Johnson Controls

CK721-A

Network Controller

Installation and Operation Manual

May 2008
24-10349-8 Revision –

CK721-A

Network Controller

Installation and Operation Manual

May 2008

24-10349-8 Revision –

Johnson Controls
Security Solutions
(805) 522-5555
www.johnsoncontrols.com

Federal Communications Commissions Notice

This equipment, CK721-A, has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user□s authority to operate this equipment.

Canadian Notice

This Class B digital apparatus, CK721-A, complies with Canadian ICES-003.

Cet appareil numerique de la classe B, CK721-A, est conforme à la norme NMB-003 du Canada.

CE

Declaration of Conformity

This product complies with the requirements of the European Council Electromagnetic Compatibility directive 89/336/EEC and amending Directive 92/31/EEC, the CE Marking Directive 93/68/EEC and the Low Voltage Directive 73/23/EEC.

This equipment must not be modified for any reason and it must be installed as stated in the Manufacturer’s instruction.

If this shipment (or any part thereof) is supplied as second-hand equipment, equipment for sale outside the European Economic Area or as spare parts for either a single unit or system, it is not covered by the Directives.

UNDERWRITERS LABORATORIES COMPLIANCE VERIFICATION SHEET
CK721-A SERIES INSTALLATION MANUAL

This product is listed under Underwriters Laboratories UL 1076 for Proprietary Burglar Alarm Units and Systems and UL 294 for Access Control Systems Units. When installed at the site the following requirements must be met to comply with these standards.

1. Transient protection devices that are installed must not be removed or defeated.
2. The CK721-A shall be mounted in subassembly S300-DIN-L or S300-DIN-S.
3. The CK721-A in combination with the S300-DIN-L or S300-DIN-S must be connected to a UL Listed Uninterruptible Power Supply that provides a minimum of 24 hours of AC emergency power.
4. The tamper switch must be enabled at all times.
5. Systems requiring the use of network hubs, routers, bridges, network switches or the like shall guarantee these devices are UL Listed for fire and shock in the category control number (CCN) NWGQ and/or EMRT. These devices shall be installed in a temperature-controlled environment. The temperature-controlled environment must be maintained between 13 - 35°C (55 - 95°F) and relative humidity of 85 ± 5% by the HVAC system. Twenty-four hour standby power shall be provided for the HVAC system.
6. The installer shall incorporate a supply line transient suppression device complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum rating of 330 V. Supply line transient suppression device is to be used with the power supply to the network hub(s) routers, bridges and/or network switches.
7. External network hubs, routers, bridges or network switches must use signal line transient suppression devices complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50V.
8. In the CK721-A user-interface, the “Network Polling [LAN]” parameter must not exceed 90 seconds.
9. Modems shall not be used for primary connection to the host computer. Modems have only been investigated by UL for supplementary use.
10. The use of the MTI-STI-MUX-KIT and MTI-STI-MUX has not been investigated by Underwriters Laboratories.
11. Do not connect equipment to an AC power source that is controlled by a switch.

TABLE OF CONTENTS

1: Introduction

2: CK721-A and S300-DIN Enclosures

3: S300 Expansion Enclosures

4: CK721-A User Interface

Appendix D: Using a Keypad Reader on a Panel

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

This chapter provides a general description of the CK721-A panel and related equipment. The conventions used throughout this manual are also described.

The manual is divided into the following chapters:

- ***Chapter 1: Introduction***, defines the key terms and conventions used throughout the manual. In addition, it describes the standard and optional equipment available for the CK721-A and the equipment's specifications. This chapter also includes information on planning a CK721-A installation.
- ***Chapter 2: CK721-A and S300-DIN Enclosures***, describes S300-DIN enclosures and the components located on the CK721-A.
- ***Chapter 3: S300 Expansion Enclosures***, provides information on the expansion enclosures, principles to consider when installing the panels, and also contains a section on preparing the panels for operation.
- ***Chapter 4: CK721-A User Interface***, explains how to configure the panel for operation and how to use the interface to commission or troubleshoot the system.
- ***Chapter 5: Maintenance***, provides information on CK721-A routine maintenance and the basic troubleshooting steps that will assist you in keeping the CK721-A system running at peak performance.
- ***Appendices*** provide reference information regarding cabling and grounding, and a guide to using a keypad reader.

MANUAL CONVENTIONS

The following items are used throughout this installation manual to indicate special circumstances, exceptions, important points regarding the equipment or personal safety, or to emphasize a particular point.

NOTE

Notes indicate important points or exceptions to the information provided in the main text.

Cautions remind you that certain actions, if not performed exactly as stated, can cause damage to equipment.

Warnings indicate that the possibility of personal injury exists if an action or actions are not performed exactly as stated.

KEY TERMS

The following terms are used throughout this manual:

Cardkey SMS – The Cardkey Security Management System: P1000, P1500 or P2000 series.

CK721-A System – This is a general term that refers to a combination of CK721-A terminals and expansion enclosures that communicate with a Cardkey SMS.

CK721-A – The CK721-A contains:

- A 10/100Base-T Network Interface
- A Hitachi SH-4 processor
- System memory for storing cardholder records, system parameters, and history
- A serial connection for communication with the user interface
- An RS-485 connector for communication to the terminals

Panel – This generic term refers to an enclosure with the CK721-A and power supply installed. The panel contains a tamper switch, a power indicator light, and an optional battery backup.

Terminals – The terminals provide additional reader interfaces, input points, or output relays to the CK721-A system. Terminals can be installed in the S300 expansion enclosures; S300-DIN-RDR2S and S300-DIN-RDR2SA modules can be installed in the S300-DIN enclosures.

Expansion Enclosure – An expansion enclosure contains only a power supply, a tamper switch and a power indicator. The indicator can be seen when the cabinet door is closed.

External Device – This general term applies to any device that is wired to the CK721-A system, such as a reader or input device. A motion sensor is one type of input device.

User Interface – The CK721-A User Interface provides access to the CK721-A panel configuration via a serial connection to a laptop (or other computer) running common terminal emulation software, or to the Cardkey SMS.

UNPACKING THE EQUIPMENT

Carefully inspect the shipping containers as soon as you receive them (with the delivery agent present). Some shipping companies want to have an agent present when a damaged container is opened. If a container is damaged, open it immediately, inspect the contents, and have the agent make note on the shipping document. Check the purchase order against the packing slips to ensure the order is complete. If the contents of a container are damaged in any way, notify the carrier and your Johnson Controls® representative immediately. Report any discrepancies to your Johnson Controls representative. Save the packing materials for possible return shipments.

GENERAL DESCRIPTION

All CK721-A panels are connected via a 10/100Base-T Ethernet network to the Cardkey SMS. The CK721-A is intended to be mounted in an S300-DIN enclosure (large or small).

Each model has a total capacity 120,000 cards and a 5000 transaction base memory.

CK721-A panels are connected via standard 10/100Base-T cabling and 10/100Base-T hubs. The CK721-A is programmed and monitored via the Cardkey SMS. The CK721-A provides its own user interface through the serial connection located on the CK721-A. This interface facilitates the initial setup, as well as commissioning and troubleshooting.

The CK721-A is an advanced, intelligent controller. You can add terminals to connect readers, monitor 2 or 4-state input points, and add output relays to perform manual or automatic control functions. In addition, input points can be linked to output relays. Communication between the CK721-A and the terminals is accomplished via RS-485 per Cardkey implementation. The CK721-A uses both S300 terminals (S300-RDR2, S300-I16, S300-IO8, S300-SIO8, and S300-SI8), the S300-DIN-RDR2S terminal and the S300-DIN-RDR2SA terminal.

NOTE
CK721-A does not support the Dial-Up feature.

CK721-A Module

Table 1-1: CK721-A

Model Number	Description
CK721-A	A CK721-A module. Total storage capacity: 120,000 cards and 5000 transactions.

Enclosures

See Table 1-2 for a description of S300-DIN enclosures and expansion enclosures.

Table 1-2: S300 and S300-DIN Enclosures

Model Number	Description
S300-DIN-S	A small enclosure containing a DIN rail, a tamper switch and a power supply. It has room for one controller (CK721-A, S300-DIN-RDR2S, or S300-DIN-RDR2SA) and for a battery back-up unit.
S300-DIN-L	A large enclosure containing DIN rails, a tamper switch and a power supply. It has room for up to three modules (CK721-A, S300-DIN-RDR2S, S300-DIN-RDR2SA, or a combination thereof), and for a battery back-up unit.
S300-XL	A large expansion enclosure containing a tamper switch, a power indicator light, and a power supply. It has room for nine additional terminals and for a battery back-up unit.
S300-XS	A small expansion enclosure containing a tamper switch, a power indicator light, and a power supply. It has room for five additional terminals and for a battery back-up unit.
S300-XXS	An extra small enclosure containing a tamper switch, a power indicator light, and a power supply. It has room for two additional terminals and for a battery backup unit.

Terminals

NOTE

General information contained in this document and pertaining to the S300-DIN-RDR2S module also applies to the S300-DIN-RDR2SA module. For differences and specific information on these modules refer to their respective user documentation.

See the table below for a description of reader and I/O terminals.

Table 1-3: Terminals

Model Number	Description
S300-DIN-RDR2SA	Stand-alone RDR2SA unit with removable connectors which can be mounted on a DIN rail or on a flat surface.
S300-DIN-RDR2S	Stand-alone RDR2S unit which can be mounted on a DIN rail or on a flat surface.

Table 1-3: Terminals

S300-RDR2	Two reader interfaces per terminal
S300-I16	Sixteen 2-state inputs.
S300-IO8	Eight 2-state inputs and eight outputs.
S300-SIO8	Eight 4-state inputs and eight outputs.
S300-SI8	Eight 4-state inputs.

Additional Equipment

See Table 1-4 for a description of batteries and their corresponding bracket kits, power supplies, transformer, and parts accessory kit.

Table 1-4: Additional Equipment

Model Number	Description
S300-BAT	Battery for uninterruptible power operation, 12 volts, 7Ah. For use in expansion enclosures and S300-DIN-L (two backup batteries are used per enclosure).
S300-DIN-BRK	Battery bracket kit for either S300-DIN-L or S300-DIN-S.
S300-BAT-2.8AH	12V, 2.8Ah battery for S300-DIN-S (two backup batteries are used per enclosure).
S300-BRK2	Battery bracket kit, bracket with mounting hardware, and interconnecting cable for installing S300-BAT to inside of door of expansion enclosures.
S300-XFMR	120 VAC to 24 VAC plug-in transformer. Required for S300-DIN-S and expansion enclosures.
S300-DIN-L-PS	Power supply, 24VDC out, 110/220VAC 50/60Hz in.
S300-DIN-S-PS	Power supply, 24VDC out, 24VAC in.
S300-PS	Power supply, 5VDC/12VDC out, 24VAC in.
S300-DIN-PA1	Parts Accessory Kit. Contains a DC power harness, a lock, a tamper switch, and two spare connectors (3-position and 4-position).

SPECIFICATIONS (ALL PANELS)

The following table lists specifications for the CK721-A systems:

Table 1-5: CK721-A System Specifications

Item	Specification
Ambient Temperature	32 to 122 °F (0 to 50° C)
Humidity	20% to 80% non-condensing
Ventilation	Cabinets require free movement of air over all exposed surfaces
S300-DIN-L	16x20x6.6 in (41x51x17 cm) Approximate weight: fully loaded 45lb (20 kg)
S300-DIN-S	12x12x6 in (30x30x15 cm) Approximate weight: fully loaded 24lb (11 kg)
S300-XL	21x16x5.5 in (53x41x14 cm) Approximate weight: fully loaded 33lb (15 kg)
S300-XS	16x13.5x5.5 in (41x34x14 cm) Approximate weight: fully loaded 22 lb (10 kg)
S300-XXS	13x9x5.5 in (39x27x14 cm) Approximate weight: fully loaded 10 lb (4.5 kg)
Cabling	Described in Chapter 2 and Chapter 3.
Backup Battery	S300-BAT in expansion enclosures: minimum three hours sustained operation at full load. S300-BAT in S300-DIN-L: minimum one hour sustained operation at full load. S300-BAT-2.8AH in S300-DIN-S: minimum one and a half hours sustained operation at full load.

CK721-A PANEL CONFIGURATION

Each CK721-A can support up to 24 terminals within the following parameters:

- A maximum of eight reader terminals can be connected to a single CK721-A for a maximum of 16 readers per CK721-A.
- All 16 physical addresses apply *only* to IO8 and I16 terminals. If you are using SIO8 or SI8 terminals (supervised, 4-state alarms), you can only use physical addresses 1 through 8; addresses 9 through 16 will be invalid.

Figure 1-1 illustrates a simple CK721-A system configuration. For more information on panel installation and network connectivity, see *Chapter 3: S300 Expansion Enclosures* and *Chapter 4: CK721-A User Interface*.

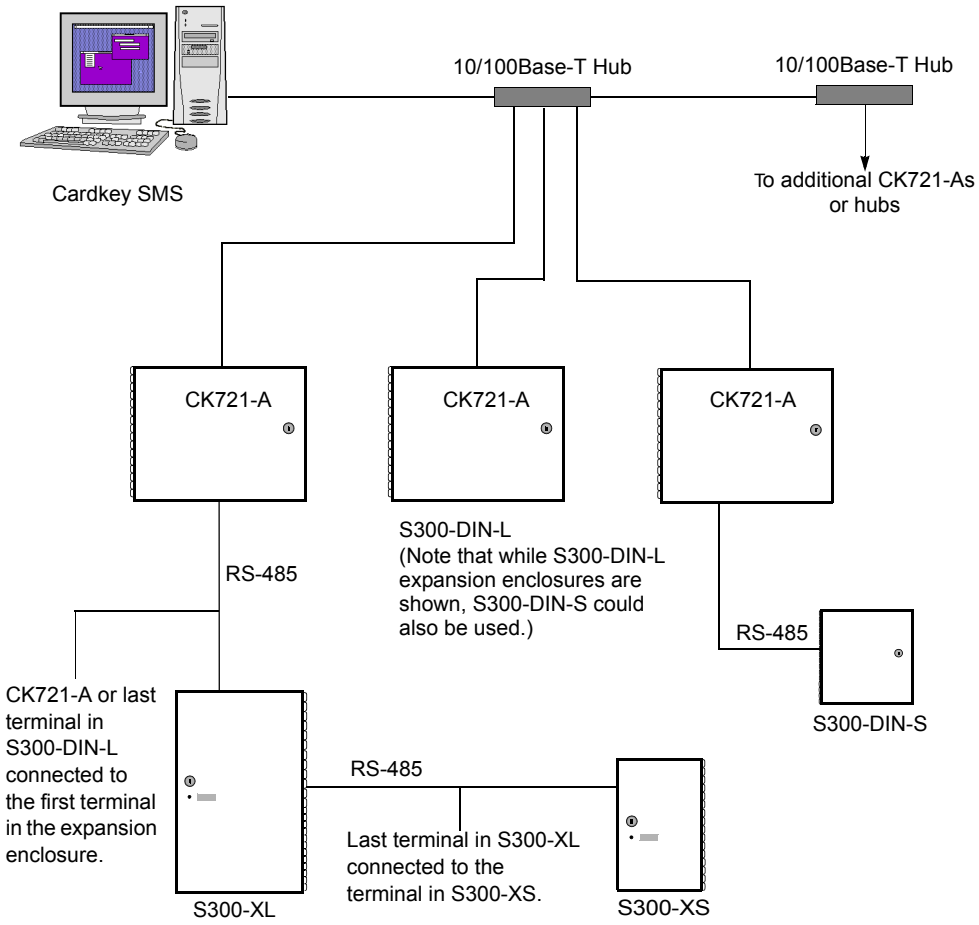


Figure 1-1: Sample CK721-A System Configuration

Maximum Enclosure Distance

CK721-A communicates with the Cardkey SMS via a 10/100Base-T Ethernet and TCP/IP protocol, therefore cabling of the system needs to comply with the industry-standard network guidelines.

10/100Base-T Networking Guidelines (specific to the CK721-A)

As a network device, the CK721-A can be installed in a variety of configurations based on the needs of your sites. The CK721-A communicates with the Cardkey SMS through one or more 10/100Base-T hubs.

The CK721-A must be installed using the standard 10/100Base-T four by five (annotated 4x5) rule. The rule states that:

- The 10/100Base-T network may contain a maximum of **four** hubs and **five** segments. Another explanation: a maximum of four hubs can be installed between the Cardkey SMS and the last CK721-A panel in the network.
- The maximum **segment length** is 354 ft (100 m). This is the distance between two hubs, or the distance between a hub and a network device such as the CK721-A.
- Wiring from a CK721-A to a hub is straight through. Specifically: CAT-5, 8 conductor cable, RJ45 connectors.

The following diagram illustrates the 4x5 rule.

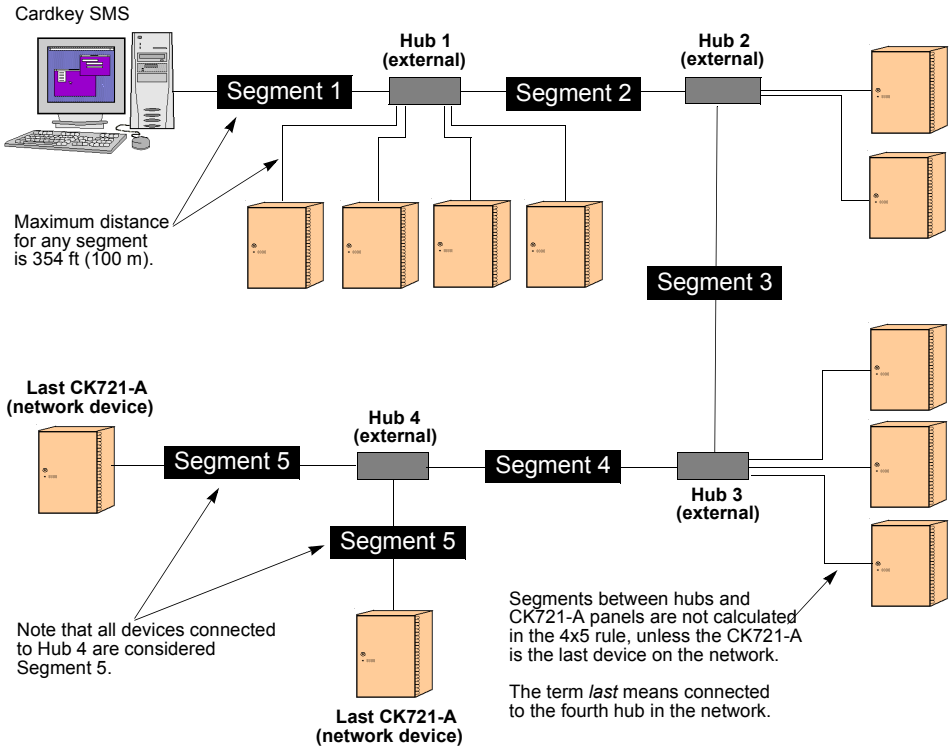


Figure 1-2: 10/100Base-T 4x5 Rule

NETWORK COMMUNICATION

The CK721-A panels communicate with the Cardkey SMS via 10/100Base-T Ethernet network. The communication protocol used is TCP/IP. The following subsections provide basic information regarding TCP/IP and 10/100Base-T networks and explain how the communication is accomplished. Because this type of network is very popular (TCP/IP is the principal protocol used on the Internet), reference materials are available in your local library or bookstore if you need more information.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a standard protocol allowing different devices, both hardware and software, to communicate over a network. For example, a network device can be a PC running an accounting application from a central server. Specific to Cardkey systems, network devices are the servers (running the Cardkey SMS software), networked remote Workstations, hubs, and the CK721-A panel.

While TCP/IP contains what may be thought of as a suite of network protocols, these two are the most important. TCP/IP is the primary network protocol used in UNIX systems. The phrase used here, *UNIX systems*, may seem confusing when one sees that computer network access is primarily accomplished through Microsoft® Windows-based operating systems, not UNIX systems. However, the servers (Web servers, for example) have generally been UNIX-based. Windows NT and Windows 2000, which have become popular as a network server operating systems in recent years, also use TCP/IP as a communication protocol. This is because the purpose of network protocols is to connect different devices.

Addressing

From an installation and operation standpoint, the only aspect of the TCP/IP protocol most users are concerned with is the IP address. Each networked device on a TCP/IP, 10/100Base-T Ethernet, must be assigned a unique IP address. The CK721-A is no exception. In basic terms, network communication is accomplished through the transmission and receipt of packets. Packets contain a variable length of data, along with the IP address of the device to which the packet is *addressed*. A network device knows its own IP address and accepts (or rejects) packets based on the match of that address. This is a very basic description, and as stated earlier, more information is available from a variety of other sources.

The network device must have a *unique* IP address. The performance of an entire network can be compromised if two devices share the same address.

10/100Base-T Ethernet

10/100Base-T Ethernet (also referred to simply as 10/100Base-T) is the physical network connecting the Cardkey SMS to the CK721-A panels. 10/100Base-T provides reliable connections using a series of hubs to lengthen a network's distance at a local level. Bridges, routers, and network switches increase a network's size to greater distances across states or over continents.

The basic unit of 10/100Base-T networks (and others as well) is the LAN (Local Area Network). Johnson Controls recommends the Cardkey SMS be on its own LAN, meaning a single self-contained network not connected to any other network. This will allow you to maintain security and implement a simple IP addressing scheme.

Communication Modes

The Cardkey SMS communicates with terminals that provide reader interfaces, input points, or output relays. Communication is bi-directional. Some messages are sent from the Cardkey SMS server to the field panels, and others are sent from the panels to the server, and then forwarded to Cardkey SMS workstations. The volume of messages across the communication link depends on the operating mode of the system.

System performance where communication is concerned can be defined as the speed at which access decisions are made after a card is used. While several factors affect overall system performance, the most significant factor is the operation mode, which you can define when programming the system. The Cardkey SMS software provides three operating modes:

- **Local**. In this mode, all access decisions are made by the field panels. This eliminates the need for panels to communicate with the server every time an access request is presented at a reader. Local mode provides the best overall system performance.
- **Central**. This mode is useful when you want to assign access restrictions on a global scale (throughout the entire system). All access requests are forwarded to the server for an access grant or deny decision.
- **Shared**. With this mode, access decisions can be made at the panel level or by the server. Field panels will first search for a card in their memory, as in Local Mode. If a card's record is not found at the panel level, the access request is then forwarded to the Server, as in Central mode. Shared mode is useful when a panel's card capacity is exceeded.

More information on the Cardkey SMS operating modes is provided in the *P2000 Software User Manual*.

Chapter 2

CK721-A AND S300-DIN ENCLOSURES

This chapter describes the equipment used with the CK721-A.

NOTE

Information in this chapter pertaining to the S300-DIN-RDR2S module also applies to the S300-DIN-RDR2SA module. For differences and specific information on these modules refer to their respective user documentation.

CK721-A

This section describes components of the CK721-A. Picture of the module is followed by a detailed description of the components.

The major functional components of the CK721-A are:

- Embedded 32-bit processor
- 128 MB onboard flash memory (for the operating system and database)
- 3V lithium battery
- IN1 and IN2 - Binary inputs, unsupervised
- Binary output - Form C Relay, SPDT, 24 VDC maximum
- LED indicators (POWER, FAULT, RS485 A, RS485 B, ETHERNET, 10/LINK, 100/LINK, and RUN)
- Connectors:

  RS232 A - RS-232 Serial Interface, DB9 port for the user interface to Workstations or laptop computers

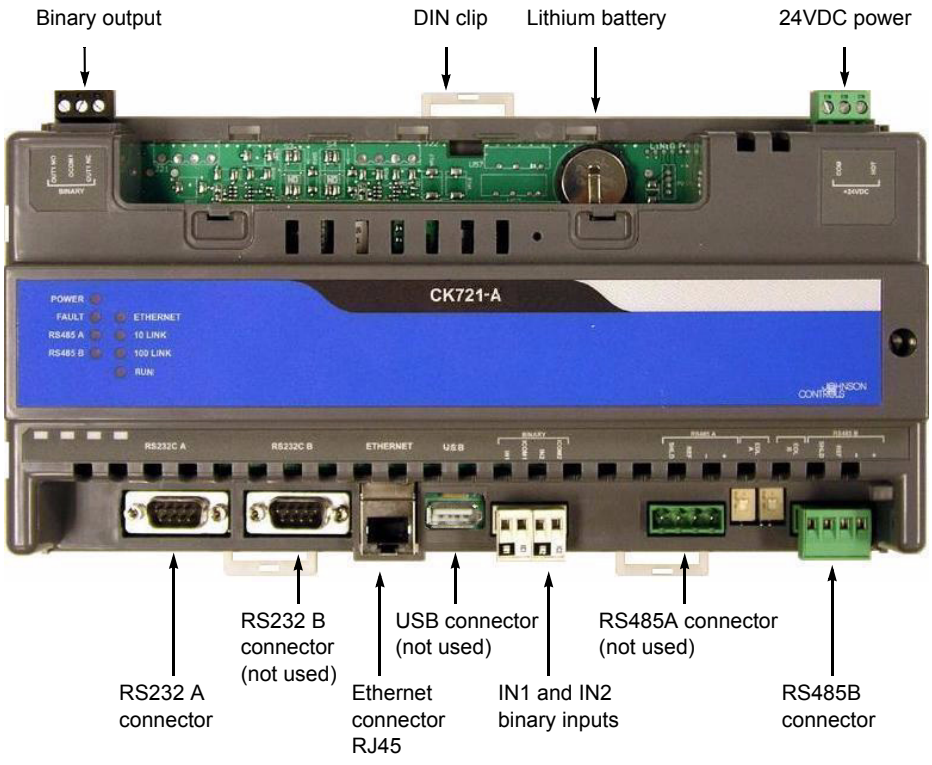
  RS232 B - Not used

  RS485A - Not used

  RS485B - For field device communication

  RJ45 - 10/100Base-T network port for host communication

  USB - Not used



LEDs on the CK721-A

There are nine LEDs on the CK721-A board. Their functions are shown in Table 2-1.

Table 2-1: CK721-A LED Functions

LED	Function
POWER	ON steady when power is applied.
FAULT	OFF to indicate normal operation.ON indicates a general fault.
RS485 A	OFF (the RS485A connector is not used in CK721-A)
RS485 B	Flashes/flickers to indicate data transmit.
ETHERNET	Flashes/flickers to indicate data traffic on the Ethernet connection. OFF indicates no Ethernet data traffic, and probably indicates a dead Ethernet network or bad Ethernet connection.
10/LINK	ON to indicate 10 Mbit connection is established.
100/LINK	ON to indicate 100 Mbit connection is established.
RUN	This LED is currently not used (always OFF).

Binary Output

The CK721-A provides a relay output for connecting to an external alarm at Binary Out1. If the alarm relay is programmed for enabled, and the individual inputs are programmed to activate the relay, the relay can be activated when any input point in the system goes into alarm. The binary output can be individually programmed for each input point, and the relay can be programmed to latch until the alarm is acknowledged or to mimic the status of the alarm inputs. The relay will switch 2A at 24 VDC.

Lithium Battery

The CK721-A contains a lithium battery that is used for realtime clock backup. The lithium battery is shipped from the factory charged and operational.

If there are no power outages, the battery should be changed every five years. If a power outage occurs, the battery life is approximately 30 days. Replace with Panasonic part number CR2025 or equivalent.

CAUTION

Before you replace the lithium battery (recommended every five years or after extended use), ensure AC power or backup battery power is supplied to the CK721. If AC power or backup battery power is not supplied before you remove the lithium battery, the realtime clock will be incorrect.

WARNING

Danger of explosion if battery is incorrectly replaced.

Input Power

The input power is described in the following table:

Table 2-2: Input Power

Inputs	V Min	V Nom	V Max
+24VDC	20	24	30

RS485

CK721-A has two RS485 ports:

- RS485A (not used)
- RS485B is used to communicate with external devices such as RDR2S, RDR2, IO8, SIO8, and I16

The controller can communicate on the serial bus by *either* of the following settings:

- 19200 bps, no parity, 8 bits per character, and one stop bit
- 9600 bps, even parity, 8 bit per character, and one stop bit

Figure 2-1 and Figure 2-2 show shows the wiring between RS485B and the devices.

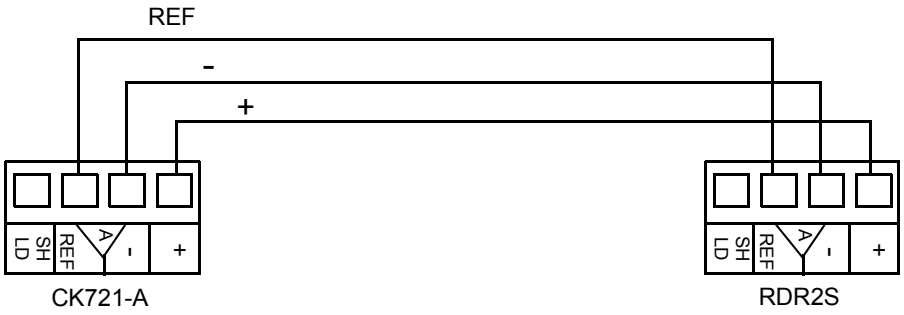


Figure 2-1: Wiring Between RS485B and RDR2S Devices

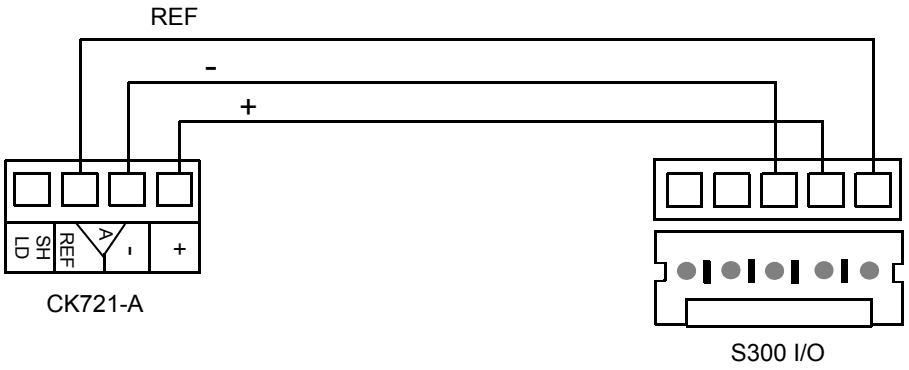


Figure 2-2: Wiring Between RS485B and S300 I/O Devices

Binary Input

CK721-A has two Binary Inputs:

- Binary Input 1

  This input is logically mapped at the host as the soft alarm Panel Lost AC.

  The Binary Input 1 is wired to the Trouble pin located on the power supply. The Trouble pin is activated when there is no AC power ***and*** the battery voltage drops to 23.9 VDC or less. For wiring details see Figure 2-3.

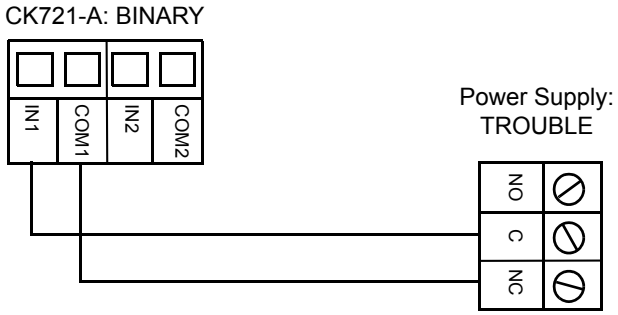


Figure 2-3: Wiring Between Binary Input 1 and Trouble Pin

- Binary Input 2

  This input is logically mapped at the host as the soft alarm Panel Tamper.

The open state means “alarm set,” and the closed state means “alarm secure.”

Connecting the Network

The CK721-A system communicates with the Cardkey SMS server via 10/100Base-T Ethernet, using the TCP/IP protocol.

The following types of wiring may be required:

- Hub to CK721-A, straight through
- Hub to hub straight-through or crossed, depending on the hub used

Hub to CK721-A Wiring

All network devices designed for 10/100Base-T networking use standard RJ45, 8 pin ports. Like other 10/100Base-T devices, the CK721-A RJ45 port is designed to connect to a hub using pins 1, 2, 3, and 6, wired straight through.

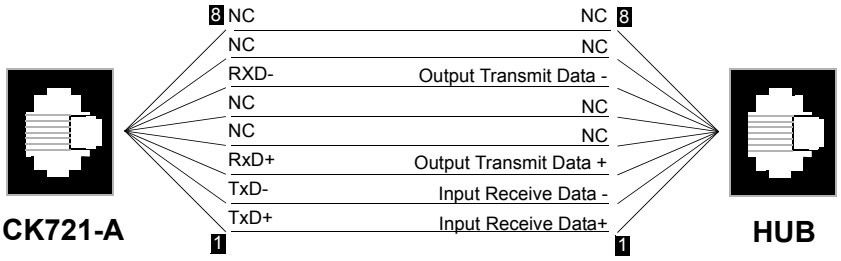


Figure 2-4: Hub to CK721-A Wiring

RS232

CK721-A has two RS232 connectors.

- RS232C A connects to a terminal emulator. The communication parameters are 115000 bps, no parity, 8 bits per character, one stop bit, and no control flow.

  The RS-232 port has the following pinout:

Pin	*Function*	*(Direction)*
1.	Carrier Detection	(In)
2.	Receive Data	(In)
3.	Transmit Data	(Out)
4.	Data Terminal Ready	(Out)
5.	Signal ground	
6.	Data Set Ready	(In)
7.	Request to Send	(Out)
8.	Clear to Send	(In)
9.	Ring Indicator	(In)

- RS232C B is not being used.

LARGE ENCLOSURE (S300-DIN-L)

The S300-DIN-L enclosure comes with a backplate, a tamper switch, a lock, and a ground strap kit that have to be installed. The backplate contains a power supply and DIN rails for module mounting.

Up to three modules can be mounted on the DIN rails (three S300-DIN-RDR2S modules, or one CK721-A module and two S300-DIN-RDR2S modules).

The enclosure can also hold a backup battery unit composed of two 12V lead-acid batteries in two battery brackets.

Figure 2-5 gives you an overview of the large enclosure with all components installed. The modules shown here are S300-DIN-RDR2S.

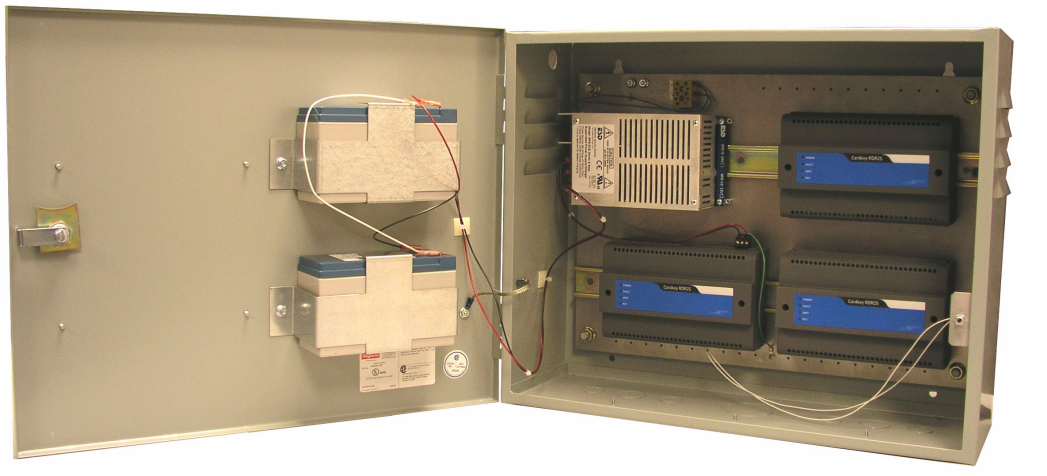


Figure 2-5: Large Enclosure With Installed Components

The figures below depict the CK721-A module mounted alone and with the S300-DIN-RDR2S modules.

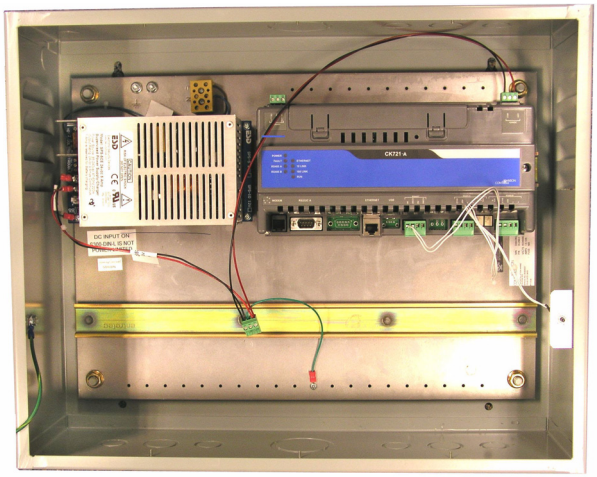


Figure 2-6: One CK721-A Module Mounted in a Large Enclosure

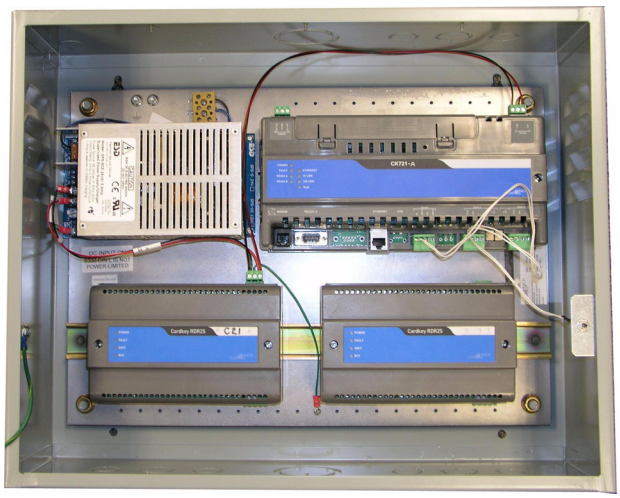


Figure 2-7: One CK721-A Module and Two S300-DIN-RDR2S Modules Mounted in a Large Enclosure

Wiring CK721-A and S300-DIN-RDR2S Modules

CK721-A Cable Requirements

Table 2-3: Cable Requirements

Description	Recommended Cable Type	Maximum Segment Length
+24VDC	Listed, 18 AWG, Stranded, Hook-up wire.	Limited to within cabinet
RS485 B	Listed, 22 AWG, Stranded, Hook-up wire.	Limited to within cabinet
	Listed, 18 AWG, 3-cond, stranded, shielded.	4000 ft (1215 m). All modules connected to a single CK721-A panel must be within 4000 feet of the panel.
Inputs ICOM1 and ICOM2	Belden 88442, 1 twisted pair, 22 AWG.	500 ft (152m)
Output/Relay OUT1	Belden 8461, 1 twisted pair, 18 AWG.	Depends on power requirements of the door strike. Voltage to the strike must not be reduced more than 10% over the 18 AWG wire.

Table 2-3: Cable Requirements

Description	Recommended Cable Type	Maximum Segment Length
RS232 A	Listed DB9 F/F AT Null Modem	25 ft (7m). Cable must remain in the same room as the CK721-A.
RS232 B	Listed, Category 5, 24 AWG, solid, 4 pair type.	25 ft (7m). Cable must remain in the same room as the CK721-A.
Ethernet	Listed, Category 5, 24 AWG, solid, 2 pair or 4 pair type.	354 ft (100 m). Cable, RJ45 connector, and RJ45 crimp tool to be supplied by customer.

Chain Module Wiring

When connecting more than one RDR2S module, wire the modules in parallel following the "daisy chain" pattern, as shown in Figure 2-8. For connector wiring details refer to Figure 2-14.)

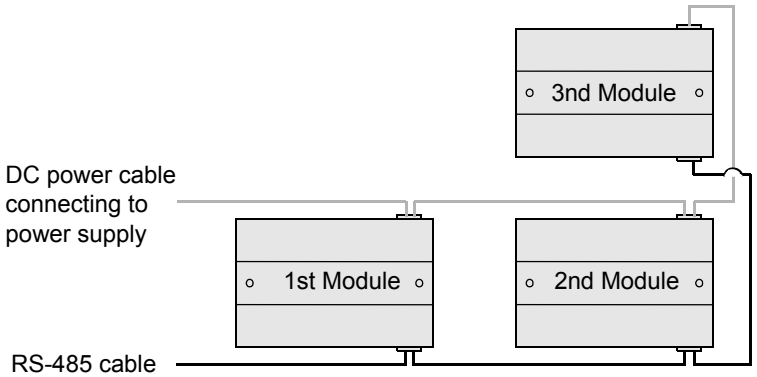


Figure 2-8: Daisy Chain Module Wiring for S300-DIN-L

CAUTION

Do not connect the DC power cable to the RDR2S until all wiring is complete.

Cable Routing

All low-level input cables, such as system data and reader cables, must be shielded types. The cables should run in grounded conduit or at least two feet from AC power, fluorescent lights, or other high energy sources.

All data cables should be physically separated from power lines. If conduit is used, do not run data cables in the same conduit as power cables or certain door strike cables, e.g. strike voltage greater that 42V or Magnetic door locks without EMI suppression.

All cables must conform with National Electrical Code, NFPA 70,* and local electrical codes. Cabling should be made using good wiring practices and should be long enough to allow service loops at their terminations in the enclosure. *For Canadian installations, refer to the Canadian Electric Code C22.1.

Grounding Cable Shields

Refer to *Appendix A: Grounding and Connectors* for details on the requirements. The grounding screws used are #6 x 1/4” self-tapping, and are provided in the hardware installation kit.

Chassis Grounding

Proper grounding of the S300-DIN-L enclosure is essential for the protection of electronic components against electrostatic discharge. A ground wire, 18 AWG minimum, must be run from the dedicated ground stud inside the enclosure to the building’s electrical ground. The dedicated ground stud is marked with the symbol ⏚.

NOTE

Cold water pipe is not an acceptable ground due to common use of non-conductive plastic pipe.

SMALL ENCLOSURE (S300-DIN-S)

The S300-DIN-S enclosure comes with a backplate, a tamper switch, a lock, and a ground strap kit that have to be installed. The backplate contains a power supply and a DIN rail for mounting of one S300-DIN-RDR2S, or CK721-A module. The enclosure can also hold a backup battery unit composed of two 12V lead-acid batteries in one battery bracket.

Figure 2-9 gives you an overview of the small enclosure with all components installed. The module shown here is S300-DIN-RDR2S.

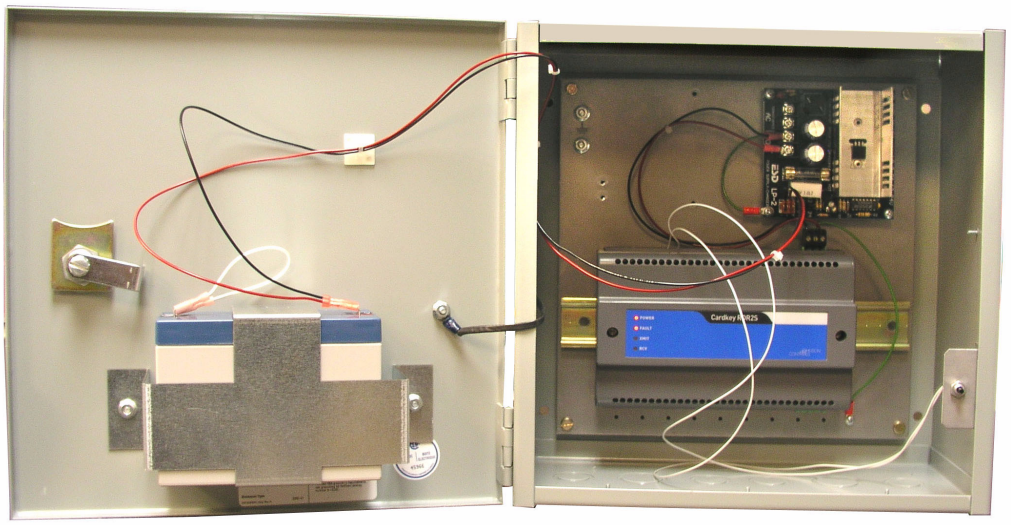


Figure 2-9: Small Enclosure With Installed Components

Verifying DC and Chassis Ground

➤ **To verify DC ground:**

1. Verify the wire connection between the power supply and COM on the S300-DIN-RDR2S or CK721-A.
2. Verify the wire connection between the power supply and its standoff.

➤ **To verify chassis ground:**

1. Verify the wire connection between the S300-DIN-RDR2S or CK721-A earth and the backplate.
2. Verify the wire connection between the AC power source and the backplate.
3. Verify the wire connection between the DC- and one of the power supply's mounting holes.

Installing CK721-A Module

The CK721-A module is mounted on a backplate's DIN rail.

To mount a module, align it with the rail and snap on. To remove a module, pull down the white clip located on the bottom of the module, then pull the bottom of the module out and lift it up.

NOTE

Do not connect the DC power cable to the CK721-A until all wiring is complete.

The figure below depicts one CK721-A module in a small enclosure.

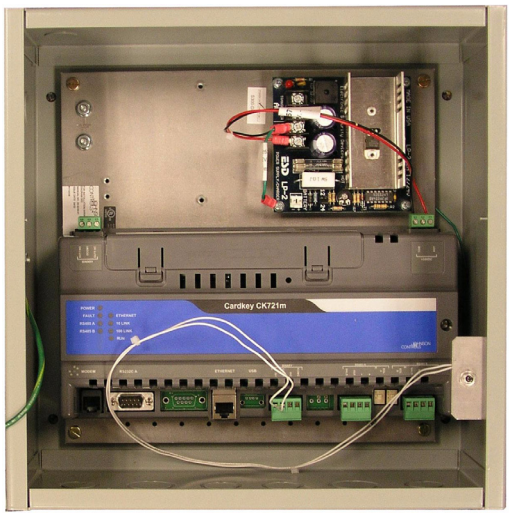


Figure 2-10: One CK721-A Module Mounted in a Small Enclosure

Cable Routing

All low-level input cables, such as system data and reader cables, must be shielded types. The cables should run in grounded conduit or at least two feet from AC power, fluorescent lights, or other high energy sources.

