No part of this document may be reproduced without the prior permission of Johnson Controls, Inc.

If this document is translated from the original English version by Johnson Controls, Inc., all reasonable endeavors will be used to ensure the accuracy of translation. Johnson Controls, Inc. shall not be liable for any translation errors contained herein or for incidental or consequential damages in connection with the furnishing or use of this translated material.

Due to continuous development of our products, the information in this document is subject to change without notice. Johnson Controls, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with furnishing or use of this material. Contents of this publication may be preliminary and/or may be changed at any time without any obligation to notify anyone of such revision or change, and shall not be regarded as a warranty.

Other Manufacturers’ Documentation

Johnson Controls does not duplicate documentation of other equipment manufacturers. When necessary, Johnson Controls provides documentation that supplements that of other manufacturers. When unpacking your equipment, keep all original manufacturer documentation for reference.

Technical Support

For factory technical support, Johnson Controls authorized field technicians can contact Global Security Solutions by phone at (866) 893-0423 or (414) 524-1214, or by email at support.globalsecuritysolutions@jci.com. They can also call the Field Support Center at (800) 524-1330 or (414) 524-5000 and use options 6, 1, 7.

Customers who require technical support or who have other support needs (maintenance contracts or on-site field support) should contact their local Johnson Controls office; visit http://www.johnsoncontrols.com/content/us/en/locations.html to find your local office.

Acknowledgments

Metasys® and Johnson Controls® are trademarks of Johnson Controls, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

Declaration of Conformity

**United States:** This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**Canada:** CAN ICES-3 (B)/NMB-3(B)

**European Union:** This product complies with the requirements of the EMC Directive 2004/108/EC and the Low Voltage Directive 2006/95/EEC.

This equipment must not be modified for any reason and it must be installed as stated in the Manufacturer’s instructions. 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.
This product is listed under Underwriters Laboratories UL™ 1076 for Proprietary Burglar Alarm Units and Systems, UL 294 for Access Control Systems Units and Underwriters Laboratories of Canada ULC/ORD-C1076-86.

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 following elevator interfaces have not been investigated by Underwriters Laboratories: Kone, Otis, and ThyssenKrupp.
11. Do not connect equipment to an AC power source that is controlled by a switch.
TABLE OF CONTENTS

Chapter 1: Introduction
  Key Terms 1-1
  Unpacking the Equipment 1-4
  General Description 1-4
  CK721-A Module 1-5
  Enclosures 1-5
  Modules 1-6
  Additional Equipment 1-6
  CK721-A System Specifications (All Panels) 1-7
  CK721-A Panel Configuration 1-8
  Network Communications 1-12
  PIV and PIV-I Smart Card (128-bit) Support 1-17
  HID Hardware PAM (M2000) Solution 1-18
  HID PIV/PIV-I Reader Connecting to RDR2S-A or RDR8S Solution 1-19
  OSDP Reader Support 1-21

Chapter 2: CK721-A and S300 DIN Enclosures
  CK721-A 2-1
  Large Enclosure (S300-DIN-L) 2-10
  Small Enclosure (S300-DIN-S) 2-14
  No Enclosure 2-17
  +24 VDC Connector 2-18

Chapter 3: S300 Expansion Enclosures
  S300-DIN Enclosures 3-1
  S300 Expansion Enclosures 3-1

Chapter 4: User Interface
  Important Notes 4-1
  Notes on Encryption 4-2
  Principle of Operation 4-2
  Basic Panel Configuration 4-11
TABLE OF CONTENTS

Direct Programming of the CK721-A  4-14

Chapter 5: Maintenance
   Routine Maintenance  5-1
   Impaired Performance Conditions  5-1
   Testing Procedure  5-2
   Field Servicing  5-3
   Troubleshooting  5-3

Appendix A: Expanded Address S300 Bus

Appendix B: Performance Analysis

Appendix C: Grounding and Connectors
   Cable Grounding  C-1
   Card Reader Unit Grounding  C-5

Appendix D: Door Open/Aux Access Supervision
   Purpose of Supervised Inputs  D-1
   Configuring the S300-SIO8  D-1
   Wiring to the Reader Module  D-2

Appendix E: Database Flash Backup from the Host

Appendix F: Using a Keypad Reader on a Panel
   Invoking Access Requests from a Keypad  F-1
   Invoking Air Crew Access Requests from a Keypad  F-2
   Invoking Timed Overrides from a Keypad  F-3
   Invoking Panel Card Events from a Keypad  F-7
   Quick Guide to Using Keypad Readers  F-11

Appendix G: Configuring SSH and SFTP Clients
   PuTTY Client  G-1
   WinSCP Client  G-7

Appendix H: Wiring Concepts
   Wiring Readers  H-1
1. INTRODUCTION

This chapter provides a general description of the CK721-A panel and related equipment.

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: 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. They also contain information on the expanded address S300 bus configuration with related performance analysis. The SSH and SFTP client configuration is explained as well.

**NOTE:** Some features described in this manual are available depending on the firmware version of your controller. For details, refer to the *CK721-A Software Release Notes*.

**KEY TERMS**

**NOTE:** Throughout this manual, the S300-DIN modules and the S300 modules are also referred to by their short name version. Refer to Modules on page 1-6 for details.
The following terms are used throughout this manual:

- **Access Control System (ACS)** – In general terms, an access control system controls access to a location or a resource. When used in conjunction with a P2000 integration, the access control system includes the P2000 Server and the CK721-A devices.


- **Cardholder** – An individual that has rights in the security system. The individual typically possesses a badge (for example, an ID card) that is used to gain access to physical areas of a facility.

- **CHUID** – Cardholder Unique Identifier.

- **CK721-A System** – This is a general term that refers to a combination of CK721-A terminals and expansion enclosures that communicate with the P2000 system.

- **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 modules

- **DCS** – Destination Selection Control Terminal.

- **Encryption** – The process of changing data into a form that can be read only by the intended receiver. To decrypt the message, the receiver of the encrypted data must have the proper decryption key (generally protected by a strong password). P2000 v3.11 encryption is implemented using the FIPS 140-2, validated, certificate number 1336, cryptographic module, from Microsoft (www.microsoft.com). CK721-A encryption is implemented using the FIPS 140-2, validated, certificate number 1051, cryptographic module, version 1.2.3, from the Open Source Software Institute (www.oss-institute.org).

- **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.
• **FASC-N** – Federal Agency Smart Credential Number.
• **FICAM** – Federal Identity Credential and Access Management.
• **File Transfer Protocol (FTP)** – A standard network protocol used to transfer files from one host to another over a TCP-based network.
• **GUID** – Global Unique Identifier.
• **IPv4** – Internet Protocol version 4.
• **IPv6** – Internet Protocol version 6.
• **LCS** – Lift Control System (from ThyssenKrupp).
• **Modules** – The modules provide additional reader interfaces, input points, or output relays to the CK721-A system. Modules can be installed in the S300 expansion enclosures; RDR2S, RDR2S-A, I8O4, RDR8S, and I32O16 modules can be installed in the S300-DIN enclosures.
• **OTIS EMS** – OTIS (High Level Interface) Elevator Management System, serial.
• **PACS** – Physical Access Control System.
• **PAM** – HID pivCLASS Authentication Module.
• **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.
• **PIN** – Personal Identification Number.
• **PIV** – Personal Identity Verification.
• **PIV-I** – Personal Identity Verification - Interoperable.
• **Secure FTP (SFTP)** – A program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. It is functionally similar to FTP, but because it uses a different protocol, you can't use a standard FTP client to talk to an SFTP server, nor can you connect to an FTP server with a client that supports only SFTP.
• **Secure Shell (SSH)** – A network protocol that allows data to be exchanged using a secure channel between two networked devices.
• **Telnet** – A network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection.
• **ThyssenKrupp Serial Elevator** – ThyssenKrupp High Level Interface Elevator Access Control, serial.
• **User Interface** – The CK721-A User Interface provides access to the CK721-A panel configuration graphical user interface (GUI) via a serial
connection to a laptop (or other computer) running common terminal emulation software or via a Telnet/SSH/SFTP network connection.

- **UUID** – Universal Unique Identifier.

**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 P2000 system. The CK721-A is intended to be mounted in an S300-DIN enclosure (large or small). Each model has a total capacity 200,000 cards and a 8000 off-line transaction base memory.

---

**NOTE:** When the number of badges exceeds 120,000, the number of access groups should be limited to 50,000.

---

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 P2000. 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 modules 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 modules is accomplished via RS-485 per Cardkey implementation.
The CK721-A uses the following modules:

- RDR2S-A
- I8O4
- RDR8S
- I32O16

**CK721-A Module**

Table 1-1: CK721-A

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CK721-A</td>
<td>A CK721-A module. Total storage capacity: 200,000 cards and 8,000 off-line transactions. <strong>Note</strong>: When the number of badges exceeds 120,000, the number of access groups should be limited to 50,000.</td>
</tr>
</tbody>
</table>

**Enclosures**

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

Table 1-2: S300 and S300-DIN Enclosures

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S300-DIN-S</td>
<td>A small enclosure containing a DIN rail, a tamper switch and a power supply. It has room for one controller (CK721-A, or S300-DIN-RDR2SA) and for a battery back-up unit.</td>
</tr>
<tr>
<td>S300-DIN-L</td>
<td>A large enclosure containing DIN rails, a tamper switch and a power supply. It has room for up to three modules (CK721-A, RDR2S-A, or a combination thereof), and for a battery back-up unit.</td>
</tr>
<tr>
<td>S300-XL</td>
<td>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.</td>
</tr>
<tr>
<td>S300-XS</td>
<td>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.</td>
</tr>
</tbody>
</table>
MODULES

See Table 1-3 for a description of reader and I/O modules.

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S300-XXS</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Table 1-3: S300 and S300-DIN Enclosures

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S300-DIN-RDR8S</td>
<td>Stand-alone unit with removable connectors which can be mounted on a DIN rail or on a flat surface. The unit supports up to eight readers. This module is also referred to as the RDR8S.</td>
</tr>
<tr>
<td>S300-DIN-I32O16</td>
<td>Stand-alone unit with removable connectors which can be mounted on a DIN rail or on a flat surface. The unit supports up to 32 4-state inputs and 16 outputs. This module is also referred to as the I32O16.</td>
</tr>
<tr>
<td>S300-DIN-RDR2SA</td>
<td>Stand-alone unit with removable connectors which can be mounted on a DIN rail or on a flat surface. The unit supports up to two readers. This module is also referred to as the RDR2S-A.</td>
</tr>
<tr>
<td>S300-DIN-I8O4</td>
<td>Stand-alone unit with removable connectors which can be mounted on a DIN rail or on a flat surface. The unit supports up to 8 4-state inputs and 4 outputs. This module is also referred to as the I8O4.</td>
</tr>
</tbody>
</table>
ADDITIONAL EQUIPMENT

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

Table 1-4: Additional Equipment

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

CK721-A SYSTEM SPECIFICATIONS (ALL PANELS)

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

Table 1-5: CK721-A System Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambient Temperature</td>
<td>32 to 122 °F (0 to 50° C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>20% to 80% non-condensing</td>
</tr>
<tr>
<td>Ventilation</td>
<td>Cabinets require free movement of air over all exposed surfaces</td>
</tr>
<tr>
<td>S300-DIN-L</td>
<td>16x20x6.6 in (41x51x17 cm) Approximate weight: fully loaded 45lb (20 kg)</td>
</tr>
</tbody>
</table>
CK721-A Installation and Operation

Introduction

Table 1-5: CK721-A System Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>S300-DIN-S</td>
<td>12x12x6 in (30x30x15 cm) Approximate weight: fully loaded 24lb (11 kg)</td>
</tr>
<tr>
<td>S300-XL</td>
<td>21x16x5.5 in (53x41x14 cm) Approximate weight: fully loaded 33lb (15 kg)</td>
</tr>
<tr>
<td>S300-XS</td>
<td>16x13.5x5.5 in (41x34x14 cm) Approximate weight: fully loaded 22lb (10 kg)</td>
</tr>
<tr>
<td>S300-XXS</td>
<td>13x9x5.5 in (39x27x14 cm) Approximate weight: fully loaded 10lb (4.5 kg)</td>
</tr>
<tr>
<td>Cabling</td>
<td>Described in Chapter 2 and Chapter 3.</td>
</tr>
<tr>
<td>Backup Battery</td>
<td>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.</td>
</tr>
</tbody>
</table>

CK721-A PANEL CONFIGURATION

Each CK721-A can support up to 64 logical terminal numbers assigned to reader modules and I/O modules.

Expanded Address S300 Bus Configuration

The expanded address S300 bus configuration requires the use of the following hardware module types:

- RDR2S-A
- I8O4
- RDR8S
- I32O16

For optimum 64 terminal access grant response time, only (RDR2S-A, I8O4, RDR8S, I32O16) hardware module types should be used. Legacy Reader and Legacy I/O hardware module types, RDR2, IO8, I16, SI08, SI8, and RDR2S, have a significant impact on access grant times, and should not be used under the expanded address S300 bus configuration.
See Appendix A: Expanded Address S300 Bus for further details on the expanded address S300 bus configuration and programming.

**NOTE:** For fastest response times, the terminals should be defined on as few S300 modules as possible, and all S300 modules should be operating in physical addressing mode. The typical response time to an access request in an idle CK721-A with 64 terminals on 8 RDR8S modules is less than 500 ms. The typical response time to an access request in an idle CK721-A with 64 terminals on 32 RDR2S-A modules is less than 1s. See Appendix B: Performance Analysis for details.

---

**Legacy Address S300 Bus Configuration**

Each CK721-A can support up to 16 logical terminal numbers assigned to reader modules, and up to 16 logical terminal numbers assigned to I/O modules.

Therefore, a CK721-A supports up to 24 hardware modules within the following parameters:

- A maximum of eight RDR2 or RDR2S reader modules can be connected to a single CK721-A for a maximum of 16 readers per CK721-A.

- All 16 logical terminal numbers apply only to IO8 and I16 hardware modules. If you are using SIO8 or SI8 hardware modules (supervised, 4-state alarms), you can only use logical terminal numbers 1 through 8; logical terminal numbers 9 through 16 will be invalid.

**IMPORTANT:** Version 3.13 P2000 software does not support legacy address S300 bus hardware modules. Refer to the Version 3.13 P2000 installation and user manuals for more information.

---
System Configuration Example

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 P2000 server 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 P2000 server 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:

- 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 P2000 server and the last CK721-A panel in the network.
- The maximum segment length is 328 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.
Figure 1-2 illustrates the 4x5 rule.

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

**NETWORK COMMUNICATIONS**

The CK721-A panels communicate with the P2000 server 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 P2000 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.

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 P2000 server 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 P2000 system 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 P2000 communicates with terminals that provide reader interfaces, input points, or output relays. Communication is bi-directional. Some messages are sent from the P2000 server to the field panels, and others are sent from the panels to the server, and then forwarded to P2000 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 P2000 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.


CK721-A/P2000 Server Encrypted Communications

This feature provides encrypted network communications between the CK721-A controller and the P2000 Server, using the Advanced Encryption Standard (AES256).

