused and resettable, and provides 12V DC power for the exit reader. On the Mx-1, this terminal provides up to 0.5 Amps; on the Mx-1-ME, this terminal provides up to 0.355 Amps. (NOTE: The maximum simultaneous current draw for this Wiegand Exit Reader terminal and the Wiegand Entry Reader terminal is 0.75 Amps.)
SNIB3 Status LEDs	This set of small LEDs displays the current status of the Mx-1-ME controller's built-in SNIB3. (The Mx-1 uses a set of larger green and yellow LEDs which is visible when the plastic case is closed.) For information about this set of LEDs, see "SNIB3 Status LEDs on the Mx-1-ME" on page 9-24.
Controller Status LEDs	This set of small LEDs displays the current status of the Mx-1-ME controller. (The Mx-1 uses a set of larger green and yellow LEDs which is visible when the plastic case is closed.) For information about this set of LEDs, see "Controller Status LEDs on the Mx-1-ME" on page 9-22.

Connector or Component	Description
OSDP RS-485 Readers terminal	This 5-pin dark blue connector is used to attach the door's entry reader when it is one that uses OSDP. (When the door has an optional exit reader that uses OSDP, it is wired "through" the entry reader.) For more information, see "Wiring Diagram for OSDP Readers" on page 9-40. This terminal is fused and resettable, and provides up to 0.75 Amps at 12V DC for the attached readers. The Open Supervised Device Protocol (OSDP) is a standard adopted by the Security Industry Association (SIA). OSDP is a secure bi-directional protocol that replaces the traditional Wiegand protocol, and manages the communication between access control panels and card readers (or other peripheral devices). NOTE: Because the door's entry reader and optional exit reader can use different protocols, this terminal can be used to attach an OSDP entry reader, and the Wiegand Exit Reader terminal can be used to attach a Wiegand exit reader.
Door Input terminal	This 3-pin white connector is used for an analog input, such as the multi-state alarm inputs provided by the line module that detects changes in the status of a door's components (for example the position of the door contacts and the press of a Request to Exit button or the triggering of a motion detector). For more information, see "Line Modules" on page 2-75 and "Connecting Line Module Inputs" starting on page 7-21.
Aux. Input terminal	This 3-pin white connector can be used for a second analog input. For more information, see "Connecting Line Module Inputs" starting on page 7-21.
Door Relay terminal	This 3-pin red connector is used to control the door's access device, such as a magnetic lock or an electric strike. The Wet or Dry Mode jumpers (described later in this table) determine the power mode for the Door Relay and the Aux. Relay terminals. • When this door relay is configured for **Wet Mode at 24V**, the Mx-1 supplies regulated power at 24 Volts, with a maximum output current of 0.25 Amps. (At 24V, the maximum simultaneous current draw for this Door Relay and the Aux Relay is 0.5 Amps.) • When this door relay is configured for **Wet Mode at 12V**, the Mx-1 supplies regulated power at 12 Volts, with a maximum output current of 0.5 Amps. (At 12V, the maximum simultaneous current draw for this Door Relay and the Aux Relay is 1.0 Amps.) • When this door relay is configured for **Dry Mode**, its maximum output current is 2.0 Amps, and the voltage is either 30 VDC or 250 VAC. **NOTE:** UL has only evaluated this relay for 30 VDC at 2 Amps for resistive and inductive loads. For more information, see "Connecting Outputs" starting on page 7-23.

Connector or Component	Description
Aux. Relay terminal	This 3-pin red connector is used to control external alarm or auxiliary devices, such as activating an audible alarm, turning on lights, or initiating the recording of surveillance video. The Wet or Dry Mode jumpers (described next in this table) determine the power mode for the Door Relay and the Aux. Relay terminals. • When this auxiliary relay is configured for **Wet Mode at 24V**, the Mx-1 supplies regulated power at 24 Volts, with a maximum output current of 0.25 Amps. (At 24V, the maximum simultaneous current draw for this Aux Relay and the Door Relay is 0.5 Amps.) • When this auxiliary relay is configured for **Wet Mode at 12V**, the Mx-1 supplies regulated power at 12 Volts, with a maximum output current of 0.5 Amps. (At 12V, the maximum simultaneous current draw for this Aux Relay and the Door Relay is 1.0 Amps.) • When this auxiliary relay is configured for **Dry Mode**, its maximum output current is 2.0 Amps, and the voltage is either 30 VDC or 250 VAC. **NOTE:** UL has only evaluated this relay for 30 VDC at 2 Amps for resistive and inductive loads. For more information, see “Connecting Outputs” starting on page 7-23.
Wet or Dry Mode jumpers	This set of pins and jumpers determines whether the devices connected to the Door Relay terminal and the Aux. Relay terminal are wired in wet mode at 24V, wet mode at 12V, or dry mode. • In **Wet mode at 24V**, the Mx-1 supplies regulated power at 24 Volts, with a maximum output current of 0.25 Amps per port. CAUTION: When configuring a relay for wet mode at 24V, make sure that the connected device will not draw more than the max limit of 0.5 Amps (which equals 12 Watts), and that the device is rated for 24 VDC. • In **Wet mode at 12V**, the Mx-1 supplies regulated power at 12 Volts, with a maximum output current of 0.5 Amps per port. CAUTION: When configuring a relay for wet mode at 12V, make sure that the connected device will not draw more than the max limit of 1.0 Amps (which equals 12 Watts), and that the device is rated for 12 VDC. • In **Dry mode**, the device is powered by an external power source. The jumper settings for these modes are printed on the top cover of the Mx-1’s plastic case, in the bottom right corner: 

Connector or Component	Description
Configuration DIP switches	This bank of 6 DIP switches is used to configure the Mx-1 controller's built-in SNIB3: • The first 4 DIP switches are used to configure certain functionality of the built-in SNIB3 (just like SW2 on the SNIB3), including resetting its encryption keys, resetting it to the factory default settings, and indicating whether this controller is the first (master) in a chain of controllers and is connected to the Velocity Server via Ethernet. • The last 2 DIP switches correspond to the first 2 DIP switches on the SNIB3's SW3 bank, and are used to configure the communications speed when this controller is part of a chain of controllers connected to each other using RS-485 wiring. For more information, see "DIP Switches on an Mx-1 Controller" starting on page 9-44.
Ethernet / POE+ connector	This Ethernet connector provides up to Gigabit data connectivity for secure communication with the Velocity server. • On the standard Mx-1 model, this connector can be used to power the controller (and some attached devices) through Power Over Ethernet Plus with a nominal 25.5 Watts of input power. • Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet functionality. For more information, see "Supplying Power to an Mx-1 Controller" on page 9-30.
Status LEDs	This set of LEDs provides information about the current status and operation of the Mx-1 controller, which is visible from the outside of the closed plastic case. (These LEDs do not appear on the Mx-1-ME's main board.) For information about this set of LEDs, see "Status LEDs on the Mx-1" starting on page 9-18.

Table 9-3 provides the detailed pin-out information for the various connectors which snap into the corresponding terminals on the Mx-1 controller's main board (which is shown in Figure 9-2 on page 9-8). (The Mx-1-ME has the same connectors, which are mounted vertically.)

Table 9-3: Pin Out Information for the Mx-1 or Mx-1-ME Controller's Terminals

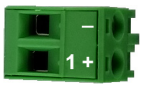
Terminal Name (and Connector Image)		Pin #	Function	Typical Wire Color	
Power or Battery		1	Power (+)		Red
		2	Ground (-)		Black

Table 9-3: Pin Out Information for the Mx-1 or Mx-1-ME Controller's Terminals (Continued)

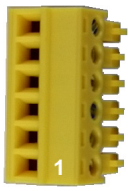
Terminal Name (and Connector Image)		Pin #	Function	Typical Wire Color	
RS-485 Controller Bus		1	Ground		Black
		2	RX-		(varies)
		3	RX+		(varies)
		4	TX-		(varies)
		5	TX+		(varies)
		6	Shield / Drain		Black with White stripe
Wiegand Entry Reader or Wiegand Exit Reader		1	Hold		Blue
		2	Buzzer		Yellow
		3	Data 1		White
		4	Tamper Output		Violet
		5	Data 0		Green
		6	LED (Green)		Orange
		7	Power (+)		Red
		8	Ground (-)		Black
OSDP RS-485 Readers		1	Ground (-)		Black
		2	+12V RDR		Red
		3	RS485+		Pink
		4	RS485-		Gray
		5	Shield / Drain		Black with White stripe
Door Input or Aux. Input		1	HI		White
		2	LO		Black
		3	Shield / Drain		Black with White stripe

Table 9-3: Pin Out Information for the Mx-1 or Mx-1-ME Controller's Terminals (Continued)

Terminal Name (and Connector Image)		Pin #	Function	Typical Wire Color	
Door Relay or Aux. Relay		1	Normally Open		(varies)
		2	Common		(varies)
		3	Normally Closed		(varies)

The following figure shows the connectors which are used by Identiv for testing, debugging, and programming.

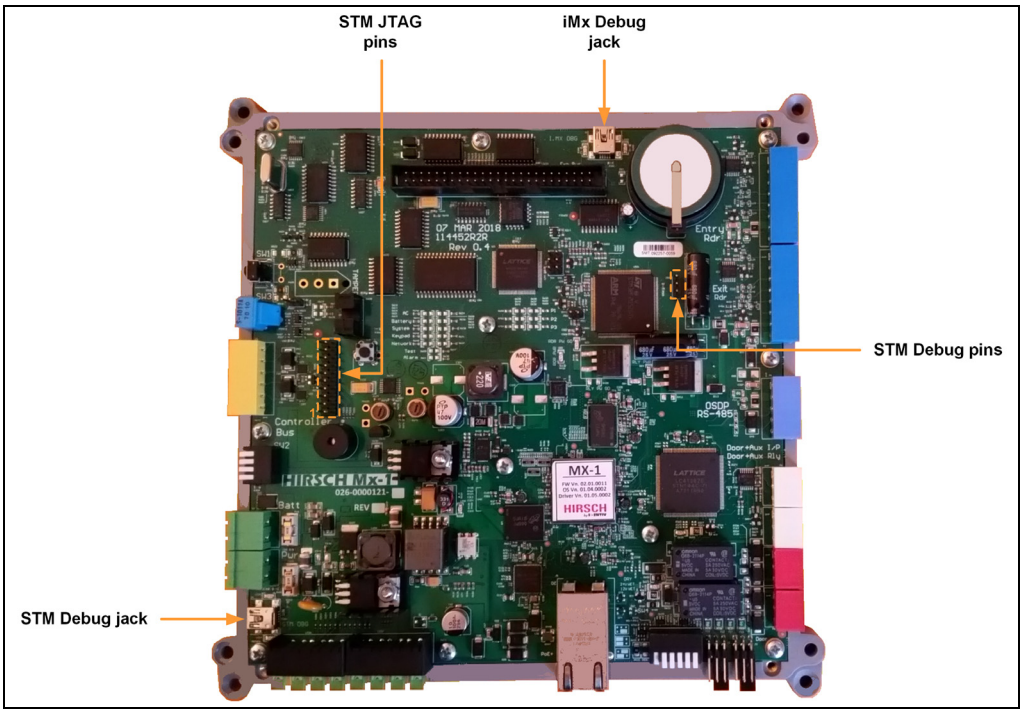


Figure 9-3: Mx-1 Controller Main Board Connectors for Testing and Debugging

The following table describes the connectors identified in Figure 9-3, starting at the lower left corner of the board and moving clockwise.

Table 9-4: Description of the Mx-1 Controller's Connectors for Testing and Debugging

Connector	Description
STM Debug jack	This jack (or the STM Debug pins) is used by Identiv to debug the STM32 processor.
STM JTAG pins	This set of 20 pins is used by Identiv to program the STM32 processor.
iMx Debug jack	This jack is used by Identiv to debug the built-in SNIB3.
STM Debug pins	This set of 3 pins (or the STM Debug jack) is used by Identiv to debug the STM32 processor.

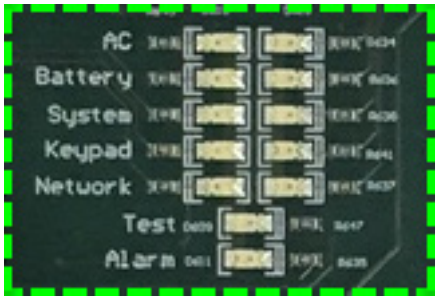
Status LEDs

The groups of status LEDs appearing on the Mx-1 controller's main board (as indicated on Figure 9-2) vary by model.

- The Mx-1 model (but not the Mx-1-ME) has two adjacent blocks of large Status LEDs near the lower left corner of its main board, providing a row of 8 green LEDs on the top and a row of 8 yellow LEDs on the bottom:

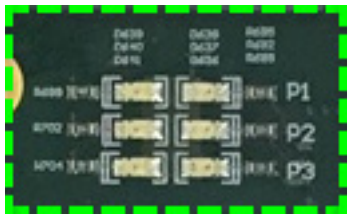
For information about this set of LEDs, see "Status LEDs on the Mx-1" starting on page 9-18.

- The Mx-1-ME model (but not the Mx-1) has a set of 12 miniature Controller Status LEDs near the middle of its main board (like those on the Mx-2/4/8 controller's main board):



For information about this set of LEDs, see "Controller Status LEDs on the Mx-1-ME" on page 9-22.

- The Mx-1-ME model (but not the Mx-1) has a set of 6 miniature SNIB3 Status LEDs near the middle of its main board (like those on the Mx-2/4/8 controller's main board for its built-in SNIB2):



For information about this set of LEDs, see "SNIB3 Status LEDs on the Mx-1-ME" on page 9-24.

Status LEDs on the Mx-1

This block of 16 larger LEDs, which appear only on the Mx-1 model's main board, provides information about the current status and operation of the Mx-1 controller which is visible outside of the closed plastic case. (This block of LEDs is not included on the Mx-1-ME, because it is not visible when the metal enclosure's door is closed.)

The following graphic includes ID numbers for the LEDs, which are used in the table describing their meanings.

Table 9-5: Meanings of the Status LEDs on the Mx-1

LED #	Purpose	Description (as of CCM/CCMx firmware version 7.6.20)
G1	Host Tx	If this controller is connected to an Ethernet network, this LED indicates when this controller's built-in SNIB3 is transmitting data to the Velocity Server. • When this LED is on, it means this controller is transmitting data to the Velocity Server. • When this LED is off, it means this controller is not currently transmitting data to the Velocity Server.
Y1	Host Rx	If this controller is connected to an Ethernet network, this LED indicates when this controller's built-in SNIB3 is receiving data from the Velocity Server. • When this LED is on, it means this controller is receiving data from the Velocity Server. • When this LED is off, it means this controller is not currently receiving data from the Velocity Server.

Table 9-5: Meanings of the Status LEDs on the Mx-1 (Continued)

LED #	Purpose	Description (as of CCM/CCMx firmware version 7.6.20)
G2	Bus Tx	Indicates when data is being transmitted (either upstream or downstream) by this controller along a chain of controllers connected using RS-485 wiring. • When this LED is on, it means data is being transmitted by this controller along a chain of controllers connected using RS-485 wiring. • When this LED is off, it means data is not currently being transmitted by this controller along a chain of controllers connected using RS-485 wiring. (This LED is also off when this controller is not part of a chain of controllers connected using RS-485 wiring.)
Y2	Bus Rx	Indicates when data is being received by this controller along the RS-485 wiring that connects a chain of controllers. • When this LED is on, it means data is being received by this controller along the RS-485 wiring that connects a chain of controllers. • When this LED is off, it means data is not currently being received by this controller along the RS-485 wiring that connects a chain of controllers. (This LED is also off when this controller is not part of a chain of controllers connected using RS-485 wiring.)
G3	Readers Tx	Indicates when the controller is transmitting commands or data to a connected reader. • When this LED is on, it means the controller is transmitting commands or data to a connected reader. • When this LED is off, it means the controller is not currently transmitting commands or data to any of the connected readers.
Y3	Readers Rx	Indicates when the controller is receiving data from a connected reader. • When this LED is on, it means the controller is receiving data from a connected reader. • When this LED is off, it means the controller is not currently receiving data from any of the connected readers.
G4	Door Relay	Indicates when the door relay is active. • When this LED is on, it means the door relay is active. • When this LED is off, it means the door relay is not currently active. A Normally Open (NO) circuit is open, and a Normally Closed (NC) circuit is closed.
Y4	Aux. Relay	Indicates when the alarm (a.k.a. auxiliary) relay is active. • When this LED is on, it means the alarm relay is active. • When this LED is off, it means the alarm relay is not currently active. A Normally Open (NO) circuit is open, and a Normally Closed (NC) circuit is closed.
G5	Door Alarm	Indicates whether a door alarm is active. • When this LED is on, it means there is an active Door Forced Open alarm. • When this LED is off, it means there is not an active door alarm. • When this LED is flashing, it means there is an active Door Open Too Long alarm.