CAUTION

All data cables should be physically separated from power lines. If conduit is used, do not run data cables in the same conduit as power cables or certain door strike cables, e.g. strike voltage greater that 42V or Magnetic door locks without EMI suppression.

All cables must conform with National Electrical Code, NFPA 70,* and local electrical codes. Cabling should be made using good wiring practices and should be long enough to allow service loops at their terminations in the S300-DIN-RDR2S or CK721-A enclosure. *For Canadian installations, refer to the Canadian Electric Code C22.1.

Grounding Cable Shields

Refer to *Appendix A: Grounding and Connectors* for details on the requirements. The grounding screws used are #6 x 1/4” self-tapping, and are provided in the hardware installation kit.

Chassis Grounding

Proper grounding of the S300-DIN-S enclosure is essential for the protection of electronic components against electrostatic discharge. A ground wire, 18 AWG minimum, must be run from the dedicated ground stud inside the enclosure to the building's electrical ground. The dedicated ground stud is marked with the symbol ⏚.

NOTE

Cold water pipe is not an acceptable ground due to common use of non-conductive plastic pipe.

NO ENCLOSURE

The CK721-A modules should be mounted on a DIN rail.

DIN Rail Mounting

To mount an CK721-A module on a DIN rail, align it with the rail and snap on. To remove a module, pull down the white clip located on the bottom of the module, then pull the bottom of the module out and lift it up.

Figure 2-11: CK721-A Module Mounted on a DIN Rail.

+24 VDC CONNECTOR

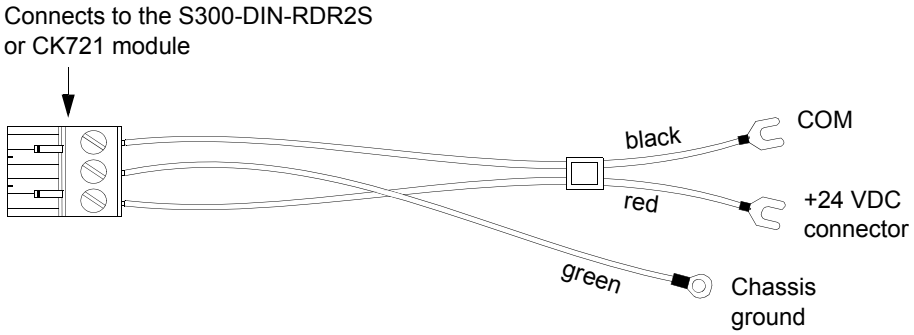


Figure 2-12: +24 VDC Connector (Part of the DC Power Harness)

Power Wiring

For power wiring with either the large or small enclosure, use the cable assembly shown in Figure 2-12.

When connecting multiple S300-DIN-RDR2S or CK721-A modules, wire the modules in parallel following the "daisy chain" pattern as shown in Figure 2-13 and Figure 2-14.

To construct the power wiring, use 18AWG wires.

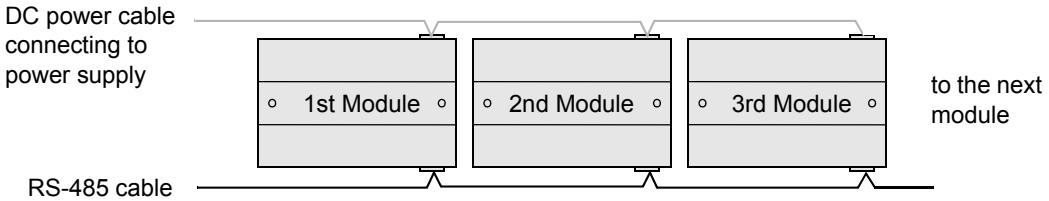


Figure 2-13: Wiring Multiple Modules - Overview

CAUTION

Make sure each wire is connected to the same corresponding connector position in the subsequent S300-DIN-RDR2S or CK721-A module. See Figure 2-14 for details.

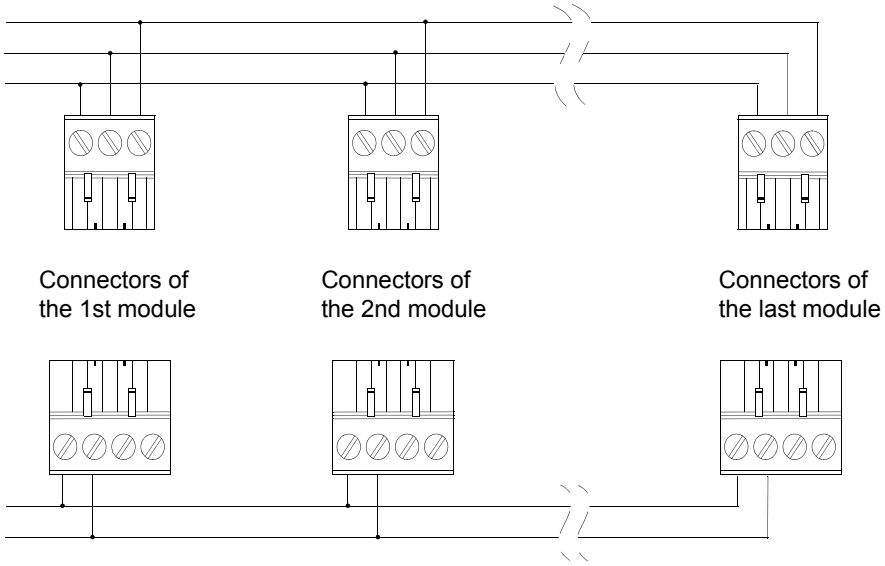


Figure 2-14: Wiring Multiple Modules - Connector Details

CAUTION

Do not connect the DC power cable to the S300-DIN-RDR2S or CK721-A module until all wiring is complete.

Ground Wiring

For ground wiring with the either large or small enclosure, use the cable assembly shown in Figure 2-12. The ground wire should be connected to the backplate by fastening the ring terminal to any one of the 0.11" holes located at the bottom of the plate with a #6 self-tapping screw.

When connecting multiple S300-DIN-RDR2S or CK721-A modules, wire the modules in parallel following the “daisy chain” pattern as shown in Figure 2-13 and Figure 2-14.

To construct the ground wiring, use 18AWG wires.

Chapter 3

S300 EXPANSION ENCLOSURES

This chapter provides information on S300 expansion enclosures and accessories, as well as their installation. It also describes terminals used with CK721-A.

S300 EXPANSION ENCLOSURES

The S300 expansion enclosures are used to host additional terminals in the CK721-A system. The cannot, however, be user with the CK721-A controller itself, because they do not have the DIN rails necessary for its mounting.

Installing the Expansion Enclosures

Before beginning, take a moment to read the following warning and caution. Careful adherence to the procedures and caution/warning statements in this manual will help ensure the successful installation and operation of your system.


WARNING

It is important to follow the installation procedures described in this chapter very carefully. Power wiring and grounding from the building to the S300 expansion enclosures must only be performed by certified electricians.

Failure to have qualified professionals perform these functions can result in personal injury, damage to a facility's electrical system and other equipment, or damage to the system and devices.


CAUTION

Electronic components such as the printed circuit board assemblies used in the S300 expansion enclosures are extremely static sensitive. To prevent electrostatic discharge (ESD) damage, a properly grounded wrist strap must be used at all times when handling the components. If a wrist strap is not available, touch any part of the metal CK721-A cabinet prior to handling components to discharge static electricity. It is advisable to avoid working on carpeted areas if possible.

Tools Required

The following tools are required to install S300 expansion enclosures:

- Mounting tools such as a drill and anchors (depending on where you mount the panels)
- Phillips screwdriver
- Small common screwdriver
- Standard wiring tools
- Hammer and punch

Sequence of Steps

Although each site configuration may differ and require different steps, the standard steps required for installing S300 expansion enclosures are:

- Planning the installation
- Mounting the enclosures
- Installing the first level terminals
- Wiring and configuring first level terminals
- Installing the second level (stacked) terminals
- Wiring and configuring second level terminals

Planning the Installation

This section provides important information you will need when planning the installation of an S300 expansion enclosure.

S300-XL (S300 Expansion Enclosure, Large)

S300-XL contains a power supply, a tamper switch, a power indicator light, and a lock.

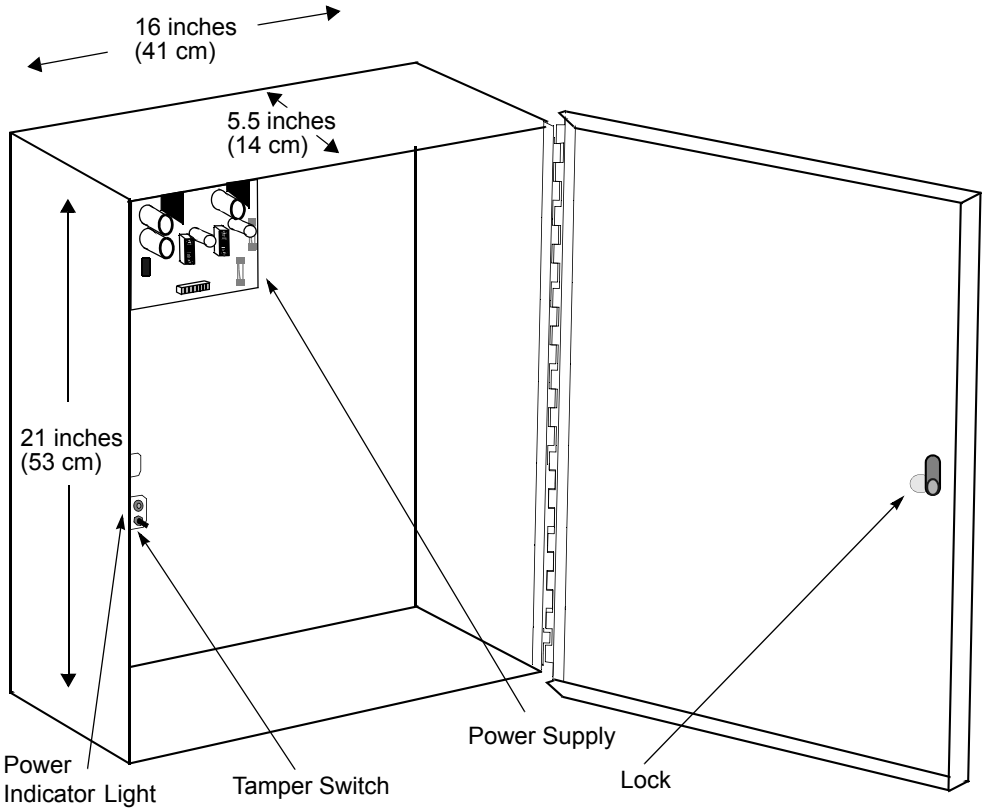


Figure 3-1: S300-L

S300-XS (S300 Expansion Enclosure, Small)

S300-XS contains a power supply, a tamper switch, a power indicator light, and a lock.

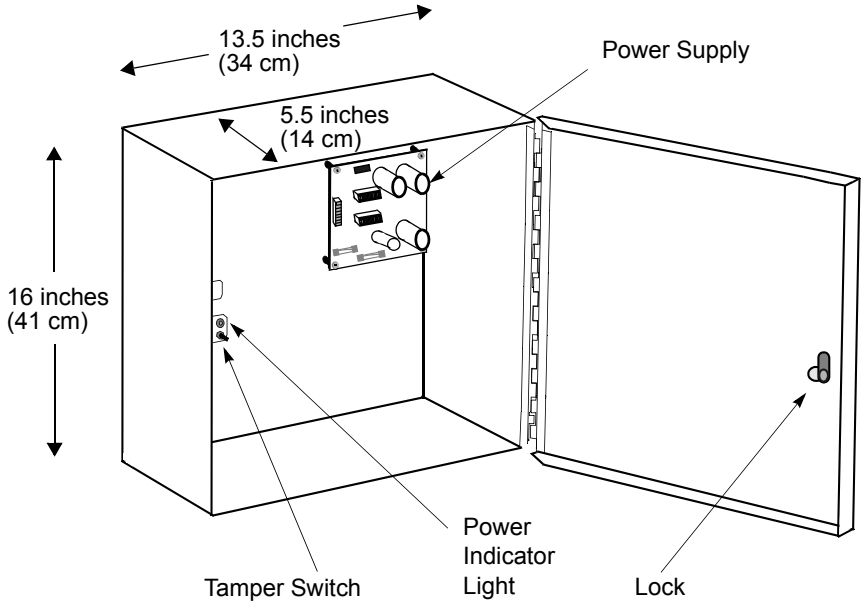


Figure 3-2: S300-XS

S300-XXS (S300 Expansion Enclosure, Extra Small)

S300-XXS contains a power supply, a tamper switch, a power indicator light, and a lock.

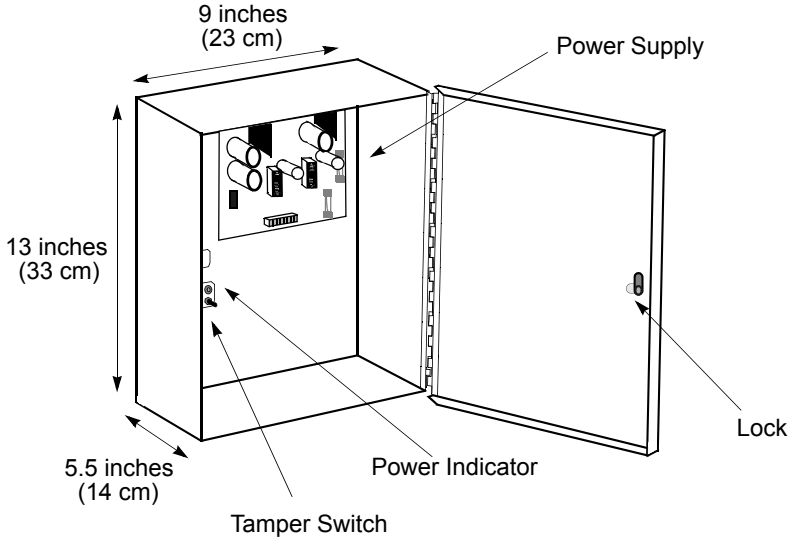


Figure 3-3: S300-XXS

Removing the Knockouts

All S300 expansion enclosures have metal knockouts around the outside edge. Use the knockouts to run your wiring to external devices and other S300 expansion enclosures. Prior to mounting the panel, determine which side or sides of the cabinet to run the wiring through. Remove the knockouts using a hammer and a punch. Remove only the knockouts required for wiring.

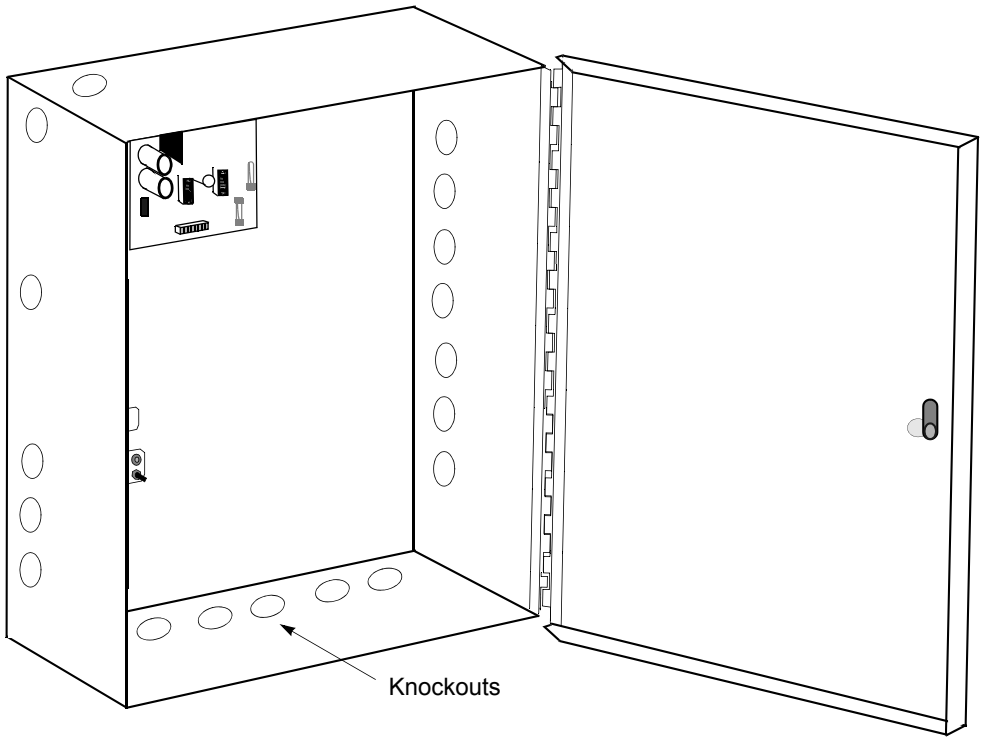


Figure 3-4: S300 Expansion Enclosure Knockouts

Mounting the Enclosures

Because applications and facilities vary, it is not within the scope of this manual to provide exact mounting instructions for S300 expansion enclosures. The surface on which you mount the panels at your site determines the type of hardware required to fasten the panels into place. Keep in mind the following principles when mounting panels.

- S300 expansion enclosures are mounted using the four mounting holes shown in Figure 3-5 through Figure 3-7.
- Adhere to the environmental requirements shown in Table 1-5.

Removing Boards from the Panels

Panels are easier to install if you:

- Do not install terminals prior to mounting the panels.
- Remove the power supply from the S300 expansion enclosures.

This also helps ensure system performance because the boards will not be subject to debris during installation. When installing expansion enclosures, you only need to remove the power supply.

Panel Location Suggestions

Mount the S300 expansion enclosures on a wall or other mounting surface located in a restricted-access area. Suggested locations are a locking utility closet, or if necessary, inside a suspended ceiling. Mount the panel so the door can swing fully open to the right. The location must allow for air to flow uninhibited over the exposed surfaces. The panel can function in any position, but it is best to mount it flat against a vertical surface with the hinge to the right.

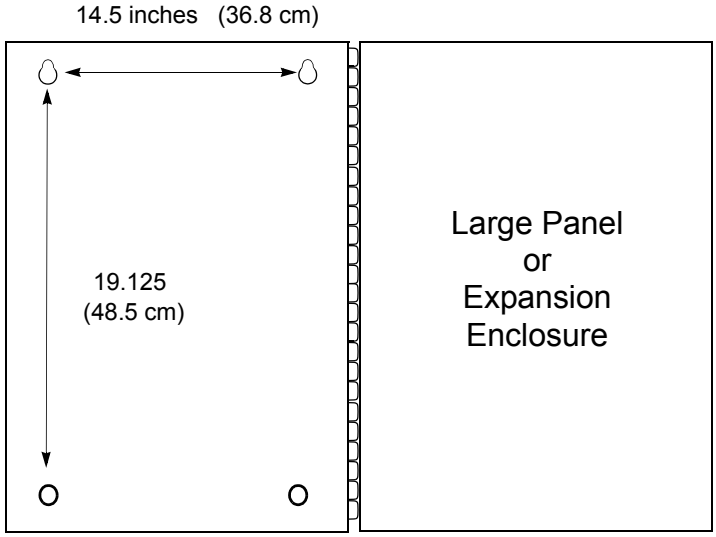


Figure 3-5: Mounting the Panels: S300-XL

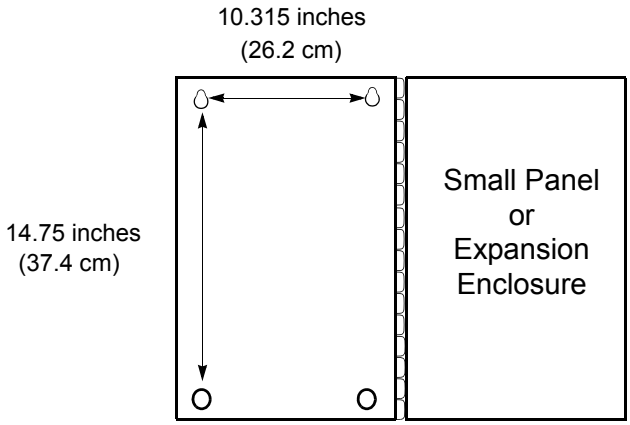


Figure 3-6: Mounting the Panels: S300-XS

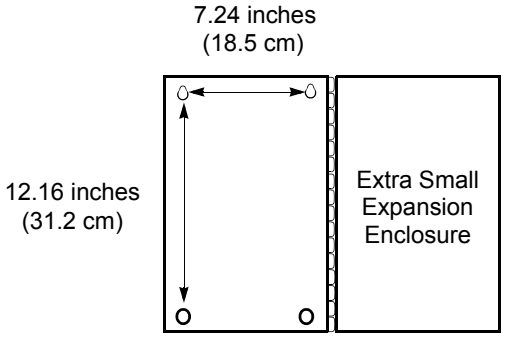


Figure 3-7: Mounting the Panels: S300-XXS

Installing the Power Supplies

If you have removed the power supplies prior to mounting the S300 expansion enclosures, it is important they are re-installed in the same location. This will preserve the proper terminal locations for fully stacked systems containing battery backup units (described later in this chapter).

Installing the First Level Terminals

NOTE

It is difficult to set first level terminals switches and connect RS-485 cables once the stacked terminals are installed.

This section describes the installation and wiring of S300 terminals. The terminals include input and output terminals and reader terminals. The wiring instructions are the same for terminals in expansion enclosures.

Terminals can be installed inside the S300 expansion enclosure. The installation of the following terminals are discussed in this chapter:

- S300-RDR2 - reader terminal
- S300-I16 - Unsupervised Input terminal
- S300-IO8 - Unsupervised Input/Output terminal
- S300-SIO8 - Supervised Input/Output terminal
- S300-SI8 - Supervised Input terminal

The maximum distance from a CK721-A to the last terminal connected to it is 4000 feet (1219 meters).

To facilitate future expansion, terminals should be installed sequentially as shown in Figure 3-8 through Figure 3-10.

CAUTION

Before installing terminals in an S300 expansion enclosure, ensure the power is OFF. The battery and transformer must be disconnected for the power to be completely OFF.

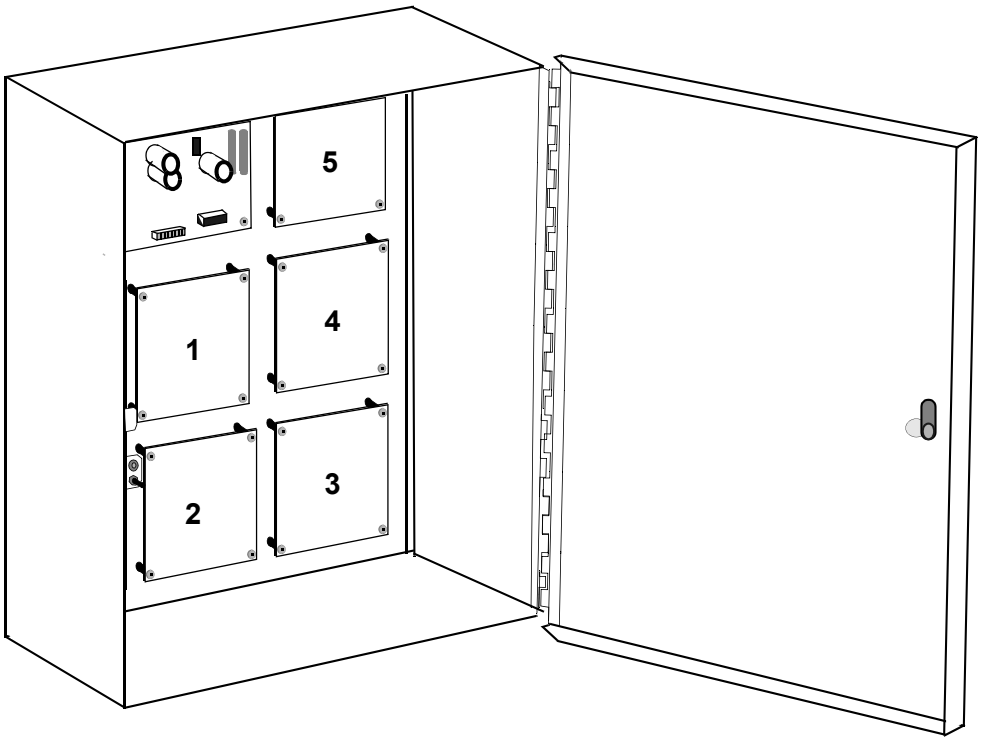


Figure 3-8: First Level Terminal Locations in S300-XL

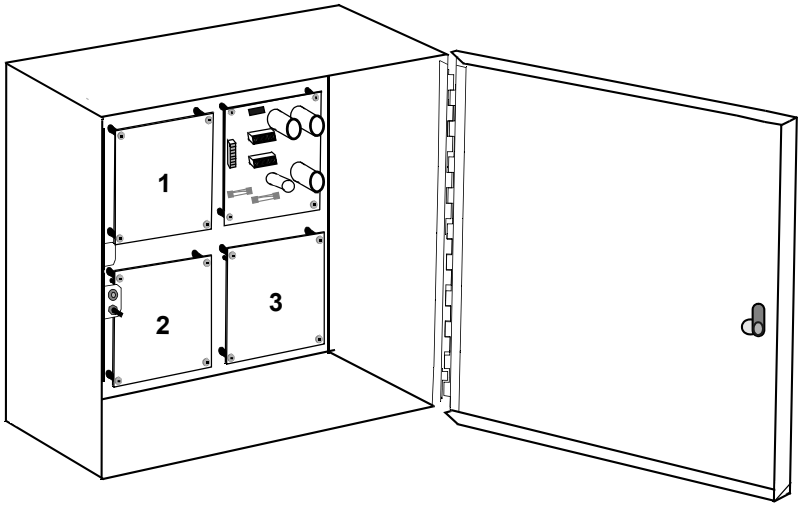


Figure 3-9: First Level Terminal Locations in S300-XS

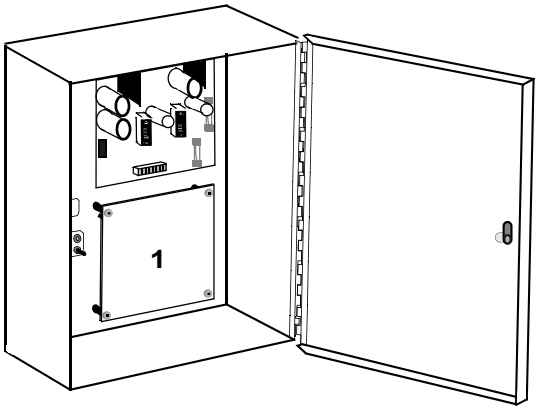


Figure 3-10: First Level Terminal Location in S300-XXS

All terminals come with the hardware required to mount them. Mount the terminals to the back of the enclosure by using the following procedure:

1. Install the four 5/8 inch standoffs into the nuts located on the back of the enclosure.
2. Position the terminal over the standoffs and secure with the mounting screws.
3. Attach RS485 cable from the CK721-A to the terminal or terminal to terminal.

NOTE

All four mounting screws must be used to ensure proper grounding.

Installing the Second Level (Stacked) Terminals

NOTE

It is difficult to set first level terminals switches and connect RS-485 cables once the stacked terminals are installed.

The S300 expansion enclosures support a stacked configuration for terminals. However, after stacked terminals have been installed, it is difficult to reach the first level terminals for purposes of switch settings or wiring.

To stack terminals, perform the following steps:

1. Remove the four screws holding the terminal to the enclosure back.
2. Secure the first level terminal with the 2 inch standoffs supplied in the kit in place of the screws removed in step 1.
3. Secure the stacked terminal in place with the four screws removed in step 1.

You can install stacked terminals in the locations shown in Figure 3-11 through Figure 3-13. Only use these locations, because room must be left inside the cabinet for the door to close with the backup battery installed.

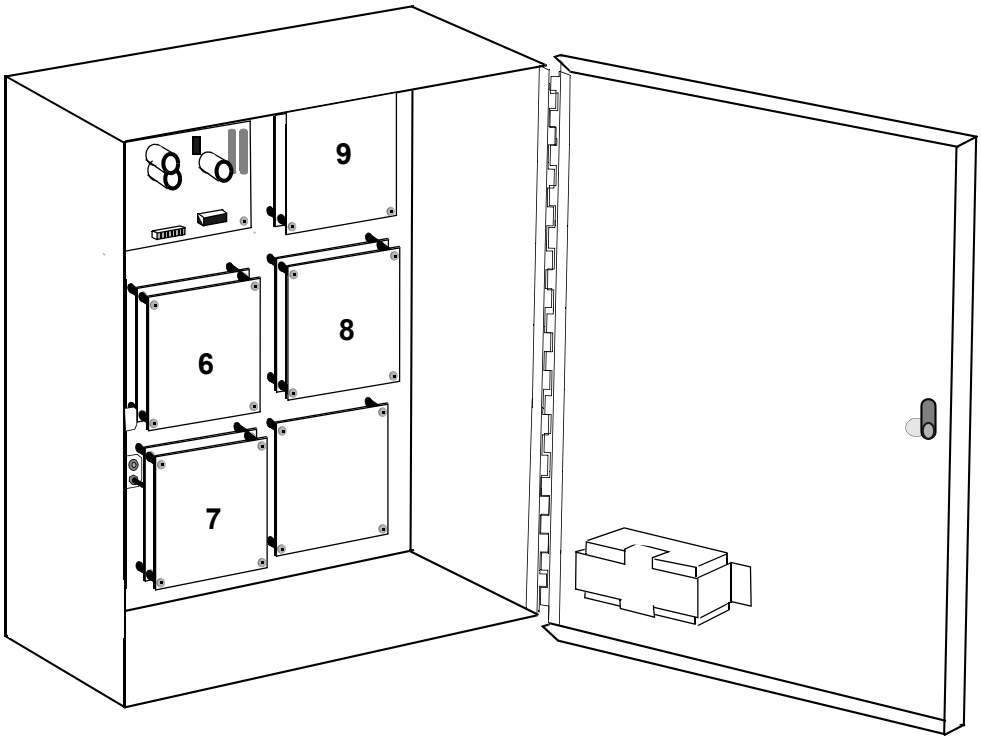


Figure 3-11: Stacked Terminal Locations in S300-XL

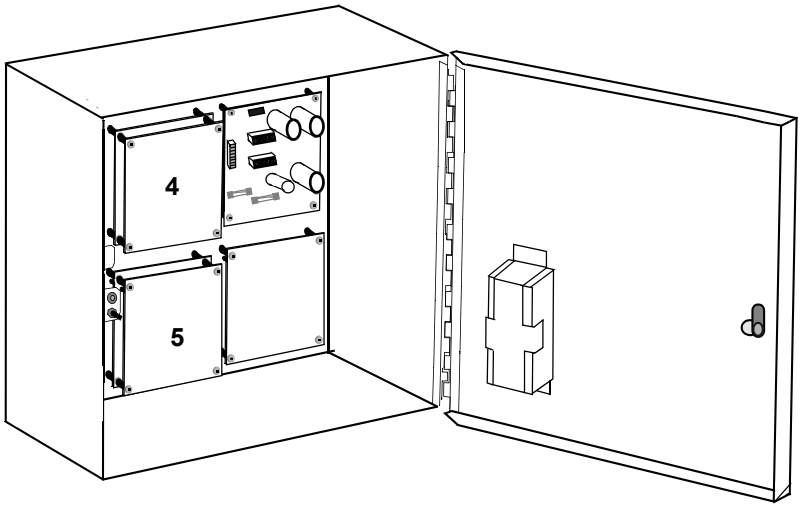


Figure 3-12: Stacked Terminal Locations in S300-XS

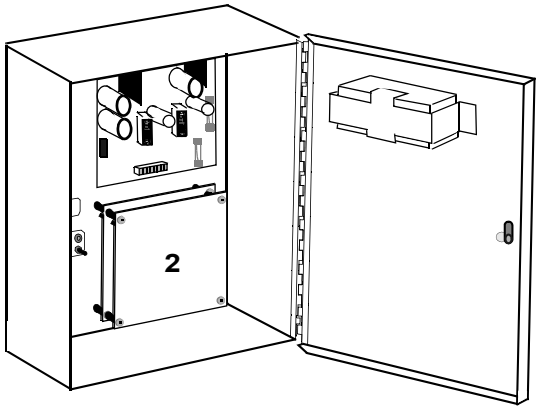


Figure 3-13: Stacked Terminal Locations in S300-XXS

Cabling

This table describes the recommended cable to use when wiring the system.

Table 3-1: Cable Types

Description	Recommended Cable Type	Maximum Segment Length
CK721-A Panel to Expansion Enclosure		
Cardkey RS-485 Standard (included with terminals)	Johnson Controls Supplied	Approximately 30 inches (18.5 cm). Note the cable shipped from Johnson Controls is 30 inches, but the length extending outside of the panel will vary depending on your wiring scheme and size of panel.
Cardkey RS-485 Extended (if additional length required)	Listed, 18 AWG, 3-conductor, Shielded	4000 feet (1219 m) maximum. All expansion enclosures connected to a single RS485 BUS must be within 4000 feet of the panel.
Door Controls		
Door Strike	Belden 8760, 1 twisted, shielded pair, 18 AWG	Length depends on power requirements of the door strike. Voltage to the strike cannot be reduced more than 10% over the 18 AWG wire.
Door Open	Belden 8761, 1 twisted, shielded pair, 22 AWG	500 ft. (152 m)
Auxiliary Access	Belden 8761, 1 twisted, shielded pair, 22 AWG	500 ft. (152 m)
Reader to S300-RDR2		
Keypad	Refer to individual reader specifications.	250 ft. (76 m)
Non-keypad	Refer to individual reader specifications.	500 ft. (152 m)

All low-level input cables, such as system data and reader cables, must be shielded types. The cables should run in grounded conduit or at least two feet from AC power, fluorescent lights, or other high energy sources.

All data cables should be physically separated from power lines. If conduit is used, do not run data cables in the same conduit as power cables or certain door strike cables, e.g. strike voltage greater that 42V or Magnetic door locks without EMI suppression.

All cables must conform with National Electrical Code, NFPA 70,* and local electrical codes. Cabling should be made using good wiring practices and should be long enough to allow service loops at their terminations in the CK721-A enclosure. *For Canadian installations, refer to the Canadian Electric Code C22.1.

Refer to *Appendix A: Grounding and Connectors* for details on the requirements. The grounding screws used are #6 x 1/4" self tapping, and are provided in the hardware installation kit.

Cabling Between Enclosures

Each S300 expansion enclosure is shipped with an installed power supply that uses the connector cable shown in Figure 3-17. The cable has three purposes:

- It provides 12V, 5V, grounds, and data signals to the terminals.
- It provides data signals and the ground for enclosure to enclosure connections as shown in Figure 3-14.
- It isolates the 5V and 12V to or from other panels as they contain their own power supplies.

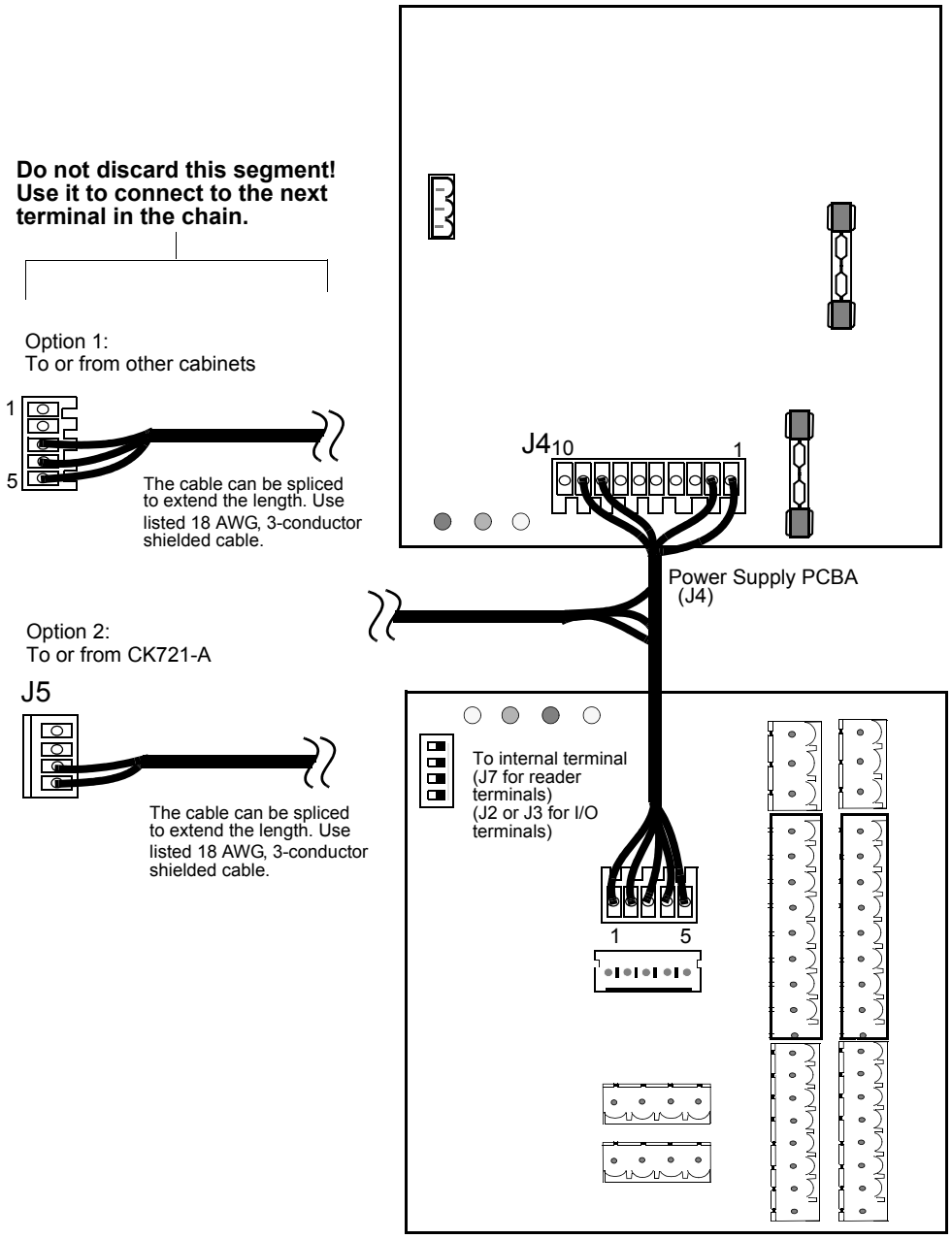
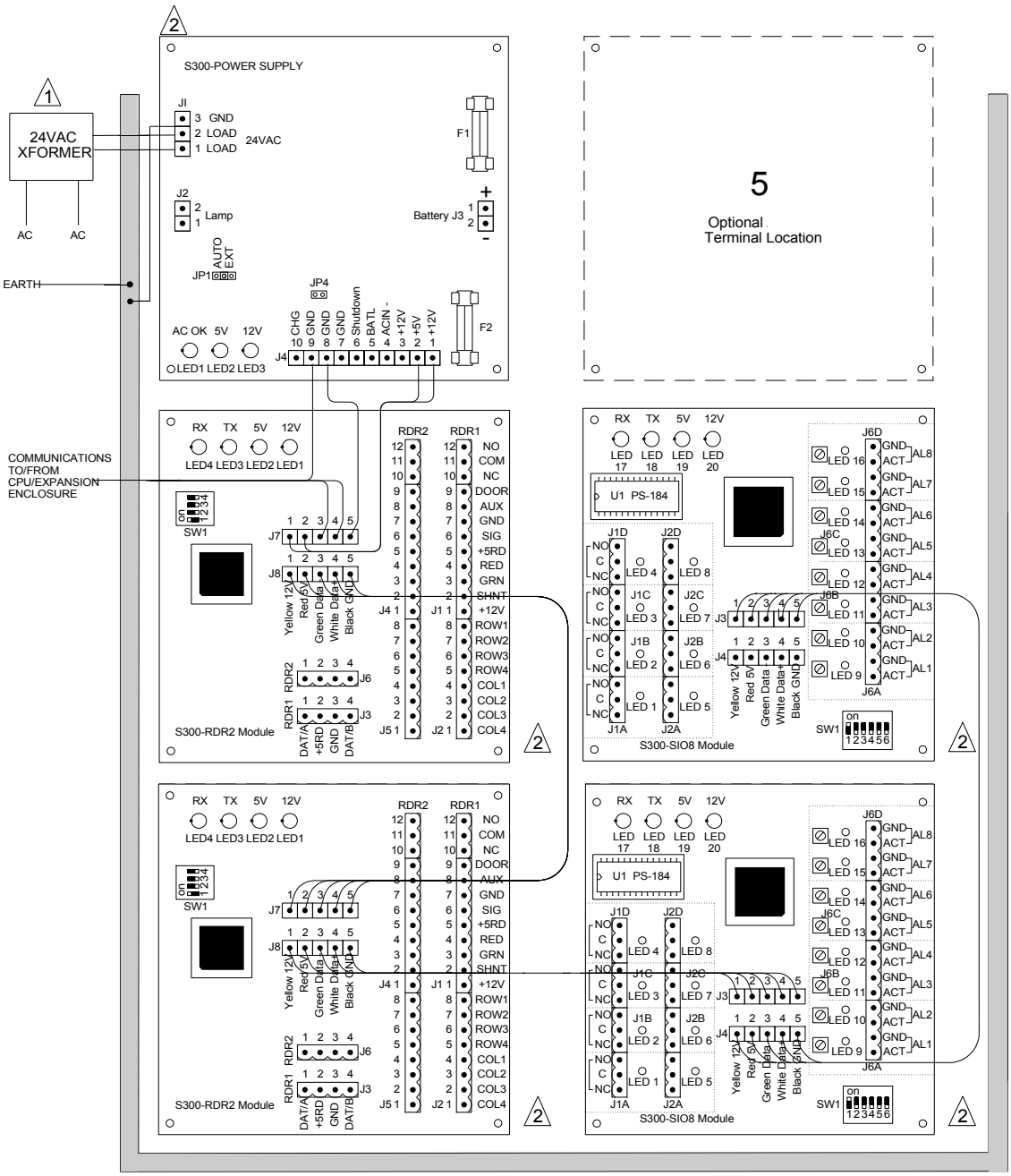


Figure 3-14: Cable Assembly for Enclosure to Enclosure Connection



1 24VAC 50VA TRANSFORMER, ONE PER POWER SUPPLY.
DO NOT PARALLEL TO MULTIPLE SUPPLIES OR TAP FOR EXTERNAL LOADS.

2 CHASSIS GROUND (EARTH) SUPPLIED THROUGH METAL STANDOFFS.
THE SYSTEM RELIES ON A CONDUCTIVE BACK PLATE, CONDUCTIVE STANDOFFS & CONDUCTIVE SCREWS TO MAINTAIN THE PROTECTION GROUND BOND.

Figure 3-15: Cable Assembly for Enclosure to Enclosure Connection - Details

NOTE

Refer to Figure 3-17 for connector orientation.

Equipment Grounding

Proper grounding of the S300 expansion enclosures are essential for the protection of electronic components against electrostatic discharge. A ground wire, 18 AWG minimum, must be run from the dedicated ground stud inside the S300 expansion enclosure to the building's electrical ground. The dedicated ground stud is marked with the symbol ⏚.

NOTE

Cold water pipe is not an acceptable ground due to common use of non-conductive plastic pipe.

POWER

This section describes the transformer and power supply, and provides tables on S3000 enclosure power consumption. Several considerations and cautions that must be considered before powering the enclosure are also detailed.

S300-XFMR Transformer

The plug-in transformer converts the 120 VAC line power to 24 AC for the power supply. The transformer is rated at 24 VAC, 50 VA. A transformer is required for each expansion enclosure to connect the power supply to local power.

NOTE

For Canadian installations use a Basler transformer. The part number is BE116450AAA, and it is rated at 24 VAC, 50 VA, 120 Volt input.

Use a 3-conductor #18 AWG cable between the power supply connector and the transformer. Connect the transformer to the nearest source of clean, unswitched AC power. At the power supply, connect AC power as follows:

- PIN 1 and 2 on J1 connects to 24 VAC.
- PIN 3 on J1 is to chassis ground.

Table 3-2: S300 Expansion Enclosure AC Power Specifications

Parameter	Specification
Line Voltage	24 VAC ± 10%
Line Frequency	50 or 60 Hz ±1%

CAUTION

Do not connect access control equipment to an AC power source that is controlled by a switch.

CAUTION

Do not attach the connector to the power supply until all setup has been completed.

NOTE

Some 24 VAC transformers have an internal fuse. If the 24 VAC output is inadvertently shorted, the internal fuse will open and AC power will not reach the CK720 power supply.

S300-PS Power Supply

The power supplies in the S300 expansion enclosures are installed at the factory. These power supplies accept 24 VAC.

CAUTION

A transformer must be used with each power supply.

CAUTION

Do not connect a single transformer to multiple power supplies.

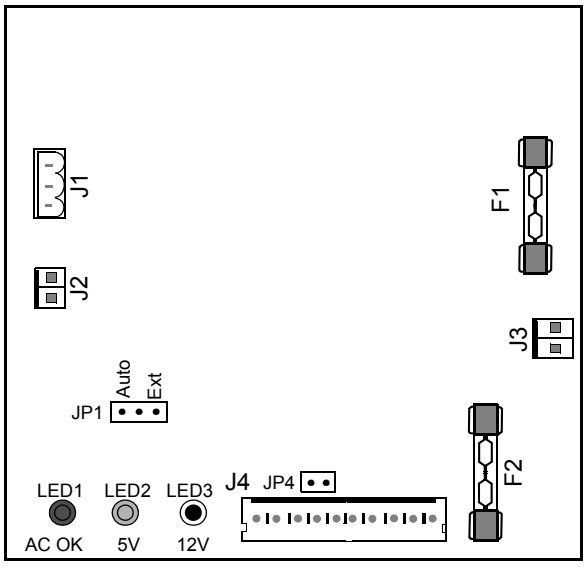


Figure 3-16: Power Supply

The power supply provides the DC power for the terminals, and the readers:

- +5 VDC at 1.5 A to power the terminals and readers.
- +12 VDC at 2.0 A to power reader lamps and output relays.