The CK721-A Encryption is implemented using the Federal Information Processing Standards (FIPS) 140-2, validated (Certificate #1051), cryptographic module (version 1.2.3) from the Open Source Software Institute (http://www.oss-institute.org).
The following network communications channels are encrypted:

- Priority
- Upload
- Download

![Diagram of CK721-A/P2000 Server Encrypted Communications]

**To enable encryption between the CK721-A controller and the P2000 Server:**

1. At the P2000 Server (see the P2000 Software User Manual for details):
   - In the Edit Panel dialog box, under the Encryption tab, enter a value for the encryption key. The value must be unique for each CK721-A controller.
   - After entering the key, enable the encryption.

2. At the CK721-A controller:
   - Log in with user name **CK720** and password **master**.
   - On page 3 of the Panel dialog, enter a unique encryption key value.
   - After entering the key, enable the encryption.
   - Perform the “write to flash” operation.
NOTE: The FIPS encryption package validation process requires a reboot of the controller after turning the encryption on or off. The FIPS Encryption validation process takes about 10-20 additional minutes to complete the controller reboot. All controller functions are disabled during that time.

NOTE: For the CK721-A controller to come on-line with the P2000 Server, the encryption key values at the CK721-A controller and at the P2000 server must match, and the encryption must be enabled at both sides.

NOTE: When encryption is enabled, Telnet and FTP network connections are rejected by the CK721-A controller.

NOTE: Administrator should change the CK721-A controller login password for CK721-A controllers that have Encryption enabled.

When encryption is enabled, the following methods are supported for CK721-A controller login connections:

- Secure Shell Telnet Client (SSH)
- Secure FTP Client (SFTP)
- Serial Port (RS-232C, Port A). Serial communications between the CK721-A controller and the PC are not encrypted.

See Appendix G: Configuring SSH and SFTP Clients for details on the SSH and SFTP connection methods.

When encryption is disabled, the following methods are supported for CK721-A controller login connections:

- Telnet client
- FTP client
- Serial Port (RS-232C, Port A)
PIV and PIV-I Smart Card (128-bit) Support

The CK721-A controller and P2000 host support PIV and PIV-I government 128-bit smart cards per FIPS-201.

The PACS management of PIV and PIV-I smart cards is split between the pivCLASS Management Station software suite and the P2000 host. The pivCLASS Management Station software also provides PAM configuration services, user credential management services, and event reporting services.

128-Bit Badge Number Requirements

The PACS stores and processes the full 32-digit FASC-N in order to be FICAM certified. PACS panel accepts and processes either a 128-bit (TIG-SCEPACS 2.3) FASC-N or a 128-bit BCD representing the FASC-N.

For PIV-I credentials to be used with the PACS, the PACS must be able to store and process the entire 128-bit GUID as the card identifier.

The following Smart Card reader output formats are supported:

- 128-bit BCD MSB representation of PIV FASC-N
- 128-bit binary representation of PIV-I and CIV GUID

HID pivCLASS PIV/PIV-I Readers

HID supports a heterogeneous PIV/PIV-I access control environment under the pivCLASS Authentication module and pivCLASS smart readers.

The CK721-A v3.2 controller supports the HID pivCLASS Authentication Module (PAM), HID pivCLASS PIV/PIV-I “PAM Compatible (Core Street Reader Protocol, Full-Duplex, 4-wire)” smart readers, and HID pivCLASS PIV/PIV-I “Wiegand Configured (Half Duplex, 2-wire)” smart readers, from HID.

**NOTE:** HID pivCLASS PIV/PIV-I “OSDP v1.1 Configured (Half Duplex, 2-wire)” smart readers are currently not orderable from HID and are not supported.

The pivCLASS PAM HID Model M2000 and pivCLASS PAM-compatible readers are installed on sites that are FICAM compliant. In such a configuration, the pivCLASS PAM is configured for 128-bit badge data.
The HID pivCLASS PIV/PIV-I “Wiegand Configured (Half Duplex, 2-wire)” smart readers are used on sites that provide PIV/PIV-I card basic access control (no validation of user credentials) and do not have to be FICAM compliant.

In such a configuration, the pivCLASS PIV/PIV-I “Wiegand Configured (Half Duplex, 2-wire)” smart reader is configured for 128-bit badge data. (You must select Wiegand Bit Stream length at time of reader order or have access to a HID Reader Configuration card that sets the Wiegand Bit Stream length.)

**HID HARDWARE PAM (M2000) SOLUTION**

The HID Global pivCLASS Authentication Module (PAM) solution allows organizations to upgrade existing Physical Access Control Systems (PACS) to full HSPD-12 compliance with all the functionality defined in FIPS-201 and associated publications. HSPD-12 compliance supports verification of the PIV card and PIV-Interoperable (PIV-I) card types.

The PAM (M2000) validates the user credentials at the time of access. This validation confirms the card is not counterfeit, cloned, copied, lost, or stolen. NIST FIPS 201 and SP 800-116 define specific authentication mechanisms and their application to authenticate PKI-based credentials for access to uncontrolled, controlled, limited, and exclusion areas.

The PAM (M2000) is installed between a PACS panel and up to two pivCLASS PAM compliant PIV/PIV-I smart card readers. The PAM validates the smart card and sends the card’s derived 128-bit badge ID to the PACS.

The PACS interface to the PAM (M2000) is formed by the CK721-A controller as well as the RDR8S or RDR2S-A module. The PAM Wiegand port is connected to the RDR2S-A module or RDR8S module Wiegand port. The PAM sends the card derived 128-bit badge ID to the RDR2S-A module or RDR8S module via the PAMs Wiegand output port, which is connected to the RDR2S-A module or RDR8S module Wiegand interface.

The RDR2S-A module or RDR8S module sends the card derived 128-bit badge ID bit stream to the CK721-A controller. The CK721-A controller performs an access decision driven by the 128-bit badge ID. (If the CK721-A reader terminal is in Shared mode and the 128-bit badge ID is not in the CK721-A badge database or the reader terminal is in Central mode, the P2000 Server will make the access decision.)
The result of the CK721-A controller access decision is reported to the P2000 Server.

**HID PIV/PIV-I Reader Connecting to RDR2S-A or RDR8S Solution**

This solution can apply to:

- HID pivCLASS PIV/PIV-I Wiegand Readers connected to RDR2S-A or RDR8S module in Wiegand mode

This smart card solution does not meet the FICAM system compliance requirements. The PIV card or PIV-I card credential is not validated during the access decision process.
The PACS interface to the pivCLASS PIV/ PIV-I Reader is formed by the CK721-A controller plus an RDR8S module or an RDR2S-A module. The pivCLASS PIV/ PIV-I Wiegand Reader is connected to the RDR2S-A module or RDR8S module via the Wiegand terminal port.

The CK721-A controller performs an access decision driven by the 128-bit badge ID. (If the CK721-A reader terminal is in Shared mode and the 128-bit badge ID is not in the CK721-A badge database or the reader terminal is in Central mode, the P2000 Host will make the access decision.)

The result of the CK721-A controller access decision is reported to the P2000 Host. See Figure 1-5 for more information.

Note: The RDR2S-A can support up to two OSDP readers or two Wiegand readers. You cannot mix the two types of reader with an RDR2S-A.

Figure 1-5: System with P2000 and CK721-A Controller
OSDP Reader Support

The OSDP Reader feature supports the use of HID OSDP Keypad Readers type and HID OSDP Reader type (no keypad).

The OSDP Reader feature:

- Adds Open Supervised Device Protocol (OSDP) v1.1 reader device support.

Note: The RDR2S-A can support up to two OSDP readers or two Wiegand readers. You cannot mix the two types of reader.

Figure 1-6: System Diagram

- In order to support OSDP readers, the RDR2S-A DIP switch must be set for RS485 and both readers connected to the RDR2S-A terminal must be of the same type.
- The OSDP reader implementation supports unencrypted communications between the RDR2S-A and OSDP device.
2. **CK721-A AND S300 DIN ENCLOSURES**

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

**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  Multiple use: Transaction logger port or KONE serial server elevator or OTIS serial server elevator controller communications port or ThyssenKrupp serial server communications port to elevator management system
  - RS485A  OTIS BMS elevator communication
  - 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

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER</td>
<td>ON steady when power is applied.</td>
</tr>
<tr>
<td>FAULT</td>
<td>OFF to indicate normal operation. ON indicates a general fault.</td>
</tr>
<tr>
<td>RS485 A</td>
<td>Flashes/flickers to indicate data transmit.</td>
</tr>
<tr>
<td>RS485 B</td>
<td>Flashes/flickers to indicate data transmit.</td>
</tr>
</tbody>
</table>
**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.

**Setting the End-of-Line Switch**

Network devices at either end of the RS485 network must be set as network terminated devices. This is done with the use of the End-of-Line (EOL) switch. The CK721-A module has two EOL switches, one for each RS485 connector. The CK721-A is shipped with the EOL switches in the factory default position, which is on (up).

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETHERNET</td>
<td>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.</td>
</tr>
<tr>
<td>10/LINK</td>
<td>ON to indicate 10 Mbit connection is established.</td>
</tr>
<tr>
<td>100/LINK</td>
<td>ON to indicate 100 Mbit connection is established.</td>
</tr>
<tr>
<td>RUN</td>
<td>This LED is currently not used (always OFF).</td>
</tr>
</tbody>
</table>

Table 2-1: CK721-A LED Functions

- **RS485 A**
- **RS485 B**
- EOL switch for RS485 A
- EOL switch for RS485 B
The CK721-A modules follow the same rules as other terminated device. See the figure below to determine the appropriate EOL switch setting for all CK721-A modules in your network and set the EOL switch to the appropriate position for each CK721-A.

**Note:** Before changing the EOL position, remove the 24VDC supply power to the CK721-A and wait for the RUN LED to go off.
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.

**IMPORTANT:** 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-A. If AC power or backup battery power is not supplied before you remove the lithium battery, the realtime clock will be incorrect.

**CAUTION:** Risk of Explosion.
Replace the battery with a lithium battery of the same type and voltage rating. Dispose of the used battery in accordance with local, national, and regional regulations. Failure to replace the battery with one of the same type and voltage rating may result in an explosion causing personal injury and property damage.
Input Power

The input power is described in the following table:

Table 2-2: Input Power

<table>
<thead>
<tr>
<th>Inputs</th>
<th>V Min</th>
<th>V Nom</th>
<th>V Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>+24VDC</td>
<td>20</td>
<td>24</td>
<td>30</td>
</tr>
</tbody>
</table>

RS485

CK721-A has two RS485 ports:

- RS485A is used by OTIS BMS elevator communications
- RS485B is used to communicate with external devices such as RDR8S, I32O16, RDR2S-A and I8O4

**NOTE:** The following modules can be assigned to logical terminals 1 though 64: RDR8S, I32O16, RDR2S-A, and I8O4.

The controller can communicate on the RS485 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 show shows the wiring between RS485B and the devices.

![Figure 2-1: Wiring Between RS485B and RDR2S-A Module](image)
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, the power supply output voltage is high, or the power supply is over the allowed temperature.

  For wiring details see Figure 2-2.

- 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 P2000 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 2-3: Hub to CK721-A Wiring

RS232

CK721-A has two RS232 connectors: RS232C A and RS232C B.

Table 2-3: RS232 Connectors

<table>
<thead>
<tr>
<th>Description</th>
<th>RS232C A</th>
<th>RS232C B</th>
</tr>
</thead>
</table>
| Port use                        | Connects to a terminal emulator              | Dual use. Connects to either: data logger device  
|                                 |                                               | KONE elevator controller interface            |
| Default communication parameters| 115000 bps  
No parity  
8 bits per character  
One stop bit  
No control flow  
CR (Carriage Return) | 57600 bps  
No parity  
8 bits per character  
One stop bit  
No control flow  
CR/LF (Carriage Return/ Linefeed) |
The two RS-232 ports have the following pinout:

### Table 2-4: RS232 Ports Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Carrier Detection</td>
<td>(In)</td>
</tr>
<tr>
<td>2</td>
<td>Receive Data</td>
<td>(In)</td>
</tr>
<tr>
<td>3</td>
<td>Transmit Data</td>
<td>(Out)</td>
</tr>
<tr>
<td>4</td>
<td>Data Terminal Ready</td>
<td>(Out)</td>
</tr>
<tr>
<td>5</td>
<td>Signal ground</td>
<td>n/a</td>
</tr>
<tr>
<td>6</td>
<td>Data Set Ready</td>
<td>(In)</td>
</tr>
<tr>
<td>7</td>
<td>Request to Send</td>
<td>(Out)</td>
</tr>
<tr>
<td>8</td>
<td>Clear to Send</td>
<td>(In)</td>
</tr>
<tr>
<td>9</td>
<td>Ring Indicator</td>
<td>(In)</td>
</tr>
</tbody>
</table>

**RS232 Serial Null Modem Cable Wiring**

The null modem cable provides an RS232 serial connection from the CK721-A RS232C A port to the computer’s COM port.

### Table 2-5: Connectors Pinout

<table>
<thead>
<tr>
<th>Connector 1 Pinout</th>
<th>Connector 2 Pinout</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 TX</td>
<td>2 RX</td>
</tr>
<tr>
<td>2 RX</td>
<td>3 TX</td>
</tr>
<tr>
<td>7 RTS</td>
<td>8 CTS</td>
</tr>
<tr>
<td>8 CTS</td>
<td>7 RTS</td>
</tr>
<tr>
<td>5 SG</td>
<td>5 SG</td>
</tr>
<tr>
<td>6 DSR</td>
<td>4 DTR</td>
</tr>
<tr>
<td>4 DTR</td>
<td>6 DSR</td>
</tr>
</tbody>
</table>

Where:
- TX=Transmit
- RX=Receive
- RTS=Request to Send
- CTS=Clear to Send
- SC=Signal Ground
- DSR=Data Set Ready
- DTR=Data Terminal Ready
The minimum required connections to a standard laptop/serial DB9 port are:

Table 2-6: RS232A to DB9 Connection

<table>
<thead>
<tr>
<th>RS232A at the CK721-A</th>
<th>Serial Port at the PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 RX</td>
<td>3 TX</td>
</tr>
<tr>
<td>3 TX</td>
<td>2 RX</td>
</tr>
<tr>
<td>5 SG</td>
<td>5 SG</td>
</tr>
</tbody>
</table>

Where:
TX=Transmit
RX=Receive
SC=Signal Ground

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

Figure 2-4 gives you an overview of the large enclosure with all components installed. The modules shown here are RDR2S-A.
The figure below depicts the CK721-A module mounted alone.

![Figure 2-5: One CK721-A Module Mounted in a Large Enclosure](image)

The figure below depicts the CK721-A module mounted with the RDR2S-A modules.