Table 9-5: Meanings of the Status LEDs on the Mx-1 (Continued)

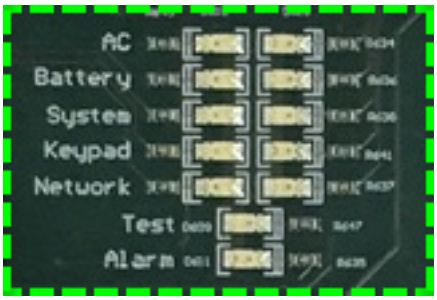
LED #	Purpose	Description (as of CCM/CCMx firmware version 7.6.20)
Y5	Fault Alarm	Indicates whether a fault condition exists on the supervised line input. • When this LED is on, it means there is a fault (such as a cut line or a short circuit). • When this LED is off, it means the supervised line is within normal specifications.
G6	Processing Events	Indicates when event information is being transmitted to the Velocity Server by the controller's CCM. • When this LED is on, it means the controller is transmitting event information to the Velocity Server. • When this LED is off, it means the controller is not currently transmitting event or configuration information to the Velocity Server. • When this LED is flashing, it means the controller is transmitting configuration information to the Velocity Server.
Y6	Processing Cred/Cfg	Indicates when user credentials or configuration information is being received by the controller's CCM. • When this LED is on, it means user credentials are being received by the controller. • When this LED is off, it means user credentials or configuration information is not currently being received by the controller. • When this LED is flashing, it means configuration information is being received by the controller.
G7	Case Tamper	Indicates when the controller's enclosure is open. • When this LED is on, it means the controller's enclosure is open. (Either an optical tamper device indicates that the Mx-1 model's plastic case is open, or a plunger switch indicates that the door is open on the Mx-1-ME model's metal enclosure.) • When this LED is off, it means no enclosure tamper is currently detected. • When this LED is flashing, it means multiple instances of an enclosure tamper have been detected (because the previous alarm was not cleared).
Y7	Reader Tamper	Indicates when a tamper condition exists at a reader attached to the controller. • When this LED is on, it means there is a reader tamper or a code tamper. • When this LED is off, it means no reader tamper or code tamper is currently detected.
G8	PSU/PoE Power	Indicates when the controller has adequate power, and whether it is 24 V - 28 V DC from an external power supply or from POE+ (via the Ethernet jack). • When this LED is on, it means the controller is being powered by DC input (through the Power terminal), and its voltage is at least 22 V. • When this LED is off, it means the controller's power is either low (between 11 V and 13 V) or has failed (less than 11 V). • When this LED is flashing, it means the controller is either being powered by POE+ (via the Ethernet jack), or its voltage is between 13 V and 22 V.

Table 9-5: Meanings of the Status LEDs on the Mx-1 (Continued)

LED #	Purpose	Description (as of CCM/CCMx firmware version 7.6.20)
Y8	Battery Power	Indicates when the connected standby battery pack is low or bad. • When this LED is on, it means the battery is bad, with a voltage of less than 6 V (and should be replaced). • When this LED is off, it means the battery is good, and its voltage is at least 23 V. • When this LED is flashing, it means the battery is either low (with its voltage between 17 V and 23 V), or is charging (with its voltage between 6 V and 17 V) if AC power is available.

Controller Status LEDs on the Mx-1-ME

This set of 12 miniature LEDs (on the Mx-1-ME controller's main board) displays the current status of the controller.



The meanings of all these controller status LEDs in version 7.5.70 of the CCM firmware are explained in the following table.

Table 9-6: Meanings of the Controller Status LEDs on the Mx-1-ME (as of CCM 7.5.70)

Name and Purpose of row of status LEDs	Meaning of First LED	Meaning of Second LED
AC = AC Power	ON = AC Power is OK	ON = AC Power Failure
	Both LEDs BLINKING = AC Power is Low (or Mx-1-ME controller is using Power over Ethernet+)	
Battery = Standby Battery	ON = Battery is OK (at 24V - 28V)	ON = Battery Failure (less than 21V)
	Both LEDs BLINKING = Battery is Low (at 21V - 23V); if AC Power is available, the Battery is Charging	
System = Controller's Status	BLINKING (and second LED is OFF) = Controller is OK	ON (and first LED is OFF) = Controller Failure
Keypad = Controller's communication with all of its connected readers	Flash = Controller is sending data to one of its connected readers	Flash = Controller is receiving data from one of its connected readers
Network = Controller's communication with the Velocity Server	ON = Transmitting an event to the Velocity Server Flash = Transmitting some other message to the Velocity Server	ON = Receiving credentials Flash = Receiving configuration or other commands
Test = Door Alarm or Controller's Power-On Self Test	ON = A door is in an alarm state SLOW BLINKING = A door is held open too long FAST BLINKING = Controller is running its Power-On Self Test	(no second LED on this row)
Alarm = Line Fault Alarm	ON = A fault condition (Out Of Spec, Open, Short, or Noisy) exists on the supervised line input for a door	(no second LED on this row)

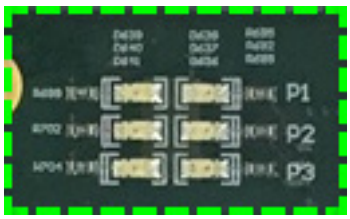
The meanings of these controller status LEDs in version 7.6.20 of the CCM firmware are explained in the following table.

Table 9-7: Meanings of the Controller Status LEDs on the Mx-1-ME (as of CCM 7.6.20)

Name and Purpose of row of status LEDs	Meaning of First LED	Meaning of Second LED
AC = AC Power	ON (and second LED is OFF) = AC Power is OK	ON (and first LED is OFF) = AC Power Failure
	Both LEDs BLINKING = AC Power is Low (or Mx-1-ME controller is using Power over Ethernet+)	
Battery = Standby Battery	ON (and second LED is OFF) = Battery is OK	ON (and first LED is OFF) = Battery Failure
	Both LEDs BLINKING = Battery is Low (at 21V - 23V); if AC Power is available, the Battery is Charging	
System = Controller's Status	Flashing (and second LED is OFF) = Controller is OK	ON (and first LED is OFF) = Controller Failure
Keypad = Controller's communication with all of its connected readers	Flash = Controller is sending data to one of its connected readers	Flash = Controller is receiving data from one of its connected readers
Network = Controller's communication with the Velocity Server	ON = Transmitting an event to the Velocity Server Flash = Transmitting some other message to the Velocity Server	ON = Receiving credentials Flash = Receiving configuration or other commands
Test = Door Alarm or Controller's Power-On Self Test	During the controller's POST: ON = Controller is running its Power-On Self Test During normal operations: ON = A door is in an alarm state Slow Blinking = A door is held open too long	(no second LED on this row)
Alarm = Line Fault Alarm	ON = A fault condition (Out Of Spec, Open, Short, or Noisy) exists on the supervised line input for a door	(no second LED on this row)

SNIB3 Status LEDs on the Mx-1-ME

This set of 6 miniature LEDs (on the Mx-1-ME controller's main board) displays the current status of the controller's built-in SNIB3. For information about them, see "Controller and SNIB3 LED Diagnostics" on page 7-94.



Internal Power Supply

The internal power supply included with the Mx-1-ME model can use either a 110 or 240 VAC supply (or 100 VAC for Japan) to provide 30 VDC power to the Mx-1 controller's main board, optional expansion boards, and readers. For additional input and output devices requiring substantial power - such as electric strikes and magnetic locks, motion detectors, retinal scanners, and surveillance cameras - auxiliary power supplies often must be used.

Standby Battery

The standby battery pack included with the Mx-1-ME model supplies 24 VDC of backup power to the controller's main board even if the primary power supply fails. This 7.2 Ah rechargeable sealed lead-acid battery pack is capable of supplying power to the controller board for several hours. The standby time is dependent on the connected devices.

Under normal conditions, the standby battery has a life span of 4 to 5 years. Its status can be interrogated using Velocity's Diagnostic Window. For more information, see the topics in the section about "Performing Periodic Maintenance" starting on page 9-49.

NOTE: If the Mx-1 controller will be part of an access control system which must meet a particular UL standard, you must use a UL-listed backup battery which provides the required duration of standby power for that standard. For more information, see the table about "Standby Power Requirements for Various UL Standards:" on page ix.

Tamper Detection

The Mx-1 controller provides a tamper detection feature. The mechanism varies depending on the type of enclosure.

- ❑ For the Mx-1 model, tamper detection uses an optical tamper mechanism that indicates whether the plastic case is closed or open. When the case is opened, the Case Tamper LED (in the group of large Status LEDs) is lit, and a "door tamper" alarm is generated in Velocity.
- ❑ For the Mx-1-ME model, tamper detection uses a plunger-style contact switch that indicates whether the door of the metal enclosure is closed or open. When the door is opened, the plunger is extended, and a "door tamper" alarm is generated in Velocity.

Expansion Boards for an Mx-1-ME Controller

Optional expansion boards increase the capabilities of Mx-1 controllers. For example, the Alarm Expansion Board increases the number of line module inputs that the controller can accept, and the Relay Expansion Board extends the number of control outputs that a controller can accommodate. The MEB series increases the controller's available memory, expanding the number of alarm and event buffers or codes the controller can hold.

- ❑ The Mx-1 controller is packaged in a compact plastic case which does not have room for any optional expansion boards.
- ❑ The Mx-1-ME controller is packaged in a traditional metal enclosure which has room for optional expansion boards.

Table 9-8 provides an overview of the available expansion boards. An Mx-1-ME controller can accommodate up to 5 expansion boards, subject to the restrictions explained in this table. (The Mx-1 and Mx-1-ME controllers include the functionality of a SNIB3, so you don't need a separate communications expansion board.)

Table 9-8: Expansion Boards for the Mx-1-ME Controller

Model #	Description	Comments
AEB8	Alarm Expansion Board with 8 Inputs	Adds 8 additional high security alarm inputs, and features removable connectors. Each input requires an appropriate Line Module. An AEB8 draws 15 mA at 28 VDC. Velocity supports up to 4 of these boards in an Mx-1-ME controller.
REB8	Relay Expansion Board with 8 Relays	Adds 8 additional 2 Amp Form C dry mode relays. Features status LEDs and removable connectors. An REB8 draws 15 mA at 28 VDC when idle, and a maximum of 80 mA when all relays are active. Velocity supports up to 5 of these boards in an Mx-1-ME controller.
MEB/BE	Memory Expansion Board - Buffer Expansion	Expands the standard buffer from 1,560 events and 1,560 alarms to approximately 20,000 events and 2,000 alarms. Protected from data loss during power failures for up to 10 days by the controller memory battery. An MEB draws 8 mA at 5 VDC. Velocity supports only 1 memory expansion board in an Mx-1-ME controller.
MEB/ CB128	Memory Expansion Board - Code Expansion of 128,000 with Buffer Option	Expands Code Memory by approximately 128,000 (from 4,352 to 135,424) on Velocity. A portion of the Code Memory may be allocated to alarm and event Buffers, which will reduce the number of users. Protected from data loss during power failures for up to 10 days by the controller memory battery. An MEB draws 8 mA at 5 VDC. Velocity supports only 1 memory expansion board in an Mx-1-ME controller.

All expansion boards have the same dimensions and shipping weight:

Dimensions:	6”H x 4.25”W x 0.75”D (15.2cm x 10.8cm x 1.9cm)
Shipping Weight:	1 lb (0.5 kg)

The ribbon cable used to connect these boards to the controller’s main board is the EBIC5, which can link up to five expansion boards. For detailed information about the setup and installation of expansion boards, see “Expansion Board Installation” on page 7-31.

Data Capacity of an Mx-1 Controller

An Mx-1 or Mx-1-ME controller includes a base amount of memory which is dedicated to storing data about credentials, events, and alarms. (This memory enables a controller to continue performing its functions even when it is temporarily unable to communicate with the Velocity server.)

The data capacity of an Mx-1-ME controller can be increased by adding optional expansion boards. An expansion board can be configured so that its memory is dedicated either solely to additional credentials, or to a mixture of additional credentials, events, and alarms.

The following table shows the maximum data capacity of an Mx-1-ME controller in its base configuration and with various optional expansion boards configured either way.

Table 9-9: Data Capacity of an Mx-1-ME Controller

Controller configuration	maximum Credentials	maximum Events	maximum Alarms
Base (no expansion boards)	4,352	1,560	1,560
With MEB/CB64 and 20% reduction Enabled	55,200	37,440	5,460
With MEB/CB64 and 20% reduction Disabled	69,888	1,560	1,560
With MEB/CB128 and 20% reduction Enabled	106,400	65,520	17,160
With MEB/CB128 and 20% reduction Disabled	135,424	1,560	1,560

Note that your system’s actual capacity could be less, as explained in “Velocity Features that Reduce Available Memory” on page 2-24.

Replaceable Parts of an Mx-1 Controller

An Mx-1 or Mx-1-ME controller has the following replaceable parts.

- ❑ Power Supply Input Fuses: 2 Amp 125 VAC/VDC fuses, part number 0451002.MRL, made by Littelfuse, Inc.

- Memory Battery: rechargeable Li-ion coin cell battery, model PD3048 by Route Jade (formerly Route JD or Korea Power Cell), 3.7 VDC, 300 mAh capacity. Dimensions: 30.0 mm diameter by 4.9 mm thick. See “Replacing the Memory Battery” on page 9-50.

- Standby Battery (included with the Mx-1-ME model): 7.2 Ah 12V rechargeable sealed lead-acid battery, made by Panasonic, part# LC-R127R2P (or LC-R127R2P1). (Two of these are wired in series to provide 24V.)

Design Considerations for the Mx-1 Controller

This section provides design and planning information about the Mx-1 one-door controller.

- ❑ The Mx-1 controller is packaged in a compact lightweight plastic case, can be powered by either PoE+ (providing a nominal 25.5 Watts) or 24 V - 28 V of DC power from an external power supply, and can be installed either “at the edge” (close to the door and readers) or stacked.
- ❑ The Mx-1-ME controller is packaged in a traditional metal enclosure with a locking door, a tamper switch, a power supply, a standby battery pack, and room for optional expansion boards. Controllers with this type of enclosure are typically located in a safe and secure area, such as an electrical room, telephone equipment room, closet, or the security operations office. The back of the metal enclosure has holes for attaching it to the studs in a wall. (Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet functionality which is included on the standard Mx-1 model.)
- ❑ An environmentally managed room is not required, because the Mx-1 controller can be operated in ambient temperatures of 0 degrees Centigrade (32 degrees Fahrenheit) to 60 degrees Centigrade (140 degrees Fahrenheit), with a maximum relative humidity of 90% (non-condensing).

In addition to monitoring, reporting, and controlling a variety of devices, an Mx-1 controller can typically power the attached entry reader and optional exit reader. Other devices, such as interior motion sensors and certain types of readers, may require power from a separate power supply.

If you are designing a security system that must meet certain standards (such as UL 294), see “UL Requirements” starting on page vii.

Electrical Ratings

An Mx-1 or Mx-1-ME controller has the following electrical ratings:

Table 9-10: Electrical Ratings of the Mx-1 or Mx-1-ME Controller's Components

Component	Specifications
Power Supply for the Mx-1	Either a UL-listed POE+ switch providing a nominal 25.5 Watts, or a UL-listed 2.0 A switching power supply at 110 - 240 V AC and 50/60 Hz providing 24 V - 28 V of DC power.
Power Supply for the Mx-1-ME	The Mx-1-ME controller includes a switching AC power supply (with 2.0 A at 110 - 240 V AC and 50/60 Hz), and two 12 V DC standby batteries connected in series to provide 7.2 Ah at 24 V DC. (Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet functionality which is included on the standard Mx-1 model.)
Wiegand reader terminals	Two 8-pin Wiegand reader terminals, fused and resettable, each providing 12 V DC power. Dedicated terminals are provided for the entry reader and the optional exit reader. On the Mx-1, these terminals provide up to 0.5 Amps each; on the Mx-1-ME, these terminals provide up to 0.355 Amps each. NOTE: The maximum simultaneous current draw for the Wiegand Entry Reader terminal and the Wiegand Exit Reader terminal is 0.75 Amps.

Table 9-10: Electrical Ratings of the Mx-1 or Mx-1-ME Controller's Components (Continued)

Component	Specifications
OSDP RS-485 readers terminal	One 5-pin OSDP RS-485 readers terminal, fused and resettable, providing 0.75 Amps at 12 V DC. (When an optional exit reader is needed, it is wired "through" the entry reader.)
Input sensor terminals	Two 3-pin input sensor terminals, used for an analog input such as the multi-state alarm inputs provided by the line module that detects changes in the status of a door's components (for example the position of the door contacts and the press of a Request to Exit button or the triggering of a motion detector). For more information, see "Line Modules" on page 2-75 and "Connecting Line Module Inputs" starting on page 7-21.
Door relay and Aux. relay terminals	Two 3-pin output relay terminals, one for the door, and one for the alarm or auxiliary devices. (For more information, see "Connecting Outputs" starting on page 7-23.) **Door Relay** • When the door relay is configured for **Wet Mode at 24V**, the Mx-1 supplies regulated power at 24 Volts, with a maximum output current of 0.25 Amps. (The maximum simultaneous current draw for the Door Relay and the Aux Relay is 0.5 Amps.) • When the door relay is configured for **Wet Mode at 12V**, the Mx-1 supplies regulated power at 12 Volts, with a maximum output current of 0.5 Amps. (The maximum simultaneous current draw for the Door Relay and the Aux Relay is 1.0 Amps.) • When the door relay is configured for **Dry Mode**, its maximum output current is 2.0 Amps, and the voltage is either 30 VDC or 250 VAC. **NOTE:** UL has only evaluated this relay for 30 VDC at 2 Amps for resistive and inductive loads. **Auxiliary Relay** • When the auxiliary relay is configured for **Wet Mode at 24V**, the Mx-1 supplies regulated power at 24 Volts, with a maximum output current of 0.25 Amps. (The maximum simultaneous current draw for the Door Relay and the Aux Relay is 0.5 Amps.) • When the auxiliary relay is configured for **Wet Mode at 12V**, the Mx-1 supplies regulated power at 12 Volts, with a maximum output current of 0.5 Amps. (The maximum simultaneous current draw for the Door Relay and the Aux Relay is 1.0 Amps.) • When the auxiliary relay is configured for **Dry Mode**, its maximum output current is 2.0 Amps, and the voltage is either 30 VDC or 250 VAC. **NOTE:** UL has only evaluated this relay for 30 VDC at 2 Amps for resistive and inductive loads.
Total Power available for Readers and Relays in wet mode	The output power that is available for peripheral devices depends on the input power that is supplied to the Mx-1 controller: • When the input power is **25.5 Watts** maximum f**rom POE+** (via the Ethernet jack), the maximum output power is 12.96 Watts. • When the input power is **24V DC x 2 Amps** from an external power supply (via the Power terminal), the maximum output power is 37.2 Watts. For more information, see "Mx-1 Controller Power Draw Capacity" starting on page 9-35.

Mx-1 Controller Design

The Mx-1 controller manages a single supervised door with an entry reader and an optional exit reader. The readers are connected either using the two Wiegand reader terminals, or using the OSDP RS-485 readers terminals. (When an exit reader is used with the Open Supervised Device Protocol (OSDP), it is wired "through" the entry reader, as shown in "Wiring Diagram for OSDP Readers" starting on page 9-40.)