Table 3-3: Power Supply Components

Component	Description
J1	24V AC Power Connector
J2	Lamp Connector
J3	Battery Backup Connector
J4	Power connector to terminals
JP1	Basic Panel - Jumper installed, EXT to center Expansion Enclosure - Jumper installed, Auto to center.
JP4	“AC-FAIL” pull-up enable, jumper installed
F1	Fuse, 5A, 3AG, 250V, Slo-Blo
F2	Fuse, 1A, 3AG, 250V, Slo-Blo
LEDs	Three LEDs indicate the presence of AC power, 5 and 12 VDC as labeled.

The power supply has three LEDs.

Table 3-4: LEDs On Power Supply

LED	State of LED	Meaning
LED1 (Red)	ON	AC is present
LED2 (Green)	ON	5 VDC is present
LED3 (Yellow)	ON	12 VDC is present

During normal operation, all LEDs should be lit. If only the green and yellow lights are lit, check your AC power connection. If LED1 is off while LED2 and LED3 are on, the power supply is getting its power from the battery. If the battery voltage goes below 9.8V, the power supply will switch off the 5V and 12V (LED2 and LED3) until AC power is restored. If none of the LEDs light when plugging in AC power, verify that AC power is active.

The power supply used in both the S300 expansion enclosures contains the following fuses:

Table 3-5: Fuse Functions and Ratings

Fuse	Function	Rating
F1	Maximum battery discharge rate.	5A, 3AG, 250 V, Slo-Blo
F2	Maximum battery charge rate.	1A, 3AG, 250 V, Slo-Blo

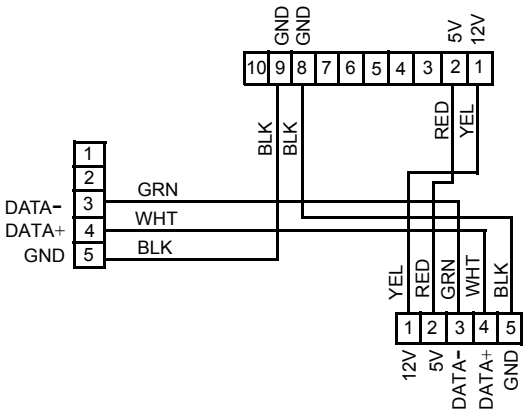


Figure 3-17: Wiring Diagram for Cable Connectors

➤ **To connect the power supply:**

1. Connect the three-wire connector to J8 for a reader terminal, J3 for an I16 terminal, or J4 for all other input/output terminals.
2. Connect the 10-pin connector to J4 on the power supply.
3. Connect the five-wire connector to J2, J3 or J7 on the next terminal.

CAUTION

Do not remove or connect the 10-pin connector or the five wire connectors before powering down the S300 expansion enclosure.

S300 Enclosure Power Consumption

Below are the raw data tables reflecting the power loads for the various electronic modules available for installation in S300 expansion enclosures. The tables are categorized to provide basic guidelines for the major power consumption devices on each electronics module. For loading calculations the worst case numbers should be used. When calculating the total current loading for a given enclosure you must account for all external loads, primarily readers, beyond the published requirements of the terminal. In some cases these numbers can be reduced when specific features of a terminal are not in use (for example, output and supervised inputs).

Table 3-6: S300-RDR2 Power Consumption

S300-RDR2	5VDC Typical (mA)	5VDC Surge (mA)	12VDC Typical (mA)	12VDC Surge (mA)	Wattage (W)
Basic Board	150	300	20	45	
Door Input (Secure)	20	200	0	0	
Aux Input (Door Unlock)	20	20	120	120	
Lamp Warmer	0	0	160	160	
Worst Case	190	520	300	325	4.55
* Typical 1 Door (Led Indicators)	170	410	140	165	
* Typical 2 Door (Led Indicators)	190	520	240	265	2.63
* Each reader Interface provides +5VDC, +12VDC, SHUNT Output, RED Output, GREEN Output. The current loading on these outputs must be derived from the reader manufacturers data sheet and added to the total load. Note +5VDC is current limited to operate Cardkey Readers (20mA).					

Table 3-7: S300-I16 Power Consumption

S300-I16	5VDC Typical (mA)	5VDC Surge (mA)	12VDC Typical (mA)	12VDC Surge (mA)	Wattage (W)
Basic Board	150	200	3	3	
Inputs (16 Secure State)	80	80	0	0	
Worst Case	230	280	3	3	1.19
Typical (4 Alarms)	170	170	N/A	N/A	
Typical (8 Alarms)	190	190	3	3	
Typical (12 Alarms)	210	210	3	3	
Typical (16 Alarms)	230	230	3	3	

Table 3-8: S300-IO8 Power Consumption

S300-IO8	5VDC Typical (mA)	5VDC Surge (mA)	12VDC Typical (mA)	12VDC Surge (mA)	Wattage (W)
Basic Board	150	200	3	3	
Inputs (8 Secure State)	40	40	3	3	
Outputs (8 Set State)	24	24	200	200	
Worst Case	214	264	206	206	3.54
Typical (8 Alarms Secure)	170	170	3	3	
Add for Each Active Output	3	3	25	25	

Table 3-9: S300-SIO8 Power Consumption

S300-SIO8	5VDC Typical (mA)	5VDC Surge (mA)	12VDC Typical (mA)	12VDC Surge (mA)	Wattage (W)
Basic Board	150	200	3	3	
Inputs 8 Secure State)	200	200	3	3	
Inputs (8 Short State)	400	400	3	3	
Outputs (8 Set State)	24	24	200	200	
Worst Case	574	624	206	206	5.34
Typical (8 Alarms Secure)	350	170	3	3	
Add for Each Active Output	3	3	25	25	

In addition to total power consumption, the total number of connections should be considered. The interconnect mechanism within the S300 expansion enclosure requires looping a 5-conductor cable between terminals. The voltage drop across this cable network can affect the operation of an enclosure sub-system. To insure proper operation, measure the +5VDC at each terminal on the 5-wire interconnect network. The working range for +5V should be between +5.20 to +4.85. If a voltage drop, between terminals, is greater than 0.05VDC, the quality of the interconnect cables should be checked.

Applying Power to the S300 Expansion Enclosure

The quality of the line power supplied to your system, the connection, and the grounding of the power and data lines, must conform to your local electrical codes. Consult with your local authorities to assure adequate installation wiring of this S300 expansion enclosure.

Before you apply power to the S300 expansion enclosure, perform the following procedures:

- Ensure proper line voltage is available
- Construct a transformer cable
- Ensure proper grounding is in place
- Check LEDs on the power supply
- Check for proper fuses

The following cautions must be observed:

- If the facility is located in an area where power lines are subject to frequent lightning strikes, verify with the electric company that the building transformer is equipped with surge protectors. These, as well as a “crowbar” type of protection can be installed at the main service entrance if the building transformer is not equipped with lightning protection.
- Do not connect the transformer to an AC power source until the hardware installation is complete.
- Do not connect a single transformer to multiple power supplies.
- AC earth/safety ground must connect directly to the enclosure.
- The S300 power supply must be powered from a dedicated 24VAC transformer. This transformer is not to be shared by any other loads.
- Circuit board assemblies interconnect to earth/safety ground through their mounting holes. All standoffs and mounting hardware must be conductive and connected to AC earth/safety ground. The S300 enclosure provides a conductive mounting system that must be field- connected to AC earth/safety ground.

READER TERMINAL

The reader terminal described in this section is RDR2. A single CK721-A can communicate with 24 terminals, but only up to 8 of them can be reader terminals.

Firmware Versions for Terminals

Table 3-10: Terminal Firmware Versions

Terminal	Model Number*
RDR2 module	PS-201E or later

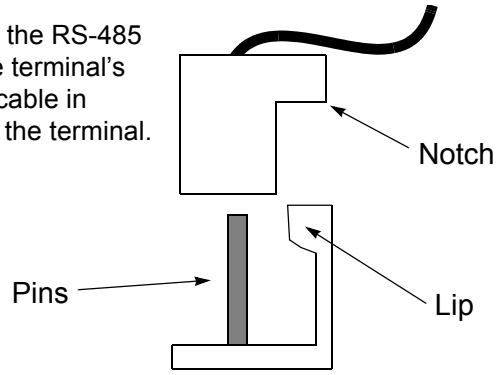
*Required for High Speed RS485 as well as for Assisted Access, Re-lock on Door Open, and Timed Shunt.

RS-485 Wiring

All terminals connected to a single CK721-A communicate through an RS-485 interface as implemented by Cardkey. Each terminal contains two RS-485 connectors.

CAUTION

Ensure that the notch on the RS-485 cable faces the lip on the terminal's connector. Plugging the cable in backwards may damage the terminal.



NOTE

It is difficult to set first level terminals switches and connect RS-485 cables once the stacked terminals are installed.

WARNING

Do not remove or connect the RS-485 connectors before powering down the S300 expansion enclosure.

Each terminal is shipped with an RS-485 cable. The first terminal connects the cable between J5 on the CK721-A and one of the RS-485 connectors listed in Table 3-11 depending on which terminal is installed.

Additional terminals are connected in daisy-chain fashion. For example, using the supplied cable shipped with a second terminal, connect the unused RS-485 on the first terminal, and then connect the other end to a RS-485 interface on the second terminal.

Table 3-11: RS-485 Connector Positions

Terminal	Connector Positions
S300-RDR2 Terminal	J7, J8

S300-RDR2 Terminal

Each reader terminal has an interface for two readers. Each interface provides:

- Cardkey/Wiegand, one wire data interface
- Sensor Wiegand, two wire data interface
- Four rows by four columns, 16 button keypad interface
- Red LED or incandescent bulb reader lamp drivers
- Green LED or incandescent bulb reader lamp drivers
- +5 VDC reader power output at 20 milliamperes
- +12 VDC reader power output at 150 milliamperes

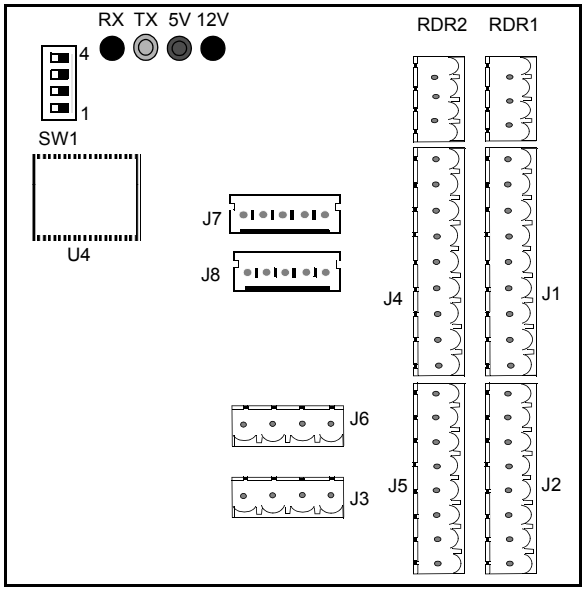


Figure 3-18: S300-RDR2 Terminal

The S300-RDR2 also provides two door input/output interfaces each consisting of:

- A two-state door monitor switch input (secure = normally closed)
- A two-state auxiliary access or exit request switch input (normally open)
- A door-strike relay (SPDT)
- An alarm shunt relay driver (open collector).

Table 3-12: S300-RDR2 Components

Component	Description
J1	Reader 1 Connector
J2	Reader 1 Keypad Reader
J3	Reader 1 Two-Wire Wiegand reader Interface Connector
J4	Reader 2 Connector
J5	Reader 2 Keypad Connector
J6	Reader 2 Two-Wire Wiegand reader Interface Connector
J7	RS-485 Input
J8	RS-485 Output
SW1	Determines reader Address (refer to *Chapter 4: CK721-A User Interface*)
System LEDs	Indicates when data is transmitted or received and the presence of 5 and 12 VDC, as labeled on page 3-24.
U4	S300-RDR2 Firmware

Table 3-13: Reader Terminal Address Settings

Readers Address	Reader Terminal SW1 Settings			
	1	2	3	4
1 & 2	Off	Off	Off	
3 & 4	On	Off	Off	*
5 & 6	Off	On	Off	*
7 & 8	On	On	Off	*
9 & 10	Off	Off	On	*
11 & 12	On	Off	On	*
13 & 14	Off	On	On	*
15 & 16	On	On	On	*

Notes:

1. All reader terminals must have different settings.
2. Reader addresses are determined only by the SW1 switch settings, not the physical location the terminals are installed within the system.

* If a reader terminal is the last in the chain (this includes I/O terminals, not just reader terminals) position 4 must be set ON.

Reader terminal addresses are assigned in pairs:

- 1 and 2
- 3 and 4
- 5 and 6
- 7 and 8

No two reader terminals connected to the same CK721-A can have the same address. Reader terminal addresses are determined by SW1 on the reader terminals as shown in Table 3-13.

NOTE

When you install terminals in a stack configuration, it is difficult to set first level terminals switches and connect RS-485 cables once the stacked terminals are installed.

Wiring Readers

Figure 3-19 shows the maximum cable distances allowed between a S300 expansion enclosure, and a reader.

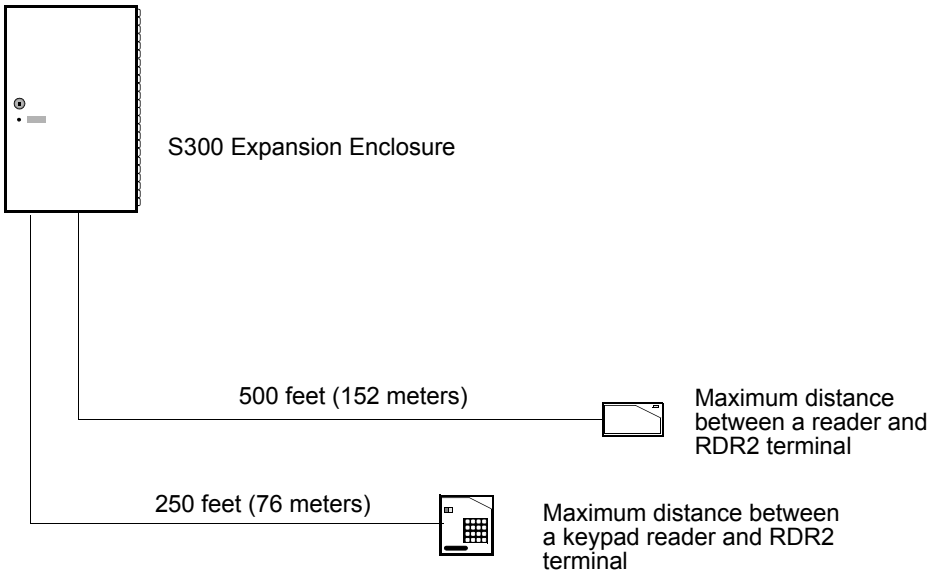


Figure 3-19: Maximum Distance Between Readers and S300 Expansion Enclosures

The S300-RDR2 terminal supports several different types of readers. This chapter provides diagrams that show the connections between the readers and the S300-RDR2 terminal. Table 3-14 shows the "J" numbers that correspond to readers 1 and 2 on the reader terminals.

Table 3-14: Reader Terminal Connector Callouts

	reader 1	**reader 2**
Reader Terminal	J1, J2, J3	J4, J5, J6

To connect your readers, refer to Figure 3-20 through Figure 3-24.

Warm-up Resistor Removal

S300-RDR2 terminals contain a filament warming circuit for use with standard readers. The standard readers use incandescent lamps for void/valid indicators. When readers with LEDs rather than incandescent indicators are connected to the reader terminal, the warming circuit causes the reader's LEDs to be constantly illuminated.

When readers with LEDs as void/valid indicators are used with S300-RDR2, the warming resistors must be removed from the printed circuit board. See Table 3-15 for the corresponding resistor to reader that must be removed.

Table 3-15: S300-RDR2 Locations of Warm-up Resistors

Remove	Description
R6	reader 1, Red Lamp
R7	reader 2, Red Lamp
R8	reader 1, Green Lamp
R9	reader 2, Green Lamp

NOTE

*Remove only the warming resistors that **must** be removed.*

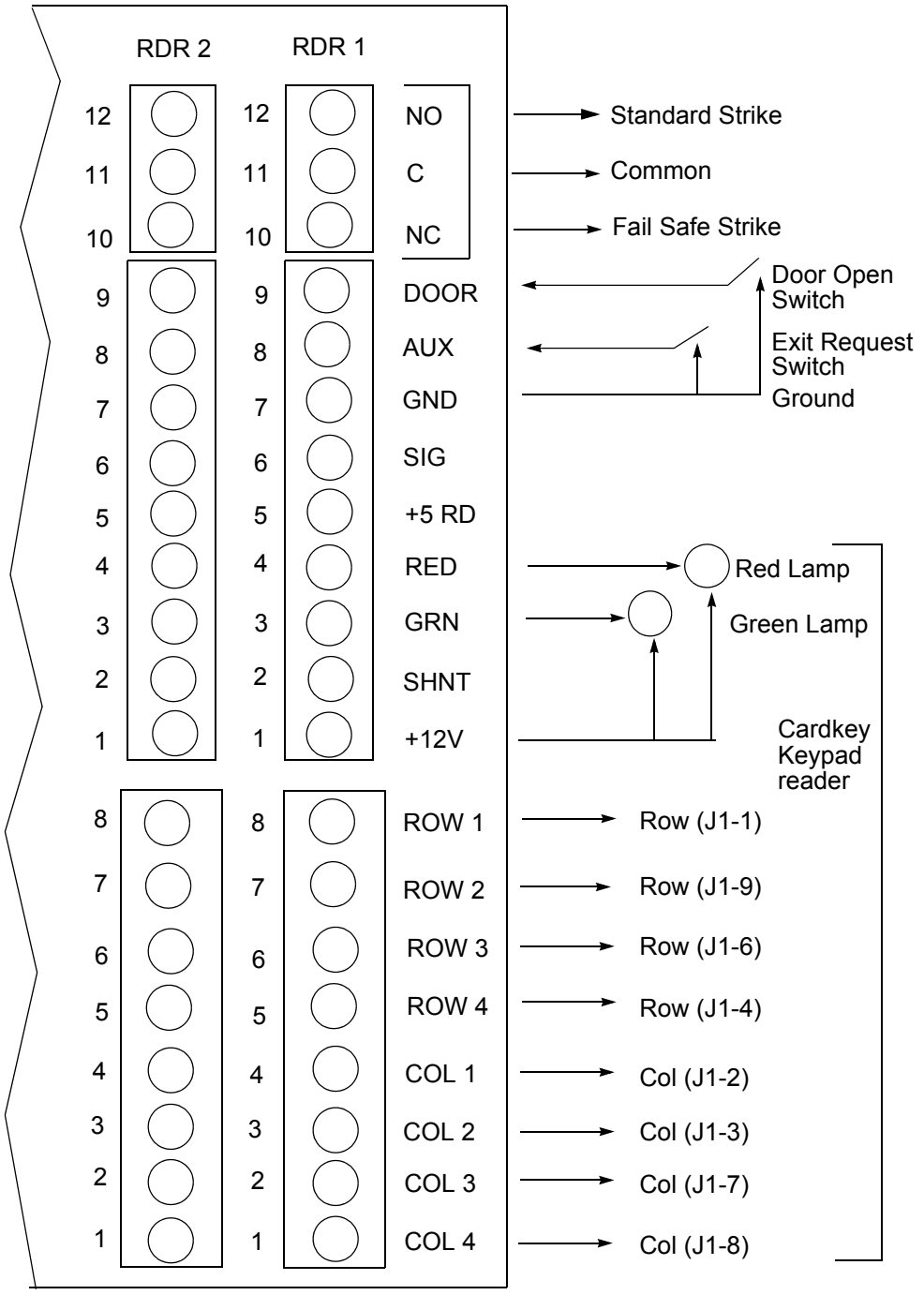


Figure 3-20: Wiring Diagram, Cardkey Keypad Reader

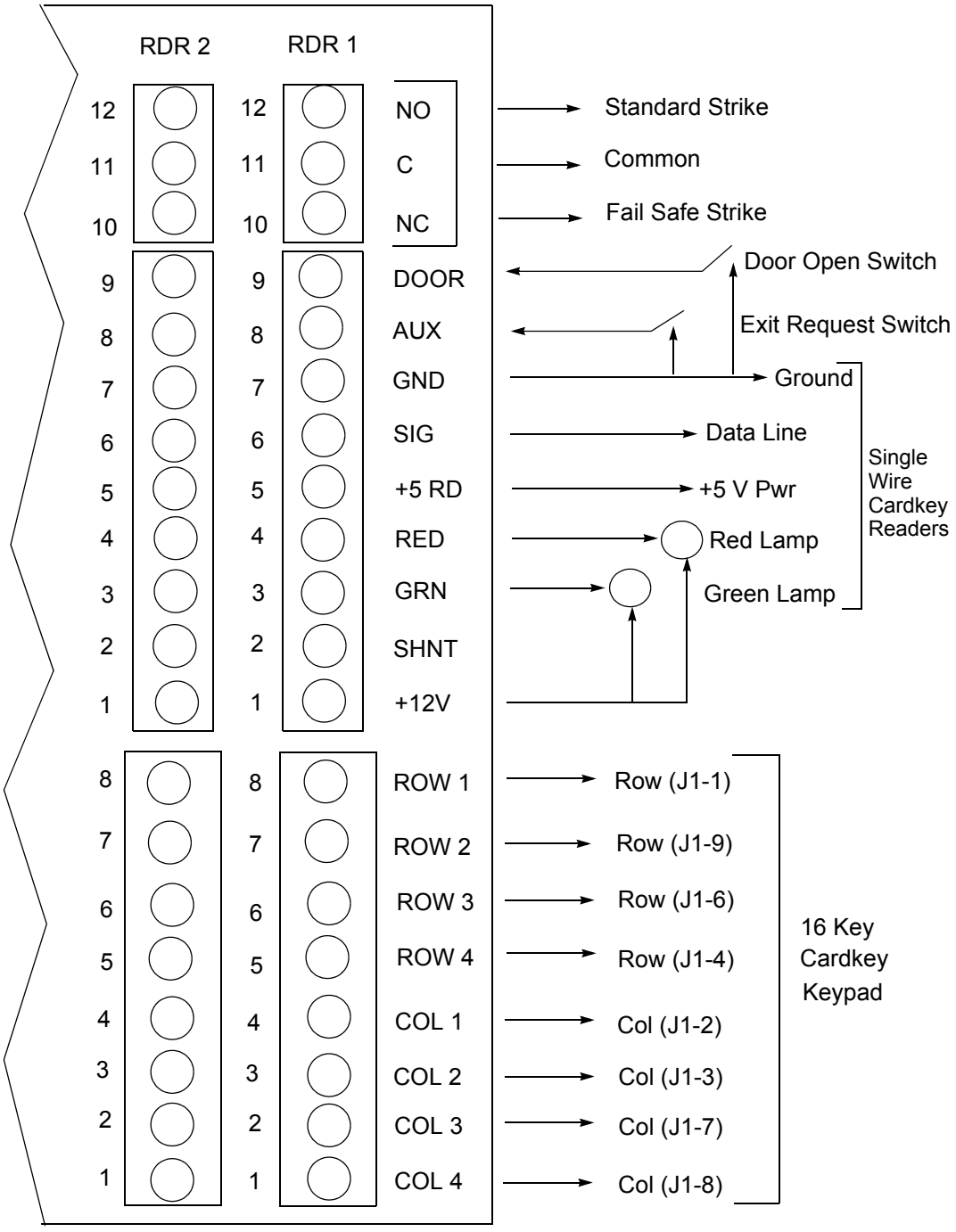


Figure 3-21: Wiring Diagram, Single Data Wire Cardkey Readers

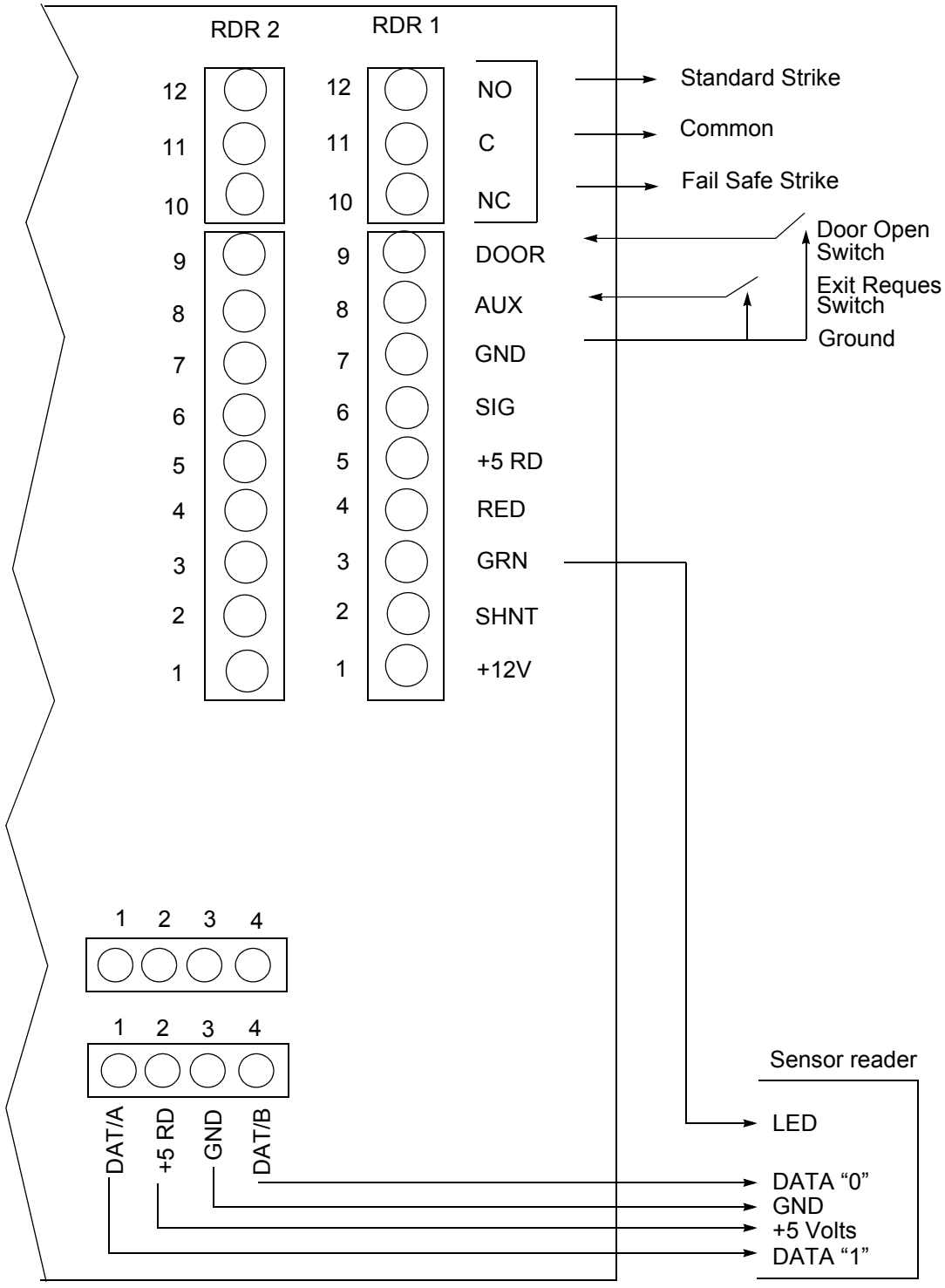


Figure 3-22: Wiring Diagram, Sensor Two Data Wire Wiegand Readers

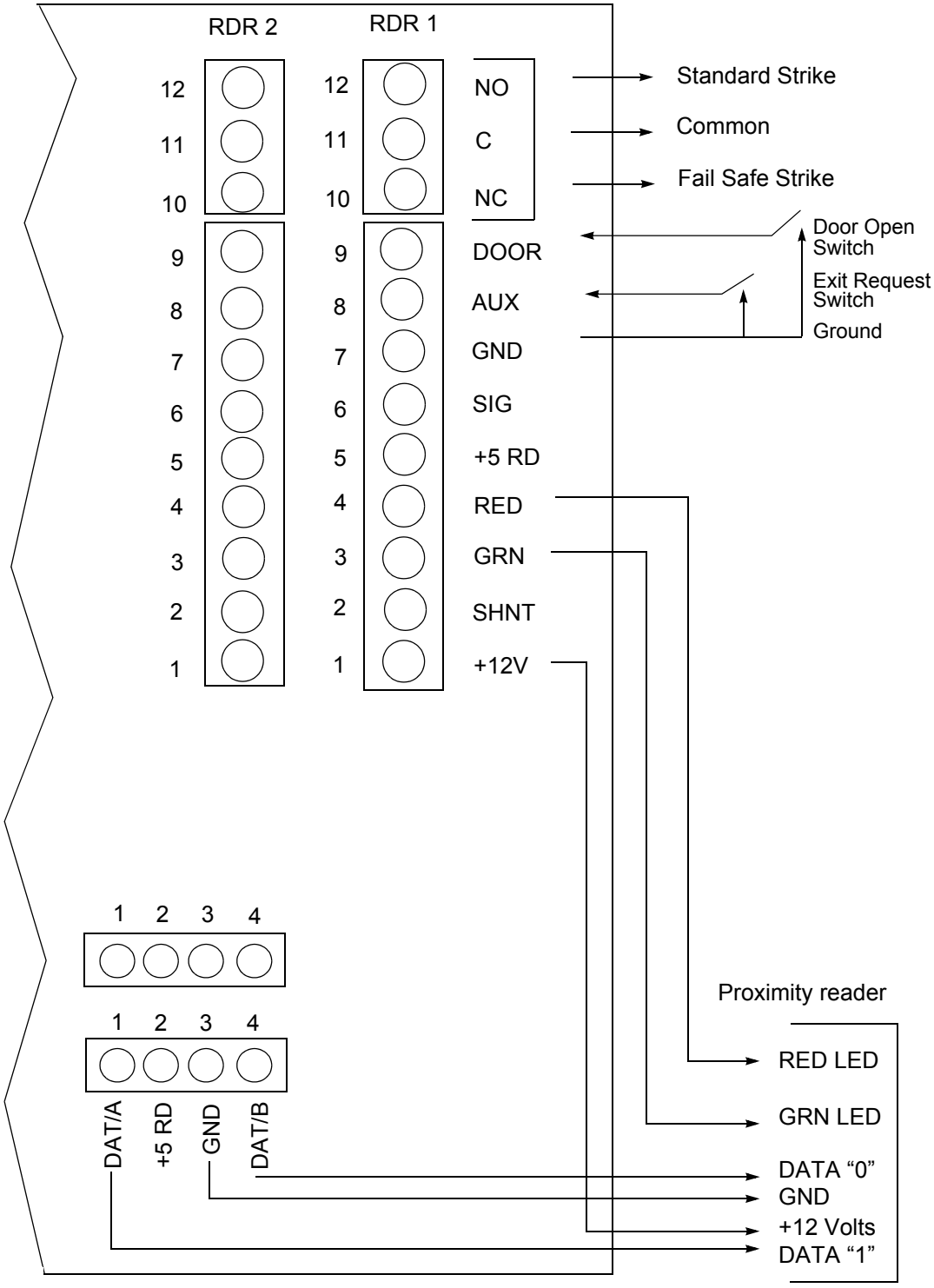


Figure 3-23: Wiring Diagram, Two Data Wire Proximity Readers

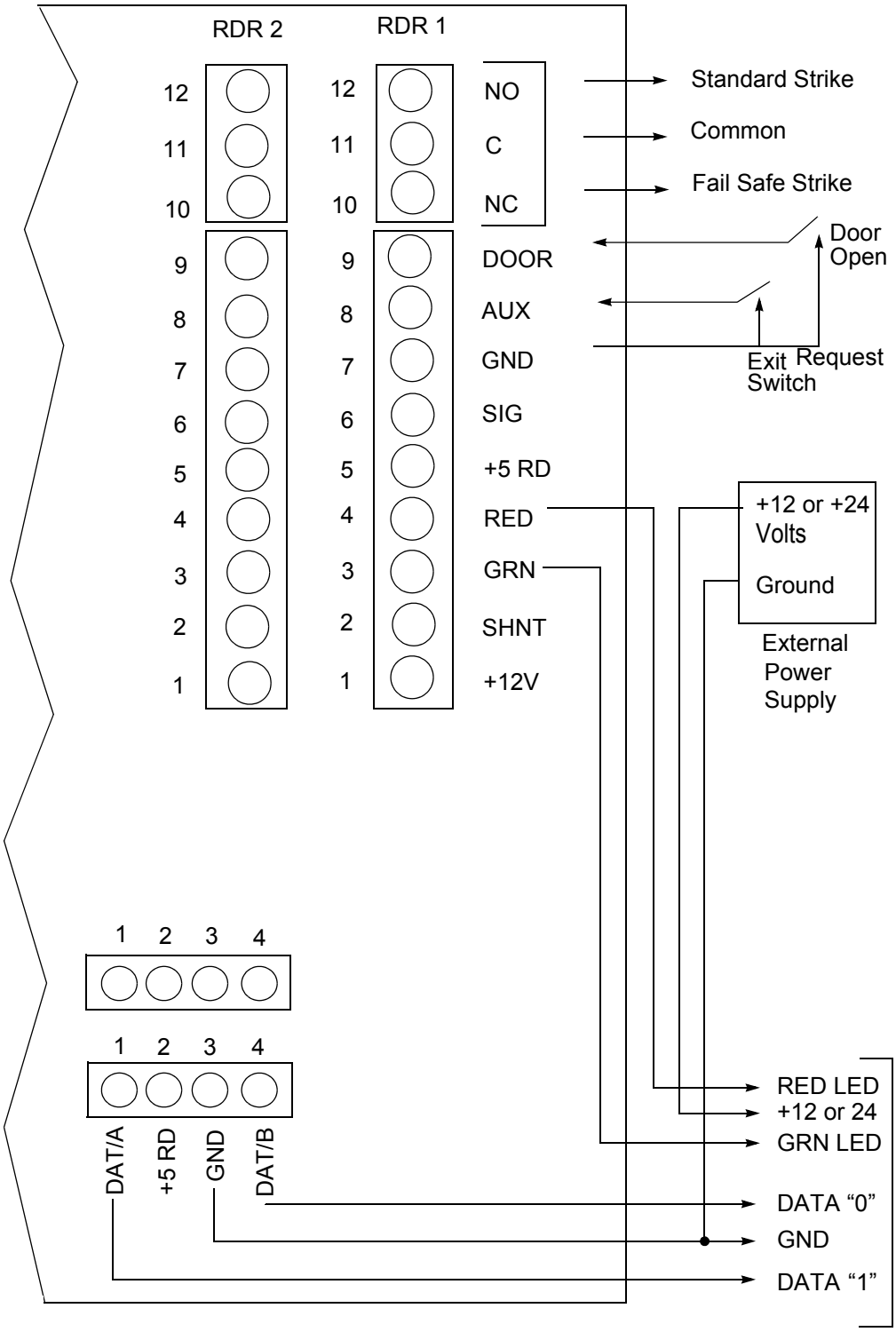


Figure 3-24: Wiring Diagram, Data Wire High Current or +24 Volt Proximity Readers

Wiring for Door Controls

Doors unlock due to signals sent by the S300-RDR2 terminal when a card or PIN access request has been approved (or an open door command has been issued manually). The access granted signal unlocks the door strike. The strike is locked after the programmed unlock time has elapsed. The S300-RDR2 terminal has the following options available (note that use of these options requires additional wiring and equipment):

- Door Strike Relay Closure
- Door Open Alarm Input
- Auxiliary Access Input
- Shunt Relay Driver

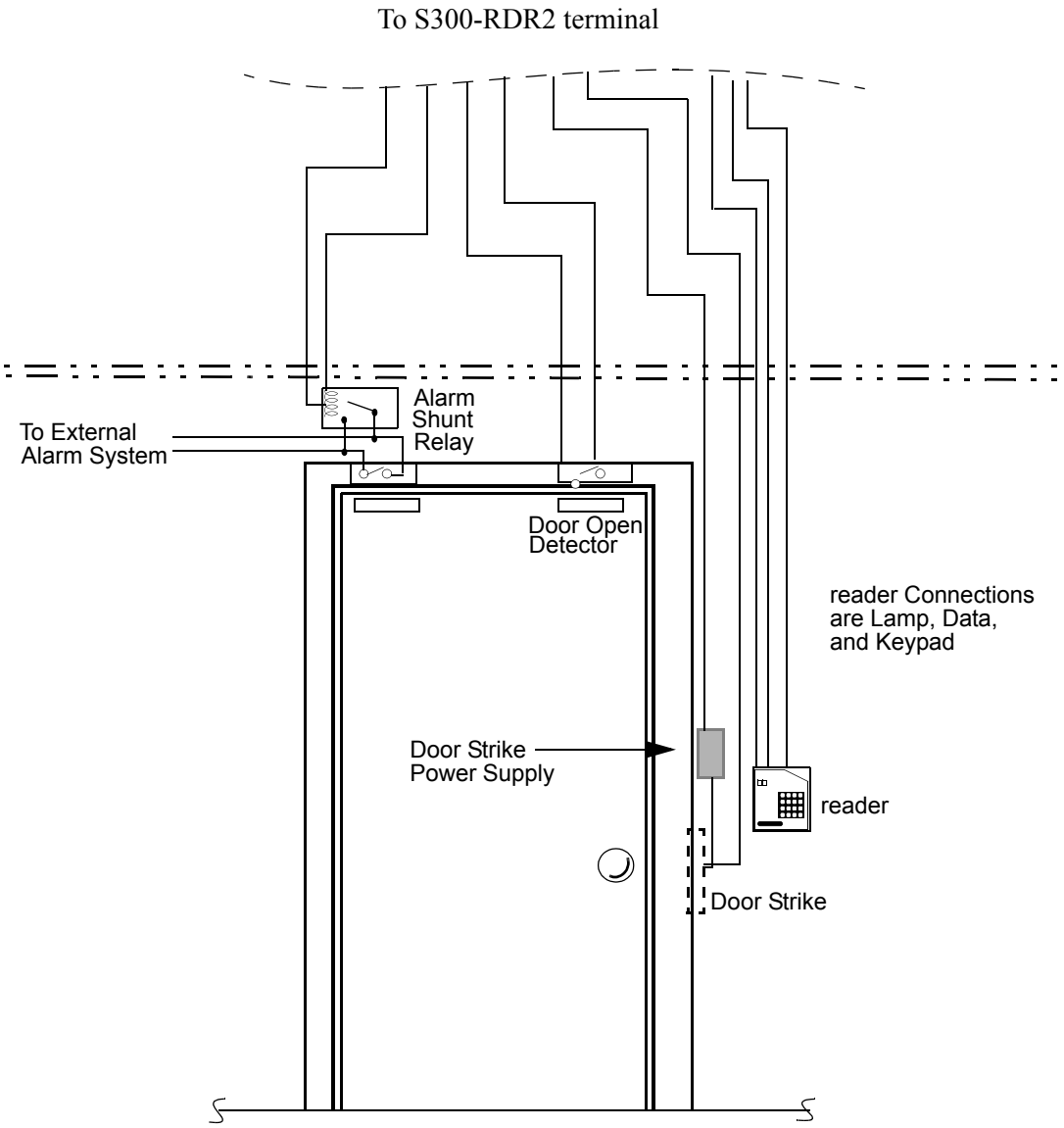


Figure 3-25: Example of a Typical CK721-A System

Door Strike Wiring

The door strike relay is located at J1 and J4 on the reader terminal.

Some door strikes are fail-secure or fail-locked. These door strikes energize to *unlock* the door and de-energize to *lock* the door. These strikes must be connected to the strike power source through the normally-open contacts of the strike relay (NO and C, pins 12 and 11).

Other door strikes are fail-safe types that energize to *lock* the door and de-energize to *unlock* the door. These strikes must be connected to the strike power source through the normally-closed contacts (NC and C, pins 10 and 11).

The maximum length of door strike wiring depends on the power requirements of the strike or latch. The resistance of the #18 AWG wire must not reduce the voltage to the strike by more than 10%. The lock's current ratings should not exceed 2 amperes at 30 VDC.

To insure proper operation and to extend the contact life of mechanical relay outputs (RDR2 STRIKE), the contacts should be protected by an external protection circuit. This protection circuit is application- specific as configured in the field. Johnson Controls would advise, at a minimum, a Metal Oxide Varistor (MOV) at the rated voltage relative to the application across the power source and power load interrupted by the mechanical relay.

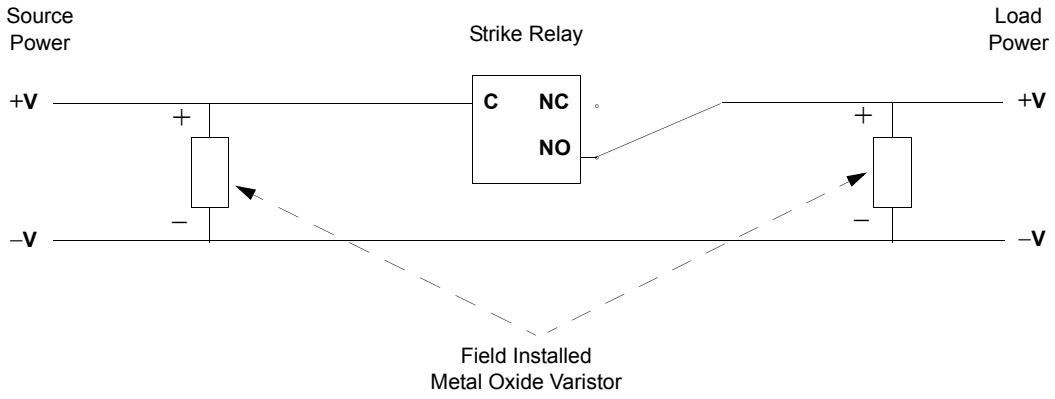


Figure 3-26: Field Installed Metal Oxide Varistor

A full line of varistor components is available from Harris Semiconductor (now Littelfuse Corp.).

CAUTION

The ZA family of components covers the complete operating range of Cardkey Strike and Output relays in a radial leaded component suitable for field wiring applications. Failure to provide these protection devices will limit the contact life of the relay resulting in failed operation.

Use a separate Class 2 transformer or power supply for door strike power. Under no circumstances connect a door strike to the S300 enclosure power supply.

NOTE

It is the responsibility of the installing contractor to ensure that the lock type and egress method meets the building, fire, and life safety requirements and codes.

Door Open Detector Wiring

A door-open detector will normally be installed at each entrance controlled by a card reader. This is an open circuit when the door is open. The S300-RDR2 terminal provides a door-open alarm input at connectors J1 or J4 for monitoring the door status. This alarm input is suppressed (shunted) for a selected period of time, allowing the door to be opened and closed after access has been granted. This time period is called the Alarm Shunt Time. If a door is opened without access being granted, or if the door is held open beyond the alarm shunt time and the alarm signal is not suppressed, the alarm is detected immediately.

Auxiliary Access Switch Wiring

When an auxiliary access is input at connectors J1 or J4 on the reader terminal, it provides a means of manually allowing access or exit from the secured area. If used, the auxiliary access input must be connected to a dry-contact normally-open switch that is installed in the secure area. The use of the auxiliary access switch actuates the door strike immediately and disables (shunts) the door open detector to prevent a false alarm. It is the responsibility of the installing contractor to ensure that the lock type and egress method meets the building, fire, and life safety requirements and codes. This input can also be connected to the relay output of a PIR (Passive Infra-Red) device mounted above the door allowing automatic operation.

Shunt Relay Driver Wiring

A driver is provided for connecting an external alarm shunt relay at connectors J1 or J4 of the S300-RDR2 terminal. When a valid access occurs, the shunt relay is energized on for the duration of time programmed at the Cardkey SMS. If an external alarm system is used, the alarm shunt will prevent the external alarm system from sounding an alarm when a valid access occurs. To use this feature, connect a relay with a 12 VDC coil (70 MA maximum) to pins 1 and 2. To protect the relay driver, connect a diode (1N4148 or equivalent) across the relay coil. The diode cathode (banded end) is connected to pin 1 and the anode to pin 2.

I/O TERMINALS

I/O terminals provide alarm inputs and output relays for the CK721-A system. A single CK721-A panel can communicate with 24 terminals: eight reader terminals and up to 16 I/O terminals. When planning what terminals to include, consider the following:

- S300-I16 have 16 input points each. The CK721-A can support sixteen of these.
- S300-SIO8 has eight supervised (4-state) inputs and eight outputs. The CK721-A can support eight of these.
- S300-IO8 has eight unsupervised (2-state) inputs and eight outputs. The CK721-A can support sixteen of these.
- S300-SI8 has eight supervised (4-state) inputs. The CK721-A can support eight of these.

Firmware Versions for Terminals

Table 3-16: Terminal Firmware Versions

Terminal	Model Number
SIO8 and SI8 modules	PS-184B or later
IO8 and I16 modules	PS-183D or later

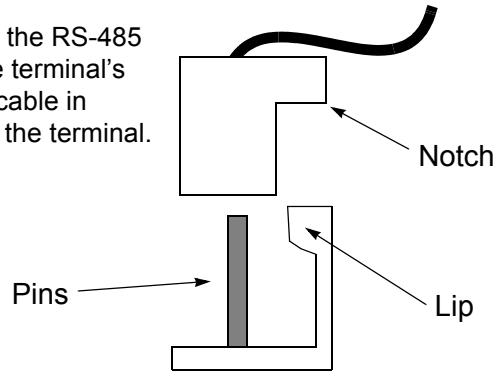
*Required for High Speed RS485

RS-485 Wiring

All terminals connected to a single CK721-A communicate through an RS-485 interface as implemented by Cardkey. Each terminal contains two RS-485 connectors.

CAUTION

Ensure that the notch on the RS-485 cable faces the lip on the terminal's connector. Plugging the cable in backwards may damage the terminal.



NOTE

It is difficult to set first level terminals switches and connect RS-485 cables once the stacked terminals are installed.

WARNING

Do not remove or connect the RS-485 connectors before powering down the S300 expansion enclosure.