![Figure 2-6: One CK721-A Module and Two RDR2S-A Modules Mounted in a Large Enclosure](image)
Wiring CK721-A and Modules

**CK721-A Cable Requirements**

Table 2-7: Cable Requirements

<table>
<thead>
<tr>
<th>Description</th>
<th>Recommended Cable Type</th>
<th>Maximum Segment Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>+24VDC</td>
<td>Listed, 18 AWG, Stranded, Hook-up wire.</td>
<td>Limited to within cabinet</td>
</tr>
<tr>
<td>RS485 A and RS485 B</td>
<td>Listed, 22 AWG, Stranded, Hook-up wire.</td>
<td>Limited to within cabinet</td>
</tr>
<tr>
<td></td>
<td>Listed, 18 AWG, 3-cond, stranded, shielded.</td>
<td>4000 ft (1215 m). All modules connected to a single CK721-A panel must be within 4000 feet of the panel.</td>
</tr>
<tr>
<td>Inputs ICOM1 and ICOM2</td>
<td>Belden 88442, 1 twisted pair, 22 AWG.</td>
<td>500 ft (152m)</td>
</tr>
<tr>
<td>Output/Relay OUT1</td>
<td>Belden 8461, 1 twisted pair, 18 AWG.</td>
<td>Depends on power requirements of the door strike. Voltage to the strike must not be reduced more than 10% over the 18 AWG wire.</td>
</tr>
<tr>
<td>RS232 A</td>
<td>Listed DB9 F/F AT Null Modem</td>
<td>25 ft (7m). Cable must remain in the same room as the CK721-A.</td>
</tr>
<tr>
<td>RS232 B¹</td>
<td>Listed DB9 F/F AT Null Modem</td>
<td>25 ft (7m). Cable must remain in the same room as the CK721-A.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Listed, Category 5, 24 AWG, solid, 2 pair or 4 pair type.</td>
<td>328 ft (100 m). Cable, RJ45 connector, and RJ45 crimp tool to be supplied by customer.</td>
</tr>
</tbody>
</table>

¹. For KONE elevator wiring diagram see Figure 4-7 on page 4-47.

**Chain Module Wiring**

When connecting more than one module, wire the modules in parallel following the “daisy chain” pattern, as shown in Figure 2-7. For wiring
details refer to the documentation provided with the S300-DIN module.

**Figure 2-7: Daisy Chain Module Wiring for S300-DIN-L**

**IMPORTANT:** Do not connect the DC power cable to the reader unit 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.

**IMPORTANT:** 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 C: 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 \( \equiv \).

**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 CK721-A or a S300-DIN module (RDR8S, I32O16, RDR2S-A, or I8O4). The enclosure can also hold a backup battery unit composed of two 12V lead-acid batteries in one battery bracket.
Figure 2-8 gives you an overview of the small enclosure with all components installed. The module shown here is RDR2S-A.

Figure 2-8: 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 hardware module.

2. Verify the wire connection between the power supply and its standoff.

To verify chassis ground:

1. Verify the wire connection between the hardware module’s 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 following figure depicts one CK721-A module in a small enclosure.

![Figure 2-9: One CK721-A Module Mounted in a Small Enclosure](image)

**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.

**IMPORTANT:** 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 C: 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 2-10: CK721-A Module Mounted on a DIN Rail.](image)

**+24 VDC Connector**

Connects to the RDR8S, I32O16, RDR2S-A, I8O4

![Figure 2-11: +24 VDC Connector (Part of the DC Power Harness)](image)
Power Wiring

For power wiring with either the large or small enclosure, use the cable assembly shown in Figure 2-11. To construct the power wiring, use 18AWG wires.

When connecting multiple CK721-A controllers or S300-DIN modules, wire the modules in parallel following the “daisy chain” pattern as shown in Figure 2-12. For details on wiring multiple modules, refer to the documentation provided with the S300-DIN module.

---

Ground Wiring

For ground wiring with the either large or small enclosure, use the cable assembly shown in Figure 2-11. 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 CK721-A to multiple S300-DIN modules, wire them in parallel following the “daisy chain” pattern as shown in Figure 2-12. For wiring details refer to the documentation provided with the S300-DIN module.

To construct the ground wiring, use 18AWG wires.
3. **S300 EXPANSION ENCLOSURES**

For details on configuring the modules for the expanded address S300 bus configuration see the following documentation:

- **Appendix A: Expanded Address S300 Bus** of this manual
- P2000 Software User Manual for P2000 v.3.12 or higher
- S300-DIN-RDR8S and S300-DIN-I32O16 Hardware Installation Manual
- S300-DIN-RDR2SA and S300-DIN-I8O4 Hardware Installation Manual
- S300-DIN-RDR2SA Address Mode Configuration Technical Bulletin

**S300-DIN ENCLOSURES**

The S300-DIN enclosures (S300-DIN-L and S300-DIN-S) are used to host additional RDR2S-A, RDR8S, I8O4 and I32O16 modules in the CK721-A system. Refer to the S300-DIN-L Hardware Installation Manual or S300-DIN-S Hardware Installation Manual for information on mounting the modules in these enclosures.

**S300 EXPANSION ENCLOSURES**

The S300 expansion enclosures (S300-XL, S300-XS, and S300-XXS) are used to host additional legacy modules in the CK721-A system. They cannot, however, be used with the CK721-A controller itself, because they do not have the DIN rails and power supply necessary for its use. Refer to the Version 3.1 CK721-A Installation and Operation manual (24-10349-8) for more information about expansion enclosures and legacy modules.
4. 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 P2000 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 (default value: 192.168.2.2)
- Enter the netmask of the CK721-A (default value: 255.255.255.0)
- Enter the IP address of the P2000 server (default value: 192.168.2.1)
- Configure the Download Port Number, Upload Port Number, and Priority Port Number
- If using encrypted communications, first enter the encryption key and then enable the encryption (in order to enable the encryption you must also perform “write to flash”)
- 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 P2000.

IMPORTANT NOTES

- As a security precaution, Johnson Controls strongly suggests changing the default controller password during the installation process.
- The CK721-A panel must be set up first using Terminal Emulation, before setting up the panel from the P2000 server. Once the IP addresses are assigned at the panel, they cannot be changed from the P2000 server.
- The CK721-A controller user interface may become unresponsive during controller database download operations. The controller database download can take several minutes to hours to complete, during which the responsiveness of user interface will be slow. After the controller interface database download has completed, the responsiveness of the user interface will operate normally.
- Do not attempt modifications to the controller database during controller database download operations.
• The CK721-A controllers have a C and a factory default host IP address. They allow the configuration of the CK721-A controller operational parameters via an Ethernet cross-over cable connected to the Ethernet port. The default values for the controller IP addresses and network mask are set at the factory or after a Clear Database/Write To Flash commands. The default values are:

<table>
<thead>
<tr>
<th>IP Address/Network Mask</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller IP Address</td>
<td>192.168.2.2</td>
</tr>
<tr>
<td>Controller Network Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Host IP Address</td>
<td>192.168.2.1</td>
</tr>
</tbody>
</table>

**NOTES ON ENCRYPTION**

When encryption is enabled, the following methods are supported for CK721-A controller login connections:

• Secure Telnet Client (SSH). See Appendix G for setup guide.
• Secure FTP Client (SFTP). See Appendix G for setup guide.
• Serial Port (RS-232C, Port A). Serial communications between the CK721-A controller and the PC are not encrypted.

See Appendix G: Configuring SSH and SFTP Clients for details on the SSH and SFTP connection methods.

When encryption is disabled, the following methods are supported for CK721-A controller login connections:

• Telnet Client
• FTP Client
• Serial Port (RS-232C, Port A)

**PRINCIPLE OF OPERATION**

During normal operation, CK721-A panels are configured using the P2000 software. When a controller is defined at the P2000 server, 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 P2000 software should be used to configure CK721-A controllers.

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 P2000.

**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 or a cross-over Ethernet cable
- Terminal emulation software

![Figure 4-1: CK721-A Controller/P2000 Host Connection Methods](image)
Using your Terminal Emulation

To start communication:

1. Connect the cables, according to the connection method you will be following:
   - Serial cable between RS232C A (J3) of the CK721-A controller and your laptop or PC serial port, or
   - Ethernet cable (see Table 4-1 for default IP addresses and network mask information)

2. Start your terminal emulator software.

3. Configure the communications parameters within your VT100 terminal emulation software to match the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Type</td>
<td>VT100</td>
</tr>
<tr>
<td>Port</td>
<td>COMn</td>
</tr>
<tr>
<td>Baud Rate</td>
<td>115K</td>
</tr>
<tr>
<td>Data</td>
<td>8 bit</td>
</tr>
<tr>
<td>Parity</td>
<td>none</td>
</tr>
<tr>
<td>Stop</td>
<td>1 bit</td>
</tr>
<tr>
<td>Flow Control</td>
<td>none</td>
</tr>
</tbody>
</table>

4. At the login prompt, type **CK720** and press <**Enter**>.

5. Type your password when prompted. (The 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.

• <Cal.>: The Calibrate command issued from the User Interface (see the screen on page 4-93) will initiate input calibration at the S300-DIN module. When the S300-DIN module 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.

• <CalRes.>: The Uncalibrate command issued from the User Interface (see the screen on page 4-93) will initiate calibration of selected inputs using the resistor connected across CAL terminals. This command is used with the S300-DIN modules.

• <Uncal.>: The Uncalibrate command issued from the User Interface (see the screen on page 4-93) will initiate input uncalibration at the S300-DIN module. When the S300-DIN module 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 and route parameters will be lost after a power cycle.

Write to flash commands must be issued after:

• Adding or deleting non-legacy input or output point(s) to the CK721-A database configuration.

• Adding or deleting a non-legacy terminal to the CK721-A database configuration.

• Modifying general terminal properties of an existing non-legacy terminal (with the exception of the name of the terminal).
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 and route parameters (if applicable) as described in “Basic Panel Configuration” on page 4-11.

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 P2000.

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 the recommended Static Route:

1. From the Main menu select Route Info.

2. From the Route Configuration screen, select 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 of 0.0.0.0.

4. For the Gateway address enter the router IP address.

5. Select Save and press <Enter>.

6. Press <Esc>.

7. Reboot the CK721-A panel.
To enter other types of Static Routes:

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:
4. If host is selected, the destination IP address is the Network ID and the specific Host ID address of the P2000 server such as 200.0.0.1
5. If net is selected, only the network ID is specified for the destination such as 200.0.0.0
6. For the Gateway address enter the router IP address.
7. Select Save and press <Enter>.
8. Press <Esc>.
9. 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 P2000 server
  - Check the CK721-A routing table using the command netstat -r
  - Use the command traceroute <host ip address> to verify route to the P2000 server
**CK721-A Static Route Examples**

Net Destination Example:

Settings in the Route Configuration screen:

<table>
<thead>
<tr>
<th>Host/Net</th>
<th>Destination</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>-net</td>
<td>0.0.0.0</td>
<td>201.0.0.1 (recommended default route)</td>
</tr>
<tr>
<td>-net</td>
<td>200.0.0.0</td>
<td>201.0.0.1</td>
</tr>
</tbody>
</table>

Host Destination Example:

Settings in the Route Configuration screen:

<table>
<thead>
<tr>
<th>Host/Net</th>
<th>Destination</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>-host</td>
<td>200.0.0.1</td>
<td>201.0.0.5</td>
</tr>
</tbody>
</table>

*Figure 4-2: 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>`.
Rebooting the Panel

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

**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 3.8 build 57 with SP2, 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 P2000 software Panel window.

<table>
<thead>
<tr>
<th><strong>Setting</strong></th>
<th><strong>Value (Direct Connect)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Primary IP Address</td>
<td>Enter the IP address for this CK721-A panel.</td>
</tr>
<tr>
<td>Primary Host IP Address</td>
<td>Enter the IP address of the P2000 Server.</td>
</tr>
<tr>
<td>Controller Secondary IP Address</td>
<td>N/A</td>
</tr>
<tr>
<td>Alternate Host IP Address</td>
<td>N/A</td>
</tr>
<tr>
<td>Preferred Primary Comm Path (Y/N)</td>
<td>Y</td>
</tr>
<tr>
<td>Network Polling [LAN]</td>
<td>Recommended to be 30 sec.</td>
</tr>
<tr>
<td>Network Polling [Dup]</td>
<td>N/A</td>
</tr>
<tr>
<td>Download Port Number</td>
<td>41014 (default value)</td>
</tr>
<tr>
<td>Upload Port Number</td>
<td>41013 (default value)</td>
</tr>
<tr>
<td>Priority Port Number</td>
<td>41012 (default value)</td>
</tr>
</tbody>
</table>
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 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 P2000 server:

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Port Number</td>
<td>41014 (default value)</td>
</tr>
<tr>
<td>Upload Port Number</td>
<td>41013 (default value)</td>
</tr>
<tr>
<td>Priority Port Number</td>
<td>41012 (default value)</td>
</tr>
</tbody>
</table>

7. If you are using encryption, enter an encryption key value unique to this CK721-A controller and matching the value defined at the P2000 server. The value must be other than 0.

After entering the key, enable the encryption.

8. After these values are entered, use the arrow keys to select **Save** and press **<Enter>**.

9. A message appears informing you the record has been saved. Press **<Esc>** to return to the CK721-A Main menu.

10. Always reboot after changing IP information or route information.

---

**NOTE:** The FIPS encryption package validation process requires a reboot of the controller after turning the encryption on or off. The FIPS Encryption validation process takes about 10-20 additional minutes to complete the controller reboot. All controller functions are disabled during that time.

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.

**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 P2000 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 P2000 software.

**Panel Screen Description**

The Panel screen is used when the CK721-A panel is configured for the P2000 server.

*Panel Screen - Page 1*
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel Name</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Controller Primary IP Address</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Controller Primary IP Netmask</td>
<td>User Def.</td>
<td>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]</td>
</tr>
<tr>
<td>Controller Secondary IP Address</td>
<td>User Def.</td>
<td>This IP address is reserved for future use in support of a secondary IP interface.</td>
</tr>
<tr>
<td>Controller Secondary IP Netmask</td>
<td>User Def.</td>
<td>This netmask is reserved for future use in support of a secondary IP interface.</td>
</tr>
<tr>
<td>Primary Host IP Address</td>
<td>User Def.</td>
<td>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. <strong>Note:</strong> Prior to entering the address, the panel must be defined in the P2000 database.</td>
</tr>
<tr>
<td>Alternate Host IP Address</td>
<td>User Def.</td>
<td>This IP address is reserved for future use in support of a secondary IP interface.</td>
</tr>
<tr>
<td>Preferred Primary Comm Path</td>
<td>Toggle</td>
<td>Enabled (Y) by default. The CK721-A will communicate via onboard network interface.</td>
</tr>
<tr>
<td>Network Polling (LAN)</td>
<td>User Def.</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 4-3: Panel Screen, Page 1

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Polling (Dup)</td>
<td>User Def.</td>
<td>The Dialup connection polling is not currently used.</td>
</tr>
<tr>
<td>Download Port Number (1 to 65535)</td>
<td>User Def.</td>
<td>A TCP port number used for downloads from the server. This number must match that configured at the server. See Step 6 on page 4-13 for details.</td>
</tr>
<tr>
<td>Upload Port Number (1 to 65535)</td>
<td>User Def.</td>
<td>A TCP port number used for uploads to the server. This number must match that configured at the server. See Step 6 on page 4-13 for details.</td>
</tr>
<tr>
<td>Priority Port Number (1 to 65535)</td>
<td>User Def.</td>
<td>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 4-13 for details.</td>
</tr>
<tr>
<td>High Speed 485</td>
<td>Toggle</td>
<td>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 3-38.</td>
</tr>
</tbody>
</table>
### Panel Parameters Data Entry

- **History Upload Time Zone (0-64):** N
- **Upload History Only When > % Full (Y/N):** N
- **Upload Only When % Full Threshold (0-99):** 50
- **Always Upload History When > % Full (Y/N):** N
- **Always Upload % Full Threshold (0-99):** 50
- **Delete History Older Than Days (Y/N):** N
- **Delete History Older Than Days (0-255):** 0
- **Delete History At (HH:MM):** 00:00
- **Timed Override/Anti-Tailgate (Y/N):** N
- **Alarm Latch Output (Y/N):** N
- **Alarm Output Delay (0-60s):** 0
- **Time Zone Offset (HH:MM):** 00:00
- **Time Zone Checking (Y/N):** N
- **Entry/Exit (Y/N):** N
- **System Override (Y/N):** N
- **PIN Code Type:** Algorithmic
- **Scramble Mode (0-7):** 0
- **Digit Pin Code (4-9):** 4