Two input terminals are used for connecting analog inputs such as the multi-state alarm inputs provided by the line module that detects changes in the status of a door's components (for example the position of the door contacts and the press of a Request to Exit button or the triggering of a motion detector); a door relay terminal is used to control the door's locking mechanism (such as a magnetic lock or an electric strike); and an alarm relay terminal is used to control external alarm devices (such as activating an audible alarm, turning on lights, or initiating the recording of surveillance video).

An Mx-1 controller has built-in SNIB3 capability, so it includes an integrated Ethernet port for easy connection to the Velocity Server, and an RS-485 Chaining terminal for connection to other controllers on a SCRAMBLE*NET network. The functionality of the Command and Control Module (CCM) is also built into the main board (unlike previous controllers where the CCM was on a separate replaceable module).

The Mx-1-ME model also supports certain DIGI*TRAC expansion boards, as discussed in "Expansion Boards for an Mx-1-ME Controller" on page 9-25. The dimensions of the Mx-1-ME controller's metal enclosure and the Mx-1 controller's plastic case appear near the end of Table 9-1 earlier in this chapter.

NOTE: Do not install other equipment in the controller's enclosure. Doing so may cause intermittent operation, product damage, and void the manufacturer's warranty. Do not attempt to tap power for any devices other than those allowed.

Supplying Power to an Mx-1 Controller

The Mx-1 controller can be powered either through its POE+ Ethernet connector, or through its 2-pin Power terminal. When using POE+, it should be sufficient to power the controller and the readers, but you might need to provide an external power supply for the door's locking mechanism.

CAUTION: If you are using the POE+ Ethernet connector to supply power, you should not use the Power terminal to supply additional power.

NOTE: If the Mx-1 controller will be part of an access control system which must meet a particular UL standard, you must use a UL-listed power source or backup battery which provides the required duration of standby power for that standard. For more information, see the table about "Standby Power Requirements for Various UL Standards:" on page ix.

For the Mx-1-ME model, the 2-pin Power connector is wired to the included power supply (a UL-listed 2.0 A switching power supply at 110 - 240 V AC and 50/60 Hz providing 30 V of DC power) at the factory. Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet (PoE) functionality which is included on the standard Mx-1 model.

When using AC power, follow these guidelines:

- ❑ Locate the controller near a dedicated AC power source. A 15 Amp dedicated, unswitched circuit is required.

- ❑ If the power in the building is correctly grounded, there is no special grounding required for the controller.
- ❑ The entry point for the primary AC power is through the bottom or back of the enclosure. Connect AC power under the protective cover onto the supplied terminal strip, as shown in Figure 9-4, “Cable Inlets of the Mx-1-ME Controller’s Enclosure”, on page 9-32.

CAUTION: Before removing or replacing fuses, or before working on the Mx-1-ME’s standby battery pack connections, be sure to turn off the main power leading into the controller.

Separation of Circuits

The Class 1 high-voltage AC input power for an Mx-1-ME controller is routed through either one of the two knockouts at the bottom of the enclosure, while the cables for the controller's Class 2 circuits (such as inputs, Wiegand reader terminals, and OSDP reader terminals) are routed through several knock-outs located across the top and sides of the enclosure. This technique is shown in the following figure.

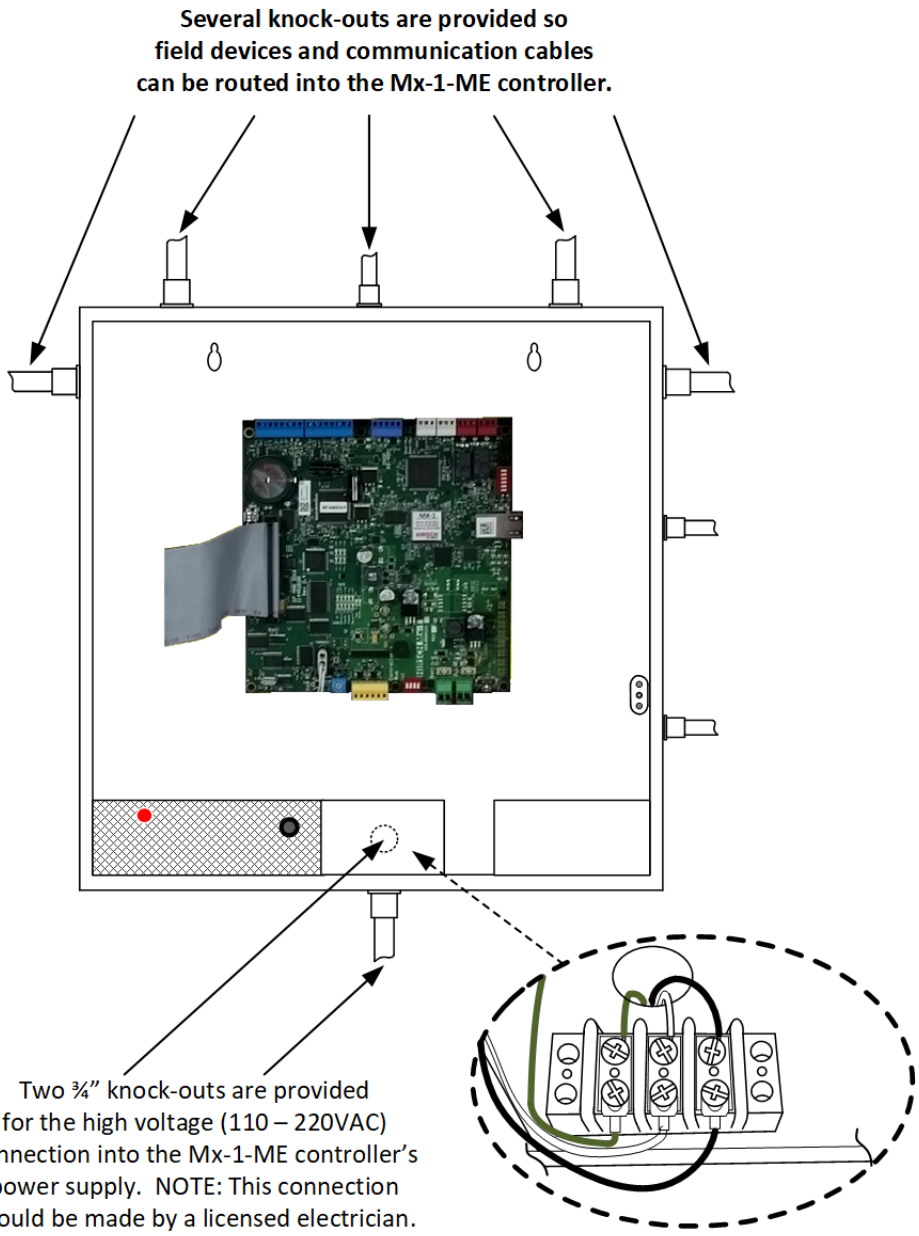


Figure 9-4: Cable Inlets of the Mx-1-ME Controller's Enclosure

The Mx-1-ME controller's Class 2 limited-power circuits include the following connections (as shown in Figure 9-2, "Mx-1 Controller Main Board Connectors and Components for Customer Use", on page 9-8):

- ❑ Two 3-wire analog Door Input and Aux. Input terminal blocks (for the line modules used to supervise doors, tamper circuits, and RQE devices).
- ❑ Two 8-wire terminal blocks (for connecting the wiring from a 12 VDC keypad or reader with a Wiegand interface). These are designed to support a variety of 125 kHz and 13.56 MHz readers and credentials.
- ❑ One 5-wire terminal block (for connecting the wiring from a 12 VDC keypad or reader with an OSDP RS-485 interface).
- ❑ One Expansion Board Connector (which is used to link any expansion boards mounted in the controller's enclosure to the controller's main board, using a flexible EBIC5 ribbon cable).
- ❑ One 6-pin RS-485 Controller Bus connector which can be used to create a chain of controllers, where the first (master) controller communicates directly with the Velocity Server using the POE+ Ethernet connector, and the other (downstream) controllers communicate along the chain using RS-485 wiring. Otherwise, an Mx-1 controller can communicate directly with the Velocity Server across a network using the POE+ Ethernet connector.

All reader circuits are protected by resettable thermal fuses, which automatically restore circuit integrity after the overcurrent has been removed. When routing the wires for the Class 2 limited-power circuits, make sure that you maintain a safe separation of at least 0.25 inches from the wires for the standby battery pack.

A complete list of the Mx-1-ME controller's Class 2 limited-power connectors is available in "ELECTRICAL SAFETY INFORMATION" which starts on page x.

NOTE: Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet (PoE) functionality which is included on the standard Mx-1 model.

Mx-1-ME Controller Standby Battery Capacity

The Mx-1-ME controller comes factory-equipped with a 24V 7.2Ah battery pack, which consists of two 12-volt batteries connected in series for a full 24-volt standby unit. (These sealed lead-acid batteries should not be fully depleted.)

If still more backup power is required, the provided internal standby battery can be replaced by larger-capacity external 24VDC batteries (up to a limit of 14 amp-hours), or by a charger and batteries (such as those made by AlarmSafe). A 120/240VAC UPS can also be tied into the main power, providing the controller with both surge protection and emergency power. (UL has not tested these configurations.)

When using external batteries or a charger and batteries, remember:

- ❑ When using an external battery pack, remove the controller's internal battery and connect the new power line into the unused standby battery input on the controller board. Remember: connecting two similar batteries in series doubles the voltage.
- ❑ When using a UPS, connect the UPS into the AC power line.

Use this formula to determine how much backup battery power a controller requires:

$$(I_{Devices} + I_{Controller}) \text{ x hours} = \text{Battery Life Required}$$

This is the sum of the load at 24VDC of all the attached devices plus the load at 24VDC of the controller itself, multiplied by the hours of battery operation required.

The next table provides the extended standby battery requirements (current draw in Amps) for the Mx-1-ME controller and several different Identiv TouchSecure readers, based on quiescent (idle) conditions.

Controller or Attached Device	Current Draw @ 24VDC	Remarks
Mx-1-ME controller	0.45 A	Normal operating current
TouchSecure Standard reader	0.075 A	These readers are rated at 12V. The current draw values shown at 24V assume 85% efficiency.
TouchSecure ScramblePad reader (non-illuminated)	0.09 A	
TouchSecure Keypad reader	0.14 A	
Normally Closed Relay (in Wet mode)	0.25 A	Assumes the Relay is always ON.

Table 9-11: Quiescent Current Draw for the Mx-1-ME Controller and Various TouchSecure Readers

For example, suppose an Mx-ME controller is connected to a door with a TouchSecure ScramblePad reader and a relay in Wet mode which is Normally Closed.

The installed example system's current draw is itemized:

Mx-1-ME = 0.45 A
TS-SP = 0.09 A
NC Relay = 0.25 A
Total = 0.79 A

A factory-installed 7.2 Ah battery pack could support this configuration for:

$$\frac{7.2 \text{ Amp-hours}}{0.79 \text{ A}} = \textbf{9.11 hours}$$

However, if you specify that the extended standby battery backup requirement must be at least 24 hours of operation without primary power, then:

0.79 A x 24 hours = 18.96 Amp-hours

Obviously the included 7.2 Ah battery pack is not sufficient for this extended requirement. To operate this system without primary power for a full 24 hours, you will need to provide either an external battery or a front-end UPS, with the necessary capacity.

Here is another example for an Mx-ME controller which connected to a TouchSecure ScramblePad reader (enabling two-factor authentication for entry) and a TouchSecure Standard reader (for card-only exit). This example system's current draw is:

Mx-1-ME = 0.45 A
TS-SP = 0.09 A
TS Standard = 0.075 A
Total = 0.615 A

The factory-installed 7.2 Ah battery pack could support this configuration for:

$$\frac{7.2 \text{ Amp-hours}}{0.615 \text{ A}} = \textbf{11.7 hours}$$

Power Provided at the Reader Terminals

An Mx-1 or Mx-1-ME controller provides 12VDC power at its two Wiegand reader terminals, and 12VDC at its RS-485 OSDP readers terminal. (For the Open Supervised Device Protocol (OSDP), when an optional exit reader is needed, it is wired "through" the entry reader.)

The following table shows the power provided for Wiegand and RS-485 OSDP keypads/readers by an Mx-1 or Mx-1-ME controller.

Table 9-12: Maximum Current Draws for an Mx-1 or Mx-1-ME Controller's Reader Terminals

Reader Terminal Type	Max. Current Draw per Terminal	Max. Simultaneous Current Draw per Controller
Wiegand	Mx-1: 0.5 Amps; Mx-1-ME: 0.355 Amps	0.75 Amps
RS-485 OSDP	0.75 Amps	0.75 Amps

Mx-1 Controller Power Draw Capacity

When planning to use Mx-1 controllers as part of your physical access security system, you must consider how to supply adequate power for each controller, its entry reader and optional exit reader, the door's access device (such as a magnetic lock or an electric strike), and any related optional devices for activating an audible alarm, turning on lights, or initiating the recording of surveillance video. This topic provides information about the power used by the Mx-1 controller and some Identiv TS readers, to help you determine whether you need to supply separate power for some of your peripheral devices.

The following table shows the current and power used by the Mx-1 controller, TS Scramblepad readers, and standard TS readers, when the controller's input power is either DC or PoE+, so you can determine whether there is sufficient power available for the door's access device (or whether you will have to provide separate power for that device).

Table 9-13: Maximum Current Draws for an Mx-1 Controller's Reader Terminals

Parameter	24V -28V DC Input		PoE+ Input		Notes
	Current	Power	Current	Power	
Starting input current and power	2.0 A	48 Watts	0.5 A	24 Watts	Either PoE+, or an external power supply providing 24 V - 28 V DC with a max of 2 Amps
Mx-1 controller in standby state	0.45 A	10.8 Watts	0.23 A	11.04 Watts	Power consumed by the Mx-1 controller alone (without any attached readers, and no relays in Wet mode)

Table 9-13: Maximum Current Draws for an Mx-1 Controller's Reader Terminals

Parameter	24V -28V DC Input		PoE+ Input		Notes
	Current	Power	Current	Power	
Power available for all peripheral devices	See the Notes	37.2 Watts	See the Notes	12.96 Watts	Peripheral devices include the attached readers and relays in Wet mode (for devices powered by the Mx-1). The current varies depending on which device is drawing power.
Power used by 2 TS Scramblepad readers (at 4.5 Watts each)	375 mA each (at 12 V out)	9 Watts	375 mA each (at 12 V out)	9 Watts	TS Scramblepad readers attached to the Wiegand Entry Reader terminal and the Wiegand Exit Reader terminal
Power available for relays when using 2 TS Scramblepad readers	—	28.2 Watts	—	3.96 Watts	TS Scramblepad readers attached to the Wiegand Entry Reader terminal and the Wiegand Exit Reader terminal
Power used by 2 standard TS readers (at 1.5 Watts each)	125 mA each (at 12 V out)	3 Watts	125 mA each (at 12 V out)	3 Watts	Standard TS readers attached to the Wiegand Entry Reader terminal and the Wiegand Exit Reader terminal
Power available for relays when using 2 standard TS readers	—	34.2 Watts	—	9.96 Watts	Standard TS readers attached to the Wiegand Entry Reader terminal and the Wiegand Exit Reader terminal

The following table shows the current provided by the Mx-1 controller to its Door relay and Aux. relay, when the controller's input power is either 24 V DC or PoE+, so you can determine whether there is sufficient current available for the devices controlled by those relays (or whether you will have to provide separate power for those devices), and you can determine the correct power mode jumper setting (either Wet at 24V, Wet at 12V, or Dry) for those relays.

Table 9-14: Current Provided for an Mx-1 Controller's Door Relay and Aux. Relay

Parameter	Current with 24V DC Input	Current with PoE+ Input	Notes
Door relay in Wet Mode at 24V	250 mA (at 24 V)	250 mA (at 24 V)	The door's access device (such as a magnetic lock or an electric strike) is powered by the Mx-1.
Door relay in Wet Mode at 12V	500 mA (at 12 V)	500 mA (at 12 V)	The door's access device (such as a magnetic lock or an electric strike) is powered by the Mx-1.
Door relay in Dry Mode	Up to 2.0 A (at 30 V)	Up to 2.0 A (at 30 V)	The door's access device (such as a magnetic lock or an electric strike) is externally powered.

Table 9-14: Current Provided for an Mx-1 Controller's Door Relay and Aux. Relay

Parameter	Current with 24V DC Input	Current with PoE+ Input	Notes
Aux. relay in Wet Mode at 24V	250 mA (at 24 V)	250 mA (at 24 V)	The external alarm or auxiliary device is powered by the Mx-1.
Aux. relay in Wet Mode at 12V	500 mA (at 12 V)	500 mA (at 12 V)	The external alarm or auxiliary device is powered by the Mx-1.
Aux. relay in Dry Mode	Up to 2.0 A (at 30 V)	Up to 2.0 A (at 30 V)	The external alarm or auxiliary device is externally powered.

Typical Connections

Like DIGI*TRAC Controllers, the Mx-1 controller can connect to a number of input and output devices. For details, see the following topics:

- ❏ "Typical Line Module Inputs" on page 2-12
- ❏ "Typical Door Relay Outputs" on page 2-13

When referring to those topics, note that the layout of the Mx-1 controller's terminals (as shown in Figure 9-2 on page 9-8) is different from the layout of the terminal blocks of the DIGI*TRAC M2 or M8 Controller.

All interconnecting devices must be UL Listed, low-voltage Class 2 power limited.