Each terminal is shipped with an RS-485 cable. The first terminal connects the cable between J5 on the CK721-A and one of the RS-485 connectors listed in Table 3-17 depending on which terminal is installed.

Additional terminals are connected in daisy-chain fashion. For example, using the supplied cable shipped with a second terminal, connect the unused RS-485 on the first terminal, and then connect the other end to a RS-485 interface on the second terminal.

Table 3-17: RS-485 Connector Positions

Terminal	Connector Positions
S300-I16 Input Terminal	J2, J3
S300-IO8 I/O Terminal	J3, J4
S300-SIO8 I/O Terminal	J3, J4
S300-SI8 Input Terminal	J3, J4

No two I/O terminals connected to the same CK721-A can have the same address. Addresses are set by switches located on the terminals. Table 3-18 shows the proper switch settings for each address.

Table 3-18: Input/Output Terminal Address Settings

Physical Address	Switch Settings					
	1	2	3	4	5	6
1	Off	Off	Off	Off	*	Off
2	On	Off	Off	Off	*	Off
3	Off	On	Off	Off	*	Off
4	On	On	Off	Off	*	Off
5	Off	Off	On	Off	*	Off
6	On	Off	On	Off	*	Off
7	Off	On	On	Off	*	Off
8	On	On	On	Off	*	Off
9	Off	Off	Off	On	*	Off
10	On	Off	Off	On	*	Off
11	Off	On	Off	On	*	Off
12	On	On	Off	On	*	Off
13	Off	Off	On	On	*	Off
14	On	Off	On	On	*	Off
15	Off	On	On	On	*	Off
16	On	On	On	On	*	Off

* If an I/O terminal is the last in the chain (this includes reader terminals, not just I/O terminals) position 5 must be set ON.

Note: All 16 physical addresses apply ONLY to IO8 and I16 terminals. If you are using SI08 or SI8 terminals (supervised, 4-state alarms), you can only use physical addresses 1 through 8; 9 through 16 will be invalid.

S300-I16 Unsupervised Input Terminal

The S300-I16 terminal provides:

- 16 two-state input points
- 16 red LED indicators which illuminate when each input is in alarm

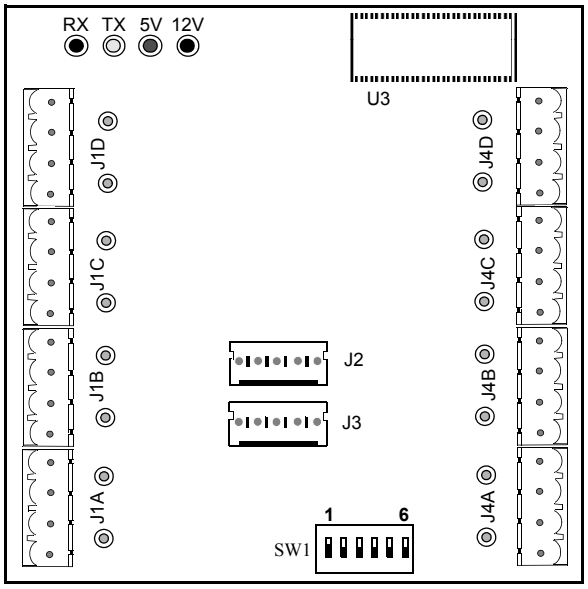


Figure 3-27: S300-I16 Terminal

Table 3-19: S300-I16 Components

Component	Description
J1A	Alarm Inputs 9 and 10
J1B	Alarm Inputs 11 and 12
J1C	Alarm Inputs 13 and 14
J1D	Alarm Inputs 15 and 16
J2	RS-485 Input
J3	RS-485 Output
J4A	Alarm Inputs 1 and 2
J4B	Alarm Inputs 3 and 4
J4C	Alarm Inputs 5 and 6
J4D	Alarm Inputs 7 and 8
SW1	Address Settings (refer to *Chapter 4: CK721-A User Interface*)
System LEDs	Indicate when data is transmitted or received and the presence of 5 and 12 VDC, as labeled in the diagram above
U3	S300-I16 Firmware

S300-IO8 Unsupervised Input/Output Terminal

The S300-IO8 terminal provides:

- Eight two-state input points
- Eight general purpose SPDT output relays
- Eight input LEDs which illuminate when each input is in alarm
- Eight output LEDs showing when each relay is energized

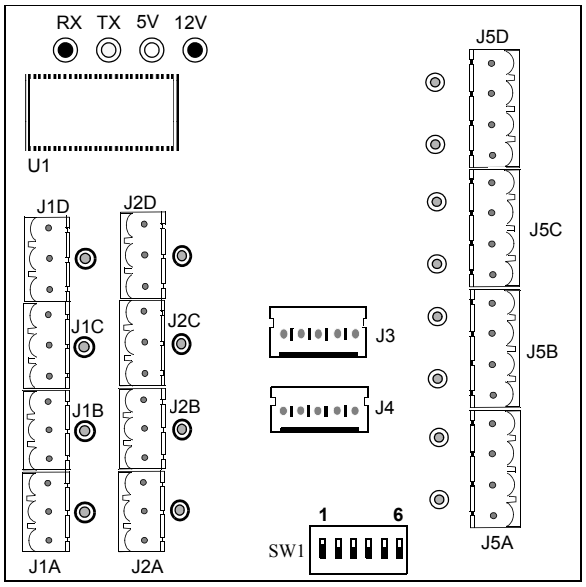


Figure 3-28: S300-IO8 Terminal

Table 3-20: S300-IO8 Components

Component	Description
J1A	Output Relay 1 Connector
J1B	Output Relay 2 Connector
J1C	Output Relay 3 Connector
J1D	Output Relay 4 Connector
J2A	Output Relay 5 Connector
J2B	Output Relay 6 Connector
J2C	Output Relay 7 Connector
J2D	Output Relay 8 Connector
J3	RS485 Input
J4	RS485 Output
J5A	Alarm Inputs 1 and 2
J5B	Alarm Inputs 3 and 4
J5C	Alarm Inputs 5 and 6
J5D	Alarm Inputs 7 and 8
SW1	Address Settings
System LEDs	Indicate when data is transmitted or received and the presence of 5 and 12 VDC, as labeled in Figure 3-28.
U1	S300-IO8 Firmware

S300-SIO8 Supervised Input/Output Terminal

The S300-SIO8 is almost identical in appearance to the S300-IO8 terminal shown in Figure 3-28. The differences in functionality between the two terminals are:

- The S300-SIO8 terminal provides eight **four-state** alarm inputs, which monitor open or short circuit, alarm, and secure states.
- The eight alarm input LEDs are three-color indicators showing:

  Off - Open **Green - Secure**

  Yellow - Short **Red - Alarm**

All other functions, including the eight output relays, are identical to the S300-IO8 terminal.

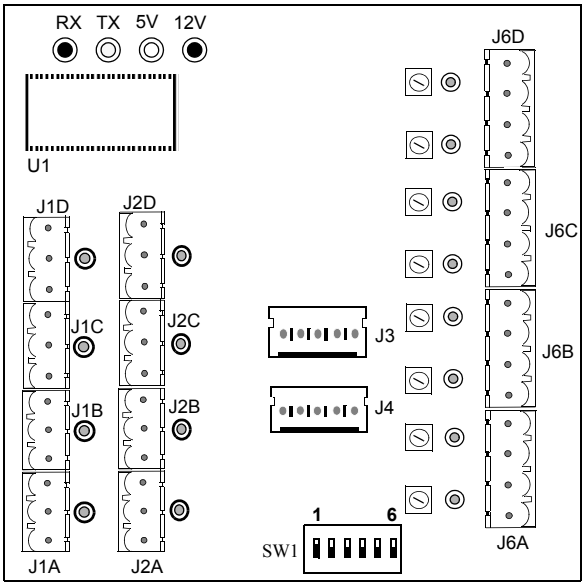


Figure 3-29: S300-SIO8 Terminal

Table 3-21: S300-SIO8 Components

Component	Description
J1A	Output Relay 1 Connector
J1B	Output Relay 2 Connector
J1C	Output Relay 3 Connector
J1D	Output Relay 4 Connector
J2A	Output Relay 5 Connector
J2B	Output Relay 6 Connector
J2C	Output Relay 7 Connector
J2D	Output Relay 8 Connector
J3	RS-485 Input
J4	RS-485 Output
J6A	Alarm Inputs 1 and 2
J6B	Alarm Inputs 3 and 4
J6C	Alarm Inputs 5 and 6
J6D	Alarm Inputs 7 and 8
SW1	Address Settings
System LEDs	Indicates when data is transmitted or received, and the presence of 5 and 12 VDC as labeled in Figure 3-30.
U1	S300-SIO8 Firmware

S300-SI8 Supervised Alarm Input Terminal

The S300-SI8 terminal provides:

- Eight four-state (open or short circuit, alarm, and secure) alarm inputs.
- A three-color LED input indicator for each alarm showing:

  Off - Open **Green - Secure**

  Yellow - Short **Red - Alarm**

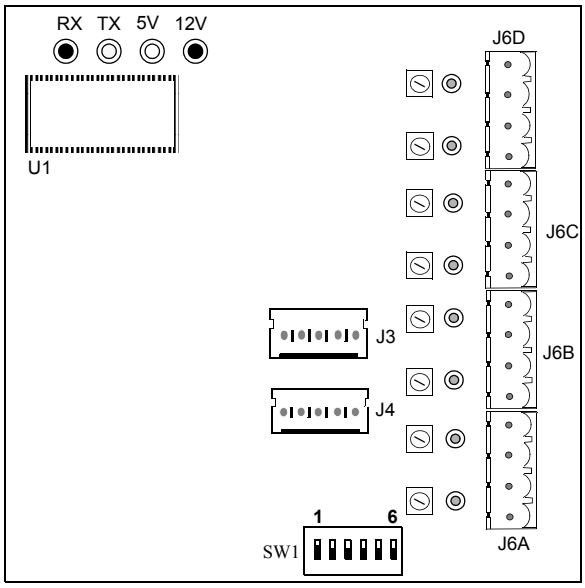


Figure 3-30: S300-SI8 Terminal

Table 3-22: S300-SI8 Components

Connectors	Description
J3	RS-485 Input
J4	RS-485 Output
J6A	Alarm Inputs 1 and 2
J6B	Alarm Inputs 3 and 4
J6C	Alarm Inputs 5 and 6
J6D	Alarm Inputs 7 and 8
SW1	Address Settings
System LEDs	Indicates when data is transmitted or received and the presence of 5 and 12 VDC, as shown in Figure 3-30.
U1	S300-SI8 Firmware

Wiring Input/Output Devices

Table 3-23: Cabling Requirements

Signal Type	Type (Stranded, Insulated)	Mfr./PN	Maximum Length
Alarm Input	1 twisted, shielded pair, #22 AWG to each detector	Belden 8761	500 ft (152 m)
Output Relay	1 twisted, shielded pair, #18 AWG to each relay	Belden 8760	Depends on load

The maximum distances between the S300 expansion enclosure and input or output devices can vary and depend on:

- The current/voltage of the device
- The gauge wire you use

The rule is a maximum of 500 feet (152 meters). This ensures the integrity of the current or voltage between the system and the input device.

The distance from a S300 expansion enclosure to an output device, and the resistance of the wire, must not reduce the current or voltage to the output device by more than 10 percent.

Expansion Enclosure Tamper Switch Wiring

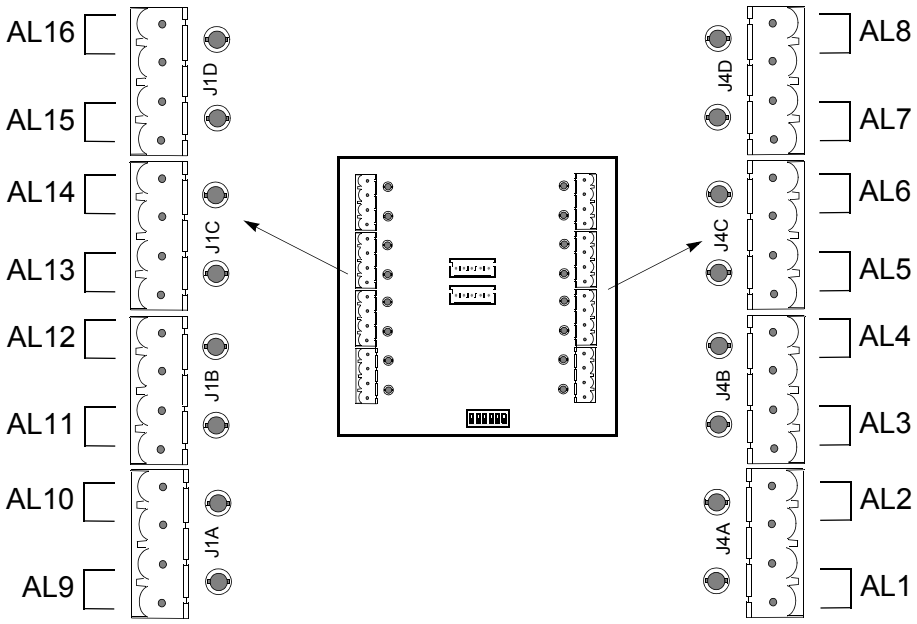
The tamper switch on an expansion enclosure must be wired to an input point located on a terminal. It must then be defined as an alarm when programming the system. Consequently, expansion enclosures that only contain reader terminals must have the tamper switch wired back to the panel or to an input terminal located in another expansion enclosure.

Unsupervised Alarm Inputs

Unsupervised alarms monitor two circuit conditions: alarm and secure.

Depending on the type of terminals you have installed, there are two-state or four-state inputs. The S300-SI8 and S300-SIO8 provide four-state alarms, and the S300-I16 and S300-IO8 provide two-state alarms.

Alarm devices are wired to both two and four-state inputs in the same way. The difference between two and four-state alarms is the use of resistors on the four-state input at the alarm device end. Resistance is monitored by the CK721-A for open, short, alarm, and secure conditions.



Note
This diagram shows an S300-I16. For every input/output terminal, the wiring of the input points are the same.

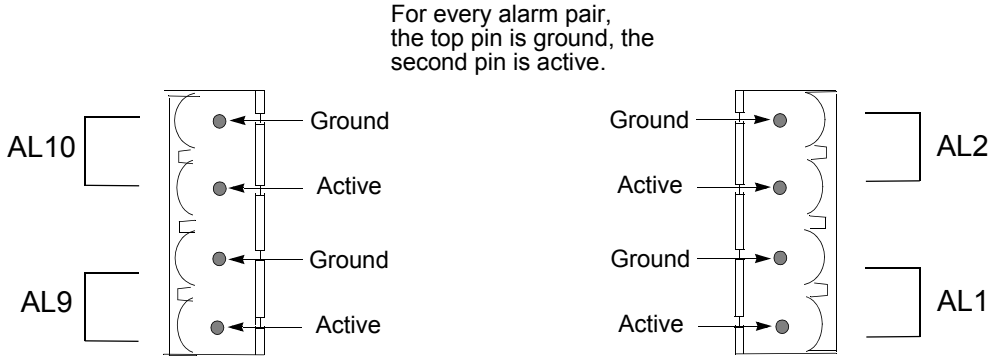


Figure 3-31: Wiring Input Points (two and four-state alarms)

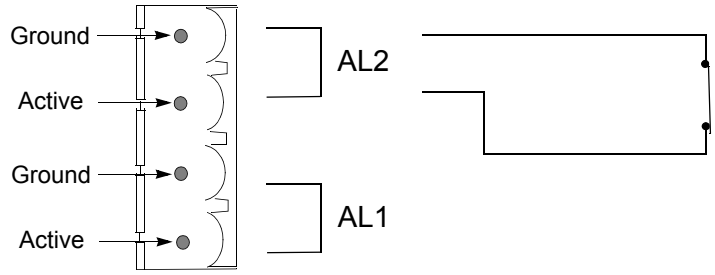


Figure 3-32: Circuit for two-state Inputs (normally closed)

Supervised Alarm Inputs

The difference between the S300-I16 or S300-IO8 and the S300-SIO8/S300-SI8 terminals is that the latter's inputs are supervised. A supervised alarm input provides two additional states. These additional states are used primarily for indicating a tamper to an external alarm device. For more information regarding supervised and unsupervised alarm inputs, see "Installing the First Level Terminals" on page 3-7.

The S300-SIO8 and S300-SI8 have four-state inputs. The state of each alarm is indicated by a multi-color LED adjacent to each pair of alarm inputs.

Green - Secure **Red - Alarm**

Yellow - Short

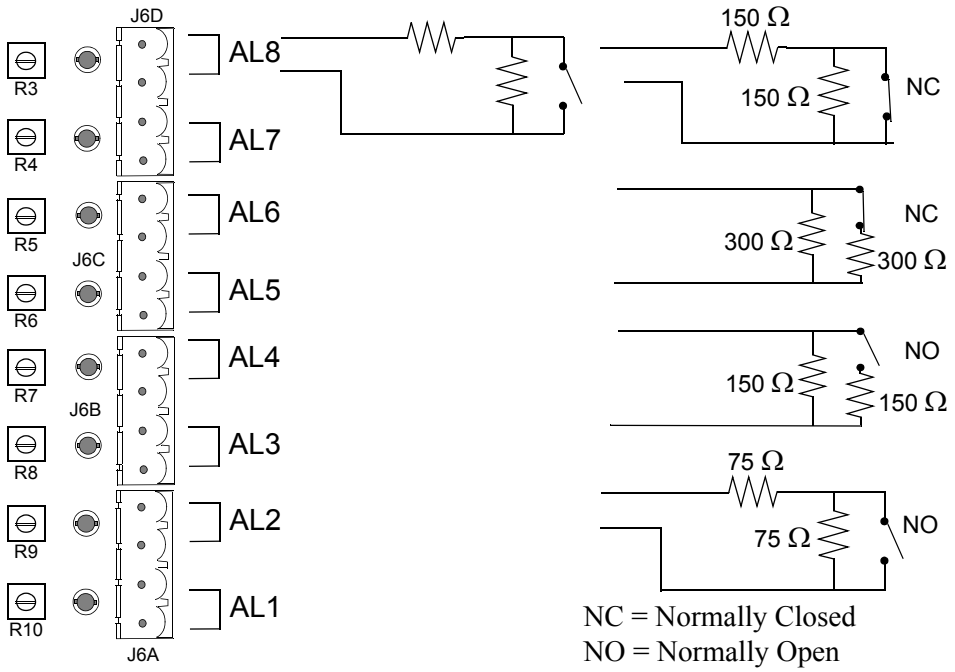


Figure 3-33: Four-state Alarm Inputs

Four-state alarms require 150 Ohms ±2%, 1/4 W resistors wired at the external device to be in the secure condition.

Resistances above and below the secure 150 Ohm range cause an alarm condition. The 300 and 75 Ohms conditions cause high and low alarms respectively, as shown in Figure 3-34.

The normal condition of the switch state (open or closed) must be considered when choosing the resistor configuration. For example, a normally open switch must have 150 Ohms when the switch is open and 75 Ohms when the switch is closed. A normally closed switch must have 150 Ohms when closed and 300 Ohms when open. Resistance values below 40 Ohms cause a short condition and resistance above 500 Ohms causes an open condition.

Calibrating Four-State Alarm Inputs

After power-up, the supervised inputs must be calibrated. To calibrate:

1. Place all inputs in their secure condition (150 Ohm state).
2. Adjust the associated trim potentiometer (R3 through R10) to the center-most position until the LED turns green.

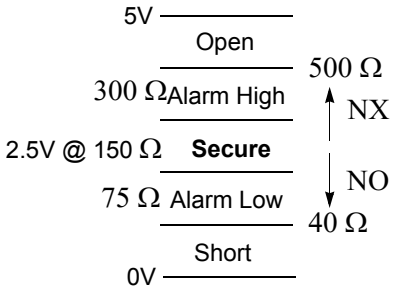


Figure 3-34: Four-State Alarm Conditions

3. If the LED remains red during the adjustment, verify that proper configuration has been used for either the NO or NC switch.

NOTE

The four-state zones actually have five detected states. The two alarms above and below the secure state are combined into one alarm state. When programming the system, this allows both normally open and normally closed switches to reflect a secure condition by adjusting the hardware, rather than configuring the switch status (NO or NC).

Output Relay Wiring

Relay outputs are provided for connecting to customer-supplied devices. Each output relay can provide general purpose low or intermediate power control to the device. The relay will switch 2A at 30 VDC.

All outputs supply a normally open, common, and normally closed relay contact. The state of each relay is indicated by a red LED adjacent to each set of relay contact outputs. The LED is lit when the relay is energized.

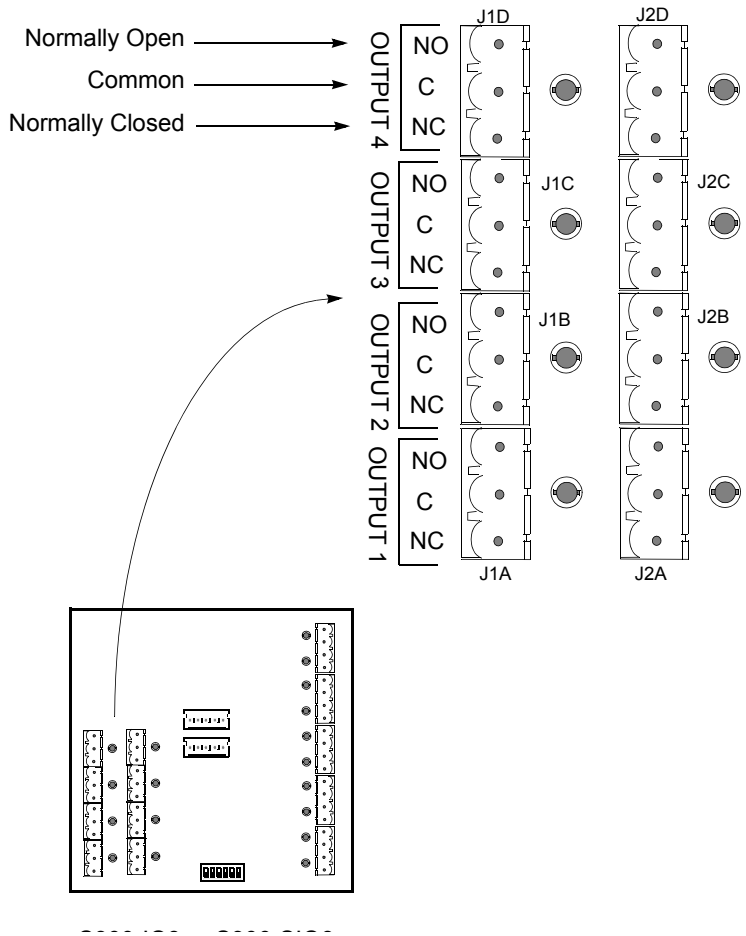


Figure 3-35: Configuration of Outputs

Output Wiring

To insure proper operation and extend the contact life of mechanical relay outputs (SIO8 Outputs and IO8 Outputs), the contacts should be protected by an external protection circuit. This protection circuit is application- specific as configured in the field. Johnson Controls would advise, at a minimum, a Metal Oxide Varistor (MOV) at the rated voltage relative to the application across the power source and power load interrupted by the mechanical relay.

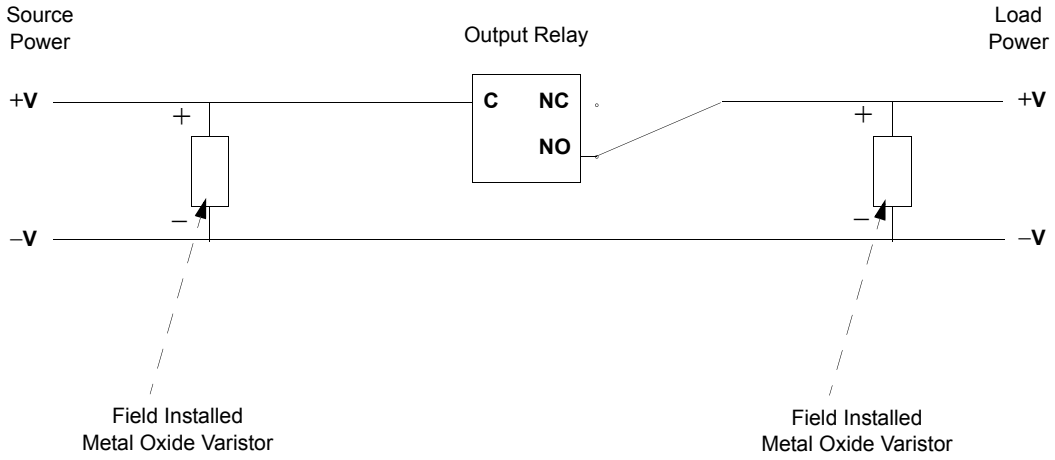


Figure 3-36: Field Installed Metal Oxide Varistor

A full line of varistor components is available from Harris Semiconductor (now Littelfuse Corp.).

CAUTION

The ZA family of components covers the complete operating range of Cardkey Strike and Output relays in a radial leaded component suitable for field wiring applications. Failure to provide these protection devices will limit the contact life of the relay resulting in failed operation.

BACKUP BATTERY

All models of S300 expansion enclosures use the same battery (S300-BAT) and bracket kit (S300-BRK2).

The location and orientation of the battery inside the enclosure depends on enclosure type.

The battery and bracket kit are sold separately and the battery can be replaced without ordering an additional bracket kit.

S300-BAT Battery

The optional S300-BAT backup battery provides an Uninterruptible Power Supply (UPS) feature.

The battery is a Power Sonic, Model PS-1270, 12 VDC, 7 Ah, sealed lead acid battery. It should be replaced every three years to ensure proper operation. Replace the battery whether or not it has been placed into use by an AC power failure.

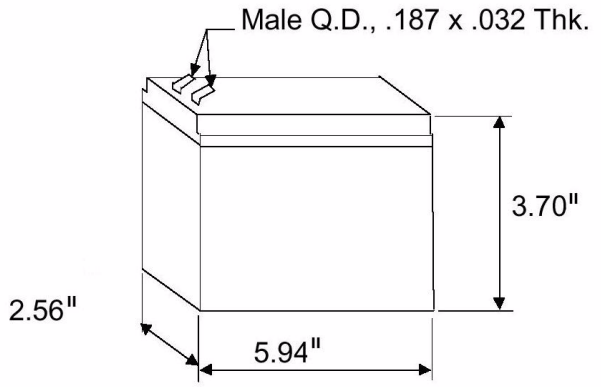


Figure 3-37: Battery Backup for Expansion Enclosures

NOTE

The backup battery is rated for a minimum of three hours on a fully loaded system in an expansion enclosure.

S300-BRK2 Battery Bracket Kit

The S300-BRK2 bracket kit is used to mount the battery to a S300 expansion enclosure as shown in Figure 3-38.

Each kit contains the following:

- One bracket
- Mounting hardware
- One 37-in. connecting cable (battery to the power supply) for large panels, small panels, and expansion enclosures. One 16.5-in. connecting cable for the S300-XXS enclosure only.

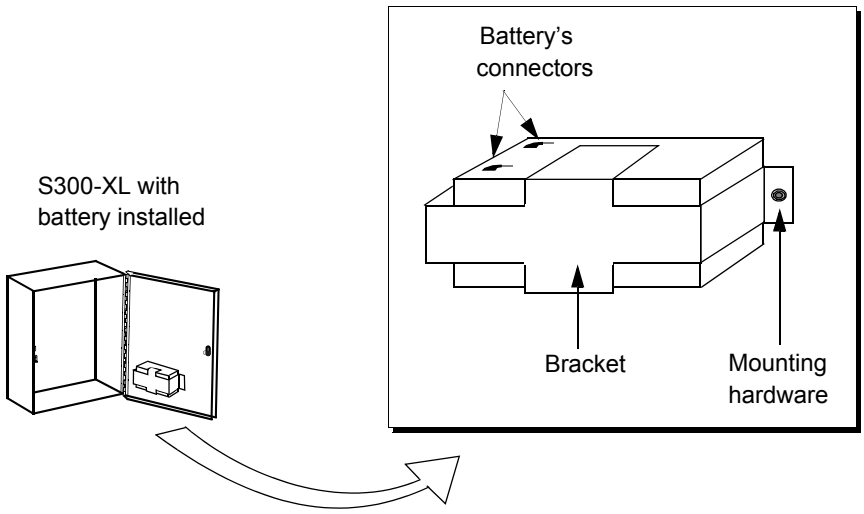


Figure 3-38: S300-BAT and S300-BRK2 Assembly

Installing the Backup Battery

Figure 3-41 through Figure 3-43 show the battery location for the panels.

➤ **Perform the following steps:**

1. Position the battery (+/- connectors on the left side) within the bracket and secure the bracket to the door with the supplied nuts.
2. Perform all other installation tasks (cabling, switch settings) before connecting the battery to the power supply.
3. Connect the battery cable from the battery terminals to J3 on the power supply.

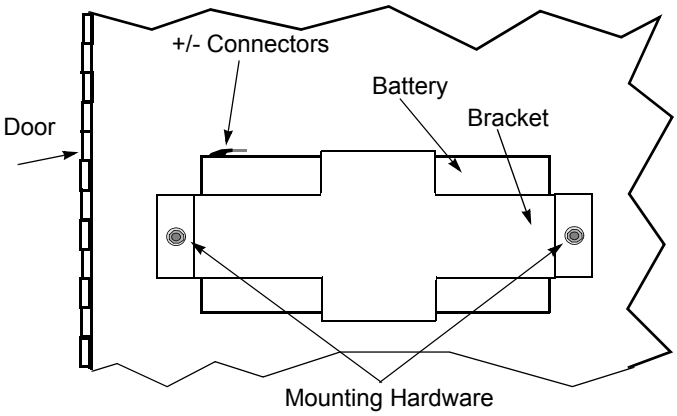


Figure 3-39: Battery Mounting for S300-XL and S300-XXS

CAUTION

Ensure the polarity connections are correct: Red wire to RED + and Black wire to BLK -.

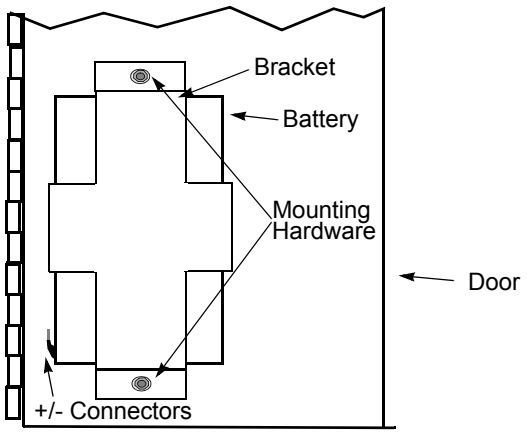


Figure 3-40: Battery Mounting for S300-XS

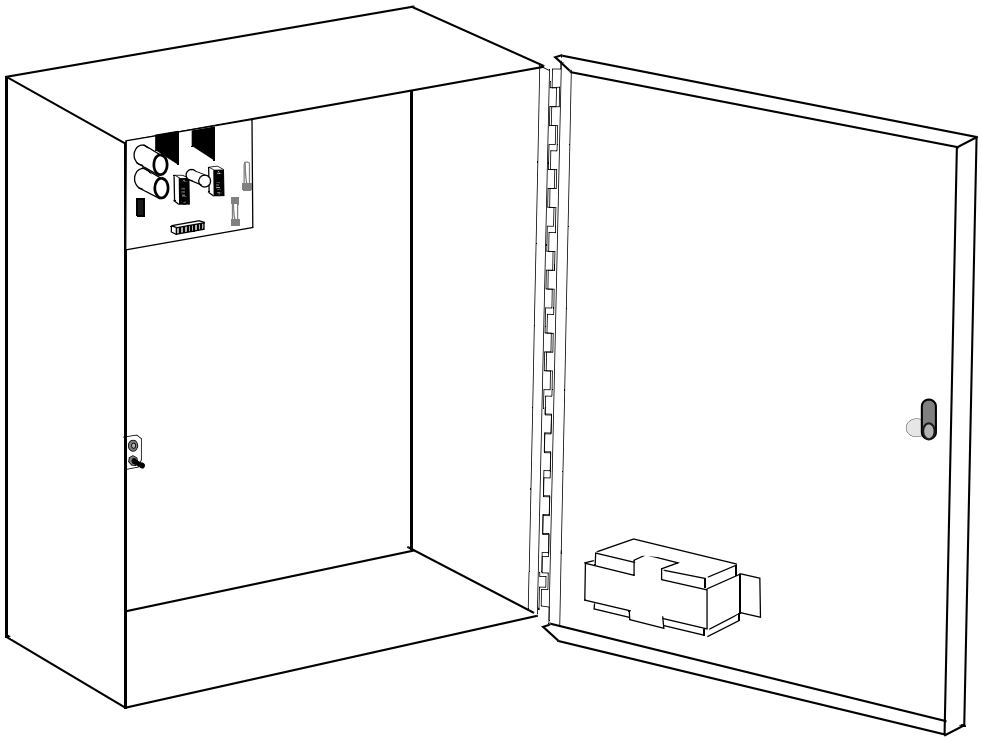


Figure 3-41: Battery Installation Location in S300-XL

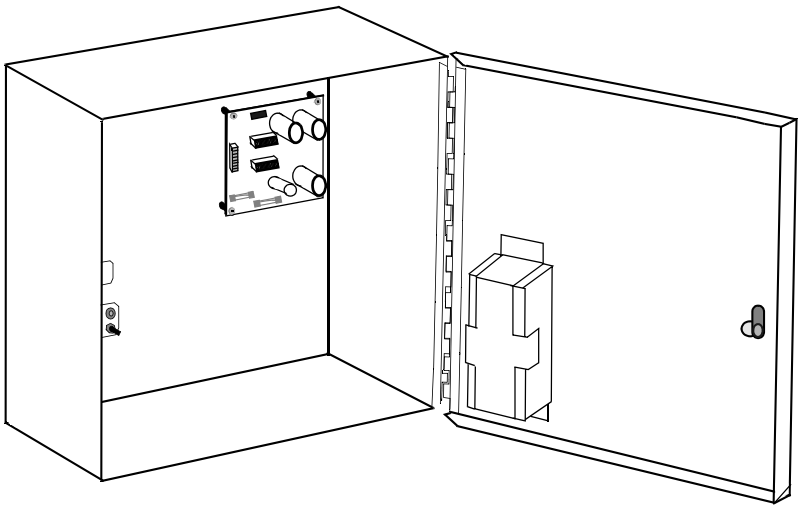


Figure 3-42: Battery Installation Location in S300-XS

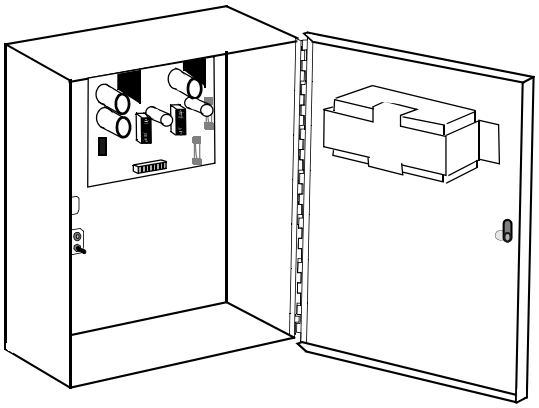


Figure 3-43: Battery Installation Location in S300-XXS

Chapter 4

CK721-A USER INTERFACE

The CK721-A intelligent controller provides a text-based user interface that you must use to configure a CK721-A for operation. The user interface gives you direct access to most CK721-A operating commands and parameters from a laptop or other remote PC before it is connected to the Cardkey SMS (Security Management System). These are useful when commissioning or troubleshooting the system.

When preparing a CK721-A for operation, you must:

- Enter the IP address of the CK721-A
- Enter the netmask of the CK721-A
- Enter the IP address of the Cardkey SMS
- Configure the Download Port Number, Upload Port Number, and Priority Port Number
- Modify the network polling delay, if needed
- Modify the network polling rate, if needed

These operations can all be performed at the CK721-A panel with the user interface. In addition, you can configure the controller for operation, such as defining terminals, inputs, and outputs. This is useful for testing the wiring between the controller, the external devices, and the Cardkey SMS.

NOTE

The CK721-A panel must be set up first using Terminal Emulation, before setting up the panel from the Cardkey SMS. Once the IP addresses are assigned at the panel, they cannot be changed from the Cardkey SMS.

NOTE

Unless noted otherwise, information contained in this document and pertaining to the S300-DIN-RDR2S module also applies to the S300-DIN-RDR2SA module. For differences and specific information on these modules refer to their respective user documentation.

PRINCIPLE OF OPERATION

During normal operation, CK721-A panels are configured using the Cardkey SMS software. When a controller is defined at the Cardkey SMS, the information downloaded to the panel automatically overwrites any information defined through the individual controller's user interface. The exceptions are the individual controller's IP and netmask addresses, the server IP and netmask, and the network polling delay. ***For this reason, the user interface should never be used to configure a panel once normal operation has begun***. After the start of normal operation, only the Cardkey SMS software should be used to configure CK721-As.

The CK721-A user interface can be used for troubleshooting purposes during normal operation.

NOTE

For identification purposes, the controller's IP address and netmask must match the IP address and netmask in the Cardkey SMS.

Communicating with the User Interface

Communicating with the user interface on a CK721-A requires:

- A laptop or personal computer with an available serial port
- A null modem serial cable
- Terminal emulation software

Using your Terminal Emulation

➤ **To start communication:**

1. Connect the serial cable between RS232C A (J3) of the CK721-A controller and your laptop or PC serial port.
2. Start your terminal emulator software.
3. Configure the communications parameters within your VT100 terminal emulation software to match the following:

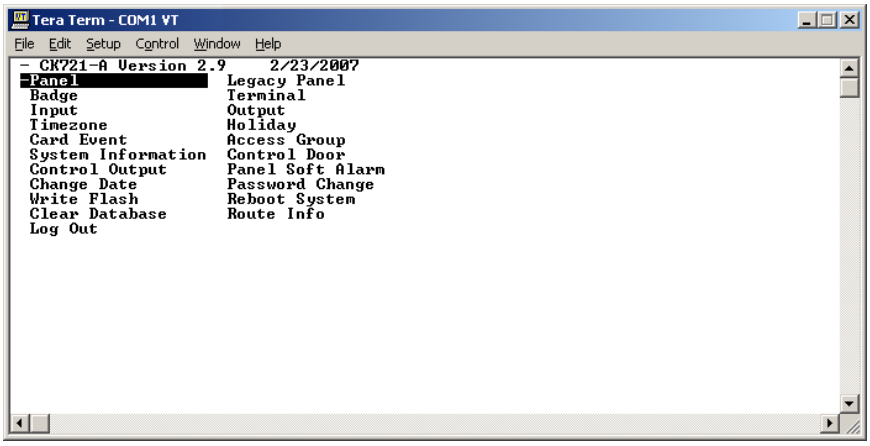
`Port`	`COMn`
`Baud Rate`	`115K`
`Data`	`8 bit`
`Parity`	`none`
`Stop`	`1 bit`
`Flow Control`	`none`

4. At the login prompt, type **CK720** and press <**Enter**>.
5. Type your password when prompted. (The initial default password is `master`.)
6. Press <**Enter**>.

NOTE

You have three chances to login to the CK721-A panel. After three attempts, the CK721-A disables login for about five minutes, after which time you may try again. (Both login and password are case-sensitive.)

7. The CK721-A panel Main menu appears as shown.



Navigating Through the User Interface

Use the following keys to navigate throughout the user interface.

Arrow Keys	Use the arrow keys to select a menu or option, or select a parameter you wish to edit.
<Enter>	Press **<Enter>** to view a selected menu or execute an option, like **<Save>** or **<Next Record>**.
<Space Bar>	Some fields contain two or more pre-set options. Pressing **<Space Bar>** toggles between available options.
User Defined Fields (abbreviation: User Def.)	Parameters that do not have pre-set options require that you type in a value using the laptop or PC keyboard.
<Esc>	Close a menu without saving changes.
<Save>	Write the current record to the database. Use the arrow keys to select this option and press <**Enter**>.
<Delete>	Remove the current record from the database. Use the arrow keys to select this option and press <**Enter**>.

<Previous Record>	Move to the previous record in the database for viewing or editing. Use the arrow keys to select this option and press <**Enter**>.
<Next Record>	Move to the next record in the database for viewing or editing. Use the arrow keys to select this option and press <**Enter**>.
<Page Up>	Move to the previous page of a multi-page screen. Use the arrow keys to select this option and press <**Enter**>.
<Page Down>	Move to the next page of a multi-page screen. Use the arrow keys to select this option and press <**Enter**>.
<Execute Command>	In some cases, such as Control Output, you will want to execute a command immediately. Select this option, when available, and press <**Enter**> to execute a command.
<Calibr.>	The Calibrate command issued from the User Interface (see the screen on page 4-63) will initiate input calibration at the S300-DIN-RDR2S controller. When the S300-DIN-RDR2S completes its calibration, typically within a few seconds, the panel will send a transaction message to the Real Time List indicating the calibration result. After a successful calibration, four-state input statuses will be available for the input point. During the entire input calibration procedure, the input's contact must be physically closed. Otherwise, the input's status will be unreliable. Once you perform a calibration procedure on an input, you should not use this feature again, unless you change the controller hardware or the input point's wiring.
<Uncalibr.>	The Uncalibrate command issued from the User Interface (see the screen on page 4-63) will initiate input uncalibration at the S300-DIN-RDR2S controller. When the S300-DIN-RDR2S completes its uncalibration, the panel will send a transaction message to the Real Time List indicating the result. After the uncalibration, four-state input statuses will no longer be available for the input, only two-state input statuses.

Write Flash

If database information is not backed up to the Onboard Flash Memory, or the panel does not have a backup battery (UPS), all database information except panel parameters will be lost after a power cycle.

➤ **To back up data to the Onboard Flash Memory:**

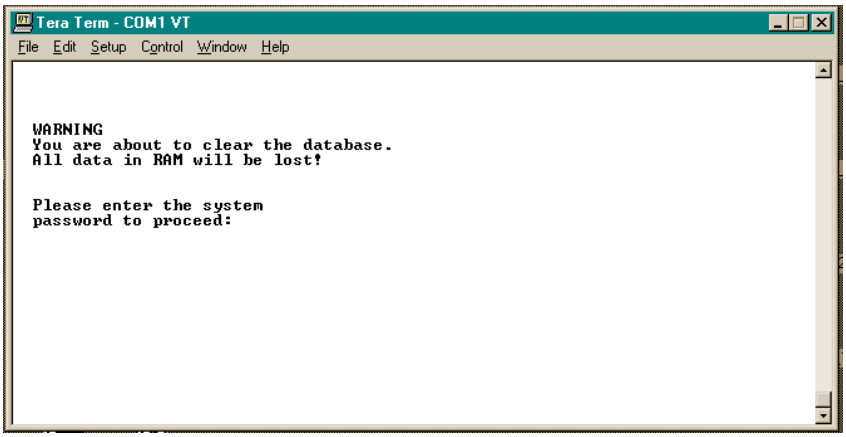
1. Select **Write Flash**.
2. Press <**Enter**>.
3. When the login prompt appears, the backup is complete.

Clearing Database

Clearing the database deletes the panel's database information, but it does not delete information from the Onboard Flash Memory.

➤ **To clear the database information:**

1. Select **Clear Database**.
2. Press <**Enter**>.
3. When prompted, type your password.
4. Press <**Enter**>.



Clearing the Flash Memory

➤ **To clear database information from the Flash Memory:**

1. Clear the database first, as instructed in the section above.
2. Select **Panel** and set the basic panel configuration as described in "Basic Panel Configuration" on page 4-8.
3. Select **Save** and press <**Enter**>.
4. Press <**Esc**>.
5. Select **Write Flash**.
6. Press <**Enter**>.
7. When the login prompt appears, the database information has been cleared from the Flash Memory. You can now download information from the Cardkey SMS.

Router Configuration

The default CK721-A Panel Routing Information Protocol (RIP) is dynamic, that is, it regularly listens for RIP from the network. If RIP is disabled, manual route information can be added using this screen. A maximum of four addresses can be entered at one time. Both Destination and Gateway addresses must be entered.

In other words, to use a router, you must define a *Gateway* IP address (which is the closest route to the panel) and a *Destination* IP address (which is the Server IP or Network IP).

➤ To enter a Static Route:

1. From the Main menu select **Route Info**.
2. From the Route Configuration screen, select **host** or **net**. *(Use the spacebar to toggle between Host/Net and use the enter key to move to the next column.)*
3. Specify the **Destination** address as follows:
   - If **host** is selected, the destination IP address is the Network ID and the specific Host ID address of the Cardkey SMS such as 200.0.0.1
   - If **net** is selected, only the network ID is specified for the destination such as 200.0.0.0
4. For the **Gateway** address enter the router IP address.
5. Reboot the CK721-A panel.

Notes on Adding IP Addresses in Route Configuration Screen:

- Do not add leading zeros in IP address field; otherwise no host connection will be made. Enter the IP address without leading zeros.
- If you cannot communicate with the server using host route, try using the net route using only the network ID as the destination.

Troubleshooting

- Verify the static route is correct under route info.
- Verify that the netmask is correct.
- Log in to the panel using “diag” (default password is `master`) and:

  - Verify that you can ping the gateway.
  - Verify that you can ping the Cardkey SMS.
  - Check the CK721-A routing table using the command `netstat -r`.
  - Use the command `traceroute <host ip address>` to verify route to the Cardkey SMS.