### Table 4-4: Panel Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Upload Time Zone</td>
<td>User Def.</td>
<td>If specified, saved history reports are uploaded in time zones defined as Active.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If not specified, history records are saved, and not reported to the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timezone range: 0 - 64</td>
</tr>
<tr>
<td>Upload History Only When &gt; % Full</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>Upload History When % Full Threshold</td>
<td>User Def.</td>
<td>Saved history reports are uploaded only when the number of saved history reports exceeds the specified “percent full” value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In order to work, this option must be enabled in the previous field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Percentage range: 0 - 99</td>
</tr>
<tr>
<td>Always Upload history When &gt; % Full</td>
<td>Toggle</td>
<td>If enabled (Y), the history is always uploaded when the number of history records exceeds the value specified in the next field.</td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Always Upload % Full Threshold</td>
<td>User Def.</td>
<td>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</td>
</tr>
<tr>
<td>Delete History Older Than Days</td>
<td>Toggle</td>
<td>If enabled (Y), saved history records, older than the specified number of days (see next field) will be deleted.</td>
</tr>
<tr>
<td>Delete History Older Than Days</td>
<td>User Def</td>
<td>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</td>
</tr>
<tr>
<td>Delete History At</td>
<td>User Def</td>
<td>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.</td>
</tr>
<tr>
<td>Timed Override/ Anti-Tailgate</td>
<td>Toggle</td>
<td>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).</td>
</tr>
<tr>
<td>Alarm Latch Output</td>
<td>Toggle</td>
<td>If enabled (Y), the alarm relay is activated whenever an input goes into alarm, and remains activated until reset. If disabled (N), “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.</td>
</tr>
<tr>
<td>Input Report Delay</td>
<td>User Def.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 4-4: Panel Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone Offset</td>
<td>User Def.</td>
<td>Values are hours and minutes (HH:MM). Used if the controller is physically in a different geographical time zone than the P2000 server.</td>
</tr>
<tr>
<td>Entry/Exit</td>
<td>Toggle</td>
<td>If enabled (Y), readers can enforce Entry/Exit rules for access control.</td>
</tr>
<tr>
<td>PIN Code Type</td>
<td>Toggle</td>
<td>Choices are: Algorithmic, Custom (User Defined).</td>
</tr>
<tr>
<td>N Digit Pin Code</td>
<td>User Def.</td>
<td>For algorithmic PIN codes select 4 or 5 digits. For custom PIN coders select 4 to 9 digits.</td>
</tr>
<tr>
<td>Alarm Output Delay</td>
<td>User Def.</td>
<td>Values are 0 to 60 seconds. This is the number of seconds the alarm relay waits before activating.</td>
</tr>
<tr>
<td>Time Zone Offset Is</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>Time Zone Checking</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>System Override</td>
<td>Toggle</td>
<td>If enabled (Y), all portals connected to this controller are set in the unlocked position.</td>
</tr>
<tr>
<td>Scramble Mode</td>
<td>User Def.</td>
<td>Values are from 0 - 7. Select one of eight algorithms if using algorithmic PIN codes.</td>
</tr>
<tr>
<td>Group Panel Output</td>
<td>Toggle</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
### Exempt Badges From Archive
- **Type:** Toggle
- **Description:** If enabled (Y), then the Badge database is not saved to Flash during a Write-Flash operation.

### Exempt Access Groups From Archive
- **Type:** Toggle
- **Description:** 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
- **Type:** Toggle
- **Description:** 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
- **Type:** Toggle
- **Description:** 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.

### Controller Peer to Peer Entry/Exit Badge ReSync
- **Type:** Toggle
- **Description:** Enable Panel Initiated Badge Entry/Exit Resynch UDP Broadcast Flag. Disabled (N) by default.
### Table 4-5: Panel Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer to Peer Entry/Exit UDP Port Number</td>
<td>User Def.</td>
<td>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. <strong>Note:</strong> This number must match that configured at the other CK721-A Panels.</td>
</tr>
<tr>
<td>Backup The Ramdisk Database Every xx Hours</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Custom Configuration Number</td>
<td>User Def.</td>
<td>Selects and enables custom features.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Toggle</td>
<td>Enables encryption at the CK721-A controller. <strong>Note:</strong> When enabled, the File Transfer Protocol (FTP) and telnet services are disabled. Use the Secure Shell (SSH) client instead. See also: “Key (for encryption).” <strong>Note:</strong> When enabled, the File Transfer Protocol (FTP) and telnet services are disabled. Use the Secure Shell (SSH) client instead. <strong>Note:</strong> The FIPS encryption package validation process requires a reboot of the controller after turning the encryption on or off. The FIPS Encryption validation process takes about 10-20 additional minutes to complete the controller reboot. All controller functions are disabled during that time.</td>
</tr>
</tbody>
</table>
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.

### Table 4-5: Panel Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key (for encryption)</td>
<td>User Def.</td>
<td>Specifies the encryption key. The same encryption key must be used on the P2000 side or the controller will not come online. Change to encryption key requires panel reboot for new values to take effect. <strong>Note:</strong> The encryption key must be defined before encryption can be enabled, and it must be non-zero.</td>
</tr>
</tbody>
</table>

**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.

![Terminal Configuration Screen]

The five screens used to configure Terminals are described in Table 4-6 through 4-10.
### Terminal Screen - Page 1

- **Table 4-6: Terminal Screen, Page 1**

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Name</td>
<td>User Def.</td>
<td>Enter a name for this terminal. Up to 25 alphanumeric characters, including spaces, are available.</td>
</tr>
<tr>
<td>Terminal Enable/Disable</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>Input Terminal</td>
<td>Toggle</td>
<td>A (Y) indicates an input or input/output module has this terminal address.</td>
</tr>
<tr>
<td>Output Terminal</td>
<td>Toggle</td>
<td>A (Y) indicates an input/output module has this terminal address.</td>
</tr>
<tr>
<td>Reader Terminal</td>
<td>Toggle</td>
<td>Selects the reader terminal interface type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• D (reader interface Disabled)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• W (Wiegand reader interface enabled)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• O (OSDP reader interface enabled)</td>
</tr>
<tr>
<td>Reader Mode</td>
<td>Toggle</td>
<td>Choices are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A (Access)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• E (Entry)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• X (Exit)</td>
</tr>
</tbody>
</table>

---

**Note:** All terminal parameters can be modified using the Terminal Parameters Data Entry screen. This screen is used to configure terminal settings for the CK721-A.
Card Processing Choices are:
- L (Local Mode)
- C (Central Mode)
- S (Shared Mode)

Access Time 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.

Shunt Time 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 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 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, it will not deactivate by itself. Additional settings, like Timed Duration of each output point in the group, is needed for automatic de-activation.

Anti-Passback 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 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Override</td>
<td>Toggle</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override Warning Time</td>
<td>User Def.</td>
<td>You can activate an output group as a warning before the Cardholder Override expires. Enter the amount of time here (0 - 10 minutes).</td>
</tr>
<tr>
<td>Override Warning Output Group</td>
<td>User Def.</td>
<td>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, it will not deactivate by itself. Additional settings, like Timed Duration of each output point in the group, is needed for automatic de-activation.</td>
</tr>
<tr>
<td>Terminal Timezone</td>
<td>User Def.</td>
<td>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.)</td>
</tr>
<tr>
<td>Terminal Override Timezone</td>
<td>User Def.</td>
<td>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.)</td>
</tr>
</tbody>
</table>
### Table 4-7: Terminal Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader Hdw Type</td>
<td>User Def.</td>
<td>Selects the reader hardware module type for the addressed S300 module. The available reader hardware module types are: RDR2S-A, RDR8S, and LEGACY (RDR2S, RDR2). Note: Any changes to this field require a controller Write-To-Flash operation.</td>
</tr>
<tr>
<td>Reader Module Number</td>
<td>User Def.</td>
<td>Selects the reader module hardware number assigned to the S300 module. The Reader Module Number is not used for legacy devices. For the RDR8S and RDR2S-A modules the hardware number range is 0 to 31. Note: Any changes to this field require a controller Write-To-Flash operation.</td>
</tr>
</tbody>
</table>
### Table 4-7: Terminal Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader Terminal Index</td>
<td>User Def.</td>
<td>Selects the reader terminal index number for the S300 module. The Reader Terminal Index is not used for legacy devices. For the RDR8S module the value range is 1 to 8. For the RDR2S-A module the value range is 1 to 2. <strong>Note:</strong> Any changes to this field require a controller Write-To-Flash operation.</td>
</tr>
<tr>
<td>I/O Hdw Type</td>
<td>User Def.</td>
<td>Selects the I/O hardware module type for the addressed S300 module. The available I/O hardware module types are: RDR2S-A, RDR8S, and LEGACY (RDR2S, IO8, SIO8, I16, and SI8). <strong>Note:</strong> Any changes to this field require a controller Write-To-Flash operation.</td>
</tr>
<tr>
<td>I/O Module Number</td>
<td>User Def.</td>
<td>Selects the I/O module hardware number assigned to the S300 module. The I/O Module Number is not used for legacy devices. For the RDR8S and RDR2S-A modules the hardware number range is 0 to 31. <strong>Note:</strong> Any changes to this field require a controller Write-To-Flash operation.</td>
</tr>
<tr>
<td>I/O Terminal Index</td>
<td>User Def.</td>
<td>Selects the I/O terminal index number for the S300 module. The I/O Terminal Index is not used for legacy devices. For the RDR8S module the value range is 1 to 8. For the RDR2S-A module the value range is 1 to 2. <strong>Note:</strong> Any changes to this field require a controller Write-To-Flash operation.</td>
</tr>
</tbody>
</table>
Terminal Screen - Page 3

Page 3 of the Terminal screen is shown, followed by Table 4-8, which contains a description of each item.

Table 4-8: Terminal Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Tailgate Enabled</td>
<td>Toggle</td>
<td>If enabled (Y), the access timer resets and the strike locks immediately when the door closes.</td>
</tr>
<tr>
<td>Reader Override Enabled</td>
<td>Toggle</td>
<td>If enabled (Y), no card is required when the Terminal Override Timezone is active.</td>
</tr>
<tr>
<td>Shunt the Alarm on AUX Access</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>Momentary AUX Only</td>
<td>Toggle</td>
<td>Allows (Y) the Access Time to begin timing when the terminal's AUX Access input point contact is shorted by a switch.</td>
</tr>
<tr>
<td>Allow PIN after Badge</td>
<td>Toggle</td>
<td>Allows (Y) the cardholder to enter a PIN after presenting a card, instead of before presenting a card.</td>
</tr>
<tr>
<td>Soft Entry/Exit</td>
<td>Toggle</td>
<td>If enabled (Y), an Entry/Exit access violation will allow access.</td>
</tr>
</tbody>
</table>
### Table 4-8: Terminal Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid and Unauthorized</td>
<td>Toggle</td>
<td>Setting this enabled (Y) allows a cardholder to present a valid badge, but the door strike will not be released automatically. <strong>Note:</strong> Terminal must be on-line with P2000.</td>
</tr>
<tr>
<td>Alarm Debounce Time</td>
<td>User Def.</td>
<td>Values range from 4-80, which corresponds to debounce times of 40-800 ms.</td>
</tr>
<tr>
<td>Reverse Card Bit Order</td>
<td>Toggle</td>
<td>If enabled (Y), a swiped card can be read in either forward or reverse direction. <strong>Note:</strong> 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 P2000 software.)</td>
</tr>
<tr>
<td>Duress on Reverse Badge</td>
<td>Toggle</td>
<td>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 P2000 software.)</td>
</tr>
<tr>
<td>PIN plus 1 Duress</td>
<td>Toggle</td>
<td>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 &lt;9&gt; key will not create a duress alarm.</td>
</tr>
<tr>
<td>PIN Suppression Timezone</td>
<td>User Def.</td>
<td>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.)</td>
</tr>
<tr>
<td>Log Output Status Message</td>
<td>Toggle</td>
<td>If enabled, will report output “set” or “reset” on the CK721-A Logger Out screen and at the Host.</td>
</tr>
<tr>
<td>Facility Code when offline</td>
<td>Toggle</td>
<td>If enabled (Y), a person needs only a valid facility code to open a door when the terminal is offline from the panel. See “Offline Access Card Type Requirements” on page 4-38 for details.</td>
</tr>
</tbody>
</table>
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. See "Offline Access Card Type Requirements" on page 4-38 for details.

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 F for details.

Access Grant on Door Open Only | Toggle | If enabled (Y), will report normal access granted only if door is opened.
When enabled (Y) the Keyless Override timer starts after swiping a badge (with override privileges) and immediately opening the door. When disabled (N), the Keyless Override timer starts after swiping a badge (with override privileges).
In the case of an elevator reader, when this flag is enabled the Elevator Access Grant message will be sent to the P2000 server only when the cardholder presents a badge at the reader and a valid floor is selected.
Re-lock on Door Open

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 an S300-DIN module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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”).</td>
</tr>
</tbody>
</table>

Timed Shunt

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Toggle</td>
<td>If enabled (Y), all Timed Overrides only extend the shunt time. The Access Time is not affected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This option requires the use of RDR2 module, firmware version PS-201E or later, or an S300-DIN module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Override Time

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For security reasons, this feature should only be used together with the Timed Shunt option.</td>
</tr>
</tbody>
</table>

Table 4-8: Terminal Screen, Page 3
### Table 4-8: Terminal Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisted Access</td>
<td>User Def.</td>
<td>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 an S300-DIN module.</td>
</tr>
<tr>
<td>Assisted Access Time</td>
<td>User Def.</td>
<td>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 an S300-DIN module.</td>
</tr>
<tr>
<td>ADA Relay Connector</td>
<td>User Def.</td>
<td>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 an S300-DIN module. For wiring details, see “Shunt Relay Driver Wiring” on page 3-37.</td>
</tr>
<tr>
<td>ADA Relay Time (0 to 120 s)</td>
<td>User Def.</td>
<td>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 an S300-DIN module. See the “Assisted Access Timing Diagram” on page 4-46.</td>
</tr>
</tbody>
</table>
### 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 an S300-DIN module.
See the “Assisted Access Timing Diagram” on page 4-46 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.

### 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 an S300-DIN module (RDR2S firmware must be revision Q or higher).
# Door Open Warning Auto Off

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

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

If enabled (Y), the low level D620-ECG Elevator Mode is enabled. For a detailed explanation, refer to “D620-ECG Low Level Interface” on page 4-49.

## Table 4-8: Terminal Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Low Level Interface” on page 4-49. |
Terminal Screen - Page 4

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Code</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Card Type</td>
<td>Toggle</td>
<td>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.</td>
</tr>
</tbody>
</table>

Terminal Screen - Page 5

Page 5 of the Terminal screen is shown below followed by Table 4-10, which contains a description of each item. Page 5 allows you to configure additional card parameters from the settings contained on Page 4.