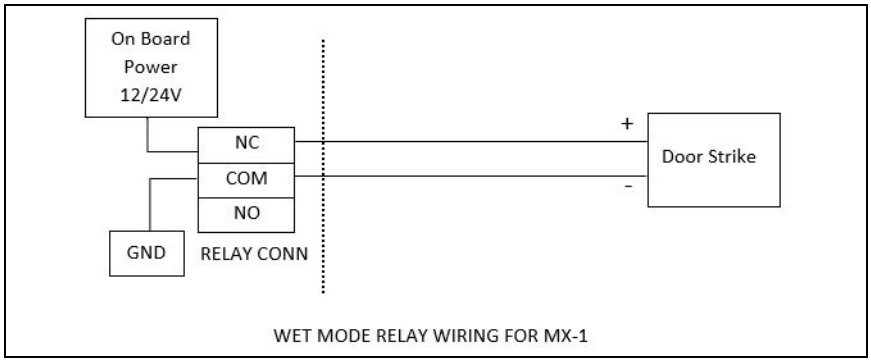
Wiring for the Door

An Mx-1 controller provides the following terminals for the door:

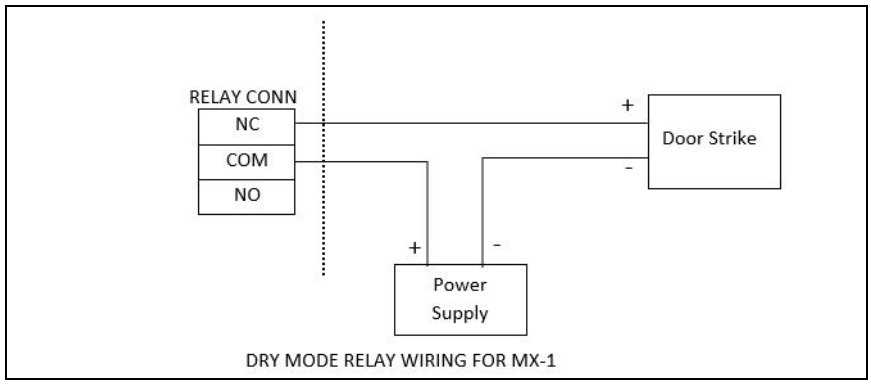
- ❏ Two 8-pin Wiegand reader terminals for connecting readers or keypads which have a Wiegand interface.
- ❏ A 5-pin OSDP RS-485 Readers terminal for connecting keypads or readers which have an OSDP RS-485 interface. (Only one of these terminals is needed, because when the door has an optional exit reader with an OSDP RS-485 interface, it is wired "through" the entry reader with an OSDP RS-485 interface.)
- ❏ A 3-pin Door Input terminal for analog inputs such as multi-state alarm inputs from the line module. (There is also a 3-pin Aux. Input terminal which can be used for a second analog input.)
- ❏ A 3-pin Door Relay terminal for two-state outputs such as a magnetic lock or electric strike.

  The following diagrams show the basic wiring for a normally closed electric door strike when it is connected to an Mx-1 controller in either:

  - Wet Mode, where power is supplied by the Mx-1, or
  - Dry Mode, where power is provided by an external power supply.



WET MODE RELAY WIRING FOR MX-1



DRY MODE RELAY WIRING FOR MX-1

- A 3-pin Aux. Relay terminal which can be used to control external alarm or auxiliary devices, such as activating an audible alarm, turning on lights, or initiating the recording of surveillance video.)

The number and types of readers you will be using on the door dictates which reader terminals you need to use:

- For only an entry reader with a Wiegand interface, use the Wiegand Entry Reader terminal.
- For only an entry reader with an OSDP RS-485 interface, use the OSDP RS-485 Readers terminal.
- For an entry reader and an exit reader, both with a Wiegand interface, use the Wiegand Entry Reader terminal for the entry reader and use the Wiegand Exit Reader terminal for the exit reader. For details, see “Wiring Diagram for Wiegand Readers” on page 9-40.
- For an entry reader and an exit reader, both with an OSDP RS-485 interface, use the OSDP RS-485 Readers terminal, with the exit reader wired “through” the entry reader. For details, see “Wiring Diagram for OSDP Readers” starting on page 9-40.
- For an entry reader with an OSDP RS-485 interface and an exit reader with a Wiegand interface, use the OSDP RS-485 Readers terminal for the entry reader and use the Wiegand Exit Reader terminal for the exit reader.

CAUTION: To avoid possible damage to your Mx-1 controller, make sure it is powered off before you add or remove a reader connected to a Wiegand terminal.

The following figure shows a typical wiring configuration for a door managed by an Mx-1 controller, where an entry reader is required on the outside of the protected area, and a Request To Exit button (or a motion detector) is used on the inside to leave the protected area. Note that if the protected area is an anti-passback zone, you will instead need to use an exit reader on the inside of the protected area.

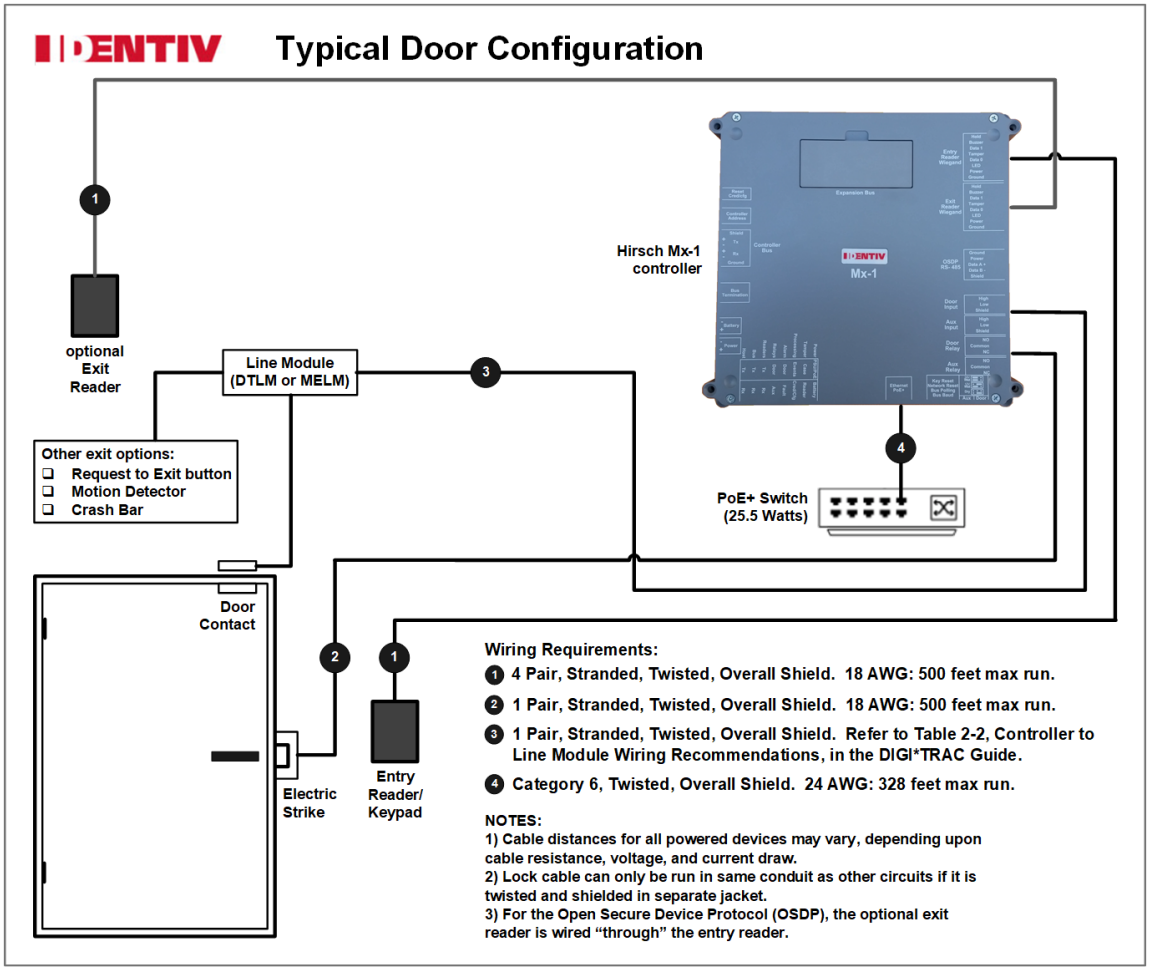


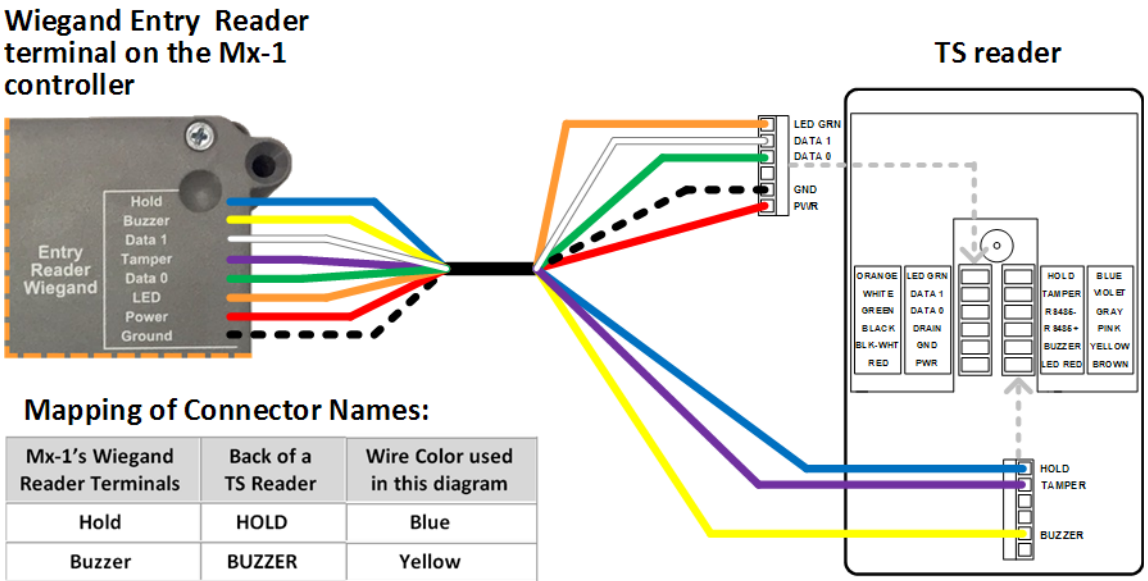
Figure 9-5: Typical Wiring Configuration for a Door Managed by an Mx-1 Controller

For a more detailed wiring diagram, see the **Mx-1 Quick Install Guide**.

NOTE: Always refer to the actual wiring diagram provided with the specific reader that you are installing.

Wiring Diagram for Wiegand Readers

The following wiring diagram shows how to connect a TS reader to an 8-pin Wiegand terminal on an Mx-1 controller.



Mapping of Connector Names:

Mx-1's Wiegand Reader Terminals	Back of a TS Reader	Wire Color used in this diagram
Hold	HOLD	Blue
Buzzer	BUZZER	Yellow
Data 1	DATA 1	White
Tamper	TAMPER	Violet
Data 1	DATA 1	Green
LED	LED GRN	Orange
Power	PWR	Red
Ground	GND	dashed Black

NOTE: The wiring is identical for an optional exit reader; just use the terminal on the Mx-1 controller marked **Exit Reader Wiegand.**

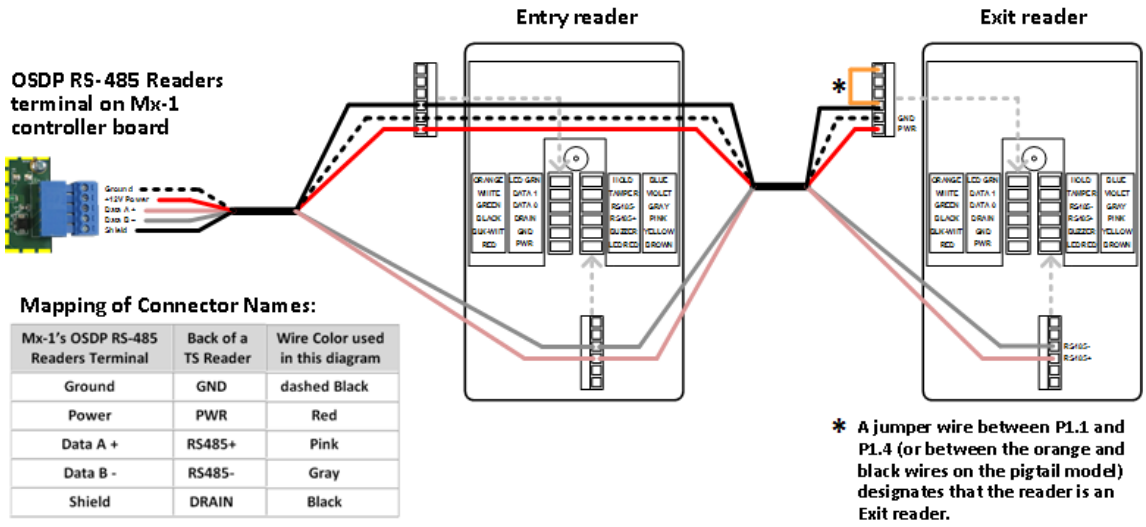
Figure 9-6: Example Wiring Diagram for a Wiegand Reader Connected to an Mx-1 Controller

Wiring Diagram for OSDP Readers

The following figure shows an example wiring diagram for an Mx-1 controller and a pair of Identiv's OSDP readers, which are the entry reader and the optional exit reader for a door. Note that:

- ❑ The exit reader is wired "through" the entry reader for a door, so it shares the OSDP RS-485 Readers terminal on the Mx-1 controller.
- ❑ On the exit reader, a jumper wire is needed between P1.1 and P1.4 (or between the orange and the black wires on the pigtail model) to designate that it is the exit reader. For details, see "Example Wiring Diagram for an RREB" on page 2-29.
- ❑ The correct value for the OSDP Address field in the Velocity software depends on the reader's manufacturer, and whether the reader is used for entry or exit. For example:
  - An Identiv reader's address should be set to 0 when it is the door's entry reader, and set to 1 when it is the door's optional exit reader.
  - A Veridt reader's address should be set to 1 when it is the door's entry reader, and set to 2 when it is the door's optional exit reader. (Values 3 through 126 are not used; a unique address is derived from the RS-485 port number on the RREB in a particular controller.)

- The diagram shows power being supplied to the readers from the Mx-1 controller. But depending on the types and quantity of readers (and other devices) being used, you might need to power some of the remotely located readers from an external power supply. For more information, see "Power Provided at the Reader Terminals" on page 9-35.



Mapping of Connector Names:

Mx-1's OSDP RS-485 Readers Terminal	Back of a TS Reader	Wire Color used in this diagram
Ground	GND	dashed Black
Power	PWR	Red
Data A +	RS485+	Pink
Data B -	RS485-	Gray
Shield	DRAIN	Black

Figure 9-7: Example Wiring Diagram for OSDP Readers Connected to an Mx-1 Controller

Setup and Installation of an Mx-1 Controller

Because the Mx-1 controller can be operated in ambient temperatures of 0 degrees Centigrade (32 degrees Fahrenheit) to 60 degrees Centigrade (140 degrees Fahrenheit) with a maximum relative humidity of 90%, an environmentally managed room is usually not required. The controller is typically installed indoors, within the protected premises.

Overall, the setup and installation of an Mx-1-ME controller is similar to that of most DIGI*TRAC controllers. For example, all the information in "General Connection Rules and Procedures" starting on page 7-10 still applies, except that you don't have to worry about blocking the printer port (because an Mx-1 or Mx-1-ME controller doesn't have one).

The Mx-1 model has a compact plastic case, and can be powered by either PoE+ (providing a nominal 25.5 Watts) or 24 V - 28 V of DC power from an external power supply. Its light weight provides more flexibility when deciding where to install it.

Most of the information in "Controller Installation" starting on page 7-17 in the DIGI*TRAC Guide also still applies, with the following differences:

- In "Controller Set Up" on page 7-17, note that an Mx-1 controller has built-in SNIB3 capability which must be configured using DIP switches. For information about setting those DIP switches, refer to "Configuring the Built-In SNIB3" on page 9-43.
- In "Mounting the Controller" on page 7-17, note that an Mx-1-ME model has the same type of enclosure as an M2 DIGI*TRAC controller or an Mx-2/4/8 controller (with a locking door, a tamper switch a power supply, a standby battery, and room for optional expansion boards).
- In "Wiring to the Controller" on page 7-18, note that an Mx-1-ME controller's status LEDs are much smaller and are located in the center of the main board, as shown in Figure 9-2 on page 9-8. (A new set of large LEDs is provided on the Mx-1 controller's main board; see "Status LEDs on the Mx-1" on page 9-18.)
- In "Upgrading the CCM" starting on page 7-27, note that the functionality of the Command and Control Module (CCM) is built into the Mx-1 controller's main board (instead of being on a separate removable module).

Wiring Distance Limits

The following table shows the wiring distance limits between the Mx-1 controller and various components, which is important information when you are designing a security system for a large facility.

Table 9-15: Maximum Current Draws for an Mx-1 Controller's Reader Terminals

Type of Wired Connection	Maximum Distance
RS-485 data only (between two controllers, or between a controller and an OSDP reader) using 22 gauge wires	4,000 feet (1,220 meters) (tested under lab conditions)
Wiegand protocol using 18 gauge wires	500 feet (150 meters)

Note that the wires must be stranded and pair twisted, with an overall shield.

Configuring the Built-In SNIB3

An Mx-1 controller has built-in SNIB3 capability, with a 5-wire RS-485 Controller Bus terminal that enables multi-drop or long hardwired serial connections, and an Ethernet/PoE+ connector for communication between the Velocity host and the master controller. For information about SNIB3 functionality, see “SNIB3” on page 2-40 and “Benefits of the SNIB3” on page 2-41.

To install a set of controllers connected using SNIB3s or built-in SNIB3 capability, perform the following procedure:

1. Run the required network cable to the controller(s) with the master SNIB3s.

   The Category 6 Ethernet cable you are connecting to each master SNIB3 should be connected to the Velocity host through a hub or switch.

2. Run RS-485 cable downstream from the master SNIB3.

   The run between the master SNIB3 and the second SNIB3 must be wired according to the instructions in “RS-485 Cabling for SNIB3s” on page 7-80.

3. Set the DIP switches on each SNIB3, which vary depending on whether it is the master, one in the middle, or the last one. On an Mx-1 controller, be sure to also set its SNIB3 address using the rotary switch.

   For details, see “DIP Switches on an Mx-1 Controller” on page 9-44.