CK721-A Static Route Examples

Host Destination Example:

Settings in the Route Configuration screen:

```
Host/Net    Destination    Gateway
-host       200.0.0.1      201.0.0.5
```

Net Destination Example:

Settings in the Route Configuration screen:

```
Host/Net    Destination    Gateway
-net        200.0.0.0      201.0.0.1
```

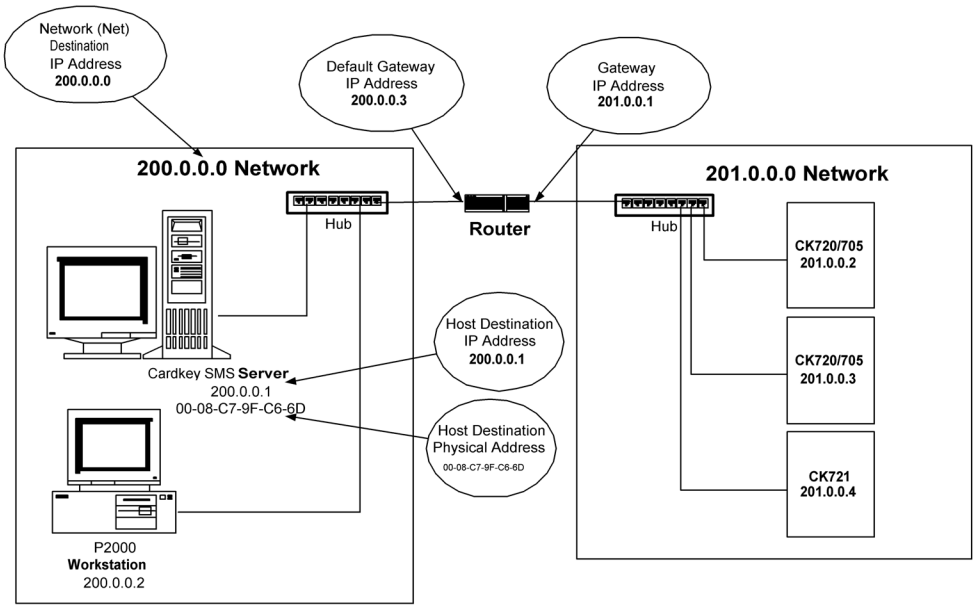


Figure 4-1: Static Route Examples

Log Out

After configuring or viewing system parameters, always log out, and then remove the serial cable. To log out from the CK721-A user interface, select **Log Out**, and press <**Enter**>.

BASIC PANEL CONFIGURATION

Panel Menu

It is necessary to perform the following steps at every CK721-A controller in your system that communicates with the following server:

- P2000 server (version 2.1 or later)

These steps set the IP address and netmask, the preferred primary comm path, and the network polling of the CK721-A, which are required for communication with the above servers. The following table shows the required settings for proper operation.

NOTE

These settings must be identical in the Cardkey SMS software Panel window.

Table 4-1: Required Settings - Panel Menu

Setting	Value (Direct Connect)
Controller Primary IP Address:	Enter the IP address for this CK721-A panel.
Primary Host IP Address:	Enter the IP address of the Cardkey SMS Server.
Controller Secondary IP Address:	N/A
Alternate Host IP Address:	N/A
Preferred Primary Comm Path (Y/N):	Y
Network Polling [LAN]:	Recommended to be 30 sec.
Network Polling [Dup]:	N/A
Download Port Number:	41014* (default value) or 1198**
Upload Port Number:	41013* (default value) or 1199**
Priority Port Number:	41012* (default value) or 1200**

* For the systems using P2000 Server version 2.1 and higher. The port numbers must match those defined at the P2000 Server.

** For the systems using P1000 Servers (any version), P1500 Servers (any version), and P2000 Servers version prior to version 2.1. The port numbers must match those defined at the Server.

Rebooting the Panel

Reboot the CK720 from the Main menu option **Reboot System**, or power cycle the panel.

If connecting over a WAN or to another segment, program the Route Information screen.

Legacy Panel Menu

It is necessary to perform the following steps at every CK721-A controller in your system that communicates with any of the following servers:

- P1000 server (any version)
- P1500 server (version 2.0 or earlier)
- P2000 server (version 2.0 or earlier)

These steps set the IP address and netmask, the preferred primary comm path, and the network polling delay of the CK721-A, which are required for communication with the above servers. The following table shows the required settings for proper operation.

NOTE

These settings must be identical in the Cardkey SMS software Panel window

Table 4-2: Required Settings - Legacy Panel Menu

Setting	Value (Direct Connect)
Controller Primary IP Address:	Enter the IP address for this CK721-A panel.
Primary Host IP Address:	Enter the IP address of the Cardkey SMS server.
Controller Secondary IP Address:	N/A
Alternate Host IP Address:	N/A
Preferred Primary Comm Path (Y/N):	Y
Network Polling Delay (5-60):	Recommended to be 10.

Rebooting the Panel

Reboot the CK720 from the Main menu option **Reboot System**, or power cycle the panel.

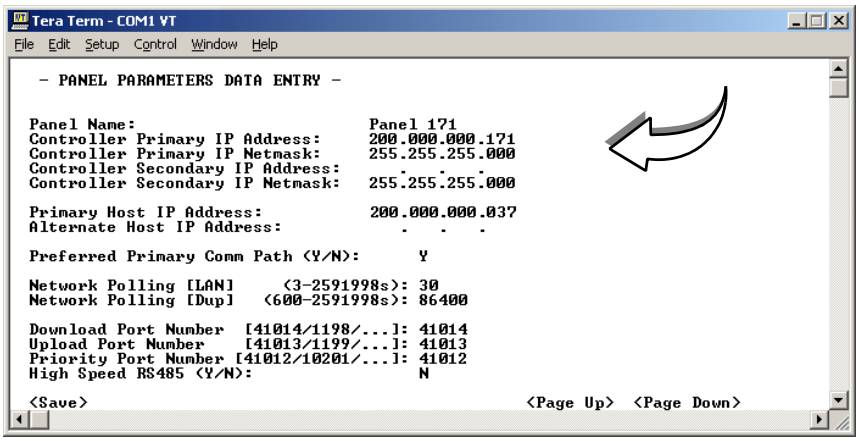
If connecting over a WAN or to another segment, program the Route Information screen.

Panel

➤ To set the CK721-A IP address and netmask, preferred primary comm path:

1. From the CK721-A Main menu, select **Panel** and press <**Enter**>.
2. Type the panel name and IP address. The IP address **must be unique**.

   The default netmask is 255.255.255.0, a standard TCP/IP value.



3. The panel uses the *primary* network interface (the onboard network interface) and the Primary Host IP Address. Enter a Primary Host IP address that matches the IP address of the server.

   The netmask default value (Class “C”) can be modified as needed.

   The Alternate Host IP Address not currently used.
4. The Preferred Primary Comm Path must be set to **Y**.
5. The recommended setting for Network Polling [LAN] is 30 seconds.

   The Network Polling [LAN] value specifies the frequency (in seconds) that the CK721-A panel polls the P2000 server (version 2.1 or higher) during LAN connections.

   The Network Polling [Dup] value is not currently used.
6. Configure the port numbers. The entered port numbers must match those defined at the server.

   For systems using P2000 Server version 2.1 and higher enter the following numbers:

Download Port Number	41014 (default value)
Upload Port Number	41013 (default value)
Priority Port Number	41012 (default value)

For systems using P1000 Servers (any version), P1500 Servers (any version), and P2000 Servers version prior to version 2.1, enter the following numbers:

Download Port Number	1198
Upload Port Number	1199
Priority Port Number	1200

7. After these values are entered, use the arrow keys to select **Save** and press <**Enter**>.
8. A message appears informing you the record has been saved. Press <**Esc**> to return to the CK721-A Main menu.
9. Always reboot after changing IP information.

Your CK721-A is now operational.

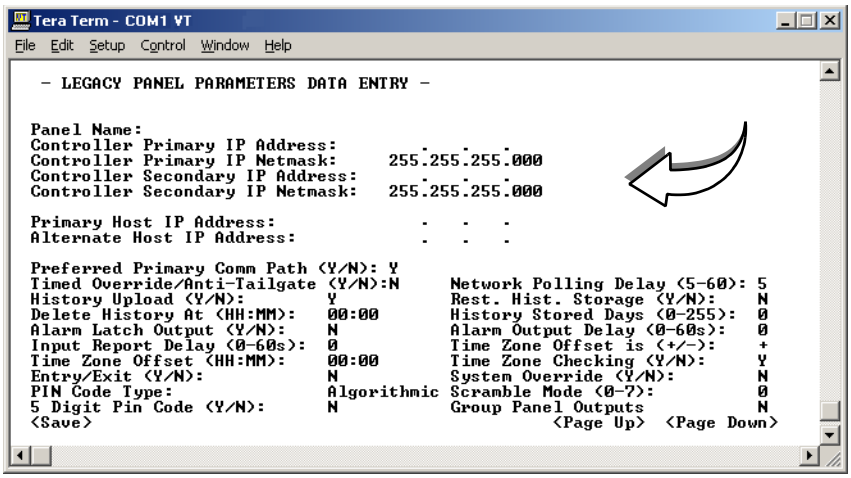
Changes to the IP address and netmask, and preferred primary comm path and the port numbers must be performed locally at the panel. All other parameters can be programmed locally or at the P2000 server. The remainder of this chapter describes the user interface, which can be used for testing installation and troubleshooting the system.

Legacy Panel

➤ To set the CK721-A IP address and netmask, preferred primary comm path, and network polling delay:

1. From the CK721-A Main menu, select **Legacy Panel** and press <**Enter**>.
2. Type the panel name and IP address. The IP address **must be unique**.

   The default netmask is 255.255.255.0, a standard TCP/IP value.



3. The panel uses the *primary* network interface (the onboard network interface) and the Primary Host IP Address. Enter a Primary Host IP address that matches the IP address of the server.

   The netmask default value (Class "C") can be modified as needed.

   The Alternate Host IP Address not currently used.
4. The Preferred Primary Comm Path must be set to **Y**.
5. The recommended setting for Network Polling Delay is 10.

   The Network Polling Delay value specifies the maximum time the panel should be without contact to the server.
6. After these values are entered, use the arrow keys to select **Save** and press <**Enter**>.
7. A message appears informing you the record has been saved. Press <**Esc**> to return to the CK721-A Main menu.
8. Always reboot after changing IP information.

Your CK721-A is now operational.

Changes to the IP address and netmask, preferred primary comm path, and network polling delay must be performed locally at the panel. All other parameters can be programmed locally or at the Cardkey SMS. The remainder of this chapter describes the user interface, which can be used for testing installation and troubleshooting the system.

DIRECT PROGRAMMING OF THE CK721-A

During normal operation, the CK721-A should always be programmed and monitored using the Cardkey Security Management System. While the user interface provides much of the same functionality as the Cardkey SMS software, key features, such as alarm monitoring cannot be done. But for testing the installation of the field controllers and related hardware, the user interface is a valuable tool.

The remainder of this chapter describes all of the features available in the CK721-A user interface. For a more in-depth description of the features, refer to the *P2000 Software User Manual*. However, most of the CK721-A parameters resemble those contained in the Cardkey SMS software.

Panel Screen Description

The Panel screen is used when the CK721-A panel is configured for the following server:

- P2000 server (version 2.1 or later)

Table 4-6 describes the available options.

Panel Screen - Page 1

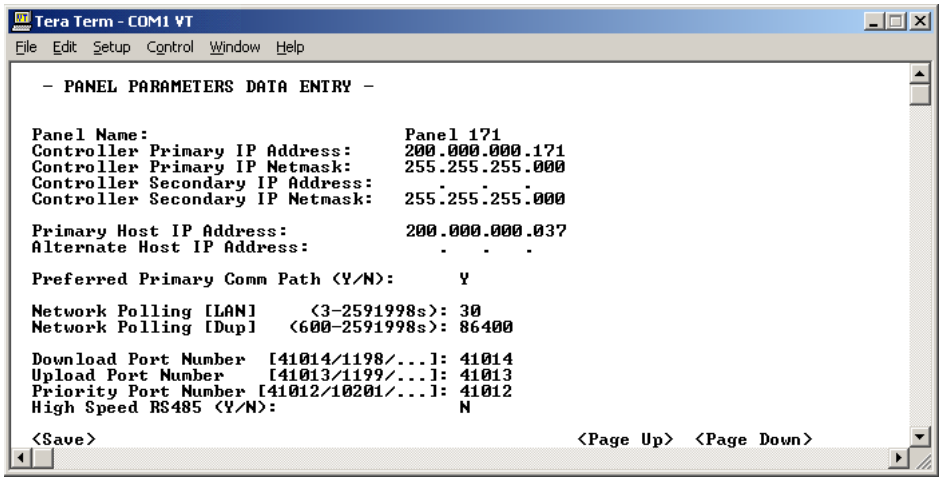


Table 4-3: Panel Screen, Page 1

Field	Type	Description
Panel Name	User Def.	The panel name is defined at the server, and then downloaded from the server to the panel. The panel name cannot be changed from the panel.
Controller Primary IP Address	User Def.	The IP address used by the onboard network interface. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. To clean the IP entry, enter the IP value of 000.000.000.000.
Controller Primary IP Netmask	User Def.	A 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, default subnet mask numbers use either 0 or 255 as values. Default value: 255.255.255.0 [Class C networks]
Controller Secondary IP Address	User Def.	This IP address is reserved for future use in support of a secondary IP interface.
Controller Secondary IP Netmask	User Def.	This netmask is reserved for future use in support of a secondary IP interface.

Table 4-3: Panel Screen, Page 1

Field	Type	Description
Primary Host IP Address	User Def.	The primary IP address used by the primary server network interface. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. To clean the IP entry, enter the IP value of 000.000.000.000. **Note:** Prior to entering the address, the panel must be defined in the P2000 database.
Alternate Host IP Address	User Def.	This IP address is reserved for future use in support of a secondary IP interface.
Preferred Primary Comm Path	Toggle	Enabled (**Y**) by default. The CK721-A will communicate via onboard network interface.
Network Polling (LAN)	User Def.	Specifies the maximum time (in seconds) the panel allows between consecutive polls to the server over the LAN connection. The network poll (LAN) interval is limited to values between 5 seconds and 30 days.
Network Polling (Dup)	User Def.	The Dialup connection polling is not currently used.
Download Port Number (1 to 65535)	User Def.	A TCP port number used for downloads from the server. This number must match that configured at the server. See step 6 on page 4-10 for details.
Upload Port Number (1 to 65535)	User Def.	A TCP port number used for uploads to the server. This number must match that configured at the server. See step 6 on page 4-10 for details.
Priority Port Number (1 to 65535)	User Def.	A TCP port number used for sending central access requests and for transactions confirming the panel and the server are online. This number must match that configured at the server. See step 6 on page 4-10 for details.
High Speed 485	Toggle	When enabled (**Y**), causes the CK721-A to communicate with the terminals at 19,200 baud. For information on firmware version required for High Speed RS485, see page 3-37.

Panel Screen - Page 2

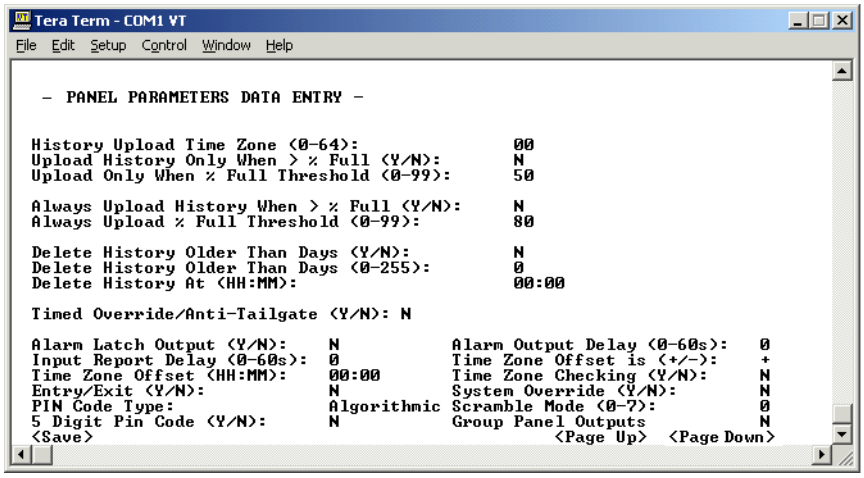


Table 4-4: Panel Screen, Page 2

Field	Type	Description
History Upload Time Zone	User Def.	If specified, saved history reports are uploaded in time zones defined as Active. If not specified, history records are saved, and not reported to the server. Timezone range: 0 - 64
Upload History Only When > % Full	Toggle	If enabled (**Y**), then saved history reports are uploaded only when the number of saved reports exceeds the specified “percent full” value specified in the next field.
Upload History When % Full Threshold	User Def.	Saved history reports are uploaded only when the number of saved history reports exceeds the specified “percent full” value. In order to work, this option must be enabled in the previous field. Percentage range: 0 - 99
Always Upload history When > % Full	Toggle	If enabled (**Y**), the history is always uploaded when the number of history records exceeds the value specified in the next field.
Always Upload % Full Threshold	User Def.	Saved history reports are always uploaded when the number of history records exceeds the specified “percent full” value. In order to work, this option must be enabled in the previous field. Percentage range: 0 - 99

Table 4-4: Panel Screen, Page 2

Field	Type	Description
Delete History Older Than Days	Toggle	If enabled (**Y**), saved history records, older than the specified number of days (see next field) will be deleted.
Delete History Older Than Days	User Def	History older than the specified number of days will be deleted. In order to work, this option must be enabled in the previous field. Value range: 0 - 255 days
Delete History At	User Def	Specifies the hours and minutes at which the saved history deletion occurs. In order to work, this option must be enabled in the “Delete History Older Than Days” toggle field.
Timed Override/ Anti-Tailgate	Toggle	If enabled (**Y**), a reader controlled door, which is in a state of Timed Override, may be locked automatically when the door is closed. This option should not be used with the “Re-lock on Door Open” option because “Timed Override/Anti-Tailgate” can only work when the door closes, and not when the door opens (shunting of the door contact is cancelled at the same time as “Timed Override/Anti-Tailgate” is cancelled).
Alarm Latch Output	Toggle	If enabled (**Y**), the alarm relay is activated whenever an input goes into alarm, and remains activated until reset. If disabled (**N**), and “Activate Relay when Set” under Input is enabled, the panel alarm relay is activated whenever an alarm occurs and deactivated when all alarms are reset.
Input Report Delay	User Def.	Enter a value between 0 and 60 seconds. Determines the number of seconds between an input going active and when it is reported at the panel.
Time Zone Offset	User Def.	Values are hours and minutes (HH:MM). Used if the controller is physically in a different geographical time zone than the Cardkey SMS.
Entry/Exit	Toggle	If enabled (**Y**), readers can enforce Entry/Exit rules for access control.
PIN Code Type	Toggle	Choices are: Algorithmic, Custom (User Defined).
5 Digit Pin Code	Toggle	If enabled, (**Y**) 5-digit PIN codes can be used at this controller. Otherwise, 4-digit codes are used.

Table 4-4: Panel Screen, Page 2

Field	Type	Description
Alarm Output Delay	User Def.	Values are 0 to 60 seconds. This is the number of seconds the alarm relay waits before activating.
Time Zone Offset Is	Toggle	A + indicates the offset value (described above) is ahead of the controller Time Zone. A - means the offset time is behind the current Time Zone.
Time Zone Checking	Toggle	When enabled (**Y**), the controller will check for valid reader and card time zones, card access requests, PIN code suppression, and upload suppression against active Time Zones.
System Override	Toggle	If enabled (**Y**), all portals connected to this controller are set in the unlocked position.
Scramble Mode	User Def.	Values are from 0 - 7. Select one of eight algorithms if using algorithmic PIN codes.
Group Panel Output	Toggle	When you change the Group Panel Outputs field on the Panel screen to (**Y**), the system will create an 599 output point. The system automatically associates Group 599 with the CK721-A relay. This enables you to control onboard relay by using the output group through I/O linking or card events. **Note:** Changes to the Panel Output Relay setup (includes Output Latching and Alarm Relay Linking settings) require a write of the database to flash before the updated Panel Output Relay settings take effect.

Panel Screen - Page 3

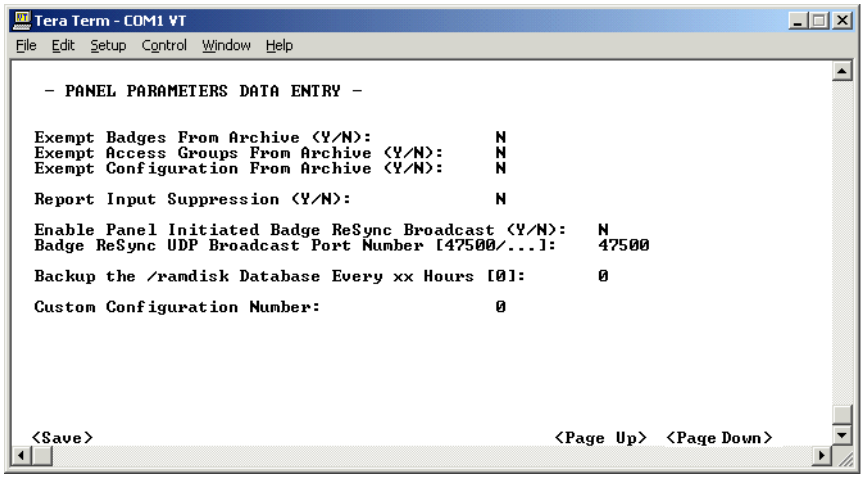
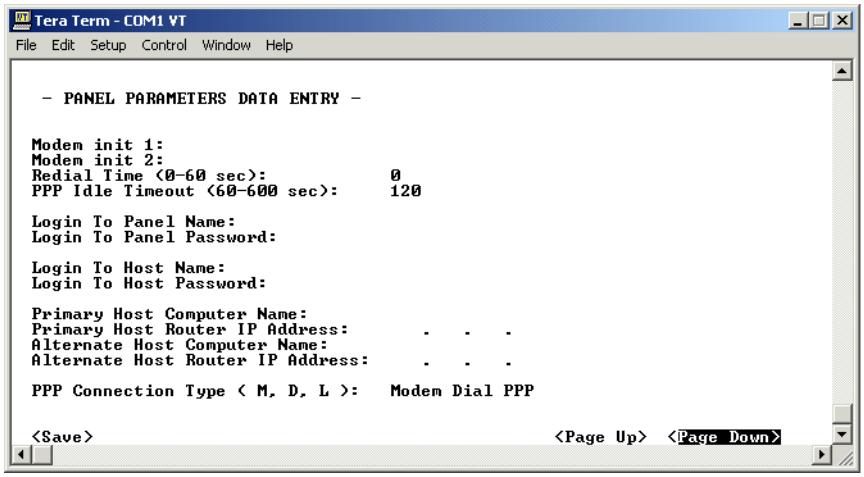


Table 4-5: Panel Screen, Page 3

Field	Type	Description
Exempt Badges From Archive	Toggle	If enabled (**Y**), then the Badge database is not saved to Flash during a Write-Flash operation.
Exempt Access Groups From Archive	Toggle	If enabled (**Y**), then the Access Groups databases (Access Groups, and Elevator Access Groups) are not saved to Flash during a Write-Flash operation.
Exempt Configuration From Archive	Toggle	If enabled (**Y**), then the Panel Configuration databases (Elevator Configuration, Terminal, Input, Output, Timezones, Holidays, Soft Alarms, and Card Events) are not to Flash during a Write-Flash operation.
Report Input Suppression	Toggle	If enabled (**Y**), input points that enter suppression are reported as being suppressed. When the input is no longer suppressed, the current input point state is reported.
Enable Panel Initiated Badge ReSync Broadcast	Toggle	Enable Panel Initiated Badge Entry/Exit Resynch UDP Broadcast Flag. Disabled (**N**) by default.
Badge ReSync UDP Broadcast Port Number	User Def.	Badge ReSynch UDP Broadcast Port Number. The UDP port number used by the Badge ReSynch UDP Broadcast agents. Value Range: 1 to 65535 Default value: 47500. **Note:** This number must match that configured at the other CK721-A Panels.
Backup The Ramdisk Database Every xx Hours	User Def.	Schedules the automatic backup of the ramdisk database to flash memory. The minimum database backup period is every hour. The maximum time between database backups is 24 hours (around 3:15 am). The default database backup period is once every 24 hours (around 3:15 am). A database backup period of 0 hours disables automatic database backups to flash memory.
Custom Configuration Number	User Def.	Selects and enables custom features.

Panel Screen - Page 4 and 5

Pages 4 and 5 of the Panel Parameters screen are not currently used.



Legacy Panel Screen Description

The legacy panel screen is used when the CK721-A panel is configured for any of the following servers:

- P1000 server (any version)
- P1500 server (any version)
- P2000 server (version 2.0 or earlier)

Table 4-6 describes the available options.

Legacy Panel Screen - Page 1

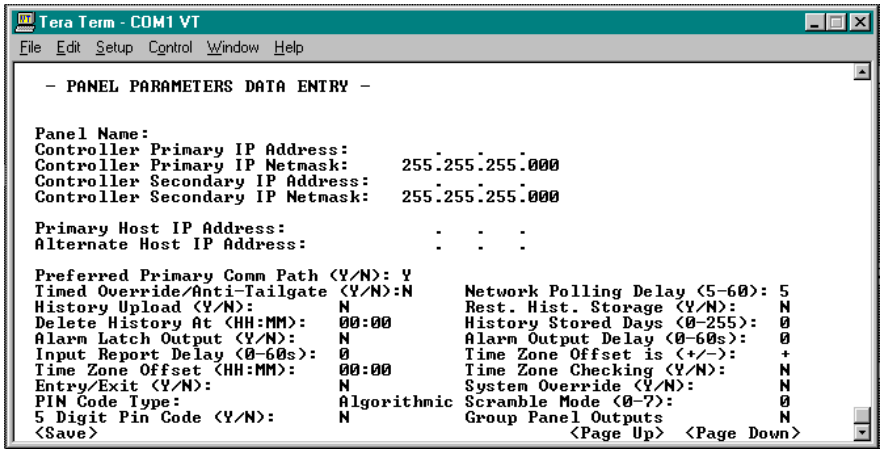


Table 4-6: Legacy Panel Screen, Page 1

Field	Type	Description
Panel Name	User Def.	The panel name is defined at the server, and then downloaded from the server to the panel. The panel name cannot be changed from the panel.
Controller Primary IP Address	User Def.	The IP address used by the onboard network interface. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods.
Controller Primary IP Netmask	User Def.	A 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, default subnet mask numbers use either 0 or 255 as values. Default value: 255.255.255.0 [Class C networks]
Controller Secondary IP Address	User Def.	This IP address is reserved for future use in support of a secondary IP interface.
Controller Secondary IP Netmask	User Def.	This netmask is reserved for future use in support of a secondary IP interface.
Primary Host IP Address	User Def.	The primary IP address used by the primary server network interface. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods.
Alternate Host IP Address	User Def.	This IP address is reserved for future use in support of a secondary IP interface.
Preferred Primary Comm Path	Toggle	Enabled (**Y**) by default. The CK721-A will communicate via onboard network interface.
Timed Override/ Anti-Tailgate	Toggle	If enabled (**Y**), a reader controlled door, which is in a state of Timed Override, may be locked automatically when the door is closed. This option should not be used with the “Re-lock on Door Open” option because “Timed Override/Anti-Tailgate” can only work when the door closes, and not when the door opens (shunting of the door contact is cancelled at the same time as “Timed Override/Anti-Tailgate” is cancelled).

Table 4-6: Legacy Panel Screen, Page 1

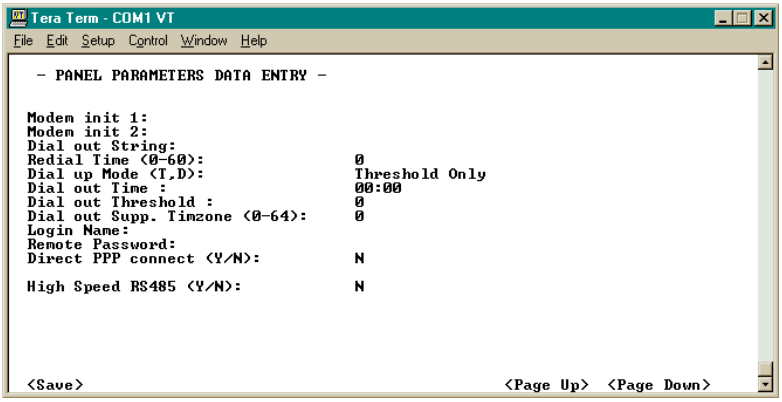
Field	Type	Description
History Upload	Toggle	If enabled (**Y**), history is uploaded to the Cardkey SMS for archival.
Delete History At	User Def.	Specify hours and minutes. Time of day when history deletion occurs, if “Rest. Hist. Storage” is enabled.
Alarm Latch Output	Toggle	If enabled (**Y**), the alarm relay is activated whenever an input goes into alarm, and remains activated until reset. If disabled (**N**), and “Activate Relay when Set” under Input is enabled, the panel alarm relay is activated whenever an alarm occurs and deactivated when all alarms are reset.
Input Report Delay	User Def.	Enter a value between 0 and 60 seconds. Determines the number of seconds between an input going active and when it is reported at the panel.
Time Zone Offset	User Def.	Values are hours and minutes (HH:MM). Used if the controller is physically in a different geographical time zone than the Cardkey SMS server.
Entry/Exit	Toggle	If enabled (**Y**), readers can enforce Entry/Exit rules for access control.
PIN Code Type	Toggle	Choices are: Algorithmic, Custom (User Defined).
5 Digit Pin Code	Toggle	If enabled, (**Y**) 5-digit PIN codes can be used at this controller. Otherwise, 4-digit codes are used.
Network Polling Delay (5-60)	User Def.	Set the frequency in seconds that the server polls CK721-A panels over the network. This option can account for any communication delays that might occur over a LAN or WAN. (The default is 5 seconds; the recommended setting is 10 seconds.)
Rest. Hist. Storage	Toggle	If enabled (**Y**), access grant transactions that do not involve a PIN are not stored.
History Stored Days	User Def.	Values are from 0 to 255 days. Specifies the number of days history is stored before being deleted, if “Rest. Hist. Storage” is enabled.
Alarm Output Delay	User Def.	Values are 0 to 60 seconds. This is the number of seconds the alarm relay waits before activating.

Table 4-6: Legacy Panel Screen, Page 1

Field	Type	Description
Time Zone Offset Is	Toggle	A + indicates the offset value (described above) is ahead of the controller Time Zone. A - means the offset time is behind the current Time Zone.
Time Zone Checking	Toggle	When enabled (**Y**), the controller will check for valid reader and card time zones, card access requests, PIN code suppression, and upload suppression against active Time Zones.
System Override	Toggle	If enabled (**Y**), all portals connected to this controller are set in the unlocked position.
Scramble Mode	User Def.	Values are from 0 - 7. Select one of eight algorithms if using algorithmic PIN codes.
Group Panel Output	Toggle	When you change the Group Panel Outputs field on the Panel screen to (**Y**), the system will create an output group 599. The system automatically associates Group 599 with the CK721-A relay. This enables you to control the onboard relay by using an output group through I/O linking or card events. **Note:** Changes to the Panel Output Relay setup (includes Output Latching and Alarm Relay Linking settings) require a write of the database to flash before the updated Panel Output Relay settings take effect.

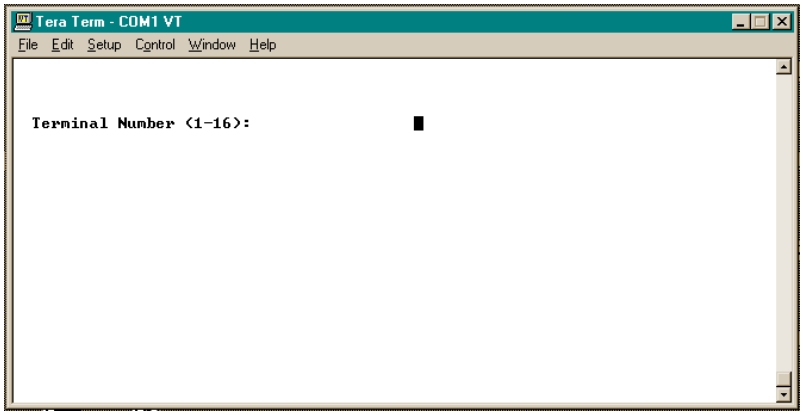
Legacy Panel Screen - Page 2

Page 2 of the Legacy Panel Parameters screen is not currently used.

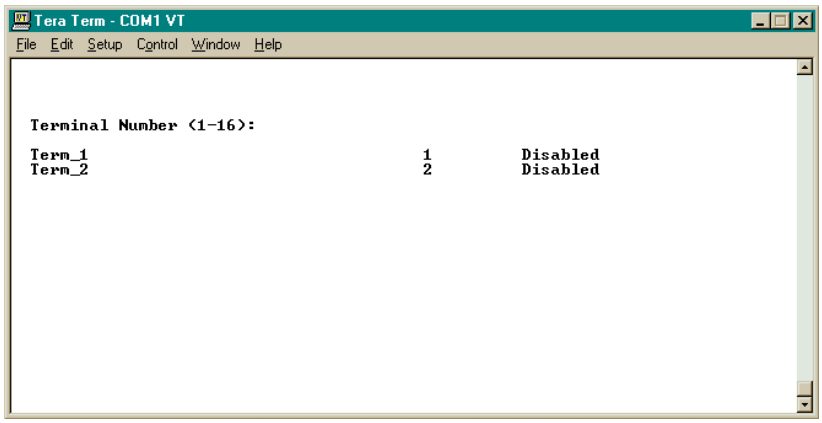


Terminal

Terminal screens are used to configure the individual readers, and input/output terminals connected to the CK721-A. You can edit an existing terminal or add a new terminal to the system. When you select the **Terminal** option and a new terminal number, the system automatically assumes you are adding a new record.



After you have defined the terminal records, they will be listed in the number selection screen. If you select a previously saved record, the system places you in editing mode.



The four screens used to configure Terminals are described in Table 4-7 through 4-6.

Terminal Screen - Page 1

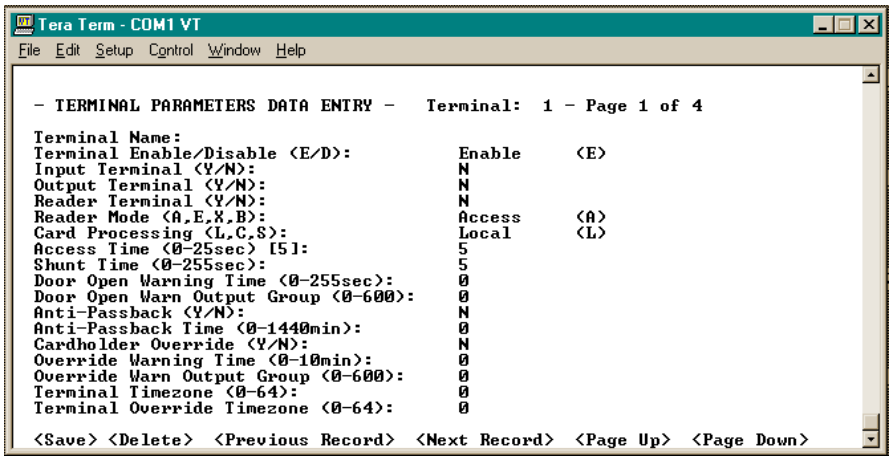


Table 4-7: Terminal Screen, Page 1

Field	Type	Description
Terminal Name	User Def.	Enter a name for this terminal. Up to 25 alphanumeric characters, including spaces, are available.
Terminal Enable/Disable	Toggle	Enabled (**E**) indicates the terminal is operational and will be polled by the CK721-A. Disabled (**D**) means the terminal can be defined, but will not be polled.
Input Terminal	Toggle	A (**Y**) indicates an input or input/output module has this terminal address.
Output Terminal	Toggle	A (**Y**) indicates an input/output module has this terminal address.
Reader Terminal	Toggle	A (**Y**) indicates a two reader module has this terminal address.
Reader Mode	Toggle	Choices are: A (Access) E (Entry) X (Exit)
Card Processing	Toggle	Choices are: L (Local Mode) C (Central Mode) S (Shared Mode)
Access Time	User Def.	Values range from 0 to 25 seconds, with 5 seconds as default. This represents the time the door strike remains energized after a valid card request.

Table 4-7: Terminal Screen, Page 1

Field	Type	Description
Shunt Time	User Def.	Values range from 0 to 255 seconds. This represents the amount of time the door open alarm is suppressed after a valid card access request. (Note: After an access grant, the shunt time will be cancelled once the door status changes to locked and closed, even if the shunt time has not yet expired.)
Door Open Warning	User Def.	Values range from 0 to 255 seconds. This represents the time prior to the expiration of the shunt time that the warning output is activated.
Door Open Warning Output Group	User Def.	Enter the number of the output group (1-600) that will be activated for the open door warning. (0 means no group is assigned.) When the output group is activated, is will not de-activate by itself. Additional settings, like Timed Duration of each output point in the group, is needed for automatic de-activation.
Anti-Passback	Toggle	If enabled (**Y**), the reader is designated as an Anti-Passback reader. Use Anti-Passback Time to set the number of minutes a card remains invalid at Anti-Passback readers after the card has been granted access at an Anti-Passback reader.
Anti-Passback Time	0-1440 min	With Anti-Passback enabled (**Y**), set the time here. When time set to 0, and Anti-Passback is enabled (**Y**), this reader will reset the Anti-Passback Time for all readers on this panel for a card that has been granted access locally.
Cardholder Override	Toggle	If enabled (**Y**), a cardholder may override access control at a keypad reader at this terminal. The amount of time is programmed at the keypad.
Note: Override Warning Time and Override Warning Output Group (the next two settings defined) work together: You can set up a time (Override Warning Time) before an override expires at which a warning (such as an audible beep) will be activated. The Override Warning Output Group setting assigns the output group that will be activated at the Override Warning Time.		
Override Warning Time	User Def.	You can activate an output group as a warning before the Cardholder Override expires. Enter the amount of time here (0 - 10 minutes).

Table 4-7: Terminal Screen, Page 1

Field	Type	Description
Override Warning Output Group	User Def.	Enter the number of the output group (1-600) that will be activated for the Override Warning Time. (0 means no group is assigned.) When the output group is activated, is will not de-activate by itself. Additional settings, like Timed Duration of each output point in the group, is needed for automatic de-activation.
Terminal Timezone	User Def.	Values range from 0 - 64 (timezone numbers). This function sets a timezone for the terminal. When the timezone is active, the terminal will be able to grant access requests. (Timezones are numbered 1 to 64; 0 means no timezone is assigned.)
Terminal Override Timezone	User Def.	Values range from 0 - 64 (timezone numbers). A timezone that, when active, puts the terminal into unrestricted access. (Timezones are numbered 1 to 64; 0 means no timezone is assigned.)

Terminal Screen - Page 2

Page 2 of the Terminal screen is shown, followed by Table 4-8, which contains a description of each item.

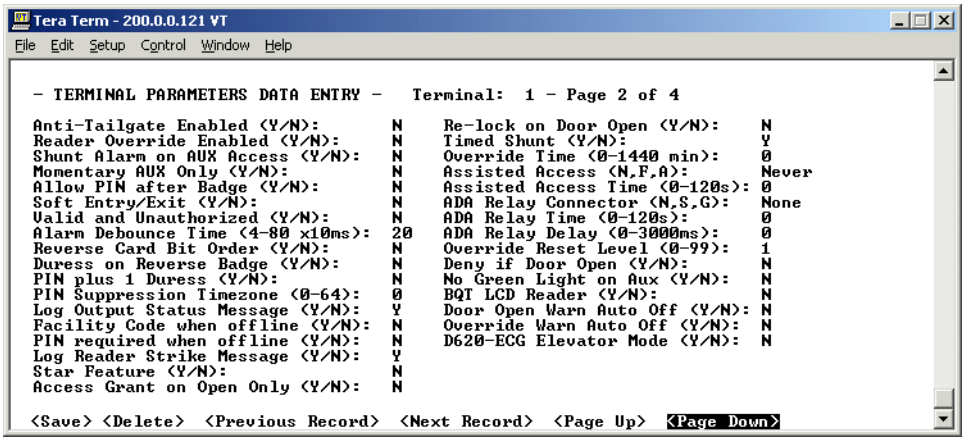


Table 4-8: Terminal Screen, Page 2

Field	Type	Description
Anti-Tailgate Enabled	Toggle	If enabled (**Y**), the access timer resets and the strike locks immediately when the door closes.
Reader Override Enabled	Toggle	If enabled (**Y**), no card is required when the Terminal Override Timezone is active.

Table 4-8: Terminal Screen, Page 2

Field	Type	Description
Shunt the Alarm on AUX Access	Toggle	If enabled (**Y**), the AUX Access Input Point on the terminal will only suppress the Door Open Alarm. If disabled (**N**), the input point will perform an access grant.
Momentary AUX Only	Toggle	Allows (**Y**) the Access Time to begin timing when the terminal's AUX Access input point contact is shorted by a switch.
Allow PIN after Badge	Toggle	Allows (**Y**) the cardholder to enter a PIN after presenting a card, instead of before presenting a card.
Soft Entry/Exit	Toggle	If enabled (**Y**), an Entry/Exit access violation will allow access.
Valid and Unauthorized	Toggle	Setting this enabled (**Y**) allows a cardholder to present a valid badge, but the door strike will not be released automatically. **Note**: Terminal must be on-line with a Cardkey SMS.
Alarm Debounce Time	User Def.	Values range from 4-80, which corresponds to debounce times of 40-800 ms.
Reverse Card Bit Order	Toggle	If enabled (**Y**), a swiped card can be read in either forward or reverse direction. **Note**: The card can be presented/swiped facing forward or backward, but must always be swiped in the same direction. (This corresponds to "Reverse Reading" in the Terminal window of the Cardkey SMS.)
Duress on Reverse Badge	Toggle	When enabled (**Y**), a reverse read on a swiped card initiates a duress alarm. The Duress soft alarm must be enabled for this feature to work. Reverse Card Bit Order must be enabled as well. (This corresponds to "Reverse Swipe duress" in the Terminal window of the Cardkey SMS.)
PIN plus 1 Duress	Toggle	When enabled (**Y**), the duress alarm can be created by entering a valid PIN number with its last digit incremented by 1. If the last digit is 9, a 0 needs to be entered to create a duress alarm. The Duress soft alarm must be enabled for this feature to work. Note that when PIN Plus 1 Duress is enabled, the <**9**> key will *not* create a duress alarm.

Table 4-8: Terminal Screen, Page 2

Field	Type	Description
PIN Suppression Timezone	User Def.	Values range from 0 to 64 (time zone numbers). When the selected time zone is active, PIN codes are not required for valid access. (Timezones are numbered 1 to 64; 0 means no timezone is assigned.)
Log Output Status Message	Toggle	If enabled, will report output “set” or “reset” on the CK721-A Logger Out screen and at the Host.
Facility Code when offline	Toggle	If enabled (**Y**), a person needs only a valid facility code to open a door when the terminal is offline from the panel.
PIN required when offline	Toggle	If enabled (**Y**), a person must have a valid algorithmic PIN code and swipe card to open a door when the terminal is offline from the panel.
Log Reader Strike Message	Toggle	If enabled (**Y**), reader strike locked and unlocked are reported to the CK721-A logger screen and at the server.
Star Feature	Toggle	If enabled (**Y**), allows all features accessible on a 16-key pad (with A, B, C and D keys) to be invoked on a 12-key pad. Press ***** key followed by: 0 Local Override, followed by number of minutes. 1 Enable event, followed by keypad code. 4 Disable event, followed by keypad code. * Clear the keypad buffer. See Appendix D for details.
Access Grant on Door Open Only	Toggle	If enabled (**Y**), will report access granted only if door is opened.
Re-lock on Door Open	Toggle	If enabled (**Y**), this option modifies the Anti-Tailgate feature to lock the strike when the door opens. When the door closes, the shunt time is cancelled. This option requires the Anti-Tailgate Enabled flag to be set to (**Y**), and the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module. This option should not be used with the “Timed Override/Anti-Tailgate” option because “Timed Override/Anti-Tailgate” can only work when the door closes, and not when the door opens (shunting of the door contact is cancelled at the same time as “Timed Override/Anti-Tailgate is cancelled”).

Table 4-8: Terminal Screen, Page 2

Field	Type	Description
Timed Shunt	Toggle	If enabled (**Y**), all Timed Overrides only extend the shunt time. The Access Time is not affected. This option requires the use of RDR2 module, firmware version PS-201E or later, or the RDR2S module. When Timed Shunt is enabled, it is recommended to also set the terminal's Anti-Tailgate Enabled flag to (**Y**), and the panel's Timed Override/Anti-Tailgate flag to (**Y**). This way the door contact will never be shunted when the door is locked and closed.
Override Time	User Def.	If a badge with the Local Override flag set is presented at the reader, the door will be put into timed override. Value range: 0 to 1440 min. A value of 0 turns the feature off. For security reasons, this feature should only be used together with the Timed Shunt option.
Assisted Access	User Def.	If never enabled (**N**), the Access Time will be in effect. If always enabled (**A**), the Assisted Access Time is in effect for all cardholders. To enable Assisted Access Time only for badges with Special Access A flag set, select (**F**). This option requires the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module.
Assisted Access Time	User Def.	Values range from 0 to 120s. The Assisted Shunt Time is automatically set to exceed the configured Shunt Time by the same amount as the Assisted Access Time exceeds the Access Time. This option requires the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module.
ADA Relay Connector	User Def.	The value selected should match the wiring method used. Use (**N**) to disable ADA relay function, (**S**) for wiring to shunt connector and (**G**) for wiring to green light connector in the RDR2. This option requires the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module. For wiring details, see "Shunt Relay Driver Wiring" on page 3-36.

Table 4-8: Terminal Screen, Page 2

Field	Type	Description
ADA Relay Time (0 to 120 s)	User Def.	Time between activation of the Assisted Access and turning the ADA relay off. Value range: from 0 to 120s. This option requires the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module. See the “Assisted Access Timing Diagram” on page 4-38.
ADA Relay Delay (0 to 3000 ms)	User Def.	The delay between activation of the Assisted Access and turning the ADA relay on. Value range: from 0 to 3000 ms, in 100 ms increments. The ADA Relay Delay value must not exceed the ADA Relay Time. Otherwise, the ADA relay will not be activated. This option requires the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module. See the “Assisted Access Timing Diagram” on page 4-38 for further explanation.
Override Reset Level (0-99)	User Def.	This feature can be configured for each reader terminal. Value range: 0 to 99. A value of 0 disables the “Override Reset” feature. A value between 1 and 99 invokes the following behavior: Whenever a terminal's “Security Level” reaches or exceeds the terminal's “Override Reset Threat Level,” all time zone based overrides, host initiated overrides and cardholder overrides are immediately disabled. Subsequent attempts to invoke host initiated overrides or cardholder overrides will be denied. Once a terminal's “Security Level” drops below the terminal's “Override Reset Threat Level,” the time zone based override is restored immediately. Host initiated overrides and cardholder overrides are not automatically restored, but subsequent attempts to invoke host initiated overrides or cardholder overrides will be granted, provided the configuration allows these overrides. The “System Override” feature is not affected by the “Override Reset Threat Level,” and will remain in effect as long as the panel's system override flag is set.