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 4-41.
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 5

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Card Allowed</td>
<td>Toggle</td>
<td>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).</td>
</tr>
<tr>
<td>Standard Wiegand</td>
<td>Toggle</td>
<td>If enabled (Y), standard Wiegand will be permitted at this terminal.</td>
</tr>
<tr>
<td>Encrypted Wiegand</td>
<td>Toggle</td>
<td>If enabled (Y), encrypted Wiegand will be permitted at this terminal.</td>
</tr>
<tr>
<td>Binary BAFE (both parity and no parity)</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>Invert Data</td>
<td>Toggle</td>
<td>Select (Y) to invert the card data reported from the reader.</td>
</tr>
<tr>
<td>BCD BAFE (both parity and no parity)</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
</tbody>
</table>
**Offline Access Card Type Requirements**

Only the first Facility Code entered in the Facility Code tab is used for offline access. Only certain card types can be used by readers while

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26-Bit Wiegand Inverted</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>Eyecam, Prox, Indala</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>26-Bit Sensor Forward</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>26-Bit Sensor Reverse</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>Standard Wiegand</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>Encrypted Wiegand</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>Mag Stripe</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>PIN Only</td>
<td>Toggle</td>
<td>Select (Y) to allow this mode. See “PIN Only” on page 4-41 for details.</td>
</tr>
<tr>
<td>Card ID</td>
<td>Toggle</td>
<td>Select (Y) to allow the Card ID mode.</td>
</tr>
<tr>
<td>PIN+Card ID</td>
<td>Toggle</td>
<td>Select (Y) to allow this mode. See “PIN + Card ID” on page 4-42 for details.</td>
</tr>
<tr>
<td>Motorola 32-Bit</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>HID Corporate 1000</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>PIV (FASCN)</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>PIV-I (UUID)</td>
<td>Toggle</td>
<td>Select (Y) to allow this card type.</td>
</tr>
<tr>
<td>Custom</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>Custom Format 1 to 8</td>
<td>Toggle</td>
<td>Select (Y) to allow this custom format. Meanings of the custom formats 1 to 8 are assigned at the host.</td>
</tr>
</tbody>
</table>
offline. Lower priority type support requires that higher priority types not be selected. Only one card type is used while offline.

Table 4-11: Offline Access Card Type Requirements

<table>
<thead>
<tr>
<th>Priority</th>
<th>Card Type</th>
<th>Facility Code</th>
<th>Offline Algorithmic PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (highest)</td>
<td>Standard Wiegand</td>
<td>Supported$^1$</td>
<td>Supported</td>
</tr>
<tr>
<td>2</td>
<td>Encrypted Wiegand</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>3</td>
<td>Binary BAFE legacy</td>
<td>Always 4$^3$</td>
<td>Not Supported</td>
</tr>
<tr>
<td>3</td>
<td>Binary BAFE modern</td>
<td>HID 1000 only$^5$</td>
<td>HID 1000 only</td>
</tr>
<tr>
<td>4</td>
<td>Mag Stripe or Custom</td>
<td>Not Supported$^6$</td>
<td>Not Supported</td>
</tr>
<tr>
<td>5</td>
<td>Eyecam, Prox, Indala</td>
<td>Supported$^7$</td>
<td>Supported</td>
</tr>
<tr>
<td>6</td>
<td>26-Bit Sensor Forward</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>7</td>
<td>26-Bit Sensor Reverse</td>
<td>Not Supported$^8$</td>
<td>Not Supported</td>
</tr>
<tr>
<td>8</td>
<td>HID Corporate 1000</td>
<td>Supported$^9$</td>
<td>Supported</td>
</tr>
<tr>
<td>9 (lowest)</td>
<td>PIV and PIV-I</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

1. The lowest two bits of the Facility Code are not verified. (The indicated code accepts four variations.)
2. All RDR2 modules and RDR2S modules using PS-215Q or older firmware.
3. Any card swiped can be used for access when the Offline Facility code is set to “4.”
4. All RDR8S, All RDR2S-A, and RDR2S modules using firmware after version PS-215Q.
5. When HID Corporate 1000 format is detected (exactly 35-bits with proper parity) the facility code and card number are used. All other card types are accepted as facility code “4” and card number zero. (This can be used to grant offline access for card types that are not directly supported.)
6. Mag Stripe or Custom types are not supported. Enabling these types can prevent processing of lower priority card types.
7. Equivalent to the Standard format, except the Facility Code must be an exact match.
8. Offline processing differs from the online processing. This format should not be used for offline access.
9. Not supported offline by RDR2 modules nor by RDR2S modules using PS-215Q or older firmware.

RDR8S Input Point and Output Point Disassociation

This feature allows RDR8S reader terminal input/output (I/O) points to be re-assigned from reader-specific functions to general purpose I/O points.

The following RDR8S reader terminal output points can be re-assigned:

- Red LED
- Green LED
- Reader Strike
- Reader Shunt

The following RDR8S reader terminal input points can be re-assigned:

- Reader Door Contact
- Reader REX
Reassignment of the special RDR8S reader terminal output points to general purpose output points is done by configuring the general purpose output points listed below:

<table>
<thead>
<tr>
<th>Reader Output Point</th>
<th>Terminal Output Point Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red LED</td>
<td>Output 1 [Open Collector Output]</td>
</tr>
<tr>
<td>Green LED</td>
<td>Output 2 [Open Collector Output]</td>
</tr>
<tr>
<td>Reader Shunt</td>
<td>Output 3 [Relay Output]</td>
</tr>
<tr>
<td>Reader Strike</td>
<td>Output 5 [Relay Output]</td>
</tr>
</tbody>
</table>

Reassignment of the special RDR8S reader input points to general purpose input points is done by configuring the general purpose input points listed below:

<table>
<thead>
<tr>
<th>Reader Input Point</th>
<th>Terminal Input Point Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader Door Sensor</td>
<td>Input 1</td>
</tr>
<tr>
<td>Reader REX</td>
<td>Input 2</td>
</tr>
</tbody>
</table>

A write to flash must be performed after completion of input point/output point disassociation configuration.

**RDR2S-A Input Point and Output Point Disassociation**

This feature allows RDR2S-A reader terminal input/output (I/O) points to be re-assigned from reader-specific functions to general purpose I/O points.

**NOTE:** This feature requires RDR2S-A firmware version PS-217E-2 or higher.

The following RDR2S-A reader terminal output points can be re-assigned:

- Red LED
- Green LED
- Reader Strike
- Reader Shunt

The following RDR2S-A reader terminal input points can be re-assigned:
• Reader Door Contact (door is always reported closed by Soft Alarm Points 18 and 24)
• Reader REX

Re-assignment of the special RDR2S-A reader terminal output points to general purpose output points is done by configuring the general purpose output points listed in the following table:

<table>
<thead>
<tr>
<th>Reader Output Point</th>
<th>Terminal Output Point Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red LED</td>
<td>Output 1 [Open Collector Output]</td>
</tr>
<tr>
<td>Green LED</td>
<td>Output 2 [Open Collector Output]</td>
</tr>
<tr>
<td>Reader Shunt</td>
<td>Output 3 [Relay Output]</td>
</tr>
<tr>
<td>Reader Strike</td>
<td>Output 5 [Relay Output]</td>
</tr>
</tbody>
</table>

Re-assignment of the special RDR2S-A reader terminal input points to general purpose input points is done by configuring the general purpose input points listed in the following table:

<table>
<thead>
<tr>
<th>Reader Input Point</th>
<th>Terminal Input Point Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader Door Contact</td>
<td>Input 1</td>
</tr>
<tr>
<td>Reader REX</td>
<td>Input 2</td>
</tr>
</tbody>
</table>

**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 page 4-19) must be set to **Algorithmic**.

2. The panel’s **N Digit Pin Code** option (see page 4-19) should be set to **5**, although it is ignored in “PIN Only” mode.

3. The panel’s **Scramble Mode** (see page 4-19) must be set to the value used to create the PINs from the card numbers.

4. The terminal’s **PIN Only** card type (see page 4-38) must be selected in. All other card types must not be selected.

5. The terminal’s **Allow PIN after Badge** (see page 4-29) has no effect.

6. The terminal’s **PIN Suppression Timezone** (see page 4-30) 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 9-digit custom PINs.

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

1. The terminal’s **PIN+Card ID** (see page 4-38) 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 page 4-29) has no effect.

3. The terminal’s **PIN Suppression Timezone** (see page 4-30) 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 9-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 page 4-38).
2. The **PIN plus 1 Duress** option is not enabled (see page 4-30).
3. All other card types should not be selected.
4. The terminal’s **PIN Only** card type (see page 4-38) must not be selected.
5. The terminal’s **PIN + Card ID** card type (see page 4-38) 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 Timezone** (see page 4-30) 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 page 4-29) 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 4-85).

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 4-82).

2. The PIN plus 1 Duress option is not enabled (see page 4-30).

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 page 4-36) 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 page 4-83).

2. The PIN plus 1 Duress option is enabled (see page 4-30).

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 Card Type) 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 4-82). 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 an S300-DIN 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 an S300-DIN module. The activation can be delayed without the use of external additional hardware (unlike when using SIO8 modules). 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 4-33.

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 3-37.
When ADA Relay Connector is set to “Shunt”, the shunt connector no longer indicates the shunt time, but the ADA Relay activation.

![Assisted Access Timing Diagram](image)

**Figure 4-3: Assisted Access Timing Diagram**

**Panel Entry/Exit**

**Badge Entry/Exit Options**

The P2000 and CK721-A controllers support the following Badge Exit/Exit Enforcement and Synchronization modes:

- Global Badge Entry/Exit Status Synchronization
- Controller Badge Local Entry/Exit Enforcement
- Controller Peer-To-Peer Global Entry/Exit Enforcement and Synchronization

For configuration details, refer to the *P2000 Software User Manual*.

Global Badge Entry/Exit Status Synchronization

The Global Badge Entry/Exit Status Synchronization feature, when enabled in P2000, allows the P2000 to interact with the controllers by
providing badge status synchronization across multiple controllers. It is not recommended for medium and large systems.

**IMPORTANT:** This feature must never be combined with the **Controller Peer-To-Peer Global Entry/Exit Enforcement and Synchronization** option selection. Selecting both features will cause badge entry/exit enforcement errors across multiple controllers.

Controller Badge Local Entry/Exit Enforcement

The CK721-A controller **Local Entry/Exit** enforcement feature limits a cardholder Badge entry/exit status enforcement to a specific CK721-A controller and a maximum of 64 readers (32 pairs of In/Out readers). Therefore, a cardholder badge swiped on a reader terminal connected to one CK721-A controller would not have their entry/exit privileges synchronized on a reader terminal connected to different CK721-A controller.

Refer to the **P2000 Software User Manual** for configuration details.

Controller Peer-To-Peer Global Entry/Exit Enforcement and Synchronization

The controller **Peer-To-Peer Global Entry/Exit** enforcement feature allows a CK721-A controller to broadcast the entry/exit status of a badge to multiple CK721-A controllers via UDP protocol. This allows an Entry/Exit zone to span across multiple CK721-A controllers within the same Subnet, or across multiple Subnets using a properly configured multicast router. In addition, by changing the controller Peer-To-Peer UDP Port Number, a new Entry/Exit zone, spanning multiple CK721-A controllers can be created.

This feature requires P2000 version 3.8 Build 55 or higher.

**IMPORTANT:** This feature must never be combined with the **Global Badge Entry/Exit Status Synchronization**. Selecting both features will cause badge entry/exit enforcement errors across multiple controllers.

**NOTE:** UDP broadcast typically does not span multiple Subnets unless the routers are specifically configured to pass multicast traffic. Refer to the router manufacturer for specific configuration details on enabling UDP traffic passing.
**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.

Panel card events cannot be used on elevator readers.

Elevator access control supports terminal range 1 through 16.

---

**NOTE:** All elevator configurations within the same controller must use the same elevator interface type.

The following elevator interface configurations are available:

- Standard Low Level Interface
- D620-ECG Low Level Interface
- KONE HLI/KONE ELINK High Level Interface
- KONE IP High Level Interface
- ThyssenKrupp High Level Interface
- OTIS Serial E.M.S. High Level Interface
- OTIS E.M.S. - Security / B.M.S. Protocol High Level Interface
- OTIS Compass High Level Interface

**Standard 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 P2000 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 Low Level Interface**

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.

**KONE HLI/KONE ELINK High Level Interface**

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 or KONE HLI. 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.

**KONE IP High Level Interface**

**KONE IP Elevator Support**

CK721-A panels version 3.1 and higher provide the communication necessary for KONE IP elevators. In this high-level elevator integration, the CK721-A panel interfaces with the elevator control system through a communications protocol. Granting access to floors is achieved by sending messages to the elevator controller; reporting destination floors is achieved by receiving messages from the elevator controller (you must select the Floor Tracking function).

Each CK721-A panel can connect to multiple KONE IP group controllers, each controller with up to 8 elevators, each elevator serving up to 128 floors. To define a KONE IP elevator, you must first select the KONE IP protocol type in the Panel Elevator tab.

The KONE IP elevator interface provides two types of group controllers, the KONE KIC and the Primary/Backup KGC. There are different rules when interfacing to a KONE KIC as opposed to a Primary/Backup KGC controller. KONE KIC controllers only support Car Operation Panels (COPs), and not Destination Operation Panels (DOPs). You can define up to 33 elevator groups for each KONE KIC controller. KONE IP
controllers, configured in primary/backup pairs, support a single elevator group per controller pair.

**NOTE:** KONE IP network communication with KONE elevator controller is not encrypted. See the P2000 Software User Manual for details on configuring KONE IP elevator.

---

**KONE IP Controllers Configuration**

Prior to configuring a KONE IP elevator, you must define the KONE IP controller that will serve as the interface to set the configuration parameters related to the elevator controller, as well as the interface to monitor the status of the elevator controller and its communication with the CK721-A panel.

The integration with KONE IP high level interface uses the following KONE controllers:

- KONE IP controller equipped with Kone Interface Computer (KIC), also called “KONE KIC”
- KONE IP controller without with KIC

**Elevator Group Configuration**

KONE KIC controllers do not support Destination Operation Panels (DOPs). You can define up to 33 elevator groups for each KONE KIC controller.

KONE IP controllers, configured in primary/backup pairs, support a single elevator group per controller pair.

**Floor Configuration**

A single floor configuration is mapped to each elevator group.

**Modes of Operation**

The CK721-A supports the following these modes of operation:

- One KONE KIC controller handling multiple elevator groups
- One KONE KIC controller handling multiple elevator groups, connected to multiple CK721-A controllers
- Pair(s) of KONE IP controllers, each pair handling one elevator group
One KONE KIC Controller for All Elevator Groups

In this scenario, all elevator groups use the same TCP port number and are connected to a single KONE KIC controller and a single CK721-A controller.

![Diagram of KONE KIC Controller with Multiple Elevator Groups](image)

One KONE KIC Controller with Multiple Elevator Groups and Multiple CK721-A Controllers

In this scenario, a single KONE IP controller communicates with multiple CK721-A controllers. The TCP port numbers are different for the KONE IP controller to distinguish the heartbeats.
In this scenario, one KONE IP controller of each pair becomes a primary controller, while the other becomes a backup controller. Both KONE IP controllers share the same floor layout. The elevator group address is set to 1.

**Pair(s) of KONE IP Controllers, Each Handling One Elevator Group**

Note: KONE IP Controllers tend to have even numbered elevator groups: 0, 2, 4, ..., 32.
ThyssenKrupp High Level Interface

The ThyssenKrupp integration is composed of the ThyssenKrupp Lift Control System (LCS), which is the ThyssenKrupp side of the integration, and an Access Control System (ACS), which refers to the P2000 Server and CK721A devices.