4. Plug the end of the Category 6 cable into the Ethernet/PoE+ connector on the Mx-1 controller.
5. Connect the RS-485 cables to their respective SNIB3.
6. Reconnect and power up the controllers.
7. At the host, open Velocity and configure the new SNIB3s.

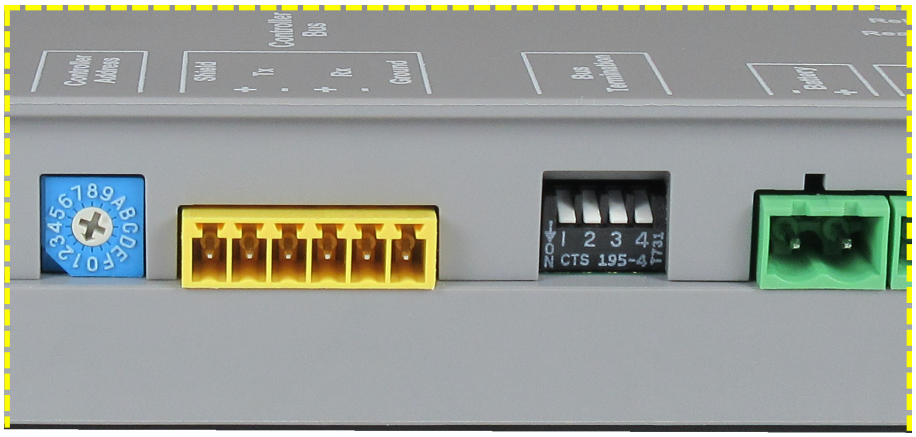
For more information about the SNIB3, refer to “Installing and Configuring the SNIB3” starting on page 7-72.

DIP Switches on an Mx-1 Controller

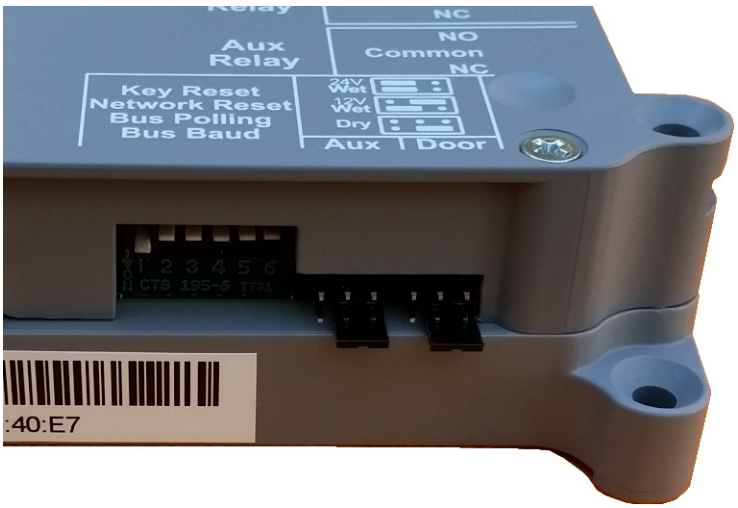
A SNIB3 expansion board includes three DIP switch banks. The first bank (SW1) and second bank (SW2) have four DIP switches each. The third bank (SW3) has eight DIP switches. The location of the three banks of DIP switches on a SNIB3 expansion board is shown in Figure 2-30, “Main Components of the SNIB3 Board”, on page 2-40.

Things are somewhat different for the built-in SNIB3 capability of an Mx-1 controller.

- The bank of four switches on the left side of the Mx-1 controller, which is marked **Bus Termination** on the top cover of the plastic casing, corresponds to the SW1 bank on the SNIB3.



- The second bank of switches on the right side of the front of the Mx-1 controller has six DIP switches, which correspond to the SNIB3’s four-switch SW2 and the first two switches of its SW3. The labeling which appears on the top cover of the plastic casing for this bank of switches is shown in the following image:



- While the SNIB3 required you to set its address using the last six DIP switches of its SW3, the address of the Mx-1 controller’s built-in SNIB3 is more easily set using the **Controller Address** 16-position rotary switch, located on the left side of the Mx-1 controller.

Bus Termination (SW1)

With their built-in SNIB3 capability, Mx-1 controllers can be used throughout an RS-485 multidrop run; however, you must specify whether a specific Mx-1 controller is at the beginning, middle, or end of a run.

To do this, set all four DIP switches on the **Bus Termination** switch bank to either all ON or all OFF, with this meaning:

S1 - S4	OFF	This Mx-1 controller is in the middle of a multidrop sequence.
	ON	This Mx-1 controller is either the first (master) or last (termination) one in the multidrop sequence.

Key Reset / Network Reset / Bus Polling / Bus Baud (SW2)

The second switch bank on the Mx-1 controller has six DIP switches, where S1 configures encryption properties, S4 configures the Mx-1 controller's location in the multidrop run, and S5 and S6 specify the built-in SNIB3's communications speed. (S2 and S3 are used to reset a SNIB3 to its factory default settings.)

S1	**OFF**	The Mx-1 controller's built-in SNIB3 communicates with the host PC using the encryption keys stored in memory.
	ON	Return the encryption keys to their default settings. If this switch is set when the Mx-1 controller's built-in SNIB3 powers up or reboots after a firmware upgrade, the keys reset This switch should be turned off after the LED patterns begin to light. You must also check the '**Reset Encryption**' option on the Port settings in Velocity.
S2 - S3	**OFF**	Normal operation.
	ON	These switches should only be ON when resetting this built-in SNIB3 to the factory default settings; see "Resetting a SNIB3 to its Factory Default Values" starting on page 7-93.
S4	OFF	Indicates this controller is NOT first in the multidrop sequence.
	ON	Indicates this controller is first in the sequence (master), and is connected to the host via Ethernet. This controller' built-in SNIB3 controls polling.
S5 - S6		These switches specify the built-in SNIB3's communications speed. • For a baud rate of 9,600 set S5 OFF and set S6 OFF. • For a baud rate of 38,400 set S5 OFF and set S6 **ON**. • For a baud rate of 57,600 set S5 **ON** and set S6 OFF. • For a baud rate of 115,200 set S5 **ON** and set S6 **ON**.

NOTE: 57,600 and 115,200 bps are only available if your RS-485 cables are made from Cat5/Cat6 data grade wire. These speeds are not recommended for installations using:

- ❑ 18-gauge to 22-gauge shielded twisted-pair cable
- ❑ NET*MUX4s

Baud rates only apply to the RS-485 ports for SNIB2s and SNIB3s. All SNIB2s and SNIB3s in an RS-485 multi-drop chain must be set to the same baud rate.

The address of the Mx-1 controller's built-in SNIB3 is set using the **Controller Address** 16-position rotary switch.

The Mx-1 controller's Ethernet/PoE+ port is used for host-to-controller connections and runs at 10/100/1G BaseT speeds. (Because the Mx-1-ME model includes a power supply, its Ethernet connection does not include the Power over Ethernet functionality which is included on the standard Mx-1 model.)

Network Configuration Options for the Built-In SNIB3

Most DIGI*TRAC controllers can be networked together and managed by a computer running Velocity, if they use an optional SNIB2 or SNIB3 expansion board. For details, see "SNIB3 Network Configuration Options" starting on page 7-78.

An Mx-1 controller can be included in that network. The primary difference is that an Mx-1 controller does not require a SNIB3 expansion board, because the Ethernet connector and the RS-485 Controller Bus terminal are integrated onto the controller's main board, as shown in Figure 9-2 on page 9-8.

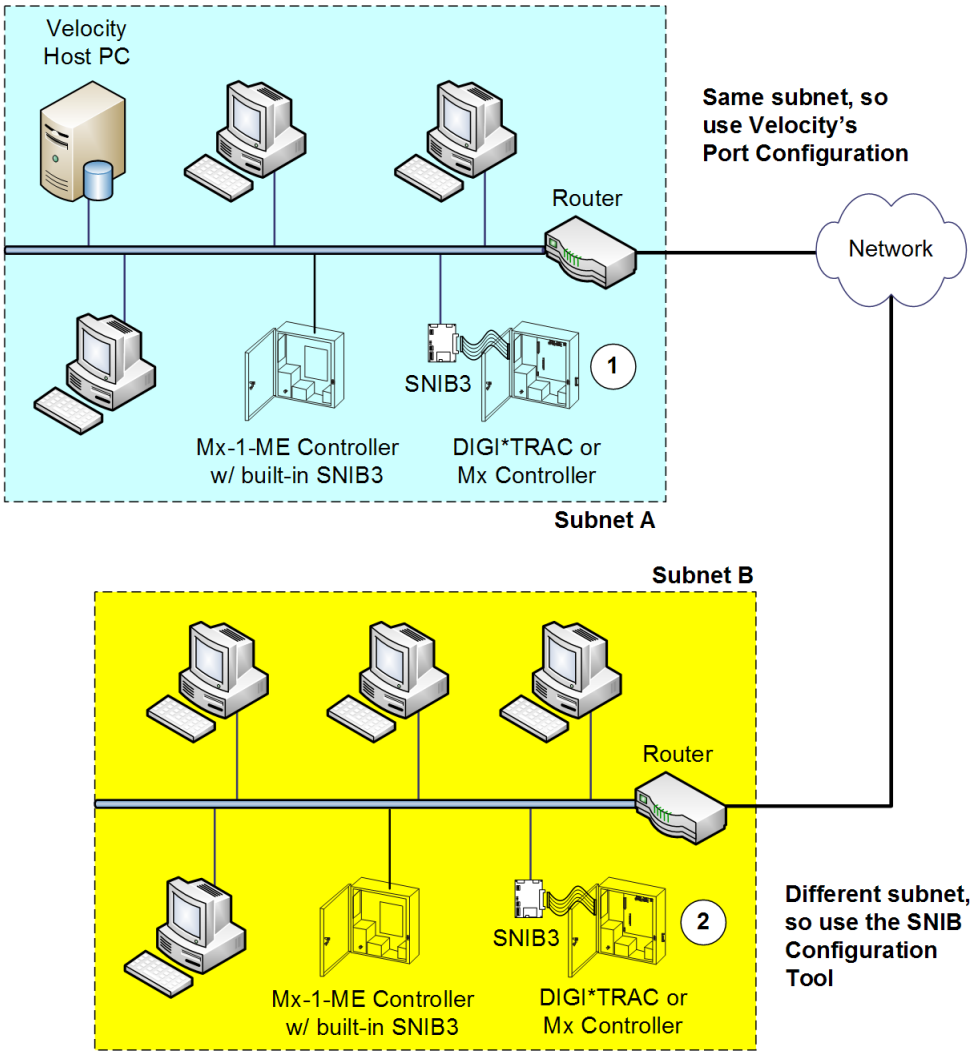
Deploying the Built-In SNIB3

Each master SNIB3 (Velocity port) must be assigned a unique IP address so it can communicate with the Velocity Server. Depending on the network location of the master SNIB3, this is accomplished in one of two ways:

- ❑ If the SNIB3 is located within the same subnet as the host PC, then you can use Velocity to assign the IP address. For more about this, refer to "Using Velocity to Configure a SNIB3 on the Same Subnet" starting on page 7-86.
- ❑ If the master SNIB3 is located outside the host PC's subnet, you must use the SNIB Configuration Utility. For more about this, refer to "Configuring a SNIB3 on a Different Subnet" starting on page 7-89.

What is a subnet? Put simply, it is any group of PCs and other devices, such as printers and scanners, connected by network cable to a network router. Anything behind the router

is considered part of the subnet. Anything beyond this router is not part of the subnet.



In the preceding illustration, the master SNIB3 on the Mx controller labeled 1 is located in the same subnet as the host PC (Subnet A). This SNIB3 can therefore be configured using Velocity; however, the master SNIB3 on the Mx controller labeled 2 is located behind a different router, in a different subnet (Subnet B), and must be configured using the SNIB Configuration Utility.

Any number of computers and devices can be behind a single router, but for reasons of security and speed, a company network often incorporates many routers. It isn't uncommon to find that each department within a company has its own router. Routers not only find the quickest way to ferry packets of information between two points, but also could serve as a rudimentary firewall against potential intrusion.

Mx-1 Controller Configuration Worksheet

The following figure provides a worksheet for an Mx-1 Controller, to help you plan your security system. (The worksheet for the Mx controller is provided in Figure 8-7 on page 8-32. Worksheets for other system components are provided in Appendix A.)

Mx-1 Controller Configuration Worksheet

Controller Name: _____ **Description:** _____

Address (1-15): _____

Time Zone of Location: _____

Communications Port Name: _____ **Protocol:** ◯ X*NET2 or ◯ X*NET3

When the Network Type is **IPv4**:

IPv4 address: ___.___.___.___

IP Port: _____ (10001 is default)

Subnet Mask: ___.___.___.___

Default Gateway: ___.___.___.___

Max retry attempts: ____ (0=infinite)

When the Network Type is **IPv6**:

IPv6 address: ____:____:____:____:____:____:____:____

IP Port: _____ (10001 is default)

Subnet Prefix length: _____

Default Gateway: ____:____:____:____:____:____:____:____

Max retry attempts: ____ (0=infinite)

Readers / base Inputs / base Relays

Entry Reader: _____

Exit Reader: _____

Door Input: _____

Aux. Input: _____

Door Relay: _____

Aux. Relay: _____

Jumper setting for relay power:

◯ Wet mode at 24V

◯ Wet mode at 12V

◯ Dry mode

Expansion Capability (available only for the Mx-1-ME model)

Board 1: ☐ **Board 2:** ☐ **Board 3:** ☐ **Board 4:** ☐ **Board 5:** ☐

Expansion Inputs (Red Icons = Installed; Black Icons = not installed)

XI01-	XI02-	XI03-	XI04-	XI05-	XI06-	XI07-	XI08-
XI09-	XI10-	XI11-	XI12-	XI13-	XI14-	XI15-	XI16-
XI17-	XI18-	XI19-	XI20-	XI21-	XI22-	XI23-	XI24-
XI25-	XI26-	XI27-	XI28-	XI29-	XI30-	XI31-	XI32-

Expansion Relays\Virtual Relays (Red Icons = Installed; Black Icons = not installed)

XR01-	XR02	XR03-	XR04-	XR05-	XR06-	XR07-	XR08-
XR09-	XR10-	XR11-	XR12-	XR13-	XR14-	XR15-	XR16-
XR17-	XR18-	XR19-	XR20-	XR21-	XR22-	XR23-	XR24-
XR25-	XR26-	XR27-	XR28-	XR29-	XR30-	XR31-	XR32-
XR33-	XR34-	XR35-	XR36-	XR37-	XR38-	XR39-	XR40-
XR41-	XR42-	XR43-	XR44-	XR45-	XR46-	XR47-	XR48-
XR49-	XR50-	XR51-	XR52-	XR53-	XR54-	XR55-	XR56-
XR57-	XR58-	XR59-	XR60-	XR61-	XR62-	XR63-	XR64-

Figure 9-8: Mx-1 Controller Configuration Worksheet

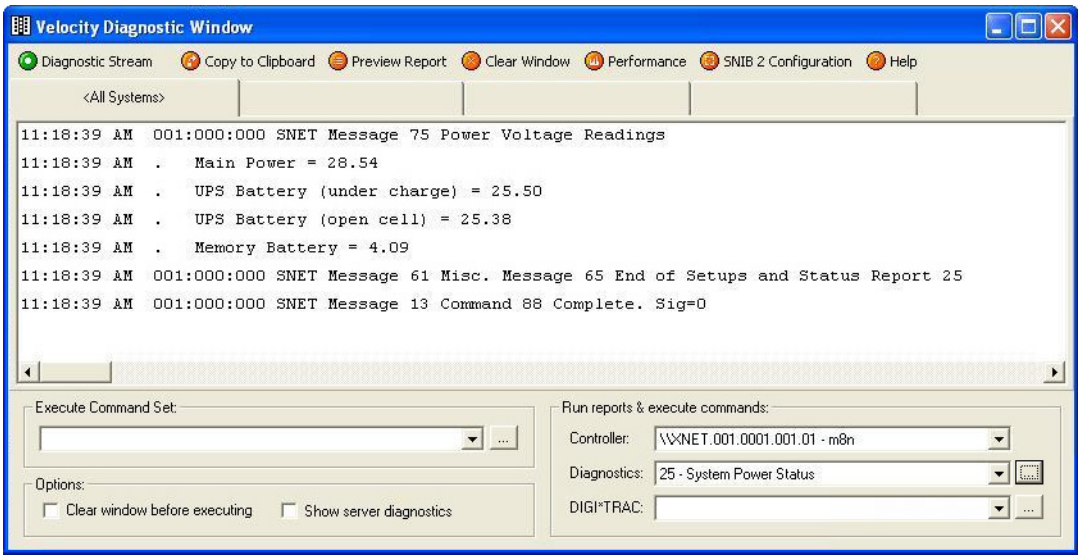
Performing Periodic Maintenance

The Mx-1 or Mx-1-ME controller was designed to be a reliable long-lasting product, with periodic maintenance consisting of these tasks:

- ❑ if you are obtaining power from PoE+, occasionally testing that the voltage is within specifications
- ❑ gathering diagnostic information (including the voltage status of the standby battery and the memory battery) once every 6 months
- ❑ visually inspecting the controller once every year for signs of:
  - exposed wires or loose connections
  - corrosion around the battery terminals
  - damaged battery leads
- ❑ replacing the memory battery when necessary (after several years)
- ❑ replacing the Mx-1-ME's standby battery pack when necessary (after several years)

Gathering Diagnostic Information

The Velocity software includes a Diagnostic Window which enables you to gather diagnostic information about a connected controller. To access this tool, click Velocity's menu button, and then select **Diagnostics/Reporting > DIGI*TRAC Diagnostic Window**.



To gather information about a controller:

1. Select the desired controller from the **Controller** drop-down list.
2. Select the appropriate diagnostic command from the **Diagnostics** drop-down list.

   This list includes all the basic 88 command options, such as 25 - System Power Status (of the AC input power, the standby battery, and the memory battery). For more information, see "CMD 88: PRINT SYSTEM SETUPS AND STATUS" starting on page 4-110.
3. Click the button located just to the right of the **Diagnostics** drop-down list.