Table 4-8: Terminal Screen, Page 2

Field	Type	Description
Deny If Door Open	Toggle	If enabled (**Y**), this option denies access if door is open.
No Green Light On Aux Access	Toggle	If enabled (**Y**), there is no green light on AUX access. **Note:** Requires S300-DIN-RDR2S firmware revision Q or higher or S300-DIN-RDR2SA.
BQT LCD Reader	Toggle	If enabled (**Y**), then BQT LCD Reader support is enabled. **Note:** Requires S300-DIN-RDR2S with firmware revision Q or higher or S300-DIN-RDR2SA.
Door Open Warning Auto Off	Toggle	If enabled (**Y**), the Door Open Warning Output Group is reset when either: ■ The door is closed ■ Access is granted ■ The door is overridden Therefore, the Door Open Warning will be deactivated when there is no Propped Door Alarm in the immediate future.
Override Warning Auto Off	Toggle	If enabled (**Y**), the Override Warning Output Group is reset when the door closes or when override is extended past the point when the warning should be triggered. Just an access grant alone does not deactivate the Override Warning. This feature is most useful in connection with the Timed Override / Anti-Tailgating option enabled. If not anti-tailgated, it is possible that the Override Warning is deactivated before the override actually expires. If you want to avoid this scenario, disable the “Override Warning Auto Off” option.
D620-ECG Elevator Mode	Toggle	If enabled (**Y**), the low level D620-ECG Elevator Mode is enabled. For a detailed explanation, refer to “D620-ECG Elevator Mode” on page 4-39.

Terminal Screen - Page 3

Page 3 of the Terminal screen is shown followed by Table 4-9, which contains a description of each item. Page 3 allows you to define facility codes.

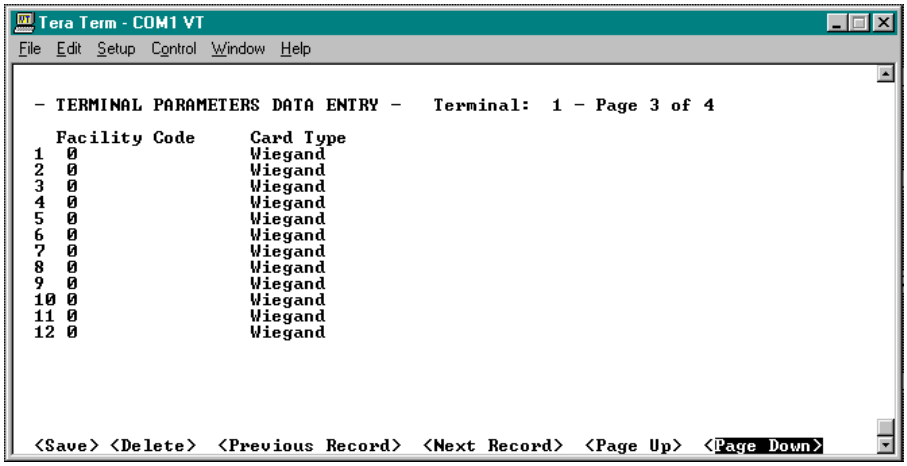


Table 4-9: Terminal Screen, Page 3

Field	Type	Description
Facility Code	User Def.	Enter the facility code for the card type listed to the right. The facility codes must be entered consecutively. When a facility code is 0, the codes that follow are ignored.
Card Type	Toggle	Select between available card types that use facility codes. Each reader terminal connected to a CK721-A can support up to 12 different facility codes.

Terminal Screen - Page 4

Page 4 of the Terminal screen is shown below followed by Table 4-10, which contains a description of each item. Page 4 allows you to configure additional card parameters from the settings contained on Page 3.

Only one type of card may be selected (**Y**), with two exceptions:

In addition to a non-PIN based card type you may select the “PIN + Card ID” flag. This gives people who have forgotten their badge the opportunity to get access by keying in their badge number and their PIN. See “Configuring PIN Codes” on page 4-34.

If you use a two-wire reader with a keypad, you must wire Data 0 and Data 1 wires so that the keypad produces the correct input to the panel. If this configuration causes the badge data to be reported inversely, you can check the “Invert Data” flag to inverse just the badge data, so that the panel can correctly interpret both the keypad data and the badge data.

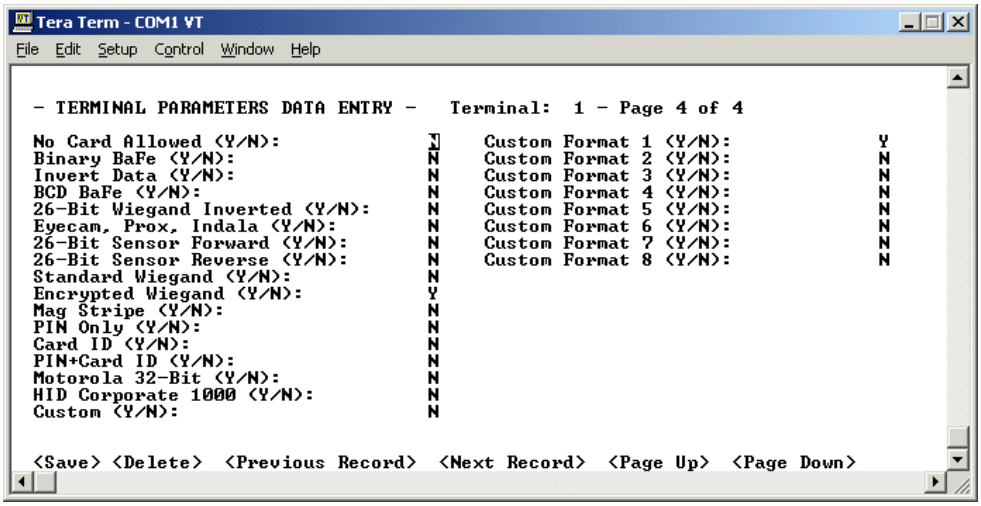


Table 4-10: Terminal Screen, Page 4

Field	Type	Description
No Card Allowed	Toggle	If enabled (**Y**), none of the listed card types will be permitted at this terminal. If you select any card type as enabled, this field automatically switches to disabled (**N**).
Binary BAFE (both parity and no parity)	Toggle	Select (**Y**) to allow this card type.
Invert Data	Toggle	Select (**Y**) to invert the card data reported from the reader.
BCD BAFE (both parity and no parity)	Toggle	Select (**Y**) to allow this card type.
26-Bit Wiegand Inverted	Toggle	Select (**Y**) to allow this card type.
Eyecam, Prox, Indala	Toggle	Select (**Y**) to allow this card type.
26-Bit Sensor Forward	Toggle	Select (**Y**) to allow this card type.
26-Bit Sensor Reverse	Toggle	Select (**Y**) to allow this card type.
Standard Wiegand	Toggle	Select (**Y**) to allow this card type.
Encrypted Wiegand	Toggle	Select (**Y**) to allow this card type.
Mag Stripe	Toggle	Select (**Y**) to allow this card type.
PIN Only	Toggle	Select (**Y**) to allow this mode. See “PIN Only” on page 4-34 for details.

Table 4-10: Terminal Screen, Page 4

Field	Type	Description
Card ID	Toggle	Select (**Y**) to allow the Card ID mode.
PIN+Card ID	Toggle	Select (**Y**) to allow this mode. See “PIN + Card ID” on page 4-35 for details.
Motorola 32-Bit	Toggle	Select (**Y**) to allow this card type.
HID Corporate 1000	Toggle	Select (**Y**) to allow this card type.
Custom	Toggle	Select (**Y**) to allow this card type. This only works if you have a custom version of the panel that supports your custom card format.
Custom Format 1 to 8	Toggle	Select (**Y**) to allow this custom format. Meanings of the custom formats 1 to 8 are assigned at the host.

Configuring PIN Codes

There are three different ways of using PINs to get access at a reader. These ways are called “PIN Only,” “PIN + Card ID,” and “PIN.” In configurations that require presenting a card to request access, it is possible to add the mode “PIN + Card ID” as an alternative for people who have forgotten their card.

PIN Only

In “PIN Only” mode all it takes for the system to identify a person is entering a PIN at a reader. Given a fixed scramble mode, an algorithm produces a unique PIN for every card number between 1 and 32767. When a PIN is entered at the keypad, the algorithm calculates the corresponding card number and the access decision is made based on that card's access rights. This feature works with 5-digit algorithmic PINs only.

For “PIN Only” to work, you need to configure the following parameters:

1. The panel’s **PIN Code Type** (see “Terminal Screen - Page 1” on page 4-24) must be set to **Algorithmic**.
2. The panel’s **5 Digit** option (see “Terminal Screen - Page 1” on page 4-24) should be enabled, although it is ignored in “PIN Only” mode.
3. The panel’s **Scramble Mode** (see “Terminal Screen - Page 1” on page 4-24) must be set to the value used to create the PINs from the card numbers.
4. The terminal’s **PIN Only** card type (see “Terminal Screen - Page 4” on page 4-32) must be selected in. All other card types must not be selected.
5. The terminal’s **Allow PIN after Badge** (see “Terminal Screen - Page 2” on page 4-26*)* has no effect.

6. The terminal's **PIN Suppression** (see "Terminal Screen - Page 2" on page 4-26) has no effect. For obvious reasons you cannot waive the requirement to enter a PIN in "PIN Only" mode.

To use "PIN Only" mode, simply enter your 5-digit algorithmic PIN at the keypad followed by the # key, and the access decision will be made.

PIN + Card ID

In this mode the card does not have to be presented at the reader. The numeric keypad is used to enter the PIN and the card number. This feature works with 4 or 5-digit algorithmic and with 4 or 5-digit custom PINs.

For "PIN + Card ID" to work, you need to configure the following parameters:

1. The terminal's **PIN+Card ID** (see "Terminal Screen - Page 4" on page 4-32) must be selected. All other card types should not be selected, unless you want to use the "PIN + Card ID" mode only as an alternative for people who have forgotten their card, or as an "Air Crew PIN" to grant access to people that do not have a card at all.
2. The terminal's **Allow PIN after Badge** (see "Terminal Screen - Page 2" on page 4-26) has no effect.
3. The terminal's **PIN Suppression** (see "Terminal Screen - Page 2" on page 4-26) has no effect, i.e., you cannot use time zones to waive the requirement to enter a PIN in "PIN + Card ID" mode.

To use "PIN + Card ID" mode, you must enter your PIN followed by your card number followed by the # key. The card number can have up to 16 digits when 5-digit PINs are used. With 4-digit PINs, the card number can have up to 17 digits.

PIN

In this mode the PIN needs to be entered in conjunction with a valid card presented at the reader. This feature works with 4 or 5-digit algorithmic and with 4 or 5-digit custom PINs.

For "PIN" to work, you need to configure the following parameters:

1. Select a card type that matches the reader's technology (see "Terminal Screen, Page 4" on page 4-33).
2. The **PIN plus 1 Duress** option is *not* enabled (see "Terminal Screen - Page 2" on page 4-26).
3. All other card types should not be selected.
4. The terminal's **PIN Only** card type (see "Terminal Screen - Page 3" on page 4-32) must not be selected.
5. The terminal's **PIN + Card ID** card type (see "Terminal Screen - Page 4" on page 4-32) should not be selected, unless you want to use the "PIN + Card ID" mode as an alternative for people who have forgotten their card.
6. The terminal's **PIN Suppression** (see "Terminal Screen - Page 2" on page 4-26) must be set to a defined time zone. PINs are only required to be entered when the time zone is inactive.

To use "PIN" mode when the terminal's **Allow PIN after Badge** option (see "Terminal Screen - Page 2" on page 4-26) is not set, you must key in the entire PIN before presenting the card. The PIN does not need to be terminated with a # key.

To use "PIN" mode when the terminal's **Allow PIN after Badge** option is set, the PIN must be terminated with a # key. You can enter the PIN and the # key before, during, or after the card is presented.

To use "PIN" mode when you also have the **PIN + Card ID** card type selected, as an alternative for people who have forgotten their card, the # key must not be entered before the card is presented.

Four-Digit PINs

A four-digit custom PIN is defined by the first four digits entered in the **PIN Code** section (see "Badge" on page 4-60).

A four-digit algorithmic PIN is defined by the last four digits produced by the PIN algorithm program. Algorithmic codes need to be requested from Technical Support.

PIN Duress

The PIN Duress feature in the Soft Alarm dialog box creates an access grant and a duress alarm only if all of the following conditions apply:

1. The **Duress** soft alarm is defined at the panel (see "Panel Soft Alarm" on page 4-57).
2. The **PIN plus 1 Duress** option is *not* enabled (see "Terminal Screen - Page 2" on page 4-26).
3. The cardholder is required to enter a PIN at the terminal.
4. Exactly one digit of the PIN is replaced by the digit 9.
5. All other digits match the badge's PIN.
6. The card type selected in the terminal's Card Type (see "Terminal Screen - Page 4" on page 4-32) is *not* "PIN Only."

PIN Plus 1 Duress

The PIN Duress feature in the Soft Alarm dialog box creates an access grant and a duress alarm only if all of the following conditions apply:

1. The **Duress** soft alarm is defined at the panel (see "Panel Soft Alarm" on page 4-57).
2. The **PIN plus 1 Duress** option is enabled (see "Terminal Screen - Page 2" on page 4-26).
3. The cardholder is required to enter a PIN at the terminal.
4. Last digit of the PIN is incremented by 1 (if the last digit is 9, enter 0).
5. All other digits match the badge's PIN.
6. The card type selected in the terminal's Card Type (see "Terminal Screen - Page 4" on page 4-32) is *not* "PIN Only."

PIN Retry Alarm

A **PIN Code Retry** alarm is generated when the respective soft alarm is defined at the panel, and three consecutive unsuccessful attempts to enter a PIN were made for the same badge (see “Panel Soft Alarm” on page 4-57). In Local mode, the three consecutive attempts can be made at any terminal of a single panel. In Central mode, the three consecutive attempts can be made at any terminal at any panel.

Assisted Access

NOTE

This feature requires the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module.

This feature allows the door to open for an extended time based on the characteristics of the presented badge. It can also operate an ADA Relay upon presentation of a badge. The Assisted Access Time parameter determines the duration of the access time. The shunt time will automatically be adjusted in the following way: the Assisted Shunt Time is automatically set to exceed the configured Shunt Time by the same amount as the Assisted Access Time exceeds the Access Time.

Assisted Access can be always enabled, never enabled, or enabled only for cards with the “Special Access A” flag.

The access time of elevators is not affected by the Assisted Access feature.

This feature satisfies the requirements for assisted access according to ADA (Americans with Disabilities Act).

ADA Relay

An external ADA Relay can be controlled by an output of the use of the RDR2 module, firmware version PS-201E or later, or the RDR2S module. The activation can be delayed without the use of external additional hardware (unlike when using S300-SIO8s). The delay is necessary to avoid operating a door-opening device before the door is fully unlocked. For detailed information on ADA Relay Time and ADA Relay Delay parameters see page 4-30.

The ADA relay can be wired to the green light or the shunt connector of the RDR2. The ADA Relay Connector should then be set to “Green” or “Shunt,” respectively. The “None” option disables the ADA relay. For wiring details, see “Shunt Relay Driver Wiring” on page 3-36.

When ADA Relay Connector is set to “Shunt”, the shunt connector no longer indicates the shunt time, but the ADA Relay activation.

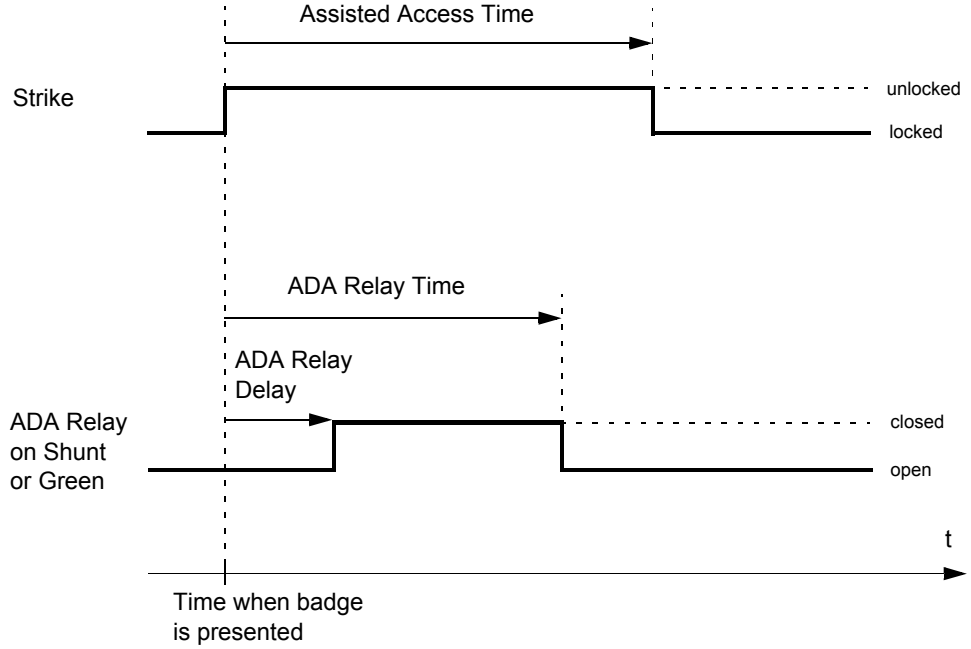


Figure 4-2: Assisted Access Timing Diagram

Elevator Access Control

General Overview

The elevator access control gives you the ability to assign cardholders the access to various elevators and floors in your facility, through their access groups.

Elevator readers cannot be overridden by a Local Cardholder Override or a Timed Override, and do not allow the Auxiliary Access input to grant access to any floors.

Also, panel card events cannot be used on elevator readers.

Low Level Interface

Low level interface elevators have readers associated with a set of output points and an optional set of input points. The field panel works with the elevator manufacturer’s control system using output points to enable car-call buttons, and input points to monitor car-call buttons.

The panel may grant access to a floor by enabling the corresponding car-call button when a badge is presented at a reader installed in the elevator cab.

An elevator cab must be equipped with one reader, and one output point needs to be assigned to every floor button in the cab that needs to be enabled by the security system. For floor tracking, one input point needs to be assigned to every floor button in the cab that is supposed to create a floor tracking message.

There's no prescribed scheme to associate outputs and inputs by their address to the elevator's floor buttons, but the reader and all outputs and inputs for an elevator must be defined on the same panel. The association of elevators, floors, readers, outputs and inputs is done by defining an Elevator in the Cardkey SMS software, and then downloading it into the panel.

When presenting a badge at the elevator cab's reader, the panel searches the badge record for floor access information. This information is then applied to energize the output relays of those floors that the person should have access to. It is the elevator control system's responsibility to ensure the elevator does not go to disabled floors. The enabled floors will be disabled after the elevator access time has expired, unless they are still enabled by public access or by direct output control. All buttons that are exclusively enabled by the elevator access grant will produce floor tracking messages.

D620-ECG Elevator Mode

The Floor Control Inputs (Elevator I/O-8 inputs) are provided with compatible signals from the Elevator Car Controller whenever a button is pushed on a cab. These inputs are "contact closure" or "contact open" and use the Transition Mode.

The Floor Grant Outputs (Elevator I/O-8 outputs) command the Elevator Car to travel to the selected floors. These outputs are momentarily activated (energized) for a grant, simulating an actual finger pushing on a button. Floor Grant Outputs are unavailable for time tasking either by point or group or from Control by Operator, or Event other than for Pulse (no Set, Reset, or Timed On).

Public Access is accomplished by linking floor inputs to floor outputs. This means that if a particular floor becomes "Public," whenever its input is triggered, its output should be momentarily activated (pulsed).

Operation of the Elevator Cab

Upon arrival at a COP (car call button panel in an elevator):

- When a badge holder presses a button assigned to a floor that is in Public Access, the associated Floor Call Output is immediately pulsed. Public Access requests, once granted, are immediately discarded, and not recorded. Public Access requests are never placed in the Floor Call Request queue.
- When a badge holder presses a button assigned to a non-Public Floor, a Floor Call Request is queued. Floor Call Requests is queued for processing for 5 seconds. If another Floor Call Request arrives before badging occurs, it should replace the previously queued request. If a badge is not presented within a 5-second period, any queued floor call request will be discarded.

Upon badging:

- If the floor call request is within the privileges associated with the badge, a momentary grant is issued by pulsing (activating/deactivating) the associated Floor Grant Output. An access granted message (floor number, cab number, badge number, time, and access granted) is then sent up to the host and the green reader indicator is lit momentarily.
- If the floor call request is not within the privileges associated with the badge, an access denied message is sent to the host (floor number, cab number, badge number, time, and invalid floor) and the red indicator is lit momentarily.
- If the time zone for the floor call requested is not within the privileges associated with the badge, an access denied message is sent to the host (floor number, cab number, badge number, time, and invalid time zone) and the red indicator is lit momentarily.
- If the badge is not valid, an access denied message is sent to the host (floor number, cab number, badge number, time, and invalid card) and the red indicator is lit momentarily.
- If there are no floor call requests queued, no further action is taken.

High Level Interface (KONE HLI/KONE ELINK)

The KONE interface is a master slave protocol over RS232 or RS485, according to KONE Elevator EPL HLI Security Protocol specification V=2.3 SO-13.20.10-KAM, with the CK721-A being the master.

Each panel connects to a KONE group controller with up to 8 elevators, with each elevator serving up to 64 floors. Connect the elevator interface to RS232C B (J2) of the CK721-A.

The panel's name has to start with a character between "1" and "8", specifying the KONE group controller's address. An incorrect setting will not permit the integration to be operational. The second character of the panel's name needs to be an "H" if the connection is to run at 9600 baud, otherwise the connection runs at 1200 baud. The 3rd and the 4th character of the panel's name need to be in the range of ASCII characters "01" through "64" with leading zeros. This value specifies the lowest level of the building served by any KONE elevator in this KONE group controller. An incorrect setting will secure and de-secure floors other than those intended.

To define a KONE elevator, the High Level Interface flag has to be checked, and the Protocol field has to be set to 1. The elevator's name has to start with a character between "1" and "8", specifying the KONE elevator address inside the KONE group controller.

To define the floors of a KONE elevator, the public access timezone must be defined, but there should be no output or input points associated with the floor. A floor is on public access when the specified timezone is active. A floor is not on public access when the specified timezone is inactive.

The rest of this integration is identical to the low level elevator interface.

High level Interface (OTIS E.M.S. - Security / B.M.S. Protocol)

The OTIS Elevator Management System (EMS) controls up to 8 groups of elevators, with each group consisting of up to 8 elevators. It interfaces to the Building Management System (BMS) through an RS422 interface. As the current CK721-A controller supports up to 16 readers, multiple CK721-A may need to be connected to control access to all elevators managed by the EMS.

The number of elevators, and their assignment to elevator groups determines the number of CK721-A controllers required. All elevators of each single group must be handled by the same CK721-A. Each CK721-A can support multiple groups, as long as the total number of elevators in these groups does not exceed 16.

One CK721-A needs to be designated the OTIS master. The master panel's COM2 port is connected with a 3 wire full duplex RS232 interface to an RS232 to RS422 converter, which is connected with a 4 wire full duplex RS422 interface to the OTIS EMS.

The recommended module is 485TBLED converter from B & B Electronics or its equivalent.

For this model both the CONTROL and the ECHO jumpers need to be completely removed to act as an RS232 to RS422 converter.

The 485TBLED is connected to the CK721-A master with a 3 wire interface, consisting of pins 2, 3 and 7. If using the adapter that is used to communicated with the CK721-A's COM1 port, wires 2 and 3 need to be crossed.

The 485TBLED is connected to the OTIS EMS with a 4 wire interface:

- OTIS EMS's TDA(-) to Converter's RDA(-)
- OTIS EMS's TDB(+) to Converter's RDB(+)
- OTIS EMS's RDA(-) to Converter's TDA(-)
- OTIS EMS's RDB(+-) to Converter's TDB(+)

Proper shielding and grounding may be required.

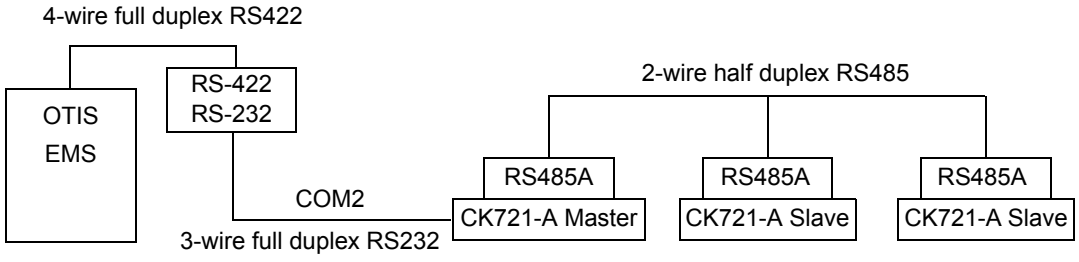


Figure 4-3: Master-Slave Elevator Configuration Layout

Panel Configuration

Panel Name

Each CK721-A that takes part in the OTIS integration must follow a certain naming pattern. Enter each character of the CK721-A panel name as described in the tables below. Only characters 2, 3, and 4 must be entered as specified. Characters 5, 6, 7, and 8 may be non numeric if default values are to be used.

1st character: **Master & Slave**. This character can be freely chosen, but "(" is recommended.

2nd character: **Master**. Defines the presence of groups 5 through 8 in the OTIS EMS. Slave: Must be 0. Any invalid character is likely to leave the OTIS integration not operational.

Defined groups	None	5	6	5,6	7	5,7	6,7	5,6,7	8	5,8	6,8	5,6,8	7,8	5,7,8	6,7,8	5,6,7,8
2nd character	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

3rd character: **Master**.This character defines the presence of groups 1 through 4 in the OTIS EMS. Slave: Must be 0. Any invalid character is likely to leave the OTIS integration not operational.

Defined groups	None	1	2	1,2	3	1,3	2,3	1,2,3	4	1,4	2,4	1,2,4	3,4	1,3,4	2,3,4	1,2,3,4
3rd character	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

4th character: **Master & Slave**. This character defines the maximum number of landings of any elevator in the OTIS EMS. Any invalid character is likely to leave the OTIS integration not operational.

Maximum number of landings	None	1-8	9-16	17-24	25-32	33-40	41-48	49-56	57-64	65-72
4th character	0	1	2	3	4	5	6	7	8	9

5th character: **Master**. This character defines the timeout of the OTIS system. A higher value gives the OTIS equipment more time to respond. Any invalid character uses the default timeout of 200 ms.
Master & Slave: Defines the RS485 bus turnaround delay. Any invalid character uses the default delay of 10 ms.

OTIS timeout [ms] (Master only)	100	200	300	400	500	600	700	800	900
RS485 turnaround delay [ms]	5	10	15	20	5	10	15	20	5
5th character	1	2	3	4	5	6	7	8	9

6th character: **Master**.This character defines the poll delay that prevents the OTIS equipment from being overloaded. A lower value speeds up the integration. A higher value slows down the integration. Any invalid character uses the default poll delay of 400 ms. **Slave**: Not used

Poll delay [ms]	0	100	200	300	400	500	600	700	800	900
6th character	0	1	2	3	4	5	6	7	8	9

7th character: **Master**. This character defines the how many times a message is retried before OTIS is declared offline. Any invalid character uses the default number of 3 retries. **Slave**: Not used

Number of retries	0	1	2	3	4	5	6	7	8	9
7th character	0	1	2	3	4	5	6	7	8	9

8th character: **Master & Slave**. This character defines the priority of the OTIS integration within a CK721-A controller. This setting should not be changed unless after consultation with Technical Support. Any invalid character uses the default priority of 19.

Priority	10	11	12	13	14	15	16	17	18	19
8th character	0	1	2	3	N/A	N/A	N/A	N/A	N/A	N/A

All subsequent characters can be freely chosen.

Example 1:

"(9D5) Controller XYZ" defines a master panel that uses a 200 ms OTIS timeout, a 400 ms poll delay, and 3 retries. The OTIS integration uses groups 1, 3, 4, 5 and 8, and the elevator with the most landings has between 33 and 40 landings. No change to the priority was made.

Example 2:

"(9D5128) Controller XYZ" defines a master panel that uses a 100 ms OTIS timeout, a 200 ms poll delay, and 8 retries. The OTIS integration uses groups 1, 3, 4, 5 and 8, and the elevator with the most landings has between 33 and 40 landings. No change to the priority was made. This OTIS integration runs faster than the one in example 1, but it exceeds OTIS's recommendation for the maximum rate of polling.

Elevator

In the P2000 user interface, select the protocol type for the panel. Refer to the *P2000 Software User Manual* for detailed information.

Elevator Configuration

Protocol

In the P2000 user interface, select the protocol type for the elevator. Refer to the *P2000 Software User Manual* for detailed information.

Elevator Name

Each elevator that takes part in the OTIS integration must follow a certain naming pattern. Enter each character of the elevator name as described below:

1st character: Group Number (1 - 8)

2nd character: Elevator Car Number (1 - 8)

3rd character: Can be freely chosen, but "-" is recommended.

4th and 5th characters: Fire floor number. The fire floor will never be secured by the OTIS integration. Leading zeros must be entered. The fire floor functionality can also be achieved by assigning the floor to a timezone that is always enabled. In this case, the 4th and 5th characters can be freely chosen, as long as they are not characters in the range of "0" through "9."

Floor Tracking

The OTIS EMS reports landing numbers that were selected after a card was used to de-secure floors. When the floor tracking option is enabled, the CK721-A creates a floor tracking message for each landing number that is reported by the OTIS EMS. The CK721-A associates the reported landing number with the last person that was granted access at the elevator.

Timed Button

The OTIS EMS may report landing numbers that were selected after a card was used to de-secure floors with a significant delay. Therefore, the CK721-A should not take any actions to re-secure those floors, as this may interfere with subsequent access requests. This implies that the Timed Button flag should always be checked. The CK721-A then re-secures the floors after the configured elevator access time has elapsed, or when a new access request is processed that de-secures different floors.

If the Timed Button flag is unchecked, the CK721-A re-secures the elevator as soon as it receives a reported landing number.

Download

When downloading elevators to a panel running the OTIS integration, make sure the "Delete Elevators From Panel Before Download" check box is unchecked, as otherwise, the temporary deletion of the elevators would temporarily disrupt communication with the OTIS EMS.

Basic Definitions

Outputs (low level interface only) – The elevator cab's floor buttons will only register being pressed when they are enabled by CK721-A outputs. The CK721-A offers one output for each elevator cab's floor button to determine whether or not that button is enabled or disabled. The outputs offer both the normally open or normally closed wiring options. The CK721-A elevator interface operates in Fail Secure mode. The Enabled state is represented by an energized output relay, the Disabled state by a de-energized output relay. The CK721-A elevator interface does not support Fail Safe mode.

Inputs (low level interface only) – Each elevator cab's floor buttons may be wired to an input to allow the CK721-A to create floor tracking messages. A pressed button needs to close the input, a button that is not pressed needs leave the input open. The CK721-A elevator interface does not support normally closed buttons.

Valid Badge – A valid badge in this context is defined as a badge that is accepted by the elevator's reader with a green light. The specific rights of this badge are dependent on the badge's access groups' floor masks, so it may be possible that a valid badge gives no access to any of the elevator's floors.

Elevator Access Grant – The valid badge's access groups' floor masks determine which of the elevator cab's call buttons are enabled by an elevator access grant. Relinquishing an elevator access grant does not disable an elevator button that is enabled by public access or by direct output control.

Public Access – Each elevator cab's floor button may be enabled by an active timezone associated with that floor in the CK721-A's elevator configuration. Relinquishing public access does not disable an elevator button that is enabled by an elevator access grant or by direct output control.

Direct Output Control (low level interface only) – Each elevator cab's floor buttons may be enabled by direct output control from the server's or the panel's user interface. Relinquishing direct output control does not disable an elevator button that is enabled by an elevator access grant or by public access.

Access Time – At the time a valid badge is presented to the elevator reader, the elevator access time starts. The elevator access time starts over with every subsequent presentation of a valid badge. At the beginning of the elevator access time certain floor buttons are enabled by CK721-A outputs per elevator access grant. Subsequent presentation of a valid badge disables the previous access grant. Only outputs exclusively enabled by elevator access grants will be disabled at the end of the elevator access time.

Access Grant Message – When a valid badge is presented, the panel sends an elevator access grant message to the server, that includes the badge's number and cardholder name.

Floor Tracking Message – Floor tracking messages, when the floor tracking option is selected, are generated only for floors whose associated output is exclusively enabled by the elevator access grant, i.e., it is not co-enabled by public access or by direct output control. A floor tracking message is generated for each elevator input that:

- Experiences a transition from the open into the closed state during the elevator access time.
- Is in the closed state at the time a valid badge is presented.

The floor tracking messages includes the badge's number and badge holder name of the last person to present a valid badge at the reader, and the floor name of the pressed button.

Override – When the reader terminal in the elevator cab is overridden, all of the associated outputs relays are energized by the public access feature. This means, that there will be no floor tracking messages generated. Except for local cardholder override, all modes of reader override are applicable to elevator terminals, i.e. override per timezone, per panel system override and per the "Unlock All Doors" command from the server.

Executive Privilege – Badges with executive privilege enable all floors of the elevator per elevator access grant.

Performance Considerations

The more readers and input/output terminals are installed at a single CK721-A, the longer the system response time gets. Also, care has to be taken not to exceed the power supplies' capabilities when all output relays are energized at once. The theoretical limit per CK721-A is set to 16 elevators with 128 elevator buttons combined. The practical limits are determined by the desired response times.

Cabinet Access Control

Cabinets are readers associated with a set of output points and an optional set of input points. The field panel interfaces with a bank of cabinets using output points to unlock cabinet doors, and input points to monitor the status of cabinet doors.

The panel may grant access to a cabinet by unlocking the corresponding door when a badge is presented at a reader installed in the cabinet definition.

The cabinet access control gives you the ability to assign cardholders the access to various cabinets and doors in your facility, through their access groups.

Cabinets are assigned doors and door groups, then these doors and door groups are included in access groups which are assigned to cardholders.

Cabinet readers cannot be overridden by a Local Cardholder Override or a Timed Override, and do not allow the Auxiliary Access input to grant access to any doors.

Also, panel card events cannot be used on cabinet readers.

Elevator or Cabinet Terminal

To display an elevator's or cabinet's configuration, select the terminal assigned to the elevator or cabinet by number or select **<Previous Record>** or **<Next Record>**. The following screens are then added to the base four screens used to display a terminal.

Elevator or Cabinet Terminal Screen - Page 5

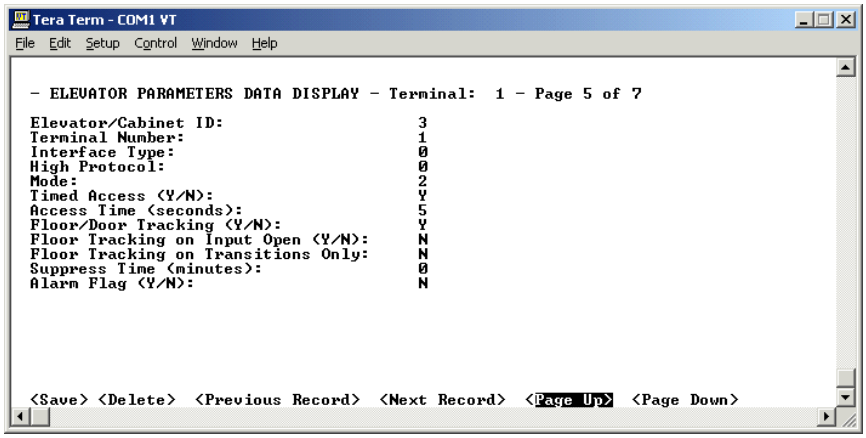


Table 4-11: Elevator or Cabinet Terminal Screen, Page 5

Field	Type	Description
Elevator/ Cabinet ID	User Def.	A numeric value that identifies the elevator or cabinet to the system. This value is assigned by the server and cannot be edited by the user.
Terminal Number	User Def.	A read-only field that identifies the terminal associated with this elevator or cabinet.
Interface Type	User Def.	A read-only field that identifies the type of elevator or cabinet control in use: 0 = low level interface 1 = high level interface (RS232) The only high level interface supported at this time is the KONE PLC-HLI/KONE ELINK interface.
High Protocol	User Def.	A read-only field that identifies the high level (RS232) protocol in use. 0 = low level interface 1 = KONE HLI/KONE ELINK The only high level interface supported at this time is the KONE PLC-HLI/KONE ELINK interface.

Table 4-11: Elevator or Cabinet Terminal Screen, Page 5

Field	Type	Description
Mode	User Def.	A read-only field that identifies the mode of operation of the elevator or cabinet: 0 = elevator, output points only 2 = elevator, input and output points 4 = cabinet, output points only 5 = cabinet, input points only 6 = cabinet, input and output points
Timed Access	Toggle	A read-only field that identifies how the access control logic reacts when an enabled input point is received: Y = enable output points for specific access time N = enable output points until input received
Access Time	User Def.	A read-only field that identifies the maximum time, in seconds, that the output points are enabled due to an access grant.
Floor/Door Tracking	Toggle	A read-only field that identifies whether the access control logic sends access granted messages to the server for each enabled input point. For a comprehensive table on setting flags for floor tracking messages, see page 4-49.
Floor Tracking on Input Open	Toggle	A read-only field that identifies when floor tracking messages should be generated. Y = generate floor tracking messages when the floor's input is open. N = generate floor tracking messages when the floor's input is closed. This setting applies only to elevators that use input points for floor tracking, and only when the Floor/Door Tracking field is set to (**Y**). For a comprehensive table on setting flags for floor tracking messages, see page 4-49.

Table 4-11: Elevator or Cabinet Terminal Screen, Page 5

Field	Type	Description
Floor Tracking on Transitions Only	Toggle	A read-only field that identifies whether floor tracking messages should not be generated when an input point is already in the off-normal state* when a badge is presented. Y = a floor tracking message is generated only on an input's transition from the normal to off-normal state. N = a floor tracking message is generated on an input's transition from the normal to off-normal state and on any presentation of a valid badge while the input is in the off-normal state. This setting applies only to elevators that use input points for floor tracking, and only when the Floor/Door Tracking field is set to (**Y**). * As determined by Floor Tracking on Input Open setting. For a comprehensive table on setting flags for floor tracking messages, see page 4-49.
Suppress Time	User Def.	A read-only field that identifies the length of time, in minutes, that an alarm is suppressed after access is granted for a door.
Alarm Flag	Toggle	A read-only field that identifies whether input points will generate alarms when they are associated with a cabinet.

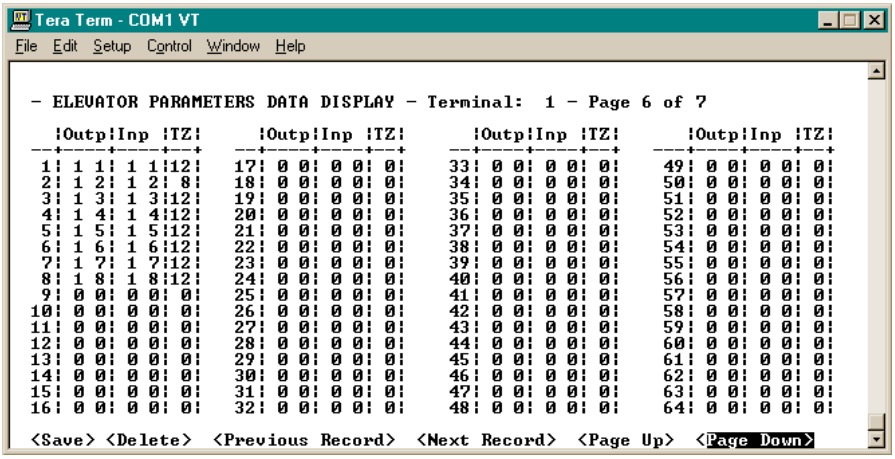
Table 4-12: Setting Flags for Generating Floor Tracking Messages

Generate floor tracking messages on input point:	Flags:		
	Floor/Door Tracking	Floor Tracking on Input Open	Floor Tracking on Transitions Only
Closed[1]	Y	N	N
Open[2]	Y	Y	N
Closing[1]	Y	N	Y
Opening[2]	Y	Y	Y
Do not generate floor tracking messages.	N	N/A	N/A

[1] Input point wired to "normally open."

[2] Input point wired to "normally closed."

Elevator or Cabinet Terminal Screen - Page 6



Elevator or Cabinet Terminal Screen - Page 7

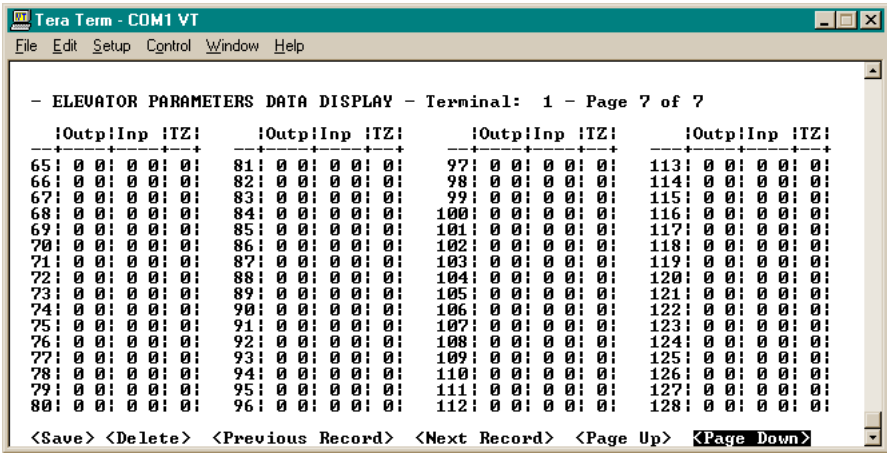


Table 4-13: Elevator or Cabinet Terminal Screen, Pages 6 and 7

Field	Type	Description
Floor Index	User Def.	A numeric value that identifies a floor's location in the array of 128 possible floors.
Outp	User Def.	A read-only field that identifies the output point associated with a floor or door. A value of 0 0 indicates no output point is assigned. If an output point is assigned, it is identified by terminal number and point number.

Table 4-13: Elevator or Cabinet Terminal Screen, Pages 6 and 7

Field	Type	Description
Inp	User Def.	A read-only field that identifies the input point associated with a floor or door. A value of 0 0 indicates no input point assigned. If an input point is assigned, it is identified by terminal number and point number.
TZ	User Def.	A read-only field that identifies the timezone associated with a floor or door. A value of 0 indicates no timezone is assigned.

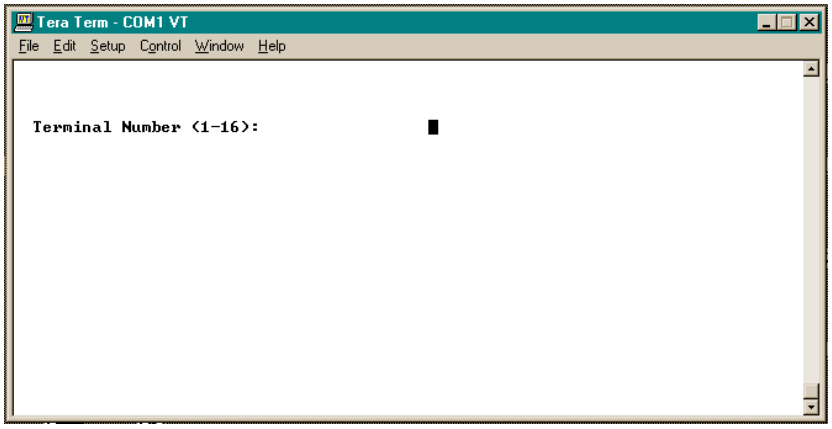
NOTE

The elevator or cabinet configuration cannot be edited from these screens. These values are set using the P2000 system configuration screens.

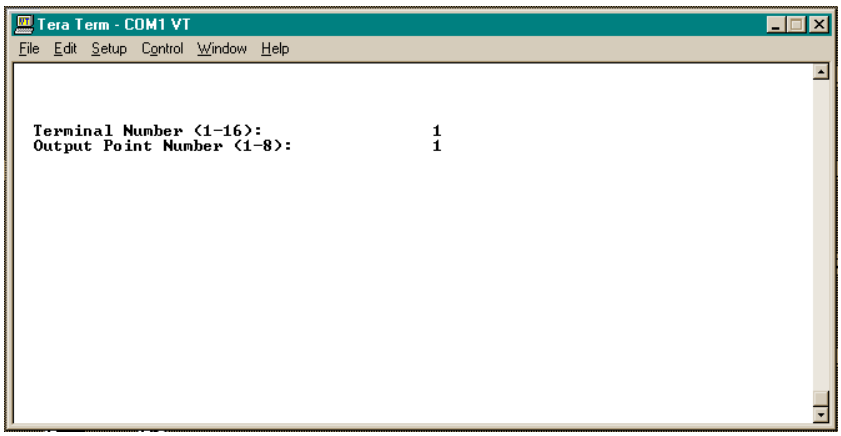
Output

The Output screen is used to enable output points and assign individual points to groups. To begin, select **Output** from the CK721-A Main menu.

You will be prompted to select a previously saved terminal.



After selecting a terminal, select an output point number. If the output you select already exists, the system places you into edit mode. If the output record does not exist, the CK721-A assumes you want to create a new record. Any output records you have defined will appear listed here.