This section only describes the ACS side; Johnson Controls has no knowledge of or control over the LCS.

The integration works as follows:

- A person presents his badge to an HID reader (ACS side).
- ACS grants or denies access.
- If access is granted, the ACS sends a 'temporal unlocking of floors' message to the LCS, which contains a bitmask of all unlocked floors. This information is presented at the Destination Selection Control terminal (DSC) via it's the touchscreen (shown below). After floor selection, the user is assigned a specific lift.
• Floors that are in public access are readily accessible by pressing one of the public access unlocked floor via the touch screen. No badge-sweep action is required to access these public access floors.

Figure 4-7: ThyssenKrupp Touch Screen

• The ACS sends a “permanent unlocking of floors” message to the LCS, which contains a bitmask of all unlocked floors that are in public access, and it sends a “permanent locking of floors” message to the LCS, which contains a bitmask of all locked floors that are not in public access.

• The LCS sends a “Destination Call” message back to the ACS once a user made a valid floor selection at the DSC terminal. This selection gets reported on the P2000 Real Time List (ACS side) if the Floor Tracking option is set for that particular device.

In order to support this functionality the P2000 must:

• Provide a mapping between a DSC terminal (LCS side) and an HID reader (ACS side).
• Allow the floor configuration of each DSC terminal.
• Allow the configuration of any floor into public access.
• Report floor tracking messages onto the RTL.

The following image depicts an actual site using ThyssenKrupp (LCS). The building has 7 elevator shafts, which cover 21 floors, and it contains 67 DSC devices.
Each of these devices is mapped to a specific shaft, as well as either a front or rear door.

![Elevator Layout Diagram]

Figure 4-8: ThyssenKrupp Building Elevator Layout
The reference to Front Door or Rear Door only identifies the location of the DCS for addressing purposes. It is not reflected in the access rights definition for accessing this floor, and is not part of the access control system.

Figure 4-7 shows the ThyssenKrupp serial elevator integration system architecture.

Communication between the P2000 Server, CK721-A clients, and the CK721-A server takes place over TCP/IP. Communication between the CK721-A server and elevator control system is done over an RS232 serial interface.

The Server CK721-A controller function provides communications between the PACS and the elevator control system. The Server CK721-A controller cannot be assigned “client” elevator control functions.

The Client CK721-A controller(s) provides the elevator control function, via communications passed through the Server CK721-A controller. The Client CK721-A controller cannot be assigned “server” communication duties.

Both the Server CK721-A controller and Client CK721-A controller(s) can be assigned Access Control door control functions, via RDR2S-A and RDR8S modules.
There can only be one CK721-A configured as server connected to a single elevator control system. A P2000 Server, however, may be using multiple CK721-A controllers configured as servers to connect to multiple elevator control systems.

The minimum hardware configuration is one CK721-A controller configured as a server, one elevator control system, and one CK721-A controller configured as a client.

**OTIS Serial E.M.S - Security / B.M.S. Protocol High Level Interface**

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 RS-232 interface. As the current CK721-A controller supports up to 16 elevator 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 controller needs to be designated the OTIS server. The server CK721-A controller RS-232C serial B port (3 wire full duplex RS232 interface) is connected to an RS232 to RS422 converter, which is connected to the OTIS EMS (4 wire full duplex RS422 interface).

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 server with a 3 wire interface, consisting of pins 2, 3 and 7.

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.
Elevator Parameters Configuration

Defined Groups: **Client**. Defines the presence of groups 1 through 8 in the OTIS EMS.

Maximum Number of Landings: **Server & Client**. This defines the maximum number of landings of any elevator in the OTIS EMS.

OTIS Timeout (ms) Server only: **Server**. This defines the timeout of the OTIS system. The default timeout is 200 ms.

Poll Delay (ms): **Server**. This 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. The default poll delay is 400 ms.

Number of Retries: **Server**. This defines the how many times a message is retried before OTIS is declared offline. Any invalid character uses the default number of 3 retries.

**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 be configured with:

- Group Number (1 - 8)
- Elevator Car Number (1 - 8)
- Fire floor number. The fire floor will never be secured by the OTIS integration. The fire floor functionality can also be achieved by assigning the floor to a timezone that is always enabled.

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.

OTIS E.M.S. - Security / B.M.S. Protocol High Level Interface

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 elevator 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 controller needs to be designated the OTIS master. The master CK721-A controller RS-232C serial B port (3 wire full duplex RS232 interface) is connected to an RS232 to RS422 converter, which is connected to the OTIS EMS (4 wire full duplex RS422 interface).

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.

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 4-11: 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.

<table>
<thead>
<tr>
<th>Defined groups</th>
<th>None</th>
<th>5</th>
<th>6</th>
<th>5,6</th>
<th>7</th>
<th>5,7</th>
<th>6,7</th>
<th>5,6,7</th>
<th>8</th>
<th>5,8</th>
<th>6,8</th>
<th>5,6,8</th>
<th>7,8</th>
<th>5,7,8</th>
<th>6,7,8</th>
<th>5,6,7,8</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd character</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Defined groups</th>
<th>None</th>
<th>1</th>
<th>2</th>
<th>1,2</th>
<th>3</th>
<th>1,3</th>
<th>2,3</th>
<th>1,2 ,3</th>
<th>4</th>
<th>1,4</th>
<th>2,4</th>
<th>1,2, 4</th>
<th>3,4</th>
<th>1,3, 4</th>
<th>2,3, 4</th>
<th>1,2, 3,4</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd character</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
<td>F</td>
</tr>
</tbody>
</table>

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.

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

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.

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

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

<table>
<thead>
<tr>
<th>Poll delay [ms]</th>
<th>0</th>
<th>100</th>
<th>200</th>
<th>300</th>
<th>400</th>
<th>500</th>
<th>600</th>
<th>700</th>
<th>800</th>
<th>900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6th character</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Number of retries</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>7th character</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Priority</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>8th character</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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.

**OTIS Compass High Level Interface**

The CK721-A controller provides access control under the OTIS Compass Elevator Integration with P2000.

The OTIS Compass interface is a high level interface that uses a TCP/IP network to send elevator commands to the OTIS system, and to receive historical information from the OTIS system. The OTIS system differs from typical elevator systems because the floor selection is done outside of the elevator cab. Access to the floor entry keypad (called a Destination Entry Computer or DEC) can be controlled by a reader connected to a CK721-A panel, if configured to do so. The OTIS system allows operation of the DECs in 4 different modes that define the availability of floors and the order in which floors and badges are presented to the system.

Once the P2000 is connected to an OTIS Compass system, the P2000 is in full control of what each DEC is able to do. This means that until an elevator is defined in the P2000 system and its access parameters are configured, no use of the elevator is permitted. Each CK721-A can control as many DECs as it has readers configured, using a 1 to 1 mapping. The P2000 allows for the configuration of public use of a DEC through the configuration of unsecured elevator entry points. The P2000 also allows for configuration of secured entry points and the association of access rights on a badge to those secured entry points. The P2000
supports the OTIS concepts of “Allowed Floors” and “Authorized Floors” through its configuration screens. The P2000 supports the ability to enter a PIN code on the DEC which is associated with a badge in the P2000 system and grant appropriate access if allowed. The P2000 also allows configuration of the ADA access and VIP access features, as well as the default floor feature in the OTIS system.

The operational modes of the OTIS Compass system are currently defined as follows:

- **Mode 1** - Initially allows entry of a floor request or the presentation of a badge. If a floor request is entered, and it is an allowed floor, an elevator is dispatched. If a badge is presented first, that badge’s default floor is used to dispatch an elevator, assuming the default floor is an authorized or an allowed floor.

- **Mode 2** - A badge must be presented before a floor is selected and if the floor is authorized or allowed, an elevator is dispatched. This is the common mode of operation for secured elevator entry points.

- **Mode 3** - Initially allows entry of a requested floor. If the floor is allowed, an elevator is dispatched. If the floor is not allowed, a request is made for the user to provide a badge and if the badge presented authorizes the floor requested, an elevator is dispatched. This is the most common mode of operation for unsecured elevator entry points.

- **Mode 4** - A badge must be presented before a floor is selected, the badge’s default floor is preselected for the user, but the user is given a short time period to select a different floor. If the floor selected after the time-out is authorized or allowed, an elevator is dispatched.

In all modes, if an invalid badge is presented or an illegal floor is entered the user is informed using the DECs display. If a valid combination of badge and floor selection is made, the user is informed what elevator to board using the DECs display. All transactions occurring at secured elevator entry points are logged in the P2000 system.

**Basic Elevator 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.

**DCS** – ThyssenKrupp Destination Selection Control Terminal

**LCS** – ThyssenKrupp Lift Control System

**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; that is, 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>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elevator/</td>
<td>User Def.</td>
<td>A numeric value that identifies the elevator or cabinet to the system. This</td>
</tr>
<tr>
<td>Cabinet ID</td>
<td></td>
<td>value is assigned by the server and cannot be edited by the user.</td>
</tr>
<tr>
<td>Terminal Number</td>
<td>User Def.</td>
<td>A read-only field that identifies the terminal associated with this elevator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or cabinet. Value range: 1 to 16.</td>
</tr>
<tr>
<td>Interface Type</td>
<td>User Def.</td>
<td>A read-only field that identifies the type of elevator or cabinet control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in use: 0 = low level interface 1 = high level interface (RS232)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following high level interfaces are supported: KONE PLC-HLI/KONE ELINK,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OTIS BMS, OTIS COMPASS, and KONE IP.</td>
</tr>
<tr>
<td>High Protocol</td>
<td>User Def.</td>
<td>A read-only field that identifies the high level (RS232) protocol in use.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = low level interface 1 = KONE HLI/KONE ELINK 2 = OTIS BMS 3 = OTIS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMPASS 4 = KONE IP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following high level interfaces are supported: KONE PLC-HLI/KONE ELINK,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OTIS BMS, OTIS COMPASS, and KONE IP.</td>
</tr>
<tr>
<td>Mode</td>
<td>User Def.</td>
<td>A read-only field that identifies the mode of operation of the elevator or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cabinet: 0 = elevator, output points only 2 = elevator, input and output</td>
</tr>
<tr>
<td></td>
<td></td>
<td>points 4 = cabinet, output points only 5 = cabinet, input points only 6 =</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cabinet, input and output points</td>
</tr>
<tr>
<td>Timed Access</td>
<td>Toggle</td>
<td>A read-only field that identifies how the access control logic reacts when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>an enabled input point is received: Y = enable output points for specific</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access time N = enable output points until input received</td>
</tr>
<tr>
<td>Access Time</td>
<td>User Def.</td>
<td>A read-only field that identifies the maximum time, in seconds, that the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>output points are enabled due to an access grant.</td>
</tr>
</tbody>
</table>
Floor/Door Tracking

| Field                  | Type   | Description | Floor Tracking on Input Open
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Floor Tracking</td>
<td>Toggle</td>
<td>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 4-73.</td>
<td>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 4-73.</td>
</tr>
<tr>
<td>Floor Tracking on Transitions Only</td>
<td>Toggle</td>
<td>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 4-73.</td>
<td></td>
</tr>
<tr>
<td>Suppress Time</td>
<td>User Def.</td>
<td>A read-only field that identifies the length of time, in minutes, that an alarm is suppressed after access is granted for a door.</td>
<td></td>
</tr>
<tr>
<td>Alarm Flag</td>
<td>Toggle</td>
<td>A read-only field that identifies whether input points will generate alarms when they are associated with a cabinet.</td>
<td></td>
</tr>
</tbody>
</table>
Table 4-13: Setting Flags for Generating Floor Tracking Messages

<table>
<thead>
<tr>
<th>Generate floor tracking messages on input point:</th>
<th>Flags:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Floor/Door Tracking</td>
</tr>
<tr>
<td>Closed¹</td>
<td>Y</td>
</tr>
<tr>
<td>Open²</td>
<td>Y</td>
</tr>
<tr>
<td>Closing¹</td>
<td>Y</td>
</tr>
<tr>
<td>Opening²</td>
<td>Y</td>
</tr>
<tr>
<td>Do not generate floor tracking messages.</td>
<td>N</td>
</tr>
</tbody>
</table>

¹ Input point wired to “normally open.”
² Input point wired to “normally closed.”

---

Elevator or Cabinet Terminal Screen - Page 6

```
--- ELEVATOR PARAMETERS DATA DISPLAY --- Terminal: 1 --- Page 6 of 7 ---

<table>
<thead>
<tr>
<th>Outp</th>
<th>Inp</th>
<th>IIZ</th>
<th>Outp</th>
<th>Inp</th>
<th>IIZ</th>
<th>Outp</th>
<th>Inp</th>
<th>IIZ</th>
<th>Outp</th>
<th>Inp</th>
<th>IIZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>8</td>
<td>1</td>
<td>31</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>27</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>28</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>32</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<Save> <Delete> <Previous Record> <Next Record> <Page Up> <Page Down>
```
### Table 4-14: Elevator or Cabinet Terminal Screen, Pages 6 and 7

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floor Index</td>
<td>User Def.</td>
<td>A numeric value that identifies a floor’s location in the array of 128 possible floors.</td>
</tr>
<tr>
<td>Outp</td>
<td>User Def.</td>
<td>A read-only field that identifies the output point associated with a floor or door. A value of 00 indicates no output point is assigned. If an output point is assigned, it is identified by terminal number and point number.</td>
</tr>
<tr>
<td>Inp</td>
<td>User Def.</td>
<td>A read-only field that identifies the input point associated with a floor or door. A value of 00 indicates no input point assigned. If an input point is assigned, it is identified by terminal number and point number.</td>
</tr>
<tr>
<td>TZ</td>
<td>User Def.</td>
<td>A read-only field that identifies the timezone associated with a floor or door. A value of 0 indicates no timezone is assigned.</td>
</tr>
</tbody>
</table>

**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 4-15.

![Output Record Definition Screen](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Point Name</td>
<td>User Def.</td>
<td>Enter up to 25 alphanumeric characters for a descriptive output point name.</td>
</tr>
<tr>
<td>Active State</td>
<td>Toggle</td>
<td>Choices are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• R (Reset)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• S (Set)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Q (Quick Flash)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• F (Slow Flash)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• T (Timed)</td>
</tr>
<tr>
<td>Timed Duration</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Override Warning</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Output Group (1 - 3)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Holiday

During normal system operation, Holidays can replace a standard time zone. At approximately one minute before midnight, the P2000 (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 4-16 describes each field.
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.