The information generated by the selected command is displayed in the Results pane.

To learn more about Velocity's Diagnostic Window, see the topics in the **Diagnostic Window** section of Velocity's help system.

Interpreting the System Power Status Information

The results of the 25 - System Power Status diagnostics command are somewhat cryptic. Here is what those results mean for an Mx-1 controller (starting with the 7.6.20 release of the CCM/CCMx firmware). Because an Mx-1 controller can be powered by a combination of PoE+ and AC power, it is able to operate within a broader range of power levels.

Main Power: This is the voltage of the main power after it has been transformed from AC to DC. The normal range when using AC input is 22 - 26 VDC. The normal range when using PoE+ is 13 - 22 VDC. AC Low is reported when the voltage is 11 - 13 VDC, and AC Failure is reported when the voltage is less than 11 VDC.

UPS Battery: This is the DC voltage of a connected standby battery pack or Uninterruptible Power Supply. The "under charge" number shows the voltage when the standby battery is being charged. The "open cell" number shows the voltage when the charging circuit is bypassed. The normal range is above 23 VDC. The voltage is considered Low when it is 17 - 23 VDC. When the voltage is less than 6 VDC, the battery is considered to be Bad and UPS Failure is reported. A weak battery will have a high "under charge" number and a low "open cell" number.

Memory Battery: This is the DC voltage of the memory protection battery, which provides up to 10 days protection of the controller's data. The normal range is 3.47 - 4.5 VDC. If the value remains below 3.47 VDC, the memory battery should be replaced.

Replacing the Memory Battery

The Mx-1 or Mx-1-ME controller's memory battery is a rechargeable Li-ion coin cell battery that supplies backup power to the controller's memory, so critical information is not lost during a power outage of up to 10 days. That information includes user credentials, configuration, and date/time.

NOTE: If the Mx-1 controller will be part of an access control system which must meet a particular UL standard, you must include a UL-listed UPS or backup battery which provides the required duration of standby power for that standard. For more information, see the table about "Standby Power Requirements for Various UL Standards:" on page ix.

This memory battery should provide several years of reliable service, but will eventually have to be replaced when its voltage remains below 3.00 VDC. The location of this battery on the Mx-1 controller's main board is shown in Figure 9-2 on page 9-8.

The battery installed at the factory is model PD3048 by Route Jade (formerly Route JD or Korea Power Cell), which provides 3.7 VDC, and has a 300 mAh capacity. Its dimensions are 30.0 mm in diameter by 4.9 mm thick. When diagnostic information determines that there is a problem with the performance of the memory battery, you should replace it with a battery that has equivalent specifications.

NOTE: The controller's power should remain on while you replace its memory battery.

If the Mx-1 controller lost data because you replaced the memory battery while the main board was disconnected from both the main AC power and the standby battery power, you can easily download its data again using Velocity. In the Administration pane of Velocity's main window, locate the controller in the system tree, right-click on the controller, and select each of the following commands from the pop-up menu:

❑ **Download > Date/Time**

- ❑ **Download > Configuration**
- ❑ **Download > Credentials**

After these three downloads have completed successfully, the Mx-1 controller is ready to use again.

Worksheets

A

The worksheet for the Mx controller is provided in Figure 8-7 on page 8-32.

The worksheet for the Mx-1 controller is provided in Figure 9-8 on page 9-48.

This Page Intentionally Left Blank

STANDARD TIME ZONE WORKSHEET

TZ0 = never / TZ1 - 64 programmable / TZ65 = Always

TIME ZONE	ZONE NAME	START TIME	END TIME	DAYS ACTIVE							
				M 1	T 2	W 3	Th 4	F 5	S 6	S 7	H 8

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 52 * Standard TZ * HHMMS * HHMME * 012345678 #*

HOLIDAY WORKSHEET

Holidays 1 - 30 programmable / 31 - 32 daylight savings control only

HOLIDAY	MMDDYY	HOLIDAY	MMDDYY	HOLIDAY	MMDDYY	HOLIDAY	MMDDYY
1		9		17		25	
2		10		18		26	
3		11		19		27	
4		12		20		28	
5		13		21		29	
6		14		22		30	
7		15		23		31 forward 1 hr.	
8		16		24		32 backward 1 hr.	

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 57 * Holiday * MMDDYY #*

STANDARD ACCESS ZONE WORKSHEET

1 TIME ZONE ALL DOORS

AZ0 = never / AZ 1 - 64 programmable / AZ 65 = Always

AZS	ZONE NAME	TZ	DOORS							
			1	2	3	4	5	6	7	8

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 17 * AZ * TZ * DOORS #*

STANDARD ACCESS ZONE WORKSHEET

1 TIME ZONE PER DOOR

AZ 0 = never / AZ 1 - 64 programmable / AZ 65 = Always

AZS	ZONE NAME	TIME ZONE PER DOOR - DOOR BY DOOR							
		1	2	3	4	5	6	7	8

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 24 * AZ * TIME ZONE FOR DOOR 1 * • • TIME ZONE FOR DOOR 8 #*

USER LOG - STANDALONE SYSTEMS

User 0 = System Code / Users 1 - 999 Programmable (expandable to 4,000 or 16,000)

ISSUE DATE	USER NAME	USER NUMBER	USER FUNCTION	ID TYPE	ID FORMAT	CODE	CARD NUMBER	AZ/CZ ZONE

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	

MASTER ACCESS ZONE WORKSHEET

AZM 66 = 127 Programmable

AZM	ZONE NAME	STANDARD ACCESS ZONES INCLUDED COLUMNS							
		1	2	3	4	5	6	7	8

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 204 * STANDARD AZ * MASTER AZ * COLUMN #*

MASTER TIME ZONE WORKSHEET

TZM 66 - 129 PROGRAMMABLE

TZM	ZONE NAME	STANDARD TIME ZONES INCLUDED COLUMNS							
		1	2	3	4	5	6	7	8

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 54 * STANDARD TZ * MASTER TZ * COLUMN #*

GRAND MASTER TIME ZONE WORKSHEET

TZG 130 - 149 PROGRAMMABLE

TZG	ZONE NAME	STANDARD AND/OR MASTER TIME ZONES INCLUDED COLUMNS							
		1	2	3	4	5	6	7	8

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 154 * MASTER TZ * GRAND MASTER TZ * COLUMN #*

STANDARD CONTROL ZONE WORKSHEET

CZ 0 = NEVER CZ 1 - 191 PROGRAMMABLE

CZS	ZONE NAME	TZ	RELAY OR LINE MODULE INPUTS								EXPANSION RELAYS OR LINE MODULE INPUTS															
			1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 45 * CZ * TZ * RELAY OR LINE MODULE INPUT #* *START 301 * X-LINE MODULE/XRELAY * CZ S #*

CONTROL ZONE WORKSHEET FOR UP TO 64 EXPANSION RELAYS

CZ 0 = NEVER CZ 1 - 191 PROGRAMMABLE

CZ	ZONE NAME	TZ	EXPANSION LINE MODULE INPUTS								EXPANSION RELAYS															
			1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
			9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
											33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
											49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 45 * CZ * TZ * RELAY OR ALARM POINTS #* *START 301 * X-LM/X-RELAY * CZ S #*

ADD EXPANSION LINE MODULE INPUTS TO A STANDARD ACCESS ZONE WORKSHEET

AZ 0 = NEVER AZ 1 - 64 PROGRAMMABLE / AZ 65 = ALWAYS

AZS	ZONE NAME	TZ	EXPANSION LINE MODULE INPUTS															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

DO NOT WRITE ON THIS MASTER, MAKE COPIES.

Date:	**System Type & Name:**
Programmer:	**Command:** *START 03 * 11 * 1/0 * ADDR * [ADDR] # START 17 * AZ * TZ * DOORS # START 201 * X-LINE MODULE INPUT * AZ # START 203 * TZ * AZ #*

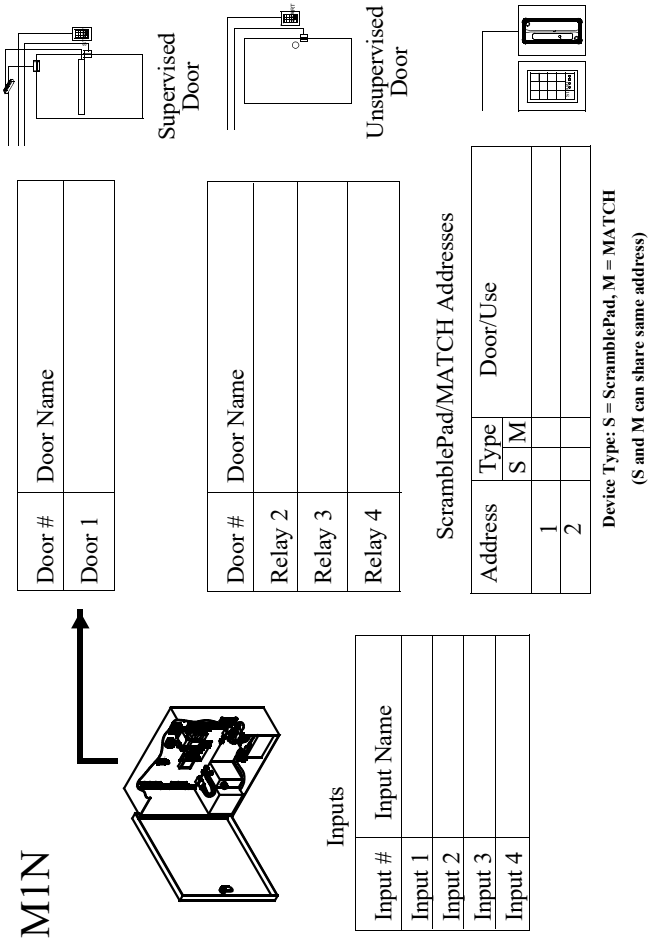


Figure A-1: M1N Worksheet

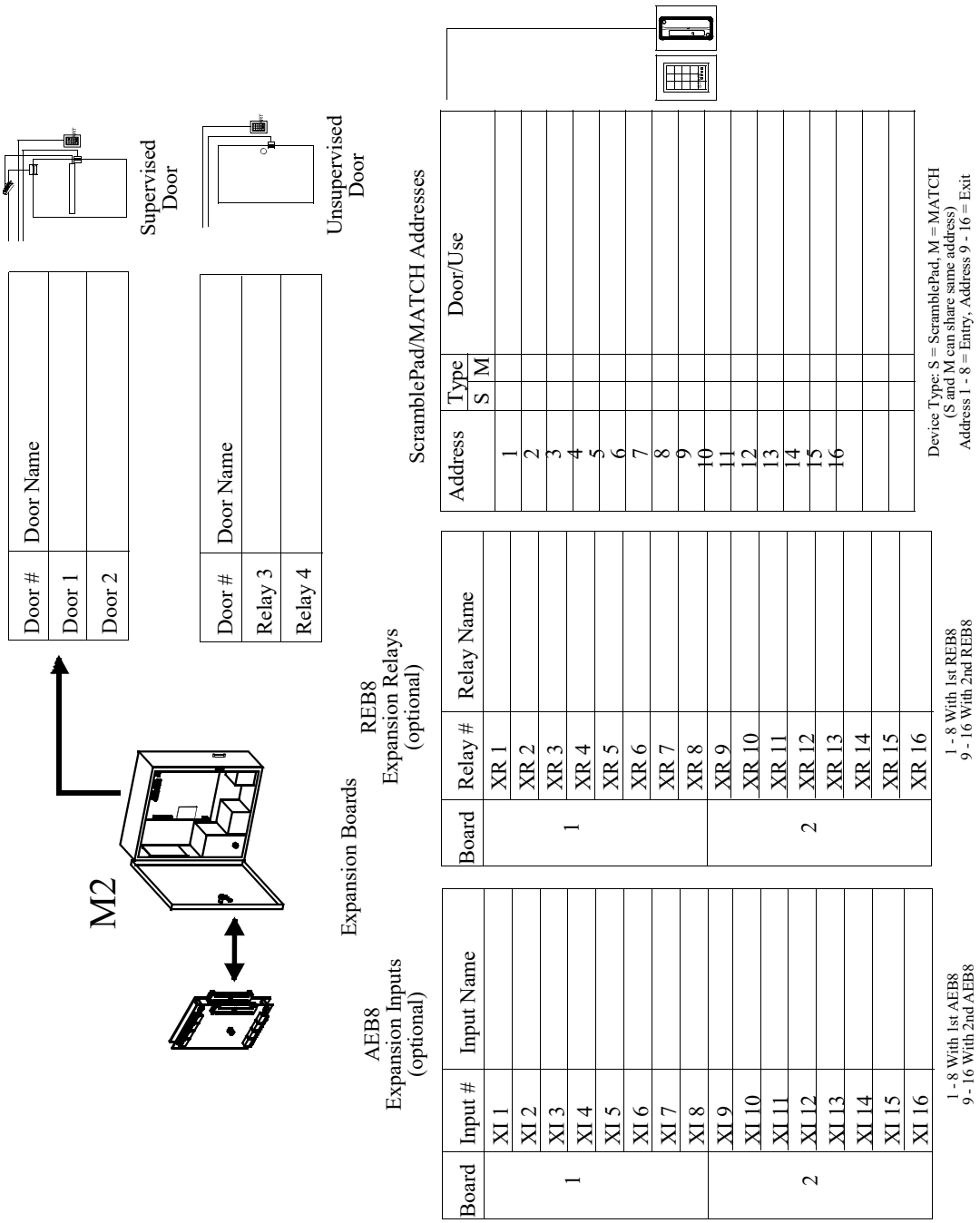


Figure A-2: M2 Worksheet

Door #	Door Name
Door 1	
Door 2	
Door 3	
Door 4	
Door 5	
Door 6	
Door 7	
Door 8	

Supervised Door

M8

Expansion Boards

AEB8 Expansion Inputs (optional)

Board	Input #	Input Name
1	XI 1	
	XI 2	
	XI 3	
	XI 4	
	XI 5	
	XI 6	
	XI 7	
	XI 8	
2	XI 9	
	XI 10	
	XI 11	
	XI 12	
	XI 13	
	XI 14	
	XI 15	
	XI 16	

1 - 8 With 1st AEB8
9 - 16 With 2nd AEB8

REB8 Expansion Relays (optional)

Board	Relay #	Relay Name
1	XR 1	
	XR 2	
	XR 3	
	XR 4	
	XR 5	
	XR 6	
	XR 7	
	XR 8	
2	XR 9	
	XR 10	
	XR 11	
	XR 12	
	XR 13	
	XR 14	
	XR 15	
	XR 16	

1 - 8 With 1st REB8
9 - 16 With 2nd REB8

ScramblePad/MATCH Addresses

Address	Type S	Type M	Door/Use
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

Device Type: S = ScramblePad, M = MATCH
(S and M can share same address)
Address 1 - 8 = Entry, Address 9 - 16 = Exit