The output record definition screen appears as shown here. Each item is described in Table 4-14.

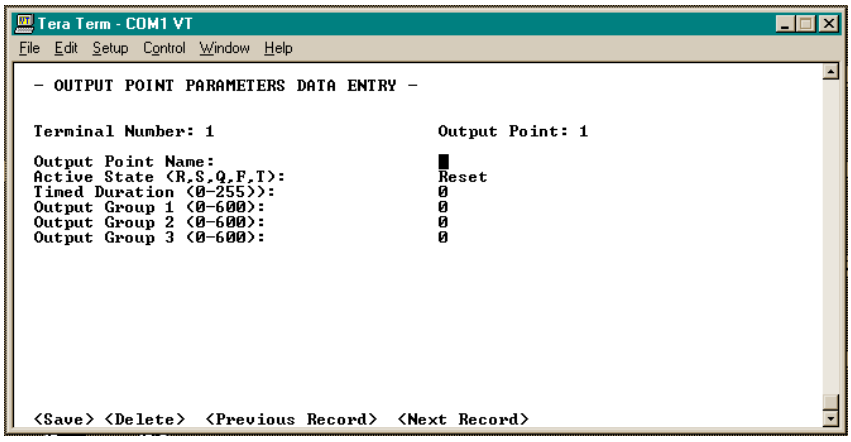


Table 4-14: Output Screen, 1 Page Only

Field	Type	Description
Output Point Name	User Def.	Enter up to 25 alphanumeric characters for a descriptive output point name.
Active State	Toggle	Choices are: R (Reset) S (Set) Q (Quick Flash) F (Slow Flash) T (Timed)
Timed Duration	User Def.	Values are between 0 and 255 seconds. If the active state is set as timed, this value represents the duration for which the point will be set.

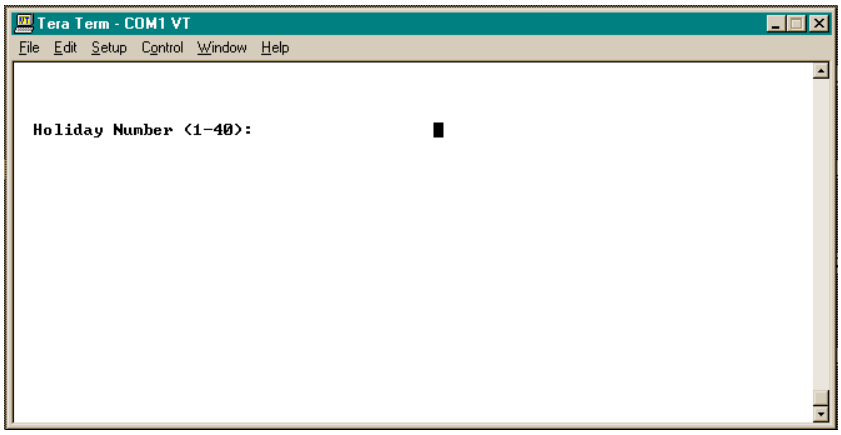
Table 4-14: Output Screen, 1 Page Only

Field	Type	Description
Override Warning Output Group (1 - 3)	User Def.	Value ranges between 0 and 600 (0 means no group is assigned). Each individual output point may belong to up to three groups, with a total of 600 available for the CK721-A. To form a group only requires that you assign one or more output points to a single group number.

Holiday

During normal system operation, Holidays can replace a standard time zone. At approximately one minute before midnight, the Cardkey SMS (and CK721-A) verify that the following day is a holiday. If so, the appropriate time zone is substituted.

To define holidays, select **Holiday** from the CK721-A Main menu. You will be prompted for a holiday number. If the record exists, it can be edited. If the holiday number does not already exist, it is considered a new record.



The Holiday screen is shown and Table 4-15 describes each field.

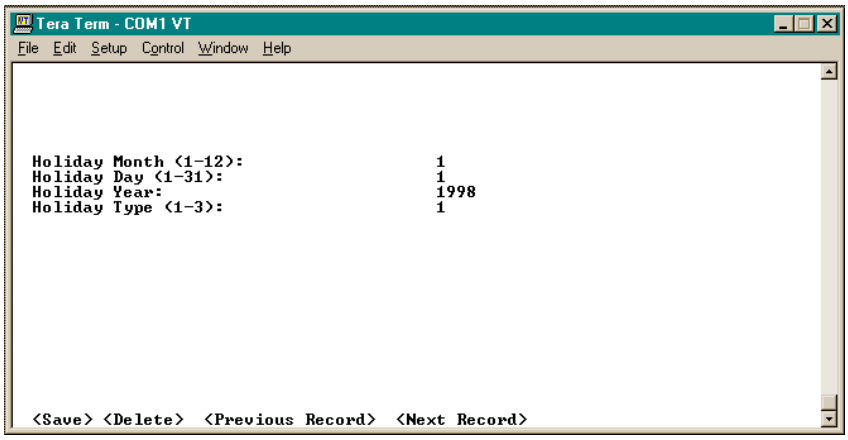


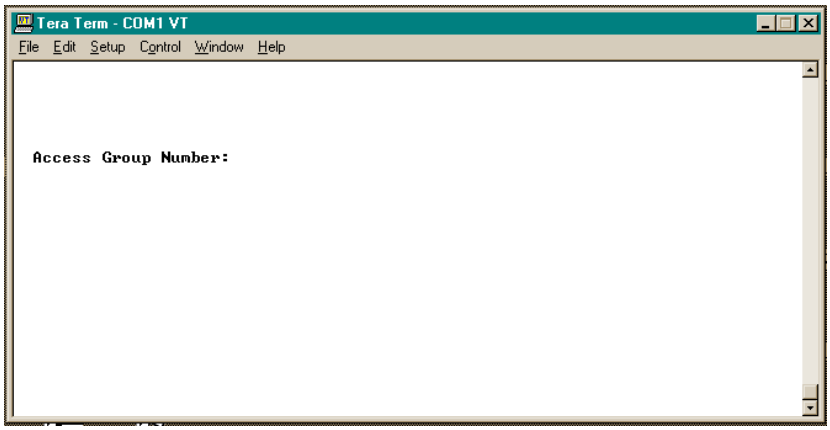
Table 4-15: Holiday Screen, 1 Page Only

Field	Type	Description
Holiday Month	User Def.	Enter a value where 1 equals January and 12 is December.
Holiday Day	User Def.	Enter day of the holiday between 1 and 31.
Holiday Year	User Def.	Type in the appropriate year.
Holiday Type	User Def.	Type in 1, 2, or 3 for a holiday type. The type is then defined as part of a time zone, described later in this chapter and in more depth in the *P2000 Software User Manual*.

Access Group

Reader terminals with like access patterns can be formed into Access Groups. Reader terminals are assigned to Access Groups as **Y** (yes), meaning that when enabled, all badges assigned to this group have access privileges (based also on time zone checking, facility code, and so forth), at the particular reader (s).

To enable or disable particular reader terminals in an Access Group, select **Access Group** from the CK721-A Main menu. You can add an access group number as 1 or greater, or select a previously defined group to edit.



When you add or edit an access group, a list of previously defined terminals will appear.

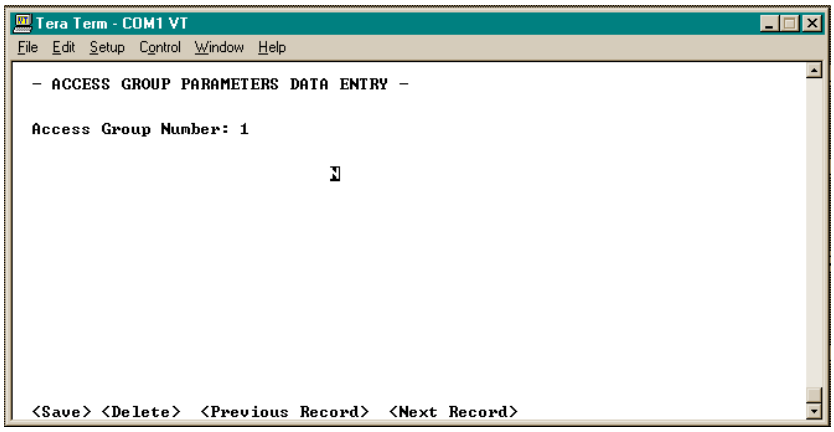


Table 4-16: Access Group Screen, 1 Page Only

Field	Type	Description
Terminal Name	Toggle	Select (**Y**) to enable a terminal for this access group. Select (**N**) to disable a terminal for this group.

Elevator Access Group

To display an access group that includes elevator access, select the group by number or select **<Previous Record>** or **<Next Record>**. The following screen is displayed.

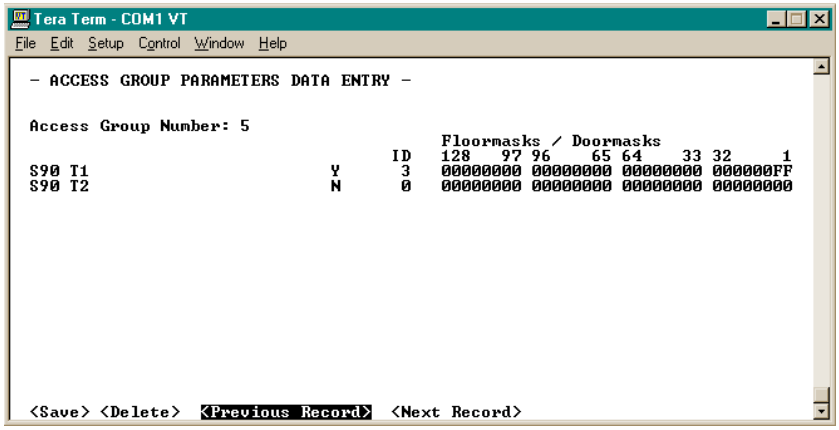


Table 4-17: Elevator Access Group Screen, 1 Page Only

Field	Type	Description
Terminal Name	Toggle	Select (**Y**) to enable a terminal for this access group. Select (**N**) to disable a terminal for this access group.
ID	User Def.	A read-only field that identifies the elevator or cabinet associated with the terminal and floormask or doormask on this line.
Floormasks/ Doormasks	User Def.	A read-only field that identifies the floors/doors enabled for the elevator on this line. The individual floors/doors are bits in an array from 1 to 128. These bits are represented as hexadecimal digits.

NOTE

The Elevator ID and Floormasks/Doormasks cannot be edited from this screen. These values are set using the P2000 system configuration screens.

Door Control

Door Control allows you to manually lock or unlock a door immediately or for a specified period of time. Select **Door Control** from the CK721-A Main menu.

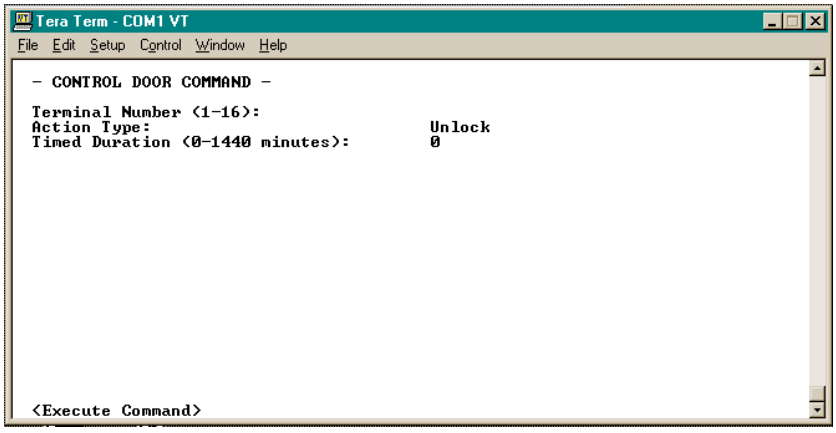


Table 4-18: Control Door Screen, 1 Page Only

Field	Type	Description
Terminal Number	User Def.	Enter the reader terminal to manipulate.
Action Type	Toggle	Choices are: Unlock Lock Timed **Note**: Unlock will unlock the door for a period of time equal to the Access Time defined in the terminal parameters screen for the selected terminal.
Timed Duration	User Def.	Values range from 0 to 1440 minutes. When you set the Action Type as Timed, this value provides the duration. For example, if a door is set timed for 10 minutes, it would remain unlocked for 10 minutes.

Panel Soft Alarm

The term “soft alarm” refers to an alarm condition triggered through a system transaction, rather than a hard-wired alarm input point.

NOTE

Soft Alarm points are preprogrammed in the system. Although you do have access to these points from this screen, they should not be changed. Reporting problems will occur.

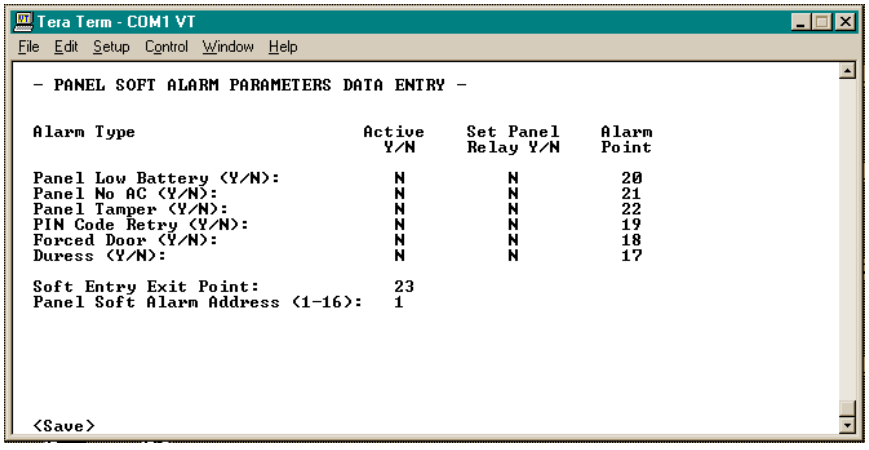


Table 4-19: Panel Soft Alarm, 1 Page Only

Field	Type	Description
Panel Tamper (22)	Toggle	The enclosure has been opened or closed. If enabled (**Y**), this type of soft alarm will be reported on the specified point. Enable Set Panel Relay (**Y**) to activate the CK721-A's alarm relay.
PIN Code Retry (19)	Toggle	The set number of PIN retry attempts (3) has been exceeded. If enabled (**Y**), this type of soft alarm will be reported on the specified point. Enable Set Panel Relay (**Y**) to activate the CK721-A's alarm relay. In this case the panel's Alarm Latch Output flag should be set (**Y**).
Forced Door (18)	Toggle	A reader-controlled door is open without an access request. If enabled (**Y**), this type of soft alarm will be reported on the specified point. Enable Set Panel Relay (**Y**) to activate the CK721-A's alarm relay. Forced Door must be enabled.
Door Held Open (soft alarm 24)	Function Only	This element does not appear in this screen, but corresponds to soft alarm 24, which is set up from the Input screen. "Forced Door" (which does appear on this screen) must be enabled for soft alarm 24 to work.
Duress (17)	Toggle	Either a 9 is substituted in a valid cardholder's PIN, or a badge is swiped in reverse, if enabled as described earlier. If enabled (**Y**), this type of soft alarm will be reported on the specified point. Enable Set Panel Relay (**Y**) to activate the CK721-A's alarm relay. In this case the panel's Alarm Latch Output flag should be set (**Y**).
Soft Entry Exit Point (23)	User Def.	The alarm point that reports soft In-X-It violations.
Panel Soft Alarm Address (1-16)	User Def.	The actual terminal number associated with the soft alarms (for *panel* soft alarms).

Password Change

Use this option to change the login password for the CK721-A. Select **Password Change** from the CK721-A Main menu.

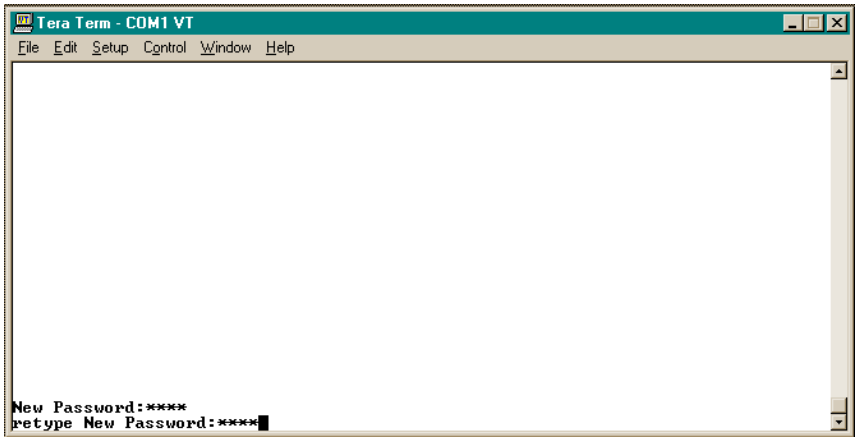
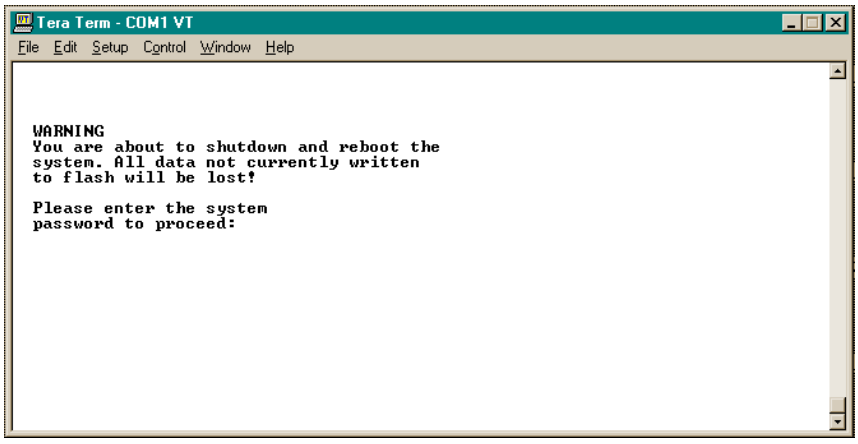


Table 4-20: Password Change, 1 Page Only

Field	Type	Description
Enter New Password	User Def.	Type in the new password, limited to 9 alphanumeric characters. Remember that your password is case-sensitive.
Retype New Password	User Def.	Re-enter the password for confirmation.

Reboot

To reboot the CK721-A panel, select **Reboot System** from the Main menu. The following screen is displayed.



Type the system password and press <**Enter**>; the CK721-A will reboot.

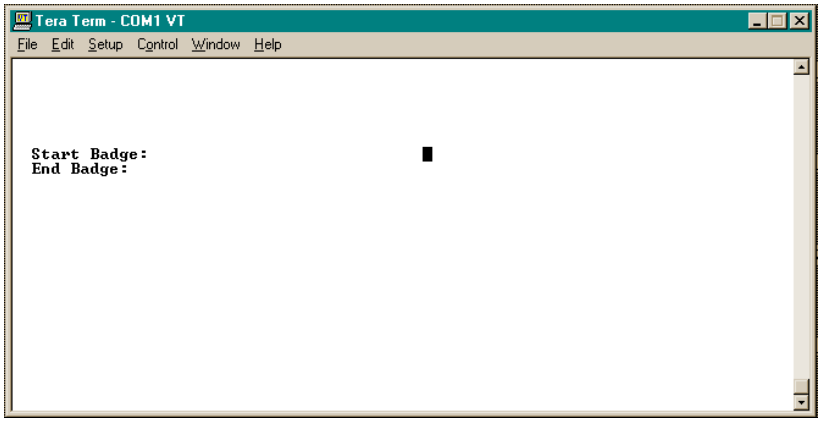
NOTE

If you are connected to the CK721-A panel via the serial port, the boot up messages will be displayed. The reboot process is complete when the Login prompt appears. If you are connected to the CK721-A panel via telnet, the connection will be lost. You must wait until the reboot process is complete before a new telnet connection can be established.

Badge

Cardholder badge records can be entered into the system individually or in batches. In the latter case, every badge in the batch must have the same definition. For testing purposes, you will normally only create individual badge records.

To create a badge, select the option from the CK721-A Main menu. If you have previously created badge records, you can select the one you want to edit. In this case leave the End Badge field blank and press <**Enter**>. If you enter a new badge number, the system assumes you are creating a new record.



The Badge screen is shown below and each field is defined in Table 4-21.

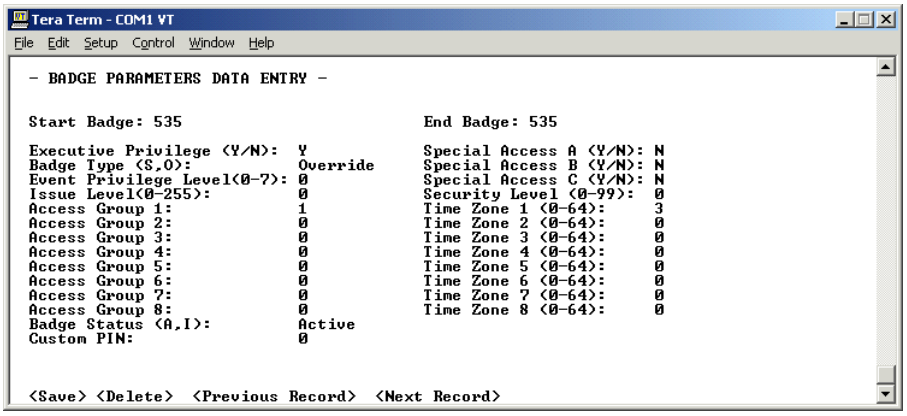


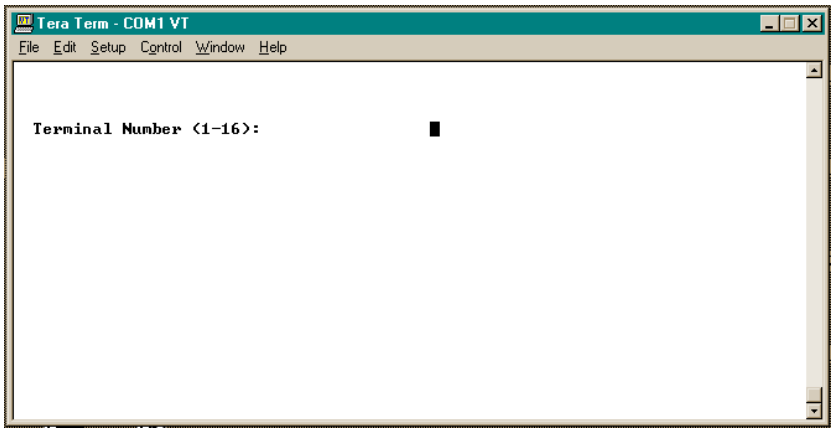
Table 4-21: Badge Screen, 1 Page Only

Field	Type	Description
Executive Privilege	Toggle	If enabled (**Y**), the cardholder has unlimited access to all controlled doors.
Badge Type	Toggle	Choices are Standard and Override. Override allows the cardholder to bypass normal access through keypad override.
Event Privilege Level	User Def.	Values range from 0 to 7, with 7 as the highest event privilege. When events are created, they are assigned a privilege level. A cardholder may execute an event that is equal to or less than their privilege level.
Issue Level	User Def.	Values range from 0 to 255. An initial issue is 0. Issue levels can be increased for lost or stolen badges when you want to retain the same badge number.
Access Group (1-8)	User Def.	A single badge can be assigned up to eight access groups.
Badge Status	Toggle	A badge can either be A(ctive) or I(nactive).
Custom PIN	User Def.	If using custom, rather than algorithmic PINs, enter the four or five digit code for the badge. (Do not assign a 9 as a digit in the PIN#.)
Special Access (A, B, C)	User Def.	The Special Access flag can be set to (**A**), (**B)** or (**C)**. See “Assisted Access” on page 4-37 for details. This feature requires the Assisted Access feature to be set to (**F**) at the terminal screen.
Security Level	User Def.	Value range: 0 to 99. The Security Level for a badge must be equal to or greater than the Security Level set up at the terminal and the panel. If the Security Level at the terminal and/or panel is raised to exceed the badge’s Security Level, such as in case of an emergency, a cardholder will be denied access unless the badge has the Executive Privilege enabled. For this feature to work Security Level must be assigned to the system, the terminals and the badges.
Time Zone (1-8)	User Def.	A single badge can be assigned up to eight time zones.

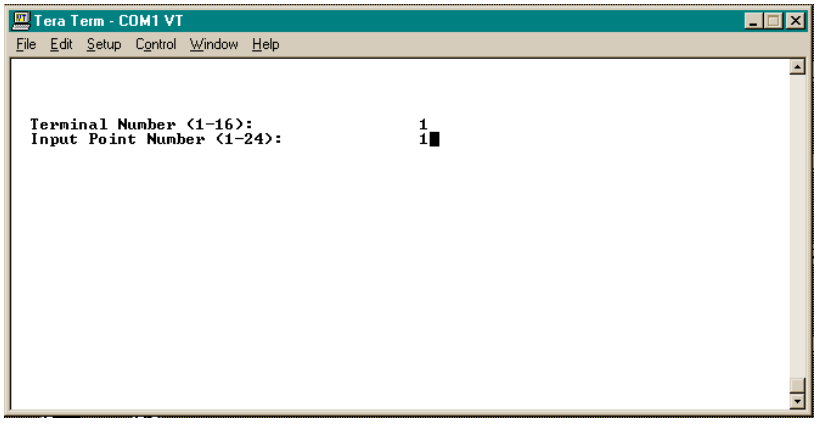
Input

The Input screen is designed to let you define inputs on any type of terminal, that is, it will allow you to define any number of input points. It is, however, up to you to know the input point capability for the terminal being programmed. For example, the input screen will let you define input point #9; however, if the terminal you are programming is an IO8, defining input point #9 will be invalid because inputs 9 through 16 do not exist on an IO8 terminal. To cite another example, on a Reader only terminal, you can program a soft alarm using its assigned number. All other numbers will be invalid.

To begin, select **Input** from the CK721-A Main menu, and then select a previously defined terminal from the displayed list.



After selecting a terminal, type in an input point number to define. If the point has already been defined, the record is displayed for editing. If the point has not been defined, it will be a new record.



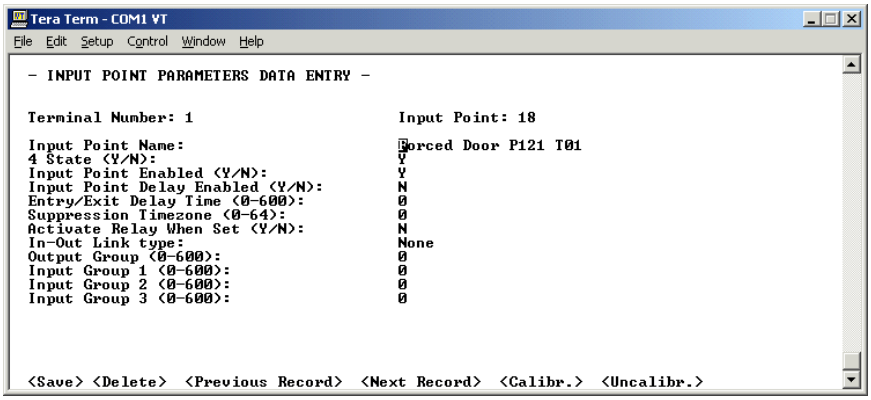


Table 4-22: Input Screen, 1 Page Only

Field	Type	Description
Input Point Name	User Def.	Type in a descriptive name, up to 25 alphanumeric characters long.
4 State	Toggle	If **Y**, the input is 4-state. **N** indicates the input is 2-state.
Input Point Enabled	Toggle	The input can be activated, meaning: able to report an alarm condition.
Input Point Delay Enabled	Toggle	If enabled (**Y**), alarm reporting is delayed for the number of seconds specified.
Entry/Exit Delay (0-600)	User Def.	Enter a time in seconds that an alarm report to the server will be delayed after a door is opened. This represents the time you allow a cardholder to enter the door and type a suppression event code into a keypad. If they do not key in the code within the set Entry/Exit Delay time, an alarm report will go to the server, even if the door is closed.
Suppression Timezone	User Def.	Values range between 0 and 64 time zones. When the selected time zone is active, the input point is suppressed (will not report an alarm condition).
Activate Relay When Set	Toggle	When an input point goes into alarm, it can trigger the CK721-A panel output relay. Enable this option by selecting (**Y**). **Note:** Changes to the Panel Output Relay setup (includes Output Latching and Alarm Relay Linking settings) require a write of the database to flash before the updated Panel Output Relay settings take effect.

Table 4-22: Input Screen, 1 Page Only

Field	Type	Description
In-Out Link Type	Toggle	You can choose an input point to link to an output group. Select the appropriate type of linkage from the following choices: **None** Default selection, indicating that there is no linkage between the input point and output group. **Active-on** When the input point is activated, the output group activates. **Secure-on** When the input point is secure, the output group activates. **Track** When the input point is activated, the output group activates. When the input point is secure, open, or short, the output group deactivates. **Mimic** When the input point is activated, open, or short, the output group activates. When the input point is secure, the output group deactivates. **Active-off** When the input point is activated, the output group deactivates. **Secure-off** When the input point is secure, the output group deactivates. **Reverse track** When the input point is activated, the output group deactivates. When the input point is secure, open, or short, the output group activates.
Output Group	User Def.	Type an output group number for I/O linking.
Input Group (1-3)	User Def.	To form input points into groups, assign the point to a group number. A group is formed when one or more individual input points are assigned the same group number. Each individual input point can be assigned up to three input groups (0 indicates the point is not assigned to a group).

Time Zone

Time zones define all the periods during which a reader, a card, an alarm point, or another system feature is active or inactive. A time zone is a set of enable and disable times which are applied to days of the week and holidays.

The period between an enabled and disabled time may be thought of as a time block. With four enabled and four disabled times (including midnight), you can configure up to eight time blocks per day (enable and disable). The principle of using multiple time blocks during a 24-hour period is shown in Figure 4-4.

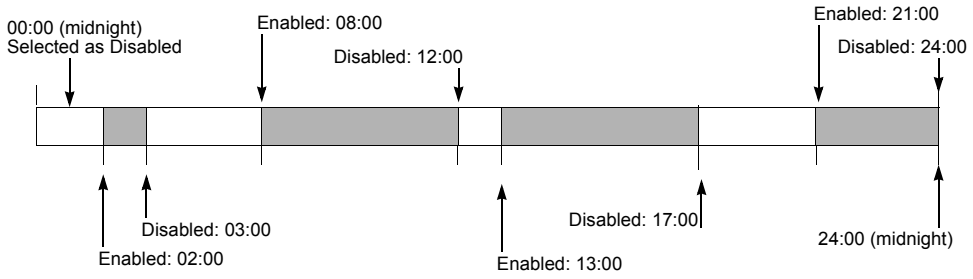
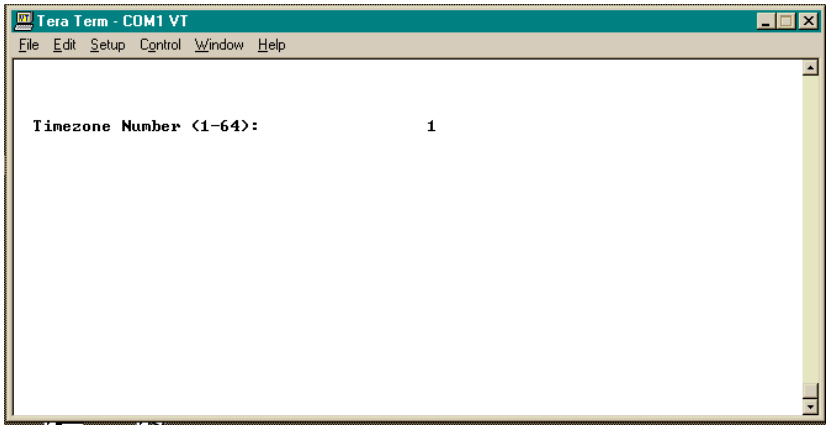


Figure 4-4: Using Multiple Time Blocks

If you assign a cardholder to this time zone, access would be denied during the white blocks of disabled time and access would be granted during the shaded blocks of enabled time as shown in Figure 4-4.

To define or edit time zones, select **Time Zone** from the CK721-A Main menu. If records have been previously defined, they will be displayed. If you enter a time zone number not previously created, the system will add it as a new record. You can configure a maximum of 64 time zones in a single CK721-A.



When you enter a Timezone number, the Timezone window is displayed.

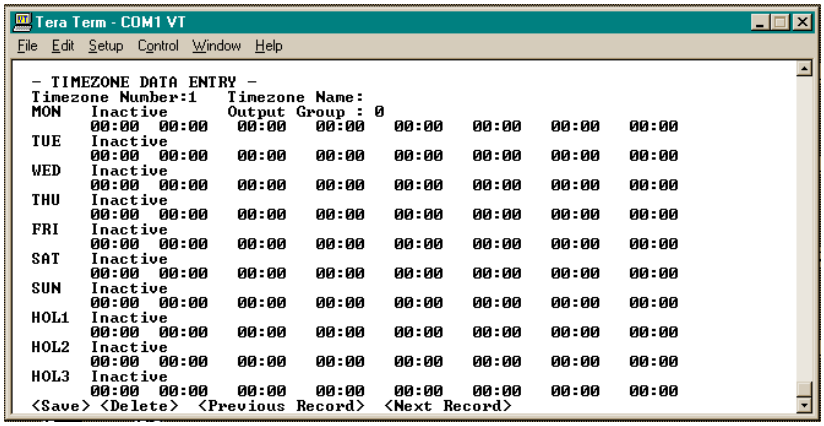


Table 4-23: Time Zone Screen, 1 Page Only

Field	Type	Description
Time Zone Name	User Def.	Enter up to 25 alphanumeric characters as a descriptive name for the time zone.
Output Group	User Def.	Enter the output group to which you want this time zone applied. (optional)
Midnight, Active/Inactive	Toggle	Select midnight as inactive or active as the first entry for a listed day or holiday.
Start/Stop Times	User Def.	Use the arrow keys to navigate through the start and stop times, typing in the appropriate values where required.

Card Events

This screen establishes an event based on card or badge (trigger) activity. The purpose (action) of this window is to allow a person at a reader terminal to suppress or unsuppress an input group, activate or deactivate an output group, operate a door strike, and/or reset a panel alarm relay.

Card events will only activate as a result of a card transaction decision made locally at a panel. If the server performs the access transaction processing (in central or shared mode), the card event will not occur.

Following is the summary of the CK721-A card event processing capability:

Table 4-24: Card Event Overview

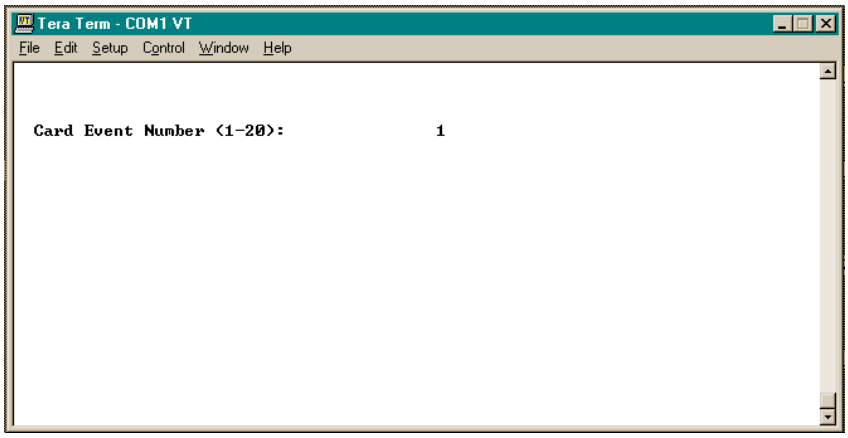
Trigger Conditions	Event Conditions	Actions
■ Card only ■ Card/PIN Code ■ Any Void Card ■ Card/Keypad Code ■ Card/PIN/Keypad Code ■ Assisted Access A ■ Assisted Access B ■ Assisted Access C	■ Privilege level ■ Valid Readers for Card Events ■ Keypad Code (required only if Keypad Code is used in trigger condition)	■ Suppress or unsuppress input group (to modify enable input group) ■ Activate or deactivate output group (to modify enable output group) ■ Operate door strike. If multiple events are executed from the same trigger and any of the events have this flag set, the door will open. ■ Reset local panel relay

The first column lists the Trigger Conditions that can trigger an Action. These Trigger Conditions are specified in the Option box in the Panel Card Event window.

The second column lists the Event Conditions that must be programmed to associate a Trigger with an Event. These Conditions are located in the **Options** box and the **Valid Readers for Card Event** box in the Panel Card Event window in the Cardkey SMS.

The third column lists the Actions that are available. These actions are linked with a Trigger Condition. This column lists the actual hardware components that can be set, reset, suppressed, or unsuppressed, or enabled.

To configure a new event or edit an existing one, select **Card Event** from the CK721-A Main menu. Next, select a previously saved event or type in a new event number to create a new card event record.



The Card Event window appears as shown here. Each field is described in Table 4-25.

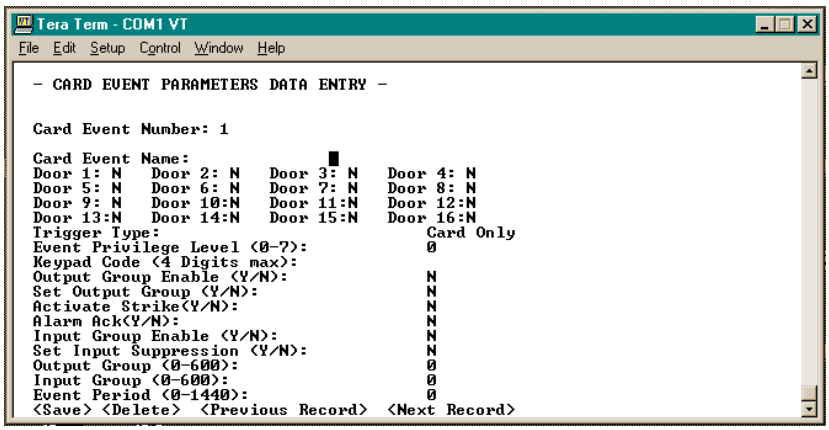


Table 4-25: Card Event Screen, 1 Page Only

Field	Type	Description
Card Event Name	User Def.	Type in a descriptive event name up to 25 alphanumeric characters long.
Door (1 - 16)	Toggle	If a door is enabled (**Y**), the event can be initiated at that location. You can enable any or all doors for a specific event.
Trigger Type	Toggle	The following choices are available: **Card Only** Present a card. **Card/PIN Code** Enter PIN and present a card. For detailed instructions refer to Appendix D. **Card/Keypad Code** Enter activation or deactivation code, followed by the code specified in the Keypad Code field, then present a card. For detailed instructions refer to Appendix D.

Table 4-25: Card Event Screen, 1 Page Only

Field	Type	Description
Trigger Type	Toggle	**Card/PIN/Keypad Code** Enter PIN and activation or deactivation code, followed by the code specified in the Keypad Code field, then present a card. For detailed instructions refer to Appendix D. **Any Void Card** Present any invalid card. In this case the card event's privilege level should be set to 0, as invalid cards do not have any privilege level. **Special Access** (**A**, **B** or **C**) Present a card with assigned Special Access flag A, B, or C.
Event Privilege Level	User Def.	Assign a privilege level to this event. Values ranges from 0 to 7, with 7 being the highest privilege level. This number corresponds to the Event Privilege Level field in the Badge screen, where a badge can execute an event equal to or less than its privilege value.
Keypad Code	User Def.	Enter up to a four-digit keypad code required to activate or deactivate this event when using a keypad trigger type. Deactivating an event can only be accomplished by using a keypad code. For detailed instructions refer to Appendix D.
Output Group Enable	Toggle	If enabled (**Y**), an output group specified by the Output Group field will be enabled. Outputs in the group will behave according to their defined active state.
Set Output Group	Toggle	Enable (**Y**) to activate the specific output group when this event is activated. Disable (**N**) to deactivate the specific Output Group when this event is activated. When this event is deactivated, the selected action is inverted: an event that activates an output group on activation, deactivates that output group on deactivation; and an event that deactivates an output group on activation, activates that output group on deactivation.

Table 4-25: Card Event Screen, 1 Page Only

Field	Type	Description
Activate Strike	Toggle	If enabled (**Y**), the door strike at the reader initiating the event is activated. If multiple events are executed from the same trigger and any events have this flag set, the door will open. If disabled (**N**), a valid event invokes the event action only, but does not unlock the door. For legacy panels and badges with executive privilege this setting does not apply. Also, events with trigger type “Any Void Card” never unlock the door.
Alarm Ack	Toggle	If enabled (**Y**), the CK721-A’s alarm relay is reset.
Input Group Enable	Toggle	If enabled (**Y**), an input group specified by the Input Group field will be enabled.
Set Input Suppression	Toggle	Enable (**Y**) to suppress the specific Input Group when this event is activated. Disable (**N**) to unsuppress the specific Input Group when this event is activated. When this event is deactivated, the selected action is inverted: an event that suppresses an input group on activation, unsuppresses that input group on deactivation; and an event that unsuppresses an input group on activation, suppresses that input group on deactivation.
Output Group	User Def.	Enter the number of an output group to activate or deactivate.
Input Group	User Def.	Enter the number of an input group to suppress or unsuppress.
Event Period	User Def.	Values range from 0 to 1440 minutes. If you set a time value, the event will deactivate on expiration. Otherwise, the event will need to be manually deactivated. If the event activates an output group, the output group will be deactivated after this time period. If the event suppresses an input group, the input group will be unsuppressed after this time period. Event Period applies only to event activation, and not to event deactivation. Furthermore, only output group activation and input group suppression may be assigned a period, but not output group deactivation and input group unsuppression.

System Information

This screen provides information regarding the CK721-A. This includes items such as reader status, IP addresses, MAC number, and current time zone status. To access this information, select **System Information** from the CK721-A Main menu.

System Information is a two-page screen, described in Table 4-26 and Table 4-27.

System Information Screen - Page 1

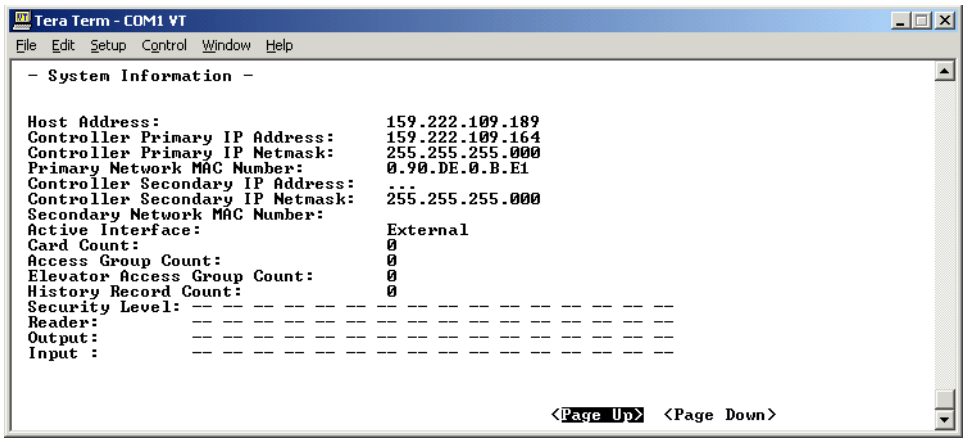


Table 4-26: System Information Screen, Page 1

Field	Description
Host Address	IP address of the Cardkey SMS. **Note**: Only the Primary Host IP address will appear here.
Controller Primary IP Address	IP address of the onboard network interface.
Controller Primary IP Netmask	IP netmask of the onboard network interface.
Primary Network MAC Number	This is a hard-coded (cannot be changed) Media Access Control number. Each network device (CK721-A) must have a unique MAC number assigned at the factory.
Controller Secondary IP Address	This IP address is reserved for future use in support of a secondary IP interface.
Controller Secondary IP Netmask	This netmask is reserved for future use in support of a secondary IP interface.
Secondary Network MAC Number	Unique MAC encoded into a secondary RS232 network adapter or modem.

Table 4-26: System Information Screen, Page 1

Field	Description
Active Interface	Current network communication status. Built-in=onboard network interface. External=RS232 interface.
Card Count	Total number of card (badge) records in the CK721-A database.
Access Group Count	Total number of Access Groups records in the CK721-A database (Normal Access Groups records plus Elevator Access Groups records).
Elevator Access Group Count	Total number of Elevator Access Groups records in the CK721-A database.
History Record Count/Total	Total number of stored history transactions in the CK721-A database.
Security Level (0 to 99) Note: At the time of this release the terminal's Security Level cannot be set by any server or the panel's User Interface. This feature is for future use.	To grant access, the terminal's Security Level must not exceed the badge's Security Level. In case of emergency, Security Level for all terminals can be quickly raised. When the Security Level exceeds that of a badge, access will be denied, except for cardholders with Executive Privilege. For this feature to work, Security Level must be assigned to the system, the terminals and the badges.
Module Status: Reader Output Input	Key: -- Not found ** Not defined and off-line Up Defined and on-line Dn Defined but off-line

System Information Screen - Page 2

Device status is listed from the first module to the last, left to right.

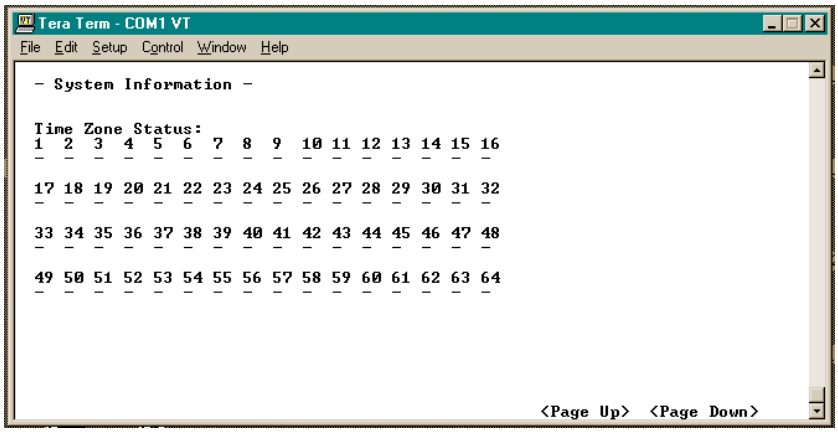


Table 4-27: System Information Screen, Page 2

Field	Description
Time Zone Status	64 time zones can be defined. Status of each is shown as **E**(nabled), **D**(isabled), or (**--**) undefined.