---

### Table 4-16: Holiday Screen, 1 Page Only

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holiday Month</td>
<td>User Def.</td>
<td>Enter a value where 1 equals January and 12 is December.</td>
</tr>
<tr>
<td>Holiday Day</td>
<td>User Def.</td>
<td>Enter day of the holiday between 1 and 31.</td>
</tr>
<tr>
<td>Holiday Year</td>
<td>User Def.</td>
<td>Type in the appropriate year.</td>
</tr>
<tr>
<td>Holiday Type</td>
<td>User Def.</td>
<td>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 <em>P2000 Software User Manual</em>.</td>
</tr>
</tbody>
</table>
When you add or edit an access group, a list of previously defined terminals will appear.

```
<table>
<thead>
<tr>
<th>Terminal Name</th>
<th>Toggle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Select (Y) to enable a terminal for this access group. Select (N) to disable a terminal for this group.</td>
</tr>
</tbody>
</table>
```

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

![Elevator Access Group Screen]

Table 4-18: Elevator Access Group Screen, 1 Page Only

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Name</td>
<td>Toggle</td>
<td>Select (Y) to enable a terminal for this access group. Select (N) to disable a terminal for this access group.</td>
</tr>
<tr>
<td>ID</td>
<td>User Def.</td>
<td>A read-only field that identifies the elevator or cabinet associated with the terminal and floormask or doormask on this line.</td>
</tr>
<tr>
<td>Floormasks/Doormasks</td>
<td>User Def.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

**Table 4-19: Control Door Screen, 1 Page Only**

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Number</td>
<td>User Def.</td>
<td>Enter the reader terminal to manipulate.</td>
</tr>
<tr>
<td>Action Type</td>
<td>Toggle</td>
<td>Choices are: Unlock, Lock, Timed</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Timed Duration</td>
<td>User Def.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 pre-programmed in the system. Although you do have access to these points from this screen, they should not be changed. Reporting problems will occur.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel Tamper (22)</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>PIN Code Retry (19)</td>
<td>Toggle</td>
<td>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).</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter New Password</td>
<td>User Def.</td>
<td>Type in the new password, limited to 9 alphanumeric characters and special characters such as: ~ → + ! ; [ ] { } &lt; &gt;. Remember that your password is case-sensitive.</td>
</tr>
<tr>
<td>Retype New Password</td>
<td>User Def.</td>
<td>Re-enter the password for confirmation.</td>
</tr>
</tbody>
</table>
Reboot

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

![Reboot Screen]

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 may be entered into the system either individually or in batches. To access an individual badge that is residing in the database, enter its number value in the **Start Badge** field. An individual badge may also be created by entering a badge number value in the first submenu, and then by
saving its data in the second submenu. The following screen shots depict the creation of badge number 2 with executive privilege:

![Badge Parameters Screen - Page 1](image)

The `<Prev Rec>` and `<Next Rec>` links are not enabled when creating a new badge as long as `<Save>` has not been selected.

To delete a previously created badge, enter the badge number in the **Start Badge** field and select `<Delete>`.
The next example shows the creation of 10 badges with numbers 25 to 35 having their **Executive Privilege** flags set:

![Image 1](image1.png)

![Image 2](image2.png)

In this case, it is not possible to access each record separately using `<Prev Rec>` and `<Next Rec>` because any change to a data field affects the entire range of badges. These links are only enabled when accessing individual badge records.

To delete a batch of badges previously created, specify a **Start Badge** and an **End Badge** value and then press `<Delete>`.
**Table 4-22: Badge Screen, Page 1**

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Privilege</td>
<td>Toggle</td>
<td>If enabled (Y), the cardholder has unlimited access to all controlled doors.</td>
</tr>
<tr>
<td>Badge Type</td>
<td>Toggle</td>
<td>Choices are Standard and Override. Override allows the cardholder to bypass normal access through keypad override.</td>
</tr>
<tr>
<td>Badge Status</td>
<td>Toggle</td>
<td>Non-editable. Displays the badge type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Legacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PIV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PIV-I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td>Event Privilege</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issue Level</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Badge Status</td>
<td>Toggle</td>
<td>A badge can either be A(ctive) or I(nactive).</td>
</tr>
<tr>
<td>Expiration</td>
<td>User Def.</td>
<td>The date/time the badge expires. If configured to 0, the badge never expires. The controller badge expiration comparisons are based on the P2000 server’s “local time” clock value (not the control's “local time” clock value). <strong>Note:</strong> The controller’s “local time” value may be the same as the P2000 server’s “local time” value, or may have been offset by the value of the panel’s database record parameter Time Offset.</td>
</tr>
<tr>
<td>Custom PIN</td>
<td>User Def.</td>
<td>If using custom, rather than algorithmic PINs, enter the code for the badge (4 to 9 digits). Do not assign a 9 as a digit in the PIN#.</td>
</tr>
</tbody>
</table>
Special Access (A, B, C) | User Def. | The Special Access flag can be set to (A), (B) or (C). See “Assisted Access” on page 4-45 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
Table 4-23: Badge Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Group (1-16)</td>
<td>User Def.</td>
<td>A single badge can be assigned up to 32 access groups (for access groups 17-32 see Badge Parameters Screen - Page 3).</td>
</tr>
<tr>
<td>Time Zone (1-16)</td>
<td>User Def.</td>
<td>A single badge can be assigned up to 32 time zones (for time zones 17-32 see Badge Parameters Screen - Page 3).</td>
</tr>
</tbody>
</table>
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 4-25: Input Screen, 1 Page Only

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Point Name</td>
<td>User Def.</td>
<td>Type in a descriptive name, up to 25 alphanumeric characters long.</td>
</tr>
<tr>
<td>4 State</td>
<td>Toggle</td>
<td>If Y, the input is 4-state. N indicates the input is 2-state.</td>
</tr>
<tr>
<td>Input Point Enabled</td>
<td>Toggle</td>
<td>The input can be activated, meaning: able to report an alarm condition.</td>
</tr>
<tr>
<td>Input Point Delay Enabled</td>
<td>Toggle</td>
<td>If enabled (Y), alarm reporting is delayed for the number of seconds specified.</td>
</tr>
<tr>
<td>Entry/Exit Delay (0-600)</td>
<td>User Def.</td>
<td>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.</td>
</tr>
<tr>
<td>Suppression Timezone</td>
<td>User Def.</td>
<td>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).</td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Activate Relay When Set</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>In-Out Link Type</td>
<td>Toggle</td>
<td>You can choose an input point to link to an output group. Select the appropriate type of linkage from the following choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>None</strong> Default selection, indicating that there is no linkage between the input point and output group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Active-on</strong> When the input point is activated, the output group activates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Secure-on</strong> When the input point is secure, the output group activates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Track</strong> When the input point is activated, the output group activates. When the input point is secure, open, or short, the output group deactivates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Mimic</strong> When the input point is activated, open, or short, the output group activates. When the input point is secure, the output group deactivates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Active-off</strong> When the input point is activated, the output group deactivates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Secure-off</strong> When the input point is secure, the output group deactivates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Reverse track</strong> When the input point is activated, the output group deactivates. When the input point is secure, open, or short, the output group activates.</td>
</tr>
<tr>
<td>Output Group</td>
<td>User Def.</td>
<td>Type an output group number for I/O linking.</td>
</tr>
</tbody>
</table>
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 ten enabled and ten disabled times (including midnight), you can configure up to 20 time blocks per day (enable and disable). The principle of using multiple time blocks during a 24-hour period is shown in Figure 4-12.

![Figure 4-12: Using Multiple Time Blocks](image)

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 4-12.

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.

![Time Zone Screen](image)

Table 4-26: Time Zone Screen, 1 Page Only

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone Name</td>
<td>User Def.</td>
<td>Enter up to 25 alphanumeric characters as a descriptive name for the time zone.</td>
</tr>
<tr>
<td>Output Group</td>
<td>User Def.</td>
<td>Enter the output group to which you want this time zone applied. (optional)</td>
</tr>
</tbody>
</table>
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 4-27: Card Event Overview

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

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

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. It is a two-page screen, described below.
Table 4-28: Card Event Screen, Page 1

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Event Name</td>
<td>User Def.</td>
<td>Type in a descriptive event name up to 25 alphanumeric characters long.</td>
</tr>
<tr>
<td>Door (1 - 64)</td>
<td>Toggle</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 4-29: Card Event Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Type</td>
<td>Toggle</td>
<td>Card/PIN/Keypad Code</td>
</tr>
<tr>
<td>Event Privilege Level</td>
<td></td>
<td>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 F.</td>
</tr>
<tr>
<td>Output Group Enable</td>
<td></td>
<td>Set Output Group (Y/N):</td>
</tr>
<tr>
<td>Activate Strike(Y/N)</td>
<td></td>
<td>Alarm Ack(Y/N):</td>
</tr>
<tr>
<td>Input Group Enable</td>
<td></td>
<td>Set Input Suppression (Y/N):</td>
</tr>
<tr>
<td>Event Period</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 F.

**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.
### Field Type Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Privilege Level</td>
<td>User</td>
<td>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.</td>
</tr>
<tr>
<td>Keypad Code</td>
<td>User</td>
<td>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 F.</td>
</tr>
<tr>
<td>Output Group Enable</td>
<td>Toggle</td>
<td>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.</td>
</tr>
<tr>
<td>Set Output Group</td>
<td>Toggle</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 three-page screen, described below.

### System Information Screen - Page 1

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>IP address of the P2000 Server.</td>
</tr>
<tr>
<td>Note:</td>
<td>Only the Primary Host IP address will appear here.</td>
</tr>
<tr>
<td>Controller Primary IP Address</td>
<td>IP address of the onboard network interface.</td>
</tr>
<tr>
<td>Controller Primary IP Netmask</td>
<td>IP netmask of the onboard network interface.</td>
</tr>
<tr>
<td>Primary Network MAC Number</td>
<td>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.</td>
</tr>
<tr>
<td>Controller Secondary IP Address</td>
<td>This IP address is reserved for future use in support of a secondary IP interface.</td>
</tr>
</tbody>
</table>
## Table 4-30: System Information Screen, Page 1

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Secondary IP Netmask</td>
<td>This netmask is reserved for future use in support of a secondary IP interface.</td>
</tr>
<tr>
<td>Secondary Network MAC Number</td>
<td>Unique MAC encoded into a secondary RS232 network adapter or modem.</td>
</tr>
<tr>
<td>Active Interface</td>
<td>Current network communication status: “Built-in onboard network interface” or “External RS232 interface.”</td>
</tr>
<tr>
<td>128-Bit Badge Number Support</td>
<td>Controller of 128-bit badge numbers is:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled.</strong> 64-bit legacy badge numbers <em>only</em> are supported.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled.</strong> 128-bit PIV/PIV-I and 64-bit legacy badge numbers are supported.</td>
</tr>
<tr>
<td>Card Count</td>
<td>Total number of card (badge) records in the CK721-A database.</td>
</tr>
<tr>
<td>Elevator Access Group Count</td>
<td>Total number of Elevator Access Groups records in the CK721-A database.</td>
</tr>
<tr>
<td>History Record Count/Total</td>
<td>Total number of stored history transactions in the CK721-A database.</td>
</tr>
</tbody>
</table>
System Information Screen - Page 2 (Terminal and Security Level Status)

Table 4-31: System Information Screen, Page 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level (0 to 99)</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Status:</td>
<td>Key:</td>
</tr>
<tr>
<td>Reader</td>
<td>-- Not found</td>
</tr>
<tr>
<td>Output</td>
<td>** Not defined and off-line</td>
</tr>
<tr>
<td>Input</td>
<td>Up Defined and on-line</td>
</tr>
<tr>
<td></td>
<td>Dn Defined but off-line</td>
</tr>
</tbody>
</table>
Device status is listed from the first module to the last, left to right.

Table 4-32: System Information Screen, Page 3

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone Status</td>
<td>64 time zones can be defined. Status of each is shown as E(nabled), D(isabled), or (-- undefined.</td>
</tr>
</tbody>
</table>

**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.
Every output point, no matter which option was selected for it, can be commanded with 5 different active states. See Table 4-34 to determine the effect of the commands on each selected state.

Table 4-33: Control Output Screen, 1 Page Only

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

Table 4-34: Results of Command Override on a Selection

<table>
<thead>
<tr>
<th>Comanded as:</th>
<th>Programmed as:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set</td>
</tr>
<tr>
<td><strong>Set</strong></td>
<td>Set</td>
</tr>
<tr>
<td><strong>Reset</strong></td>
<td>Reset</td>
</tr>
<tr>
<td><strong>SlowFlash</strong></td>
<td>SlowFlash</td>
</tr>
<tr>
<td><strong>QuickFlash</strong></td>
<td>QuickFlash</td>
</tr>
<tr>
<td><strong>Timed</strong></td>
<td>Timed (to the Set state)</td>
</tr>
</tbody>
</table>
Change Date

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

![Date Time Display](image)

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.
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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Information Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit environment not as specified.</td>
<td>Table 1-5.</td>
</tr>
<tr>
<td>Unit power and grounding not as specified.</td>
<td>Page 2-17, Table 3-2, and Appendix C.</td>
</tr>
<tr>
<td>Cable length or type not as specified.</td>
<td>Page 2-11, Table 3-1, and Figure 3-19.</td>
</tr>
<tr>
<td>Backup battery not replaced correctly.</td>
<td>This chapter.</td>
</tr>
</tbody>
</table>
**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.

**IMPORTANT:** The lithium battery is polarized. Ensure the side marked ‘+’ faces out or towards you.

**CAUTION:** Replace the battery with a lithium battery of the same type and voltage rating. Dispose of the used battery in accordance with local, national, and regional regulations. Failure to replace the battery with one of the same type and voltage rating may result in an explosion causing personal injury and property damage.

**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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reader down</td>
<td>Incorrect wiring from reader to reader terminal</td>
</tr>
<tr>
<td></td>
<td>Reader is unassigned</td>
</tr>
<tr>
<td></td>
<td>Defective reader terminal</td>
</tr>
<tr>
<td>Red light or no reader light illuminates when card is used at reader, and access is not granted.</td>
<td>Invalid Time zone/Reader/Issue Level/Facility Code</td>
</tr>
<tr>
<td></td>
<td>Card no longer in database</td>
</tr>
<tr>
<td></td>
<td>Incorrect card type</td>
</tr>
<tr>
<td></td>
<td>Card is being swiped backwards</td>
</tr>
<tr>
<td></td>
<td>Reader inoperative</td>
</tr>
<tr>
<td></td>
<td>Damaged card</td>
</tr>
<tr>
<td></td>
<td>Bad cabling</td>
</tr>
<tr>
<td></td>
<td>Failed PCB</td>
</tr>
<tr>
<td></td>
<td>Multiple proximity cards in reader antenna field</td>
</tr>
</tbody>
</table>
## Table 5-2: Troubleshooting Guidelines

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door will not go into “Override Mode” but grants access when a card is used.</td>
<td>Override time zone is incorrectly programmed, or not programmed. Override option not set.</td>
</tr>
<tr>
<td>Alarm not reporting</td>
<td>Alarm is suppressed (i.e., not in an active time zone) Associated input point not defined Bad wiring or input device</td>
</tr>
<tr>
<td>PIN Code function not operating</td>
<td>PIN is not programmed as part of the access condition Broken wire or incorrect wiring from the keypad to PCBA Defective keypad</td>
</tr>
<tr>
<td>Card or data loss from database</td>
<td>Noise on power line Improper grounding Defective CK721-A</td>
</tr>
<tr>
<td>System restarts continuously</td>
<td>System improperly grounded Severe power variations Defective CK721-A</td>
</tr>
<tr>
<td>Red or Green lamp does not illuminate, but access is denied or granted if card is used.</td>
<td>Open wire at lamp connection Burned out lamp bulb Defective reader terminal</td>
</tr>
<tr>
<td>Holiday time zones not followed</td>
<td>Improperly programmed Holiday time zones or Holiday dates.</td>
</tr>
</tbody>
</table>
A. EXPANDED ADDRESS S300 BUS

The CK721-A version 3.2 firmware release supports an Expanded Address S300 Bus feature. This feature increases the number of logical terminals allowed on the S300 bus from 16 to 64. The terminals are addressed Logical Terminal 1 to Logical Terminal 64.