Figure A-3: M8 Worksheet

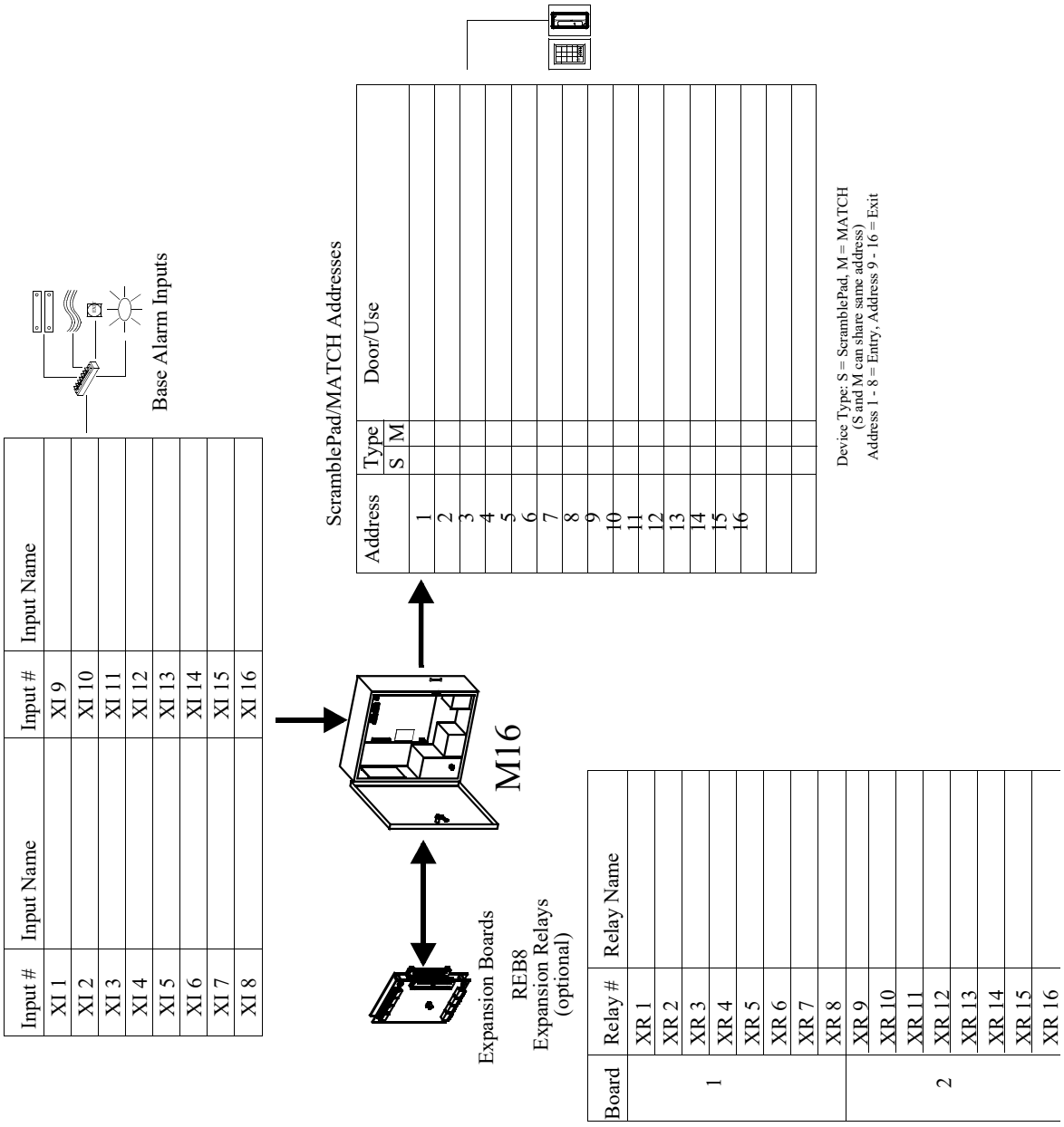


Figure A-4: M16 Worksheet

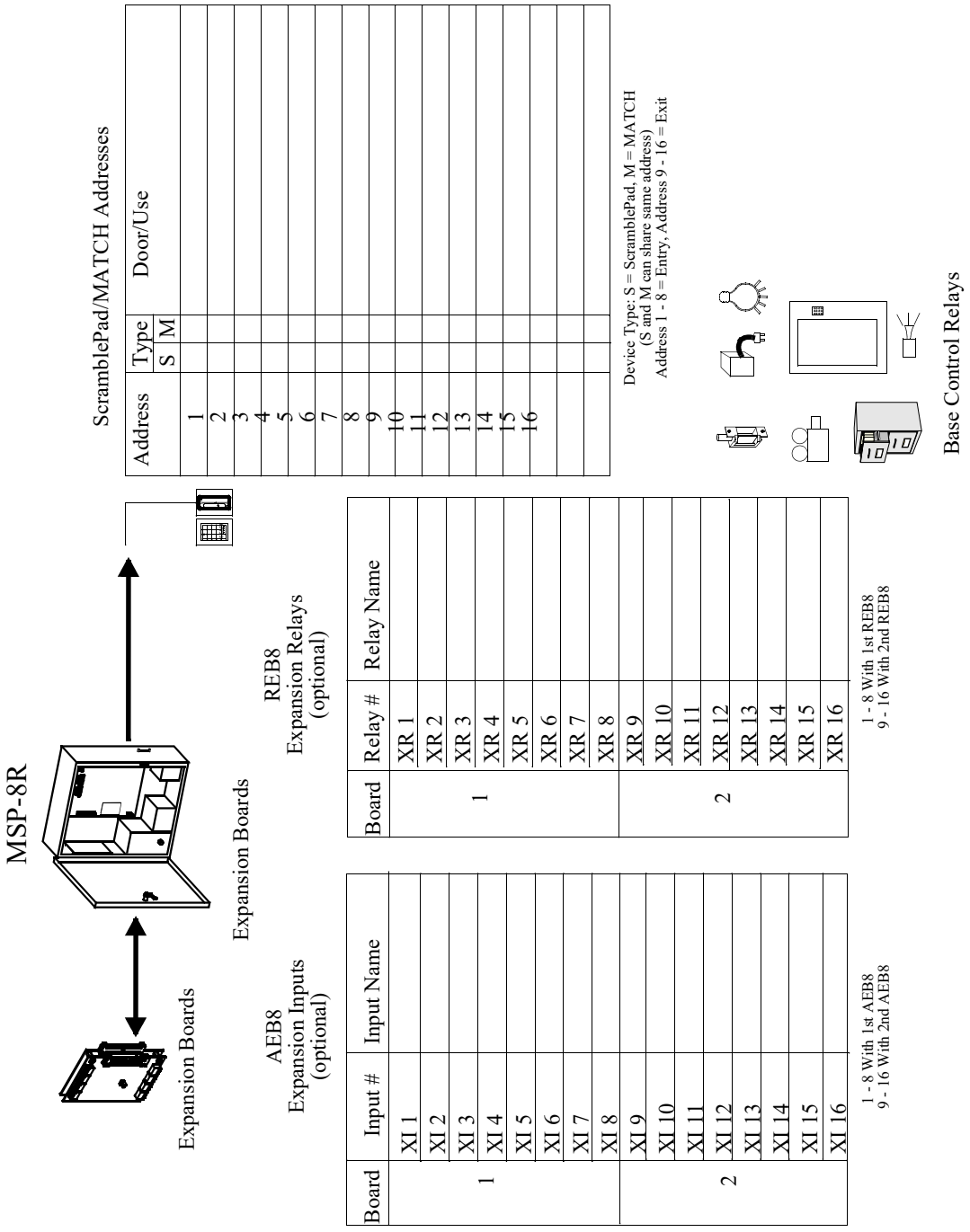


Figure A-5: MSP-8R Worksheet

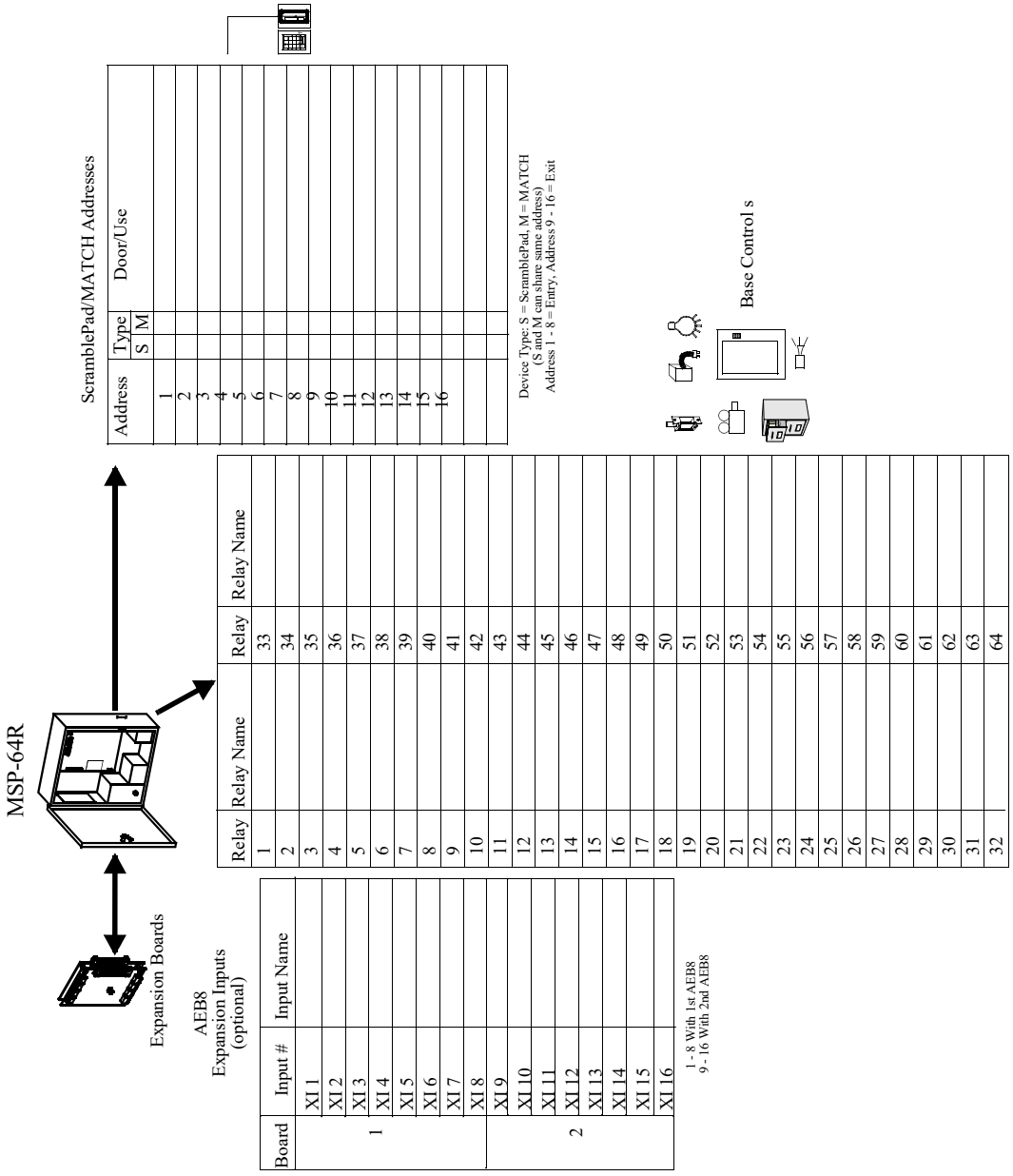


Figure A-6: M64 Worksheet

The worksheet for the Mx controller is provided in Figure 8-7 on page 8-32.

The worksheet for the Mx-1 controller is provided in Figure 9-8 on page 9-48.

Glossary

B

HIRSCH by IDENTIV

This Page Intentionally Left Blank

Glossary

2-person rule

The 2-person rule feature can be used to require that two people enter valid access codes to access a secure area. This is typically used in high security areas or in areas where industrial safety is an issue.

AATL - Alarm Active Too Long

This applies to “non-door” locations that allow an alarm condition to occur for a specified time period before an alarm is actually issued. Doors report DOTL (door open too long) alarms rather than AATL alarms. In this situation, an alarm is issued when the door is held open longer than a specified time.

Absentee Rule Mode

A User Management Command. Sets the maximum number of days for non-use of an ID (1 – 255 Days). On expiration (no ID usage - for the maximum number of days set) the User will be automatically disabled or deleted.

ACB - Alarm Action Control Block

The ACBs, Alarm Action Control Blocks, are the means by which DIGI*TRAC controllers control actions and events based on Alarm conditions. ACBs are Factory programmed for specific actions; however, they are all reprogrammable, if required. For a complete list of ACBs, refer to Table 4-2 starting on page 4-188.

Access Control

Electronic access control systems restrict, record and report access to facilities, services, information, and other protected assets. They also detect and deny unauthorized access attempts or intrusion into supervised areas of a monitored facility.

Access Delay Time

An Access Delay Timer can be set to delay the actuation of a Relay for special Access and Exit applications. The relay actuation can be delayed for 1-8100 seconds after the use of a valid Access ID or an RQE Exit request.

Access Zones

Every Access User in a Hirsch System is assigned to an Access Zone. An Access Zone determines When and Where access is granted and denied. It consists of one or more Time Zones and a set of valid doors. Expansion Line Module Inputs can be assigned to an Access Zone for special control applications. There are two types of Access Zones: Standard and Master Access Zones.

Standard Access Zones (0 - 65)

Consists of a Time Zone Per Door (CMD 24 or CMD 117) or one Time Zone For All Doors (CMD 17), and a set of valid Doors. (AZ 0 = Never/No Doors - AZ 65 = Always/All Doors)

Master Access Zones (66 - 127)

Consists of up to 8 Standard Access Zones

Address

Each ScramblePad Reader requires an Address setting from 1-16. Each MATCH Reader Interface Board also requires an Address setting from 1-16. The address alerts the controller from which ScramblePad/MATCH Reader the access or control request originated.

Alarm Cancel

Cancels all alarms within the specified control zone. This also enables the DIGI*TRAC Annunciator.

Alarm Control

The practice of controlling the alarm monitoring and reporting capabilities of a controller automatically by time and manually by individual User ID.

Alarm Masking

The controller can Mask any line module input to allow authorized use of a monitored door or area. Masking prevents alarm conditions from being reported but still allows line trouble alarms and tamper alarms to be reported during the masking condition.

Alarm Relays

Dedicated Alarm Relays are for interfacing to local alarm annunciators or to digital communicators for monitoring the controller's alarm status from off-premise central alarm stations.

Alarm Shunting

Alarm shunting is different than alarm masking. Masking is performed by the controller's software for its own line module inputs. Alarm shunting is performed by the controller's relays to shunt the alarm reporting of line module inputs of other controllers or alarm panels. Shunting of alarms is an insecure and outmoded technique no longer in use by state-of-the-art systems.

Alarm Triggers Control Zone

Any Line Module Input can trigger a Control Zone. This is used for point-by-point annunciation of Inputs or for special control applications such as turning on security lighting when an alarm has been tripped.

Arm

See ‘Unmask’.

Auto-Add Users

The controller can automatically add one Access User, or any number of Users, with Keypad Code IDs, to the controller memory. The controller assigns a randomly generated Keypad Code ID of the specified length to unused User Records. This feature makes adding new Users simple, secure and quick. Any set of Users can also be deleted from the controller memory.

Alarm Types

There are over 150 alarm types. See ACBs for more details.

Auto-Relock

A monitored Door will automatically relock ¾ second after it is opened, thereby reducing the chance of unauthorized follow-on entry by tailgating after a valid access. To accommodate various types of electric locks and door operators, auto-relock can be set to relock ¾ second after the door closes, or can be disabled.

For example, if the door time is set to 45 seconds to allow access by a handicapped person, but someone accesses the door in ten seconds, auto-relock can be used to automatically relock and rearm the door as soon as the door is opened. Therefore, the door does not remain unlocked and unarmed to allow an unauthorized person access. In a "non-door" situation, there is no lock to relock so auto-relock will only rearm the alarm. This can be used for doors not used for normal access (such as a fire door). For example, someone (such as a maintenance person or inspector) could be granted one-time access through a fire door that is set up to trigger an alarm if opened; auto-relock can be used to automatically rearm the alarm for the door as soon as the door is closed.

Batch-Add

The process of adding new Card Code ID Only Users in a single batch process. See Command 220.

Batch-Change

The process of changing the Card Code ID and/or Dual Code ID for an existing User. See Command 224.

Batch-Enroll

The process of filling in the Card Code ID and Dual Code ID for an existing User. This is the second step of a two step process for Auto-Add Access Users (CMDs 320, 321, 322). See Command 223.

Batch-Restore

The process of manually restoring from a ScramblePad a damaged, corrupted or deleted User Database by re-entering each User Record including Keypad Code ID, Card Code ID, and Dual Code ID data. For emergency restoral use when Cards cannot be retrieved for batch re-enrollment. Requires a printout of the database listing the codes to be restored. See Command 225.

Cancel Entry Delay

Cancels the entry delay timer and prevents reporting of an alarm.Use an Entry Delay Timer to control access to secure areas covered by the ScramblePad. This function is defined by CMD 42.

Card Code ID Only

A description of User ID Format 2 (IDF 2). This ID Format is for Card Code ID Only Users. This ID takes up 1 User Record in the DIGI*TRAC User Record database. See Command 310.

CCM (Command & Control Module)

This daughter board sits on the Controller Board and contains all the logical instructions the Controller Board uses to process its information including the DIGI*TRAC Programming Language.

Circuits, electrical

High voltage—a circuit involving a potential or not more than 600 volts and having circuit characteristics in excess of those of a low-voltage power-limited circuit.

Low-voltage—a circuit involving a potential of not more than 30 volts alternating current (AC), 42.4 volts direct current (DC), or AC peak.

Power-limited—a circuit whose output is limited as described in the following tables. The first table lists power limitations for inherently limited power sources; the second specifies power limitations for sources not inherently limited. The power limitation is provided by the design of the transformer, a fix impedance, a non-interchangeable fuse, a nonadjustable manual reset circuit protective device, or a regulating network.

Circuit voltage V_{max} AC-DC (volts)	Maximum nameplate ratings		Current limits I_{max} (amps)
	VA (volt-amps)	Current (amps)	
0 - 20	5.0 x V_{max}	5.0	8.0

Table B-1: Power Limitations for Inherently Limited Power Sources

Circuit voltage V_{max} AC-DC (volts)	Maximum nameplate ratings		Current limits I_{max} (amps)
	VA (volt-amps)	Current (amps)	
over 20 - 30	100	100 / V_{max}	8.0
over 30 - 100	100	100 / V_{max}	150 / V_{max}
over 100 - 250 DC only	0.030 x V_{max}	0.030	0.030

Table B-1: Power Limitations for Inherently Limited Power Sources

where V_{max} = maximum output voltage regardless of load with rated input applied and I_{max} = maximum output after one minute of operation under any non-capacitive load, including short circuits.

Circuit voltage V_{max} AC-DC (volts)	Maximum nameplate ratings		Current limits I_{max} (amps)	Power limits $(VA)_{max}$ (volt-amps)	Maximum over-current protection (amps)
	VA (volt-amps)	Current (amps)			
0 - 20	5.0 x V_{max}	5.0	1000/V_{max}	250	5.0
over 20 - 100	100	100 / V_{max}	1000/V_{max}	250	100/V_{max}
over 100 - 250 (DC only)	0.030 x V_{max}	0.030	1.0	NA	1.0

Table B-2: Power Limitations for Sources Not Inherently Limited

where V_{max} = maximum output voltage regardl`ess of load with rated input applied, I_{max} = maximum output after one minute of operation under any non-capacitive load, including short circuits and with over-current protection, and $(VA)_{max}$ = maximum volt-amp output regardless of load with over-current protection bypassed. If the power source is a transformer, $(VA)_{max}$ is 350 or less when V_{max} is 15 or less.

Channel

Describes the 2 card reader ports on the MATCH Reader Interface Board. See Commands 103, 104.

Code

Access codes are used to gain access to secure areas. Each user is assigned a unique access code, and when an access code is entered, the controller knows which user the access code belongs to and whether the user is authorized to access the area. Access codes can be entered manually on a ScramblePad, or they can be entered by scanning a card in a MATCH reader.

There are 3 Code ID Formats: Keypad Code ID, Card Code ID, and Dual Code ID (Keypad Code ID + Card Code ID). IDs can be programmed to perform different Functions and are controlled by time, day, location and User Management Limits.

They can be issued when an event occurs to perform designated activities (such as a turning on lights, unlocking doors, and masking alarms), by selecting a button on the Control window (to lockdown a door, for example), by scanning a card with a control code in a MATCH reader, or by manually entering codes on a ScramblePad. Programming codes can be used by trained personnel to program optional features or to test and troubleshoot a controller from a keypad.

Code ID Tamper Alarms

The controller can detect and Report Code ID Tampers. A Code ID Tamper results from an invalid Keypad Code ID being entered at a ScramblePad Keypad or an invalid Card Code ID at a MATCH Card Reader. An invalid Code ID is one that does not exist in the controller's

database, or one that is being used at the wrong door at the wrong time. The controller reports Code ID Tampering on the system printer and on the Tamper Relay after three invalid Code ID entries and may be programmed to alarm on from one invalid Code ID to none.