Control Output

This option allows you to manually control an output. Select **Control Output** from the CK721-A Main menu to access Control Output options.

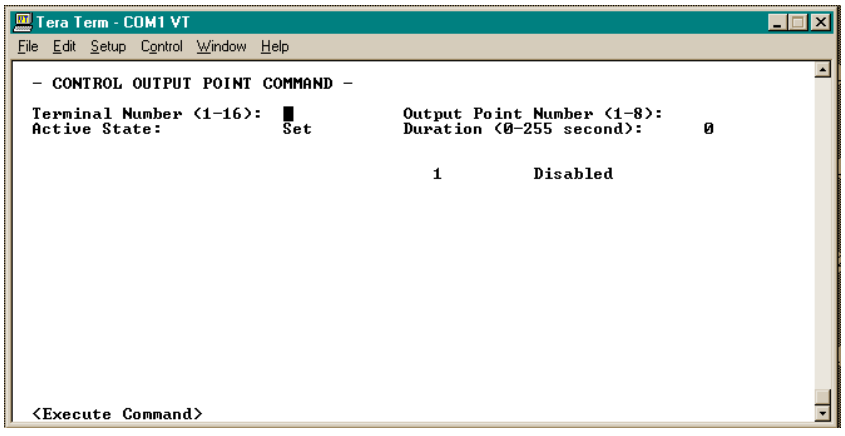


Table 4-28: Control Output Screen, 1 Page Only

Field	Type	Description
Terminal Number	User Def.	Enter the number of the terminal containing the output you wish to control.
Output Point Number	User Def.	Type in a specific output point number.
Active State	Toggle	Select **Set**, **Reset**, **Quick Flash**, **Slow Flash**, or **Timed**.
Duration	User Def.	Choose a value between 0 and 255 seconds if you selected **Timed** as the active state.

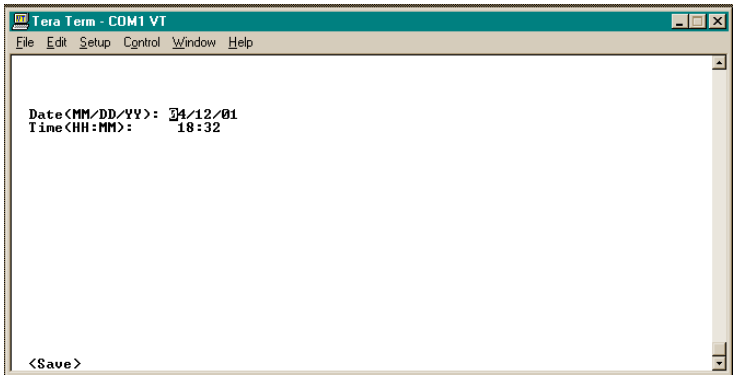
Every output point, no matter which option was selected for it, can be commanded with 5 different active states. See Table 4-29 to determine the effect of the commands on each selected state.

Table 4-29: Results of Command Override on a Selection

		Programmed as:				
		Set	**Reset**	**SlowFlash**	**QuickFlash**	**Timed**
Commanded as:	**Set**	Set	Reset	SlowFlash	QuickFlash	(nothing)
	Reset	Reset	Reset	Reset	Reset	Reset
	SlowFlash	SlowFlash	SlowFlash	SlowFlash	SlowFlash	SlowFlash (Timed)
	QuickFlash	QuickFlash	QuickFlash	QuickFlash	QuickFlash	QuickFlash Timed)
	Timed	Timed (to the Set state)	Timed (to the Set state)	Timed (to the Set state)	Timed (to the Set state)	Timed (to the Set state)

Change Date

To set the CK721-A realtime clock, select **Change Date** from the CK721-A Main menu. The following screen is displayed.



Enter the date in month/day/year format as shown above. Enter the time in 24-hour format as shown above.

NOTE

This screen is only used when the CK721-A panel is the operating standalone. If the CK721-A panel is communicating with a server, then the server time will be downloaded and overwrite the settings made here.

Chapter 5

MAINTENANCE

This chapter provides maintenance instructions, operational testing procedures, troubleshooting guidelines, and instructions on how to obtain replaceable parts for the CK721-A system.

ROUTINE MAINTENANCE

➤ **Perform the following routine maintenance on the CK721-A:**

1. Periodically check the continuity of the grounding circuit.
2. Perform operational testing monthly (see "Testing Procedure" on page 5-2).
3. Replace the lithium battery every five years or after extended (five days) power interruption (Panasonic CR 2025 or equivalent).
4. If installed, replace the lead-acid backup batteries every three years (either Power Sonic PS-1270, 12 VDC, 7 Ah or equivalent; or Power Sonic PS-1228, 12 VDC, 2.8 Ah or equivalent.)

IMPAIRED PERFORMANCE CONDITIONS

A list of conditions that may cause impaired performance is provided in Table 5-1, with reference pages.

Table 5-1: Impaired Performance Conditions

Condition	Information Location
Unit environment not as specified.	Table 1-5.
Unit power and grounding not as specified.	Page 2-15, Table 3-2, and Appendix A.
Cable length or type not as specified.	Page 2-8, Table 3-1, and Figure 3-19.
Backup battery not replaced correctly.	This chapter.

TESTING PROCEDURE

➤ **Check for proper operation of the CK721-A as follows:**

1. Verify POWER LED on the CK721-A.
2. Verify that the FAULT LED on the CK721-A is not on.
3. Verify the RS485B LED is flashing to show activity on the bus.
4. Present a *valid* card to a reader, and then verify that access is granted (green lamp lights).
5. Present an *invalid* card to a reader, and then verify that access is denied (red lamp lights).

Check Backup Battery Operation

➤ **If the optional backup battery is installed:**

1. Disable primary AC input voltage to the enclosure.
2. Verify that the CK721-A continues to operate.
3. Reapply primary AC voltage to the enclosure.

Lithium Battery Replacement

➤ **To replace the lithium battery:**

1. Ensure that AC power is supplied to the panel.
2. With a narrow blade (1/8 in. blade) carefully pry up the battery until a portion of the battery is out of the plastic holder.
3. With your free hand gently move the battery out of the holder while keeping the battery pried up.
4. Dispose of the old battery according to local requirements.
5. Insert the new battery into holder.

The lithium battery is polarized. Ensure the side marked '+' faces out or towards you.

Danger of explosion if battery is incorrectly replaced.

FIELD SERVICING

Troubleshoot the CK721-A by substituting the suspected defective panel with a new component.

All replaceable parts are available from Johnson Controls, Inc.

Consult your Customer Success Center representative at (800) 482-2778 for domestic orders or for instructions on how to obtain replaceable parts.

TROUBLESHOOTING

Use the following table to quickly assess problems you may have with your access control system.

Table 5-2: Troubleshooting Guidelines

Problem	Possible Causes
Reader down	■ Incorrect wiring from reader to reader terminal ■ Reader is unassigned ■ Defective reader terminal
Red light or no reader light illuminates when card is used at reader, and access is not granted.	■ Invalid Time zone/Reader/Issue Level/Facility Code ■ Card no longer in database Incorrect card type ■ Card is being swiped backwards ■ Reader inoperative ■ Damaged card ■ Bad cabling ■ Failed PCB ■ Multiple proximity cards in reader antenna field
Door will not go into “Override Mode” but grants access when a card is used.	■ Override time zone is incorrectly programmed, or not programmed. ■ Override option not set.
Alarm not reporting	■ Alarm is suppressed (i.e., not in an active time zone) ■ Associated input point not defined ■ Bad wiring or input device

Table 5-2: Troubleshooting Guidelines

Problem	Possible Causes
PIN Code function not operating	■ PIN is not programmed as part of the access condition ■ Broken wire or incorrect wiring from the keypad to PCBA ■ Defective keypad
Card or data loss from database	■ Noise on power line ■ Improper grounding ■ Defective CK721-A
System restarts continuously	■ System improperly grounded ■ Severe power variations ■ Defective CK721-A
Red or Green lamp does not illuminate, but access is denied or granted if card is used.	■ Open wire at lamp connection ■ Burned out lamp bulb ■ Defective reader terminal
Holiday time zones not followed	■ Improperly programmed Holiday time zones or Holiday dates.

GROUNDING AND CONNECTORS

This appendix gives instructions for grounding cable shields at data and low voltage installations, and at grounding card reader units. Follow these guidelines for electromagnetic compatibility (EMC) conformity, and to improve system reliability. In some cases, European requirements (EN standards) differ from the USA requirements (FCC standards). Refer to the relevant sections for these requirements.

Every unit in a Johnson Control's installation must have its chassis bonded to a verified electrical ground (earth). In all cases, the local wiring codes apply.

The National Electrical Code NFPA 70 must be followed for installations in the USA.

The Canadian Electric Code, C22.1 must be followed for installations in Canada.

BSI Standard BS7671 (latest edition) must be followed for installations in Great Britain. Additional information is given in the Cardkey Installers' Code of Practice.

Conduit ground, cold water pipes, unbrazed joints or dissimilar metals are unacceptable in the path of either building or supplemental ground. Where grounding is required, connect only to the proven building electrical system ground (earth).

CABLE GROUNDING

All data and low voltage cabling must be shielded (as specified by the relevant manual). Connecting shields to chassis ground differs, depending on the nature of the installation.

The following subparagraphs describe recommended grounding requirements in the USA and in Europe. Note that in the illustrations accompanying the descriptions:

- The outer cover of the cable has been stripped back to reveal the cable's shield.
- The shield is cut back so it just enters the enclosure.
- The drain wire that extends from the shield shown in the illustrations must be kept as short as possible (typically, 2.5 cm or 1 inch). Connect a lug to the end of the wire, as shown, and screw securely to the wall of the enclosure or nearest stud.
- All internal ground (earth) bonding straps must be left intact after installation.
- Check that grounding points are clean and free from paint or corrosion.

"D-Type" Connectors

All D-type connectors must use Electromagnetic Interference (EMI) shielded shroud. Ensure that a good contact is made when connecting D-type connector shrouds to cable shields.

Figure A-1 shows a critical contact throughout the 360 degrees of the cable's shield at the point of entry to the shell. To ensure a good fit, strip back the cable's outside layer to reveal the metal shield and extend the shield to the very edge of the metal shroud's connector. If the shield does not fit snugly, apply metallic tape to ensure a firm contact.

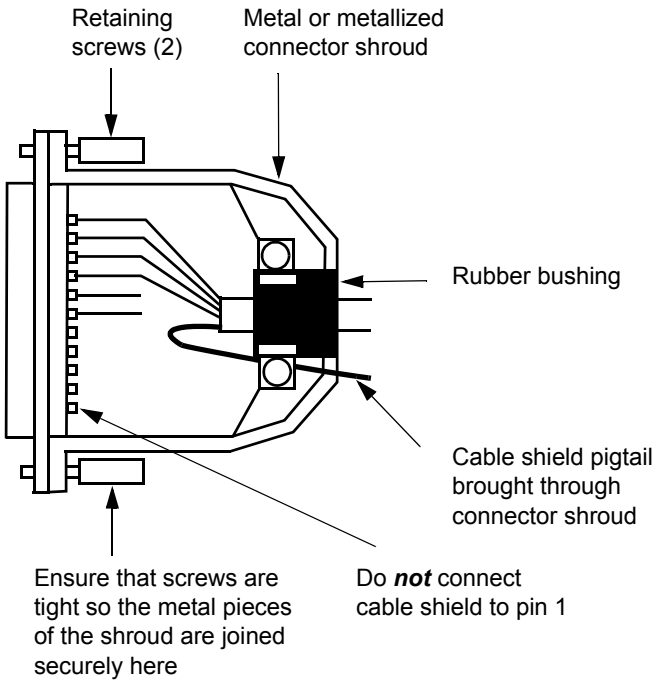


Figure A-1: Example of D-Type Connector Grounding

The two curved parts of the shroud shown in Figure A-1 make contact with the flat plate of the shroud. Tighten the two remaining screws to ensure a firm fit.

Do not remove the drain wire from the shield.

CAUTION

Do not connect the shield to connector pin 1 in any way.

Non “D-Type” Grounding Connections

As shown in Figure A-2, incoming wires that are foil shielded with a drain wire are connected to the grounding bus.

When using incoming wires that are foil shielded without a drain wire, strip back the insulation, twist the foil shield together, and using a customer-supplied crimp terminal, splice a wire to the end of the shield. Terminate the wire with an insulated spring spade terminal, and attach it to the enclosure ground stud.

Installations in the USA

In the USA, the two units are connected using shielded cable. As shown in Figure A-2, ground the shield at both ends.

In some USA installations, operation of the system can be compromised by excess ground currents travelling along the shield. Figure A-3 shows an alternate method of shielding. Cables connected to user peripherals (printers, VDTs, etc.) should have shields connected at both ends.

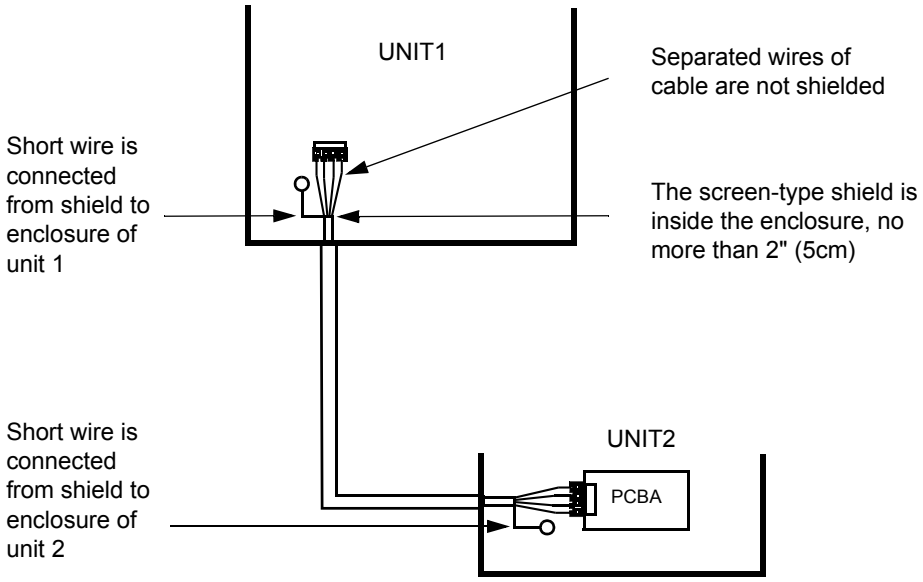


Figure A-2: Example of Grounding Shielded Cable at Both Ends

Installations in Europe

All Cardkey equipment panels must be connected to a proven building electrical system ground (earth).

Connect the shield of low voltage and data system cabling to ground at only one end (see Figure A-3). This is generally at the higher end of the system hierarchy.

Cables to user peripherals (printers, VDTs, etc.) should have shields connected at both ends.

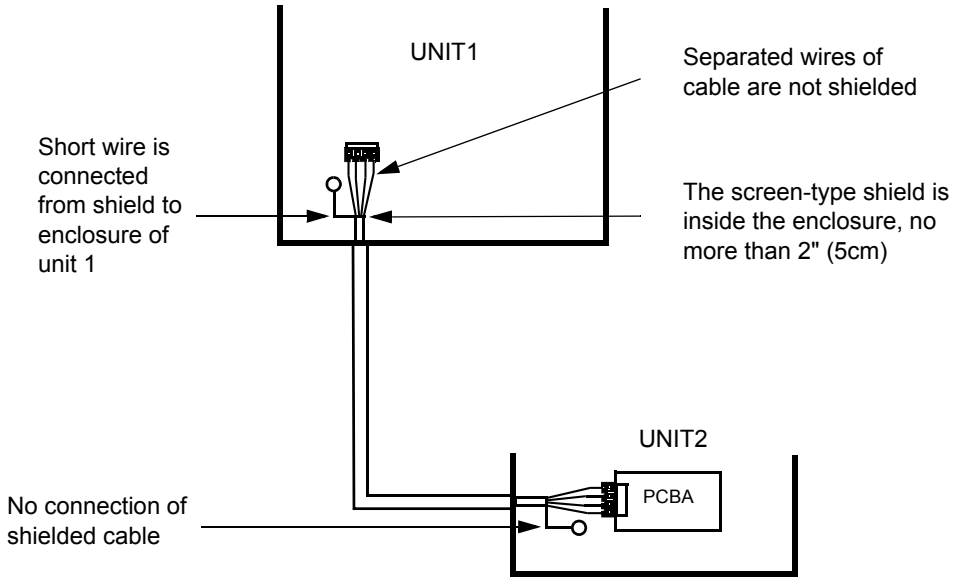


Figure A-3: Example of Grounding Shielded Cable at Only One End

CARD READER UNIT GROUNDING

If the card reader unit ground *is not mounted on a metal surface*, connect a grounding wire to the card reader unit housing. Run the wire to the associated unit, and as shown in Figure A-3, connect the cable shield to the grounding bus. The screws for the ground bus are bagged separately for installation.

If the card reader unit *is mounted on a metal surface which may contact ground*, select either one of two options:

- Insulate the card reader unit from the metal surface and connect the grounding wire described above.
- Leave the card reader attached to the metal surface if insulating it is not practical, and do ***not*** connect the grounding wire described above. This will prevent a possible ground loop or other problems, since building framework or structural metal is often subject to stray AC or DC voltages and transients.

DOOR OPEN/AUX ACCESS SUPERVISION

Using the S300-SIO8 module, you can provide four-state supervision of the DOOR OPEN and AUXILIARY ACCESS contacts on an S300-RDR2 module. The basic steps required are:

- On the S300-SIO8, set position four of SW1 to ON.
- Wire relays five through eight on the S300-SIO8 to the DOOR and AUX inputs on the S300-RDR2 module.
- Wire the corresponding inputs from J6C and J6D on the S300-SIO8, which are alarms five through eight (AL5 - AL8), to your door open and auxiliary access contacts.

Each step is explained in detail in the remainder of this appendix.

PURPOSE OF SUPERVISED INPUTS

By design, the DOOR (open) and AUX (auxiliary access) inputs on an S300 reader module are two-state. For installations requiring supervised inputs (two additional states: open and short), the S300-SIO8 modules provides the capability to link alarms five through eight to output relays five through eight. Three main points are important to remember:

- The four-state inputs are linked to the output relays through the S300-SIO8 PS-184A (or later) firmware. No additional hardware is required.
- Normal operation of the modified output relays (five through eight) is disabled. Specifically, the relays will no longer respond to output control and output control status messages from the CK721-A. The modified outputs will always be reported as reset.
- Inputs five and eight will only report the two trouble conditions: circuit open and circuit shorted. They will not report anything when the switches open and close.

CONFIGURING THE S300-SIO8

To link alarms five through eight to output relays five through eight, place position four of SW1, on the S300-SIO8 module, to ON. This links AL5 through AL8 to output relays five through eight as shown in Table B-1.

Table B-1: Input/Output Linking, S300-SIO8, SW1 position 4 set ON

Input State for Inputs 5-8	Output Relay State for Outputs 5-8	SIO8 Reports
Secure	Unenergized	Secure
Alarm	Energized	Secure
Open	Unenergized	Open
Short	Unenergized	Short

From the S300-SIO8, AL5 through AL8 are wired to the door open indicator and auxiliary access switches as shown on the following page. AL5 and AL7 are used for auxiliary access switches; AL6 and AL8 are used for door open indicators.

Note the location of the 150 Ohm resistors in the circuits, which is standard wiring used for the S300's four-state input points.

With respect to wiring inputs, the following diagram assumes the following:

- DOOR OPEN is closed (secure) when the door is closed.
- AUX ACCESS is normally open (secure). Contact closure initiates an auxiliary access request.

WIRING TO THE READER MODULE

The contacts from the output relays (five through eight) on the S300-SIO8 module are hard-wired to the DOOR or AUX inputs on the S300-RDR2 module. The Normally Open contact (NO) is used for AUX inputs (see the following subsection for additional information). The Normally Closed (NC) is used for door inputs. Ground is provided by wiring the Common (C) contacts of the output relays together and wiring them to the GND input on the reader module.

Open or short circuit conditions at the four-state inputs will be reported to the CK721-A by the S300-SIO8 module without affecting the reader module's inputs. As a result, the relay contacts will appear to the S300-RDR2 module exactly as if two-state contacts were being used. Shunting of the door alarm and generation of door open and forced door conditions will occur normally.

The following page shows the wiring from the S300-SIO8 output relays to the S300-RDR2 module.

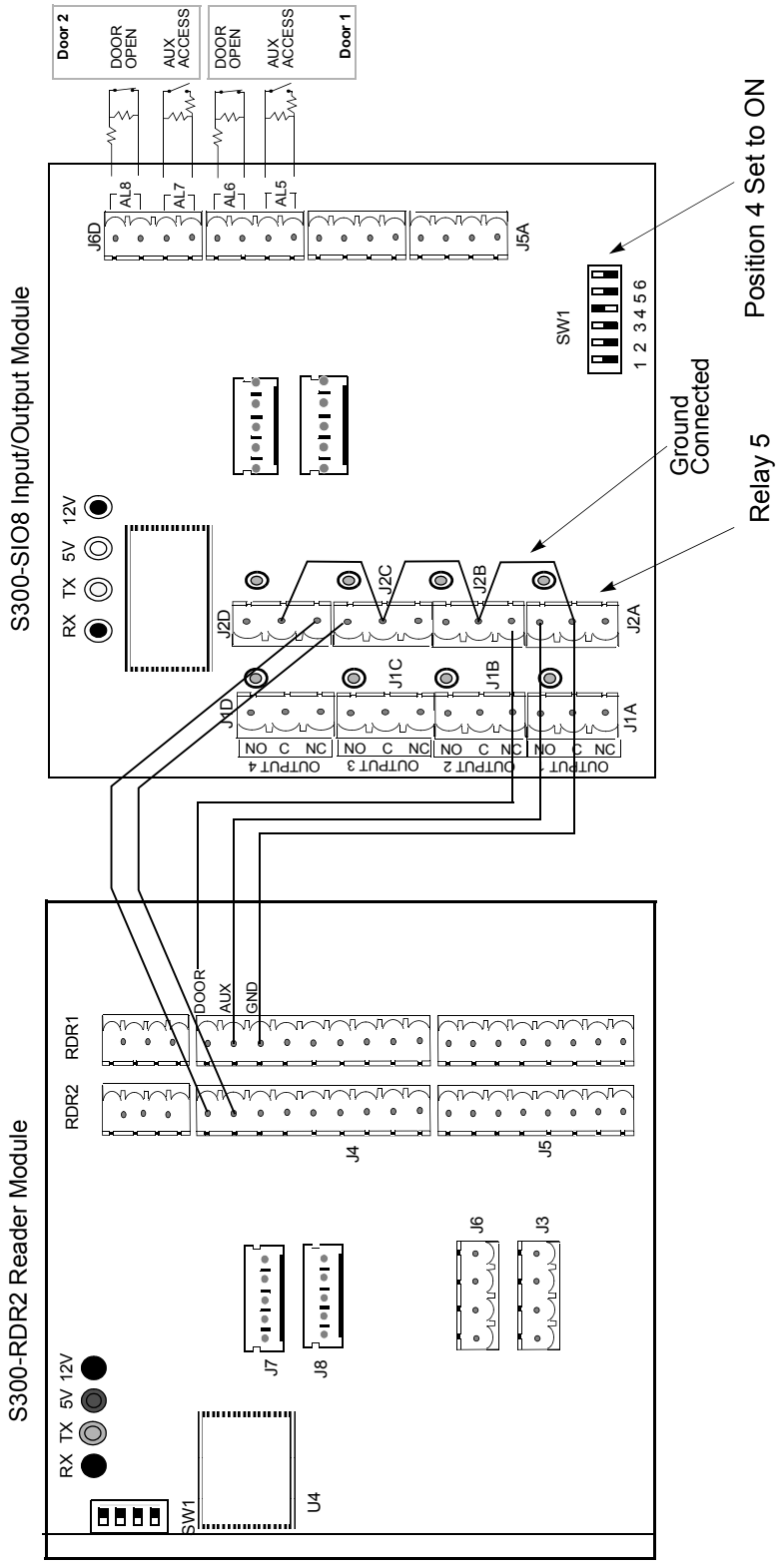


Figure B-1: Input/Output Contact Wiring

Appendix C

DATABASE FLASH BACKUP FROM THE HOST

This appendix explains the procedure for performing a Database Flash Backup. It will enable you to backup CK721-A data to the CPU's on board flash memory. Consequently, if the panel does not have a backup battery (UPS) or the data is not backed up to the on board flash memory, all database information will be lost after a power cycle.

NOTE

The Database Flash Backup procedure must be configured at the host. The following sections describe the procedures from both the P1000 and P2000 Hosts.

CK721-A PANEL DATABASE FLASH BACKUP PROCEDURE FROM THE P1000 HOST

NOTE

Before starting the procedure, verify that the CK721-A panel is online.

➤ **To configure the Database Flash Backup:**

1. From the P1000 Main menu, select **Configuration>Utilities>SCO Terminal**. The password dialog box appears.

Figure C-1: Password Dialog Box

2. Type your password, press <**Enter>**, or click the check box.
   After typing your password, the SCO Terminal window appears.

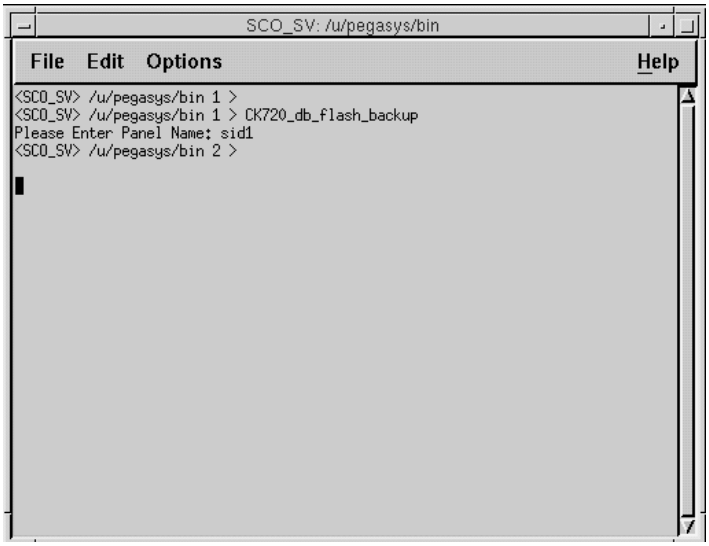


Figure C-2: SCO Terminal Window

3. At the SCO Terminal window you will see the prompt:
   `<SCO_SV> /u/pegasys/bin 1>`
4. Type the following command:
   `CK720_db_flash_backup`
5. Press <**Enter>**.

NOTE

Remember, SCO commands are case-sensitive and should be typed exactly as shown.

---

6. At the prompt:
   `Please Enter Panel Name:`
7. Type the panel's name, and then press <**Enter>**.
8. Select **File>Exit** to exit the SCO Terminal window.

The procedure is now complete.

NOTE

After writing the database to Flash memory, the panel will reboot.

CK721-A Panel Database Flash Backup Procedure From the P2000 Host

NOTE

Before starting the procedure, verify that the CK721-A panel is online.

➤ **To configure the Database Flash Backup:**

1. From the P2000 Main menu, select **System>CK705/CK720 Write DB To Flash**. The CK721-A Write DB to Flash dialog box appears.

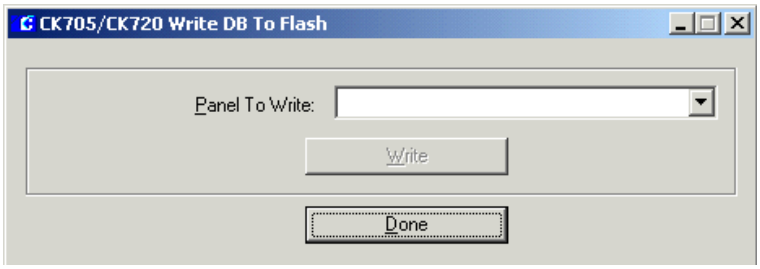


Figure C-3: CK705/CK720 Write DB to Flash Dialog Box

2. Select the **Panel To Write** from the drop-down list.
3. Click **Write**. All data stored in the panel's RAM is backed up to its flash memory.
4. Click **Done**.

The procedure is now complete.

NOTE

After writing the database to Flash memory, the panel will reboot.

USING A KEYPAD READER ON A PANEL

The following sections describe how to invoke access requests, Air Crew access requests, Timed Overrides, and Panel Card Events using a keypad reader.

There is a 15-second time out on keypads. Whenever the keypad is idle for more that 15 seconds, all keys entered so far will be ignored, and the entire key sequence needs to be re-entered.

NOTE

Card ID (the badge number) can have up to 19 digits. However, the total number of keys pressed for PIN and Card ID combined must not exceed 21.

INVOKING ACCESS REQUESTS FROM A KEYPAD

➤ **To invoke access with Badge:**

1. To be able to invoke access using a badge at any time, set the terminal's **PIN Suppression Timezone** to **<0>**. Otherwise, access will be granted only during active timezones.
2. At the keypad reader, present the badge.

➤ **To invoke access with PIN Only:**

1. The terminal's **PIN Only** flag must be set. **PIN Only** works exclusively with 5-digit algorithmic PINs.
2. Set the panel's **PIN Code Type** to **Algorithmic**.
3. The panel's **5 Digit PIN Code** flag must be set.
4. At the keypad reader, enter PIN, and press the # key.

➤ **To invoke access with Card ID:**

1. To be able to invoke access with Card ID at any time, set the terminal's **PIN Suppression Timezone** to **<0>**. Otherwise, access will be granted only during active timezones.
2. The terminal's **Card ID** flag must be set.
3. Make sure the terminal's **PIN Only** flag is *not* set.

4. Make sure the terminal's **PIN + Card ID** flag is *not* set.
5. At the keypad reader, enter the Card ID number and press the # key.

➤ **To invoke access with PIN and Card ID:**

1. The terminal's **PIN + Card ID** flag must be set.
2. Make sure the terminal's **PIN Only** flag is *not* set.
3. At the keypad reader, enter PIN, then enter the Card ID number and press the # key.

➤ **To invoke access using PIN and badge:**

1. The terminal's **PIN Suppression Timezone** must be set to an inactive timezone.
2. Make sure the terminal's **Allow PIN After Badge** flag is *not* set.
3. At the keypad reader, enter PIN and then present the badge.

➤ **To invoke access with PIN and badge, allowing PIN after badge:**

1. The terminal's **PIN Suppression Timezone** must be set to an inactive timezone.
2. The terminal's **Allow PIN After Badge** flag must be set.
3. At the keypad reader, present the badge[1], enter PIN and press the # key.

[1] The badge can be presented at any time before the # key is pressed.

INVOKING AIR CREW ACCESS REQUESTS FROM A KEYPAD

➤ **To invoke Air Crew access:**

1. The host must be online.
2. The respective **Air Crew PIN** must be enabled for the terminal.
3. To request Air Crew access:

   Without the Star Feature, press the B key followed by the Air Crew PIN number and the # key.

   With the Star Feature, press the star (*) key, then press number 2, followed by the Air Crew PIN number and the # key.

INVOKING TIMED OVERRIDES FROM A KEYPAD

➤ **To invoke Timed Override with Badge:**

1. The terminal's **Cardholder Override** flag must be set.
2. The badge's **Override** flag must be set.

3. To be able to invoke Timed Override using badge at any time, set the terminal's **PIN Suppression Timezone** to **<0>**. Otherwise, Timed Override will be invoked only during active timezones.
4. To start Timed Override:

   Without the Star Feature, press the star (*) key, enter the number of minutes, and present the badge.

   With the Star Feature, press the star (*) key followed by number 0, enter the number of minutes, and present the badge.
5. To stop Timed Override:

   Without the Star Feature, press the star (*) key, enter 0 (for minutes), and present the badge.

   With the Star Feature, press the star (*) key followed by number 0 and present the badge.

➤ To invoke Timed Override with PIN Only

1. The terminal's **Cardholder Override** flag must be set.
2. The badge's **Override** flag must be set.
3. The terminal's **PIN Only** flag must be set. **PIN Only** works exclusively with 5-digit algorithmic PINs.
4. Set the panel's **PIN Code Type** to **Algorithmic**.
5. The panel's **5 Digit PIN Code** flag must be set.
6. To start Timed Override:

   Without the Star Feature, enter PIN, press the star (*) key, enter the number of minutes, and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 0, enter the number of minutes, and press the # key.
7. To stop Timed Override:

   Without the Star Feature, enter PIN, press the star (*) key, enter 0 (for minutes), and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 0, and press the # key.

➤ To invoke Timed Override with Card ID:

1. The terminal's **Cardholder Override** flag must be set.
2. The badge's **Override** flag must be set.
3. To be able to invoke Timed Override using badge at any time, set the terminal's **PIN Suppression Timezone** to **<0>**. Otherwise, Timed Override will be invoked only during active timezones.
4. The terminal's **Card ID** flag must be set.
5. Make sure the terminal's **PIN Only** flag is *not* set.

6. Make sure the terminal's **PIN + Card ID** flag is *not* set.
7. To start Timed Override:

   Without the Star Feature, enter the Card ID number, press the star (*) key, enter the number of minutes, and press the # key.

   With the Star Feature, enter the Card ID number, press the star (*) key followed by number 0, enter the number of minutes, and press the # key.
8. To stop Timed Override:

   Without the Star Feature, enter the Card ID number, press the star (*) key, enter 0 (for minutes), and press the # key.

   With the Star Feature, enter the Card ID number, press the star (*) key followed by number 0, and press the # key.

➤ To invoke Timed Override with PIN and Card ID:

1. The terminal's **Cardholder Override** flag must be set.
2. The badge's **Override** flag must be set.
3. Terminal's **PIN + Card ID** flag must be set
4. Make sure the terminal's **PIN Only** flag is *not* set.
5. To start Timed Override:

   Without the Star Feature, enter PIN, enter the Card ID number, press the star (*) key, enter the number of minutes, press the # key.

   With the Star Feature, enter PIN, enter the Card ID number, press the star (*) key followed by number 0, enter the number of minutes, and press the # key.
6. To stop Timed Override:

   Without the Star Feature, enter PIN, enter the Card ID number, press the star (*) key, enter 0 (for minutes), and press the # key.

   With the Star Feature, enter the PIN, number, enter the Card ID number, press the star (*) key followed by number 0, and press the # key.

➤ To invoke Timed Override with PIN and Badge:

1. The terminal's **Cardholder Override** flag must be set.
2. The badge's **Override** flag must be set.
3. The terminal's **PIN Suppression Timezone** must be set to an inactive zone.
4. Make sure the terminal's **Allow PIN After Badge** flag is *not* set.
5. To start Timed Override:

   Without the Star Feature, enter PIN, press the star (*) key, enter the number of minutes, and present the badge.

   With the Star Feature, enter PIN, press the star (*) key followed by number 0, enter the number of minutes, and present the badge.

6. To stop Timed Override:

   Without the Star Feature, enter PIN, press the star (*) key, enter 0 (for minutes), and present the badge.

   With the Star Feature, enter PIN, press the star (*) key followed by number 0, and present the badge.

➤ To invoke Timed Override with PIN and Badge, allowing PIN after badge:

1. The terminal's **Cardholder Override** flag must be set.
2. The badge's **Override** flag must be set.
3. The terminal's **PIN Suppression Timezone** must be set to an inactive zone.
4. The terminal's **Allow PIN After Badge** flag must be set.
5. To start Timed Override:

   Without the Star Feature, enter PIN, press the star (*) key, enter number of minutes, present the badge[1], and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 0, enter number of minutes, present the badge[1], and press the # key.
6. To stop Timed Override:

   Without the Star Feature, enter PIN, press the star (*) key, enter 0 minutes, present the badge[1], press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 0, present the badge[1], and press the # key.

   [1] The badge can be presented at any time before the # key is pressed.

INVOKING PANEL CARD EVENTS FROM A KEYPAD

➤ To invoke Panel Card Events with Badge:

1. The event's **Trigger Type** must be set to **Card/Keypad Code.**
2. To be able to invoke a Panel Card Event using a badge at any time, set the terminal's **PIN Suppression Timezone** to **<0>**. Otherwise, the Panel Card Event will be invoked only during active timezones.
3. To activate event:

   Without the Star Feature, press A, enter the keypad code, and present the badge.

   With the Star Feature, press the star (*) key followed by number 1, enter the keypad code, and present the badge.

4. To deactivate event:

   Without the Star Feature, press D, enter the keypad code, and present the badge.

   With the Star Feature, press the star (*) key followed by number 4, enter the keypad code, and present the badge.

➤ To invoke Panel Card Events with PIN Only:

1. The event's **Trigger Type** should be set to **Card/Keypad Code** or **Card/PIN/Keypad Code.**
2. If set to **Card/PIN/Keypad Code**, the terminal's **PIN Suppression Timezone** must be set to an inactive timezone.
3. The terminal's **PIN Only** flag must be set. **PIN Only** works exclusively with 5-digit algorithmic PINs.
4. Set the panel's **PIN Code Type** to **Algorithmic**.
5. The panel's **5 Digit PIN Code** flag must be set.
6. To activate event:

   Without the Star Feature, enter PIN, press A, enter the keypad code, and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 1, enter the keypad code, and press the # key.
7. To deactivate event:

   Without the Star Feature, enter PIN, press D, enter the keypad code, and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 4, enter the keypad code, and press the # key.

➤ To invoke Panel Card Events with Card ID:

1. The event's **Trigger Type** must be set to **Card/Keypad Code**.
2. To be able to invoke a Panel Card Event using Card ID at any time, set the terminal's **PIN Suppression Timezone** to **<0>**. Otherwise, the Panel Card Event will be invoked only during active timezones.
3. The terminal's **Card ID** flag must be set.
4. Make sure the terminal's **PIN Only** flag is *not* set.
5. Make sure the terminal's "**PIN + Card ID** flag is *not* set.
6. To activate event:

   Without the Star Feature, enter the Card ID number, press A, enter the keypad code, and press the # key.

   With the Star Feature, enter the Card ID number, press the star (*) key followed by number 1, enter the keypad code, and press the # key.

7. To deactivate event:

   Without the Star Feature, enter the Card ID number, press D, enter the keypad code, and press the # key.

   *With the Star Feature, ent*er the Card ID number, press the star (*) key followed by number 4, enter the keypad code, and press the # key.

➤ To invoke Panel Card Events with PIN and Card ID:

1. The event's **Trigger Type** should be set to **Card/Keypad Code** or **Card/PIN/Keypad Code**.
2. If set to **Card/PIN/Keypad Code**, the terminal's **PIN Suppression Timezone** must be set to an inactive timezone.
3. The terminal's **PIN + Card ID** flag must be set.
4. Make sure the terminal's **PIN Only** flag is *not* set.
5. To activate event:

   Without the Star Feature, enter PIN, enter the Card ID number, press A, enter the keypad code, and press the # key.

   With the Star Feature, enter PIN, enter the Card ID number, press the star (*) key followed by number 1, enter the keypad code, and press the # key.
6. To deactivate event:

   Without the Star Feature, enter PIN, enter the Card ID number, press D, enter the keypad code, and press the # key.

   With the Star Feature, enter PIN, enter the Card ID number, press the star (*) key followed by number 4, enter the keypad code, and press the # key.

➤ To invoke Panel Card Events with PIN and Badge:

1. The event's **Trigger Type** must be set to **Card/Keypad Code** or **Card/PIN/Keypad Code**.
2. The terminal's **PIN Suppression Timezone** must be set to an inactive timezone.
3. Make sure the terminal's **Allow PIN After Badge** flag is *not* set.
4. To activate event:

   Without the Star Feature, enter PIN, press A, enter the keypad code, and present the badge.

   With the Star Feature, enter PIN, press the star (*) key followed by number 1, enter the keypad code, and present the badge.
5. To deactivate event:

   Without the Star Feature, enter PIN, press D, enter the keypad code, and present the badge.

   With the Star Feature, enter PIN, press the star (*) key followed by number 4, enter the keypad code, and present the badge.

➤ **To invoke Panel Card Events with PIN and Badge, allowing PIN after badge:**

1. The event's **Trigger Type** must be set to **Card/Keypad Code** or **Card/PIN/Keypad Code**.
2. The terminal's **PIN Suppression Timezone** must be set to an inactive timezone.
3. The terminal's **Allow PIN After Badge** flag must be set.
4. To activate event:

   Without the Star Feature, enter PIN, press A, enter the keypad code, present the badge[1], and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 1, enter the keypad code, present the badge[1], and press the # key.
5. To deactivate event:

   Without the Star Feature, enter PIN, press D, enter the keypad code, present the badge[1], and press the # key.

   With the Star Feature, enter PIN, press the star (*) key followed by number 4, enter the keypad code, present the badge[1], and press the # key.

   [1] The badge can be presented at any time before the # key is pressed.

QUICK GUIDE TO USING KEYPAD READERS

Use the following quick guide to determine the key sequence at a keypad reader required for a particular action. This section assumes all terminal's and panel's settings have already been configured for this action.

NOTE

Use the terminal's Star Feature if you want to invoke Panel Card Events on a keypad that does not have the keys A and D.

Legend

Keypad Code	Enter the Keypad Code.	badge	Present the badge.
PIN	Enter the PIN number.	* 0 1 / # A D	Press the specified key.
Card ID	Enter the Card ID number.		
Minutes	Enter the number of minutes.		

Invoking Access Requests from a Keypad

With Badge

To request access: badge

With PIN Only

To request access: PIN #

With Card ID

To request access: Card ID #

With PIN and Card ID

To request access: PIN Card ID #

With PIN and Badge

To request access: PIN badge

With PIN and Badge, allowing PIN after Badge

To request access: PIN badge[1] #

[1] The badge can be presented at any time before the # key is pressed, that is, before, during or after the PIN is entered.

Invoking Air Crew Access Requests from a Keypad

To request access without Star Feature: B Air Crew PIN #

To request access with Star Feature: * 2 Air Crew PIN #

Invoking Timed Overrides from a Keypad

With Badge

To start override without Star Feature:	*		Minutes	badge
To stop override without Star Feature:	*		0	badge
To start override with Star Feature:	*	0	Minutes	badge
To stop override with Star Feature:	*	0		badge

With PIN Only

To start override without Star Feature:	PIN	*		Minutes	#
To stop override without Star Feature:	PIN	*		0	#
To start override with Star Feature:	PIN	*	0	Minutes	#
To stop override with Star Feature:	PIN	*	0		#

With Card ID

To start override without Star Feature:	Card ID	*		Minutes	#
To stop override without Star Feature:	Card ID	*		0	#
To start override with Star Feature:	Card ID	*	0	Minutes	#
To stop override with Star Feature:	Card ID	*	0		#

With PIN and Card ID

To start override without Star Feature:	PIN	Card ID	*		Minutes	#
To stop override without Star Feature:	PIN	Card ID	*		0	#
To start override with Star Feature:	PIN	Card ID	*	0	Minutes	#
To stop override with Star Feature:	PIN	Card ID	*	0		#

With PIN and Badge

To start override without Star Feature:	PIN	*		Minutes	badge
To stop override without Star Feature:	PIN	*		0	badge
To start override with Star Feature:	PIN	*	0	Minutes	badge
To stop override with Star Feature:	PIN	*	0		badge

With PIN and Badge, allowing PIN after Badge

To start override without Star Feature:	PIN	*		Minutes	badge[1]	#
To stop override without Star Feature:	PIN	*		0	badge[1]	#
To start override with Star Feature:	PIN	*	0	Minutes	badge[1]	#
To stop override with Star Feature:	PIN	*	0		badge[1]	#

[1] The badge can be presented at any time before the # key is pressed, that is, before, during or after the PIN and the Timed Override sequence are entered.

Invoking Panel Card Events from a Keypad

With Badge

To activate event without Star Feature:	A		Keypad Code	badge
To deactivate event without Star Feature:	D		Keypad Code	badge
To activate event with Star Feature:	*	1	Keypad Code	badge
To deactivate event with Star Feature:	*	4	Keypad Code	badge

With PIN Only

To activate event without Star Feature:	PIN	A		Keypad Code	#
To deactivate event without Star Feature:	PIN	D		Keypad Code	#
To activate event with Star Feature:	PIN	*	1	Keypad Code	#
To deactivate event with Star Feature:	PIN	*	4	Keypad Code	#

With Card ID

To activate event without Star Feature:	Card ID	A		Keypad Code	#
To deactivate event without Star Feature:	Card ID	D		Keypad Code	#
To activate event with Star Feature:	Card ID	*	1	Keypad Code	#
To deactivate event with Star Feature:	Card ID	*	4	Keypad Code	#

With PIN and Card ID

To activate event without Star Feature:	PIN	Card ID	A		Keypad Code	#
To deactivate event without Star Feature:	PIN	Card ID	D		Keypad Code	#
To activate event with Star Feature:	PIN	Card ID	*	1	Keypad Code	#
To deactivate event with Star Feature:	PIN	Card ID	*	4	Keypad Code	#

With PIN and Badge

To activate event without Star Feature:	PIN	A		Keypad Code	badge
To deactivate event without Star Feature:	PIN	D		Keypad Code	badge
To activate event with Star Feature:	PIN	*	1	Keypad Code	badge
To deactivate event with Star Feature:	PIN	*	4	Keypad Code	badge

With PIN and Badge, allowing PIN after Badge

To activate event without Star Feature:	PIN	A		Keypad Code	badge[1]	#
To deactivate event without Star Feature:	PIN	D		Keypad Code	badge[1]	#
To activate event with Star Feature:	PIN	*	1	Keypad Code	badge[1]	#
To deactivate event with Star Feature:	PIN	*	4	Keypad Code	badge[1]	#

[1] The badge can be presented at any time before the # key is pressed, that is, before, during or after the PIN and the Panel Card Event sequence are entered.