Command & Control

Describes the ability for the owner, operator or authorized user to issue Commands & Control the way in which the security system manages access, alarms, relays and users. See also *CCM*.

Conditional Unmask

Unmasks/arms all inputs in the specific control zone only if all inputs have been previously detected as secure.

Control Delay Time

A Control Delay Timer can be set to delay the actuation of a control relay for special control applications. The relay actuation can be delayed for 1-8100 seconds after a valid Control ID entry, or after a relay has been triggered by a Time Zone or by an Alarm or Relay triggering a Control Zone.

Control Time

Relays have a Control Time setting for use by Control Users, and Control Zones triggered by Alarms or other Relays. The Control Time can be set for 1-8100 seconds. It can be set to 0 (Zero) seconds for Toggle ON/OFF operation by consecutive uses of a Control ID or event.

Control Zones

Control Zones are used to control Relays and Line Module Inputs by Control IDs, and for special Control applications. A Control Zone includes a Time Zone and a set of Relays or Line Module Inputs to be controlled. There are two types of Control Zones: Standard Control Zones and Master Control Zones.

Standard Control Zones: 0 - 191
Consists of a Time Zone and a combination of the Line Module Inputs and Relays to be controlled. (CZ 0 = Never/No Inputs or Relays)

Master Control Zones: 192 - 255
Consists of a combination of Standard Control Zones each capable of performing different access and control functions simultaneously.

Deadman Timer

A Deadman Timer Code is a special control code used to track the safety and security of a user while a specific task is being performed. The use of “deadman timers” is common in many industrial applications such as railroads, refineries and other dangerous or hazardous locations. This condition allows the system to track the safety and security of a user while a specific task is being performed. Deadman timers are common in many industrial applications such as railroads, refineries, and other dangerous or hazardous locations.

Disarm

See ‘Mask’.

Door Alarms

The controller can monitor the doors it controls for two types of door alarm conditions: Door Forced Open and Door-Open-Too-Long. Door Forced Open is reported on the system printer and the General Alarm Relay whenever a monitored door is opened without the entry of a valid ID, or an RQE Input first. Door-Open-Too-Long is reported whenever a monitored door that has first been opened by an authorized User and is held or propped open beyond an owner settable time period. The DOTL alarm is reported on the system printer and on the General Alarm

Relay.

Door Delay

A specified period of time before a door is actually unlocked. For example, a bank vault might have a 10-minute door delay before it is opened.

Door Time

Relays have a Door Time setting for use by Access Users and RQE devices. The Door Time can be set for 1-8100 seconds. It can be set to 0 (Zero) seconds for Toggle ON/OFF by consecutive uses of an Access ID, or RQE device.

DOTL - Door Open Too Long

Door-Open-Too-Long is reported whenever a monitored door has been opened by an authorized User and is held or propped open beyond an owner-assigned time period. The DOTL alarm is reported on the system printer and on the General Alarm Relay.

Dry Contact

A switch or relay which provides no power to the circuit but redirects or turns on/off power supplied from another source.

DTLM

To monitor door switches, or other alarm sensors, the controller requires a DIGI*TRAC Line Module, DTLM, to be installed for each monitored input. The Line Module provides line supervision of 2% sensitivity for line security and line trouble reporting. The DTLM1 provides one input terminal for the alarm sensor. The DTLM2 has two terminals, one is for the alarm sensor and one for the RQE Push-button or sensor Input. The DTLM3 has three input terminals, one for an alarm sensor, one for an RQE device, and one for a Tamper switch. The MELM may be substituted.

Dual Code ID Only

Description of User ID Format 3 (IDF 3). This ID Format is for Dual Code ID (Card Code + Keypad Code) Users only and is entered on a Dual Technology Reader (ScramblePad + MATCH Reader). This ID takes up 1 User Record in the DIGI*TRAC User Record database. See Command 311.

Dual Technology Reader

The use of 2 reader technologies at 1 location, usually a ScramblePad and a MATCH reader. Either or both IDs may be used for Access or Control Functions.

Duress Alarms

The controller can detect and report a user under duress at any ScramblePad when a Keypad Code ID along with an additional Duress Digit is used. The Duress Digit is added at the end of a User's normal Code. Any Function of Keypad Code ID may have a Duress Digit. When a Keypad Code ID with Duress Digit is entered, it will perform its normal function plus report Duress by User by ScramblePad on the System printer and trip the Duress Alarm Relay. Duress Keypad Code IDs may be used at either a keypad or dual technology door, but not on a reader only door.

Event Report

An Event Report is the result of an action or event generated by the controller automatically, or an event that occurred to the controller from outside the controller. There are two types of System Events: Internal Events and External Events.

External Event Types

•AC OK
•Line Module Input Secure
•Box Tamper Secure
•Forgive All Users
•Keypad Tamper Secure
•Keypad On-line
•Line Fault Cleared
•Multiple Keypads Alert
•Parallel Printer On-line
•Passback Violation
•Serial Printer On-line
•UPS Restored

Internal Event Types

•End Of Time Zone Masking Of Input
•End Of Time Zone Disable Of Relay
•End Of Time Zone Actuation Of Relay
•End Of Time Zone
•Relay Clear At End Of Time Zone
•Relay State Change
•Start Of Time Zone
•Start Of Time Zone Masking Of Input
•Start Of Time Zone Actuation Of Relay
•Start Of Time Zone Disable Of Relay

Fault-tolerant computer system

A computer system containing multiple power supplies, disk drives, processors, and controllers, each of which back up and check on the processes of the others. In the event of a component failure, the other modules take over the function performed by the failed components without affecting the operation of the computer. In addition to the duplicating hardware, a fault-tolerant system includes the necessary software to make the system operational.

ID

Hirsch controllers enable the use of a Personal ID to perform different control Functions: access control, door control, elevator control, alarm control, etc. When used, the ID identifies the user. There are 3 ID Formats supported: Keypad Code ID, Card Code ID and Dual Code ID (Card Code ID or biometric + Keypad Code ID.)

Hirsch controllers are code based. Codes can be entered by using a ScramblePad. Codes can be entered by using a Card. Cards are converted by the MATCH Reader Interface Board to a Card Code and a combination of Card plus Keypad Code is converted to a Dual Code. Each ID Format is stored in the controller's internal memory by a User Record Number and checked for code conflicts (duplicates) during programming.

Keypad Code ID Only

Description of User ID Format 1 (IDF 1). This ID is used for Keypad Code ID only Users. This ID takes up 1 User Record in the DIGI*TRAC User Record database. See Command 10.

Keypad Tamper

See Physical Tamper.

LED

Light emitting diode. LEDs are used on ScramblePads, MATCH readers, SNIBs and Net*Adapts to indicate status and respond to entries.

Line Modules

Line modules are used to monitor door switches or other alarm sensors. There are two types of line modules: DIGI*TRAC line module (DTLM) and miniature embedded line module (MELM). Line modules provide line supervision of 2% sensitivity for line security and line trouble reporting. The DTLM1 and MELM1 provide one input terminal for the alarm sensor. The DTLM2 and MELM2 have two terminals: one for the alarm sensor and one for the RQE push-button or sensor input. The DTLM3 and MELM3 have three input terminals: one for an alarm sensor, one for an RQE device, and one for a tamper switch.

Line voltage

The voltage at any field-connected source of supply, nominally 50 – 60 Hz and 115, 208, or 230 volts (depending on the country standard).

Mask

Turns off reporting of all alarms from any of the line module inputs as defined by the code's control zone. Also called ‘Unarm’.

MATCH

The term MATCH is an acronym for Multiple Access Technology Control by Hirsch. It describes the ability to use multiple compatible technologies such as card readers, biometrics, fingerprint/retinal scanners, smart cards, etc. on a DIGI*TRAC controller, one at a time, or all at the same time.

MATCH Reader Interface Board (MRIB)

This board is required to interface compatible card readers, by themselves or in combination with ScramblePads, to a DIGI*TRAC controller. Each MRIB supports 2 ScramblePads and 2 Readers (ABA/ISO or Wiegand).

MELM

The MELM is a Miniature Embedded Line Module version of the DTLM. Available in MELM1, MELM2 and MELM3, 1, 2 and 3 input versions performing the same functions as the DTLM. See also *DTLM*.

Momentary Single Mask

Momentarily disables the reporting of a single alarm condition from any of the line module inputs as defined by the card/code's control zone.

Multiple ID User

Describes a User who can Use different IDs (Keypad, Card, Dual) on the same controller at different locations. See ID Formats 4, 5, 6, & 7.

Occupancy Control

Occupancy Controls are used to keep track of the number of users within a designated secure area or zone. The controller can be programmed to perform automatic mode changes based on the occupancy count such as automatically mask the interior alarm sensors on the first person to enter the area and unmask them on the last person to exit the area. Occupancy controls require entry and exit readers on the controlled area.

Passback Control

Passback Controls are used to require users to pass through an entry reader followed by passing through an exit reader before their ID will be accepted a second time at another designated entry reader. Passback is used to reduce multiple entries on a single ID by different persons (ID sharing by “passing the card back” to another entrant) and tailgating (more than one person entering on the single use of an ID).

Partial Unmask

Unmasks all inputs in the specified control zone previously detected as secure. All unsecured inputs are left unarmed.

Physical Tamper

When the keypad’s DIP switch for the Tamper Enable is set to ON, and the outer keypad bezel is pried up or removed, the keypad goes into a physical tamper mode. This will be evident when all four of the keypad's LEDs flash on and off.

There are two distinct behaviors that can occur with the keypad in physical tamper mode, depending on which model keypad you are using:

- ❑ DS37L - 4 LEDs flash on and off and the START button is disabled, so pressing it does not generate the numbers display that allows code entry. The keypad will beep once every few seconds.
- ❑ DS47L - 4 LEDs flash on and off. Pressing the START button will generate numbers and allow a valid access code to be entered to unlock the door. The keypad will beep once every few seconds.

Physical Zone (PZ)

Extensions of common passback and occupancy definitions that enable programmers to create an arbitrary topology around a reader or group of readers. A defined area inside of which passback and occupancy definitions are observed. If users are detected inside a prescribed PZ during an emergency or other predefined condition, they are reported to the controller according to existing definitions.

Pre-Arm Status

Tests all available inputs within the specified control zone and reports whether they are inactive (secure) or active (unsecured).If all inputs are secure, the ScramblePad flashes its green LED once for an access grant and twice for a control. If there are unsecured inputs detected, the ScramblePad flashes its red LED and beeps—one beep for each active input.

Programming Mode

The controller must be in Programming Mode in order to enter Programming Commands.

The ScramblePad will scramble its display to a normal pattern when in Programming Mode for ease of Command entry. The right most Yellow LED will be flashing while in Programming Mode. Both Yellow LEDs will be flashing while in Programming Mode if the System Code is to the Factory Default code of 123.

A ScramblePad and MATCH Reader combination is required to enroll cards into a stand-alone DIGI*TRAC controller. Contact Hirsch for information on pre-configured Enrollment Stations.

Reader

A generic term applied to an access or alarm control device such as a keypad, card reader, dual keypad+card reader combination, or biometic reader.

Redundant

Possessing a backup in case the original is corrupted.

Relay Control

The practice of controlling equipment, systems or processes, such as elevators or HVAC, automatically by time or by individual User IDs.

Relay Triggers Control Zone

Any Relay can trigger a Control Zone. This is for special control applications such as shunting other alarm systems when doors are unlocked or when relays are actuated.

RQE Devices

RQE means Request-To-Exit. An RQE device can be used to mask an alarmed Door for authorized exit and to unlock magnetic locks for exit. RQE devices can be push-button or motion sensors. An RQE Push-button can be installed at a receptionist's desk to manually grant access at an intercom controlled visitor's entry door. RQE Devices are connected to a controller through a DTLM2, DTLM3, MELM2, or MELM3 Line Module.

RQE Devices may also be used to locally mask an expansion line module input, either for momentary passage through an alarmed door, or using a key switch for masking interior motion sensors prior to area occupancy.

ScramblePad Keypad

The unique and patented Hirsch ScramblePad Keypad. This type of keypad is the most secure keypad available because it scrambles the display - places the illuminated digits under different keys every time it is used - to protect codes from being stolen by pattern recognition. It also includes a built-in optical viewing restrictor to prevent anyone except the authorized user from reading the display.

S*NAP

SCRAMBLE*NET Application Pack. The DOS-based predecessor to the Windows-based SCRAMBLE*NET Access Manager (SAM), used to manage and program DIGI*LOCK and DIGI*TRAC Controllers within the DOS environment.

START Key

The START Key of the ScramblePad Keypad. Push to activate the ScramblePad to start the Keypad Code ID entry process.

Single Zone Access

This feature allows a controlled area to be occupied by only a single Access Zone at a time. More than one Access Zone may be authorized for the same secure area, however, when it is unoccupied, the first Access Zone to enter will automatically exclude all other authorized Access Zones until the area is again unoccupied.

Style

User Records can be printed in up to 6 Styles: User Code, Temporary Day Limited, Use Count Limited, Absentee Rule Limited, User Tracking, and Deadman Time. Each printout style lists a different combination of User setups or status.

System Code

The System Code must be entered on a ScramblePad to enter Programming Mode. The System Code, a settable 3-8 digit Keypad Code ID, protects the controller from unauthorized programming.

Tamper Alarms

The Controller can detect and report several types of Tamper Alarms. It will report a Box Tamper whenever the controller enclosure is opened. It will report a Tamper whenever the ScramblePad or MATCH Reader Bezel is removed and if Address Tamper reporting is set to on. It can also report a Code Tamper if so programmed.

A Line Module Input Tamper will be reported from an Input equipped with a DTLM3 or MELM3 Line Model with Tamper Switch installed. Tampering with alarm monitoring circuits will trip line trouble alarms. Tamper Alarms report on the System printer and trip the Alarm Relay.

Temporary-Day Mode

A User Management Command. Describes the ability to set which days this week, next week, and the week after (up to 14 days) that a User will be authorized to use their ID. Upon expiration, the User will be disabled or optionally deleted automatically.

Time Log

Logs code entry for recording the arrival and departure times of time log code holders.

Time Zones

Time Zones are used to manage the use of IDs and the scheduling of automatic events. Time Zones are made up of a start time, an end time, and a set of valid days. There are three types of Time Zones available: Standard, Master, and Grand Master Time Zones.

Standard Time Zones: 0 - 65

Consists of a start time, end time and set of days. (TZ 0 = Never; TZ 65 = Always)

Master Time Zones: 66 - 129

Consists of up to 8 Standard Time Zones

Grand Master Time Zones: 130 - 149

Consists of up to 8 Standard or Master Time Zones

Transaction Report

A Transaction Report results from an ID being used. An RQE transaction also generates a transaction report.

Trouble Alarms

The controller can detect and report several types of Trouble Alarms. These alarms include line module input circuit troubles such as opens, shorts, excessive noise, and line out-of-spec. Trouble alarms also include printer off line, printer out-of-paper, UPS fail and other internal controller conditions. Trouble Alarms are reported on the printer and the Trouble Relay.

Turnstile

This type of gate allows one person at a time to pass its point. It is frequently used for access control in crowded areas, such as airports or department stores. There are three basic types of turnstiles: full-height, half-height, and optical.

Unmask

Restores alarm reporting of any input(s) as defined by the code's control zone. Also called ‘Arm’.

Use-Count Mode

A User Management Command. Describes the ability to set the number of times a user can use

their ID (1-31 times) before it is automatically disabled or optionally deleted.

User

A User is an individual who is issued a personal ID or set of Multiple IDs, to perform a variety of functions from ScramblePad Keypads or MATCH Readers.

User Function

Description of what Function DIGI*TRAC controller will perform upon a valid transaction; e.g. Access, Unlock, Mask, etc.

User Function and Priority

Each User in the controller can perform one of the functions listed below. The Functions are prioritized. Each higher priority Function can override the lower priority Functions. For example, a Force Off Function User can override an Unlock Function that is in effect. A Lock Open Function User can override a Force Off Function that is in effect. Time Zone controlled Functions fall in the middle of the priority list and override lower priority User Functions, but can be overridden themselves by higher priority User Functions.

ACCESS USERS (***Lowest Priority)***
•Momentary Access
•Single Use Access
•Temporary Access
•Unlock
•Relock

CONTROL USERS
•Trigger Relays
•Force Relays ON
•Force ON Release
•Force Relays OFF
•Force OFF Release

TIME ZONE CONTROLS
•Time Zone Actuate
•Time Zone Disable
•Time Zone Clear

TOP-PRIORITY CONTROL USERS (***Highest Priority)***

•Lock DOWN
•Lock DOWN Release
•Lock OPEN
•Lock OPEN Release

User ID Format

The type of ID issued to a User determines the Format of the User Record in the controller database. There are 7 available User ID Formats which include Keypad Code ID Only, Card Code ID Only, Dual Code ID (Card Code ID + Keypad Code ID) Only, as well as all in combination.

User Number

When added to a controller, each User is assigned a User Number as well as issued a personal ID or set of Multiple IDs. If a User is issued Multiple IDs, then more than one User Number will be associated with that User. The User Number is used to change or delete a user as well as to track and report transaction activity. Available User Numbers are 1-999 in a standard controller. User Expansion is available to 4,000 or 16,000.

User Record

The controller maintains in its internal Database a Record on every User. The User Record is listed by User Number and contains all the information needed on every User: The User Number, User Function, ID Format, Access Zone or Control Zone, Duress Digit if assigned, and current Passback Status. The Record also maintains the User's Alert and Tag status and any Use-Count and Absentee-Rule Limits. For Temporary-Day Users, the Record also contains their valid days. Whenever Users are printed on the System printer, they are listed in the User Record format listing most of the above information, but selectively with or without Code IDs showing. See Command 330 to be able to selectively print out User Records by printout style, each showing different user setups and status information.

Virtual Relays

Non-physical relays available for programming use for special applications.

Watch Log

Logs code entry for tracking guards on their appointed rounds.

Index

Symbols

Numerics

A

B

C

D

E

F

G

I

J

K

L

M

N

Q

R

S

T

U

V

W

X

Z