The CK721-A version 3.2 firmware is backwards compatible with the Legacy Address S300 Bus method, which uses Logical Terminal 1 to Logical Terminal 16.

The following table compares the two addressing modes, including the required module and firmware version:

<table>
<thead>
<tr>
<th></th>
<th>Legacy Address S300 Bus</th>
<th>Expanded Address S300 Bus</th>
<th>OSDP Support and Expanded Address S300 Bus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. number of logical terminals</td>
<td>16</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Terminal address</td>
<td>Logical Terminal 1 to Logical Terminal 16</td>
<td>Logical Terminal 1 to Logical Terminal 64</td>
<td>Logical Terminal 1 to Logical Terminal 64</td>
</tr>
<tr>
<td>Module/ firmware version</td>
<td>RDR2S, v. PS-215R or later</td>
<td>RDR2S-A, v. PS-217E or later</td>
<td>RDR2S-A, v. PS-217F or later</td>
</tr>
<tr>
<td></td>
<td>RDR2S-A, v. PS-217C3 or earlier</td>
<td>I8O4, v. PS-217E or later</td>
<td>I8O4, v. PS-217F or later</td>
</tr>
<tr>
<td></td>
<td>RDR2, v. PS-201E or later</td>
<td>RDR8S, v. PS-218A or later</td>
<td>RDR8S, v. PS-218B or later</td>
</tr>
<tr>
<td></td>
<td>SI08/SI8, v. PS-184B or later</td>
<td>I32O16, v. PS-218A or later</td>
<td>I32O16, v. PS-218B or later</td>
</tr>
<tr>
<td></td>
<td>IO8/I16, v. PS-183D or later</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The following elevator access interfaces support up to 16 terminals (readers) per controller and P2000 logical terminal range 1 through 64:
- Standard Low Level Interface
- D620-ECG Low Level Interface
- KONE HLI/KONE ELINK High Level Interface
- KONE IP High Level Interface
- ThyssenKrupp High Level Interface
The Expanded Address S300 Bus allows a CK721-A version 3.2 controller to communicate with up to 32 modules on the RS485 bus.

New modules (RDR2S-A, I8O4, RDR8S, I32O16) allow greater flexibility in the mapping of the logical terminal number (1-64) to a physical device (0-31) through the use of physical addressing mode. The logical terminal number (1-64) is mapped to the physical address.

The RDR8S module allows up to 8 reader terminal index numbers to be mapped to a single physical address.

The I32O16 module allows up to 32 inputs, 16 relay outputs, and 16 open collector outputs to be mapped to a single physical address.

The RDR2S-A module allows up to 2 reader terminal index numbers to be mapped to a single physical address. Numerous possibilities of logical to physical mappings exist.

The I8O4 module allows up to 8 inputs, 4 relay outputs, and 4 open collector outputs to be mapped to a single physical address.

The following table contains several examples for mapping a logical terminal number to a physical device:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Hardware Module Number (Physical Address), Value Range 0-31</th>
<th>Reader Terminal Index, Value Range 1-8</th>
<th>Logical Terminal Number, Value Range 1-64</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDR2S-A</td>
<td>0</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>RDR2S-A</td>
<td>1</td>
<td>2</td>
<td>31</td>
</tr>
<tr>
<td>RDR2S-A</td>
<td>27</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>RDR8S</td>
<td>14</td>
<td>7</td>
<td>63</td>
</tr>
<tr>
<td>RDR8S</td>
<td>28</td>
<td>8</td>
<td>17</td>
</tr>
<tr>
<td>LEGACY</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
B. PERFORMANCE ANALYSIS

The data presented in this section was derived by connecting a number of modules on the RS-485 bus. The test measured the response time between reading two badges by two readers on the same module and unlocking two doors.

Table B-1: CK721-A Using Legacy Addressing Mode

<table>
<thead>
<tr>
<th>Number of modules with I/O enabled</th>
<th>Average response time in ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>695</td>
</tr>
<tr>
<td>8</td>
<td>1258</td>
</tr>
<tr>
<td>16</td>
<td>1744</td>
</tr>
</tbody>
</table>

Table B-2: CK721-A Using Physical Addressing Mode

<table>
<thead>
<tr>
<th>Number of modules with I/O enabled</th>
<th>Average response time in ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>344</td>
</tr>
<tr>
<td>9</td>
<td>367</td>
</tr>
<tr>
<td>16</td>
<td>541</td>
</tr>
<tr>
<td>24</td>
<td>755</td>
</tr>
<tr>
<td>32</td>
<td>976</td>
</tr>
</tbody>
</table>
Figure B-1: CK721-A Access Time Performance Graph

- - - Legacy addressing mode
--- - Physical addressing mode

Response time in milliseconds

- Number of modules
C. 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.

IMPORTANT: Conduit ground, cold water pipes, unbrazed joints, or dissimilar metals are unacceptable in the path of either building or supplement 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 C-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.
The two curved parts of the shroud shown in Figure C-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.

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

**Non “D-Type” Grounding Connections**

As shown in Figure C-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 C-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 C-3 shows an alternate method of shielding. Cables connected to user peripherals (printers, VDTs, etc.) should have shields connected 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 C-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 C-2: Example of Grounding Shielded Cable at Both Ends**

- **UNIT1**
  - Separated wires of cable are not shielded
  - The screen-type shield is inside the enclosure, no more than 2" (5cm)

- **UNIT2**
  - Short wire is connected from shield to enclosure of unit 1
  - Short wire is connected from shield to enclosure of unit 2

- PCBA

---
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 C-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.
**D. DOOR OPEN/AUX ACCESS SUPERVISION**

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

- On the SIO8 module, set position four of SW1 to ON.
- Wire relays five through eight on the SIO8 module to the DOOR and AUX inputs on the RDR2 module.
- Wire the corresponding inputs from J6C and J6D on the SIO8 module, 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 SIO8 modules provides the capability to link alarms five through eight to output relays five through eight.

These main points are important to remember:

- The four-state inputs are linked to the output relays through the SIO8 module 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 SIO8 module, to ON. This links AL5 through AL8 to output relays five through eight as shown in Table D-1.

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

<table>
<thead>
<tr>
<th>Input State for Inputs 5-8</th>
<th>Output Relay State for Outputs 5-8</th>
<th>SIO8 Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>Unenergized</td>
<td>Secure</td>
</tr>
<tr>
<td>Alarm</td>
<td>Energized</td>
<td>Secure</td>
</tr>
<tr>
<td>Open</td>
<td>Unenergized</td>
<td>Open</td>
</tr>
<tr>
<td>Short</td>
<td>Unenergized</td>
<td>Short</td>
</tr>
</tbody>
</table>

From the SIO8 module, 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 SIO8 module are hard-wired to the DOOR or AUX inputs on the 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 SIO8 module without affecting the reader module’s inputs. As a result, the relay contacts will appear to the 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 SIO8 output relays to the RDR2 module.
E. 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 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 E-1: 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.

After writing the database to Flash memory, the panel will reboot.
F. 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 than 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** must be set to 5.

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 badge¹, 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.

**INVOKEING 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** must be set to **5**.

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\footnote{The badge can be presented at any time before the # key is pressed.}, and press the # key.

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** must be set to 5.

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 time zones.

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, 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 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.
Invoking Access Requests from a Keypad

**With Badge**
To request access: Present the badge.

**With PIN Only**
To request access: Enter the PIN number.

**With Card ID**
To request access: Enter the Card ID number.

**With PIN and Card ID**
To request access: Enter the PIN and Card ID.

**With PIN and Badge**
To request access: Enter the PIN and present the badge.

**With PIN and Badge, allowing PIN after Badge**
To request access: Enter the PIN and present the badge.

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: Enter the Air Crew PIN.

To request access with Star Feature: Enter the Air Crew PIN.

---

Legend

<table>
<thead>
<tr>
<th>Keypad Code</th>
<th>Enter the Keypad Code.</th>
<th>badge</th>
<th>Present the badge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>Enter the PIN number.</td>
<td>#</td>
<td>Press the specified key.</td>
</tr>
<tr>
<td>Card ID</td>
<td>Enter the Card ID number.</td>
<td>#</td>
<td># A D</td>
</tr>
<tr>
<td>Minutes</td>
<td>Enter the number of minutes.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Invoking Timed Overrides from a Keypad

**With Badge**

To start override without Star Feature: 

To stop override without Star Feature: 

To start override with Star Feature: 

To stop override with Star Feature: 

**With PIN Only**

To start override without Star Feature: 

To stop override without Star Feature: 

To start override with Star Feature: 

To stop override with Star Feature: 

**With Card ID**

To start override without Star Feature: 

To stop override without Star Feature: 

To start override with Star Feature: 

To stop override with Star Feature: 

**With PIN and Card ID**

To start override without Star Feature: 

To stop override without Star Feature: 

To start override with Star Feature: 

To stop override with Star Feature: 

**With PIN and Badge**

To start override without Star Feature: 

To stop override without Star Feature: 

To start override with Star Feature: 

To stop override with Star Feature: 

**With PIN and Badge, allowing PIN after Badge**

To start override without Star Feature: 

To stop override without Star Feature: 

To start override with Star Feature: 

To stop override with Star Feature: 

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: \( \text{A} \) Keypad Code \( \text{badge} \)
- To deactivate event without Star Feature: \( \text{D} \) Keypad Code \( \text{badge} \)
- To activate event with Star Feature: \( \text{*1} \) Keypad Code \( \text{badge} \)
- To deactivate event with Star Feature: \( \text{*4} \) Keypad Code \( \text{badge} \)

### 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 \( \text{badge} \)
- To deactivate event without Star Feature: PIN D Keypad Code \( \text{badge} \)
- To activate event with Star Feature: PIN *1 Keypad Code \( \text{badge} \)
- To deactivate event with Star Feature: PIN *4 Keypad Code \( \text{badge} \)

### With PIN and Badge, allowing PIN after Badge
- To activate event without Star Feature: PIN A Keypad Code \( \text{badge} \) #
- To deactivate event without Star Feature: PIN D Keypad Code \( \text{badge} \) #
- To activate event with Star Feature: PIN *1 Keypad Code \( \text{badge} \) #
- To deactivate event with Star Feature: PIN *4 Keypad Code \( \text{badge} \) #

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.
G. CONFIGURING SSH AND SFTP CLIENTS

On the CK721-A controller, the FTP and Telnet services are disabled when encryption is turned on. You can use the PuTTY or WinSCP client software to log into the CK721-A controller via remote connections (see chapter 4 for CK721-A user interface options).

NOTE: This appendix provides information about third-party client software installation and configuration, as available at the time of publication. For the latest and most accurate information refer to online sources. Some screens and selections described in this appendix may differ; however, the general guidelines can still be follow.

PUTTY CLIENT

PuTTY is an SSH and Telnet client for the Windows platform. PuTTY is an open source software that is available with source code and is developed and supported by a group of volunteers. It can be downloaded from www.putty.org.

To use PuTTY to initiate secure remote connection:

1. Install PuTTY application from one of the free download sources on the web.

2. Run the application:
3. The PuTTY Session configuration window opens up.

![PuTTY Configuration Window]

To configure PuTTY session before loading it for the first use:

1. In the Putty Configuration window, with **Session** selected in the left window pane, configure the following in the right window pane:

   - Enter the IP address of the controller in the **Host Name (or IP address)** dialog box.
   - Select the **SSH** radio button.
• Enter name for the configuration in the **Saved Sessions** field (in the example below, “CK721-A”):
2. Select **Kex** selected in the left window pane. In the right window pane, select the **Diffie-Hellman group 14** for **Algorithm selection policy**. Use the **Up** button to move it to the top of the list.
3. Select **Data** in the left window pane. For **Terminal type-string** enter value **vt100**.

4. Click **Save** to save the session. To open communication to the panel at this point, click **Open**. Otherwise, close the window.

After the session configuration has been saved, when you re-open PuTTY you can simply select it from the Saved Sessions list and click **Load** button.

---

**NOTE:** The very first time a Controller is configured, a PuTTY Security Alert message may pop up about the Server’s host key not being cached in the registry. Click **Yes** to continue.

---

**To log in to PuTTY:**

1. Launch the PuTTY application.
2. Select the saved session configuration (in this example, “CK721-A”) and click **Load**.

![PuTTY Configuration](image1)

3. To open communication to the panel, click **Open**.

   The login screen appears.

![Login Screen](image2)
4. Proceed with login as you would using the TeraTerm.

**WinSCP Client**

WinSCP is a free SFTP client for Windows operating systems. It can be downloaded from www.winscp.net.

**To install WinSCP:**

1. Install the latest version of WinSCP secure SFTP client application. (At the time of publication of this manual, version 4.3.4 was the latest WinSCP release available.)
2. The Setup – WinSCP window opens. Verify that the **Typical installation** is selected and click **Next**.

3. Select Commander interface. This will allow you to display both the local and the remote directory entries.
4. Click **Install**. Desktop location for the installation is recommended.

5. Verify that the **Launch WinSCP** button is selected and click **Finish**.

To configure WinSCP session before loading it for the first use:

1. Launch the WinSCP application.
2. In the WinSCP Login screen appears.

![WinSCP Login Screen]

3. With **Session** selected in the left window pane, configure the following in the right window pane:

   - **Host name** - the IP address of the controller panel
   - **Port number** - port number 22 (default value) is required for secure SFTP connection
   - **User name** - the name with which to login to the controller
   - **Password** - the password with which to login to the controller (In the example below, `diag` user name and `master` password are used)
   - **File Protocol** - select SFTP
Do not close the window yet.

4. Select the **Advanced options** radio button to access the SSH key exchange settings.

5. Select **Key exchange** in the left window pane. In the right window pane, select the **Diffie-Hellman group 14** for **Algorithm selection policy**. Use the **Up** button to move it to the top of the list.

6. Select **Directories** in the left window pane. In the right window pane, specify:
• **Remote directory** - location to which the files will be transferred
• **Local directory** - location that contains the files to be transferred over to the controller

Leave remaining settings at their default values.

7. Specify a name and click **Save** to save the session.

8. Close the window.

After the session configuration has been saved, when you re-open WinSCP you can simply select it from the list and click **Login** button.

**NOTE:** Note that the directories, specifically the **Local directory**, may need modification to point to the correct path for the source files.

**To log in to WinSCP:**

1. Launch the WinSCP application.
2. Select the saved session configuration (in this example, “diag@159.222.109.253”) and click **Login**.

3. Specify **Password** and click **OK**.
The WinSCP commander interface opens, providing access to the source and destination folders, with the files to be transferred.
H. WIRING CONCEPTS

This appendix described wiring concepts that apply to the CK721-A.

WIRING READERS

Figure H-1 shows the maximum cable distances allowed between a S300 expansion enclosure and a reader.

![Figure H-1: Maximum Distance Between Readers and S300 Expansion Enclosures](image)

Wiring for Door Controls

Doors unlock due to signals sent by the S300-RDR2S-A or S300-RDR8S module 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-RDR2S-A or S300-RDR8S module 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

**Door Strike Wiring**

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).
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).

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 (RDR2S-A or RDR8S 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.

![Field Installed Metal Oxide Varistor](image)

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

**IMPORTANT:** Observe the following precautions: 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.

Output Wiring

To insure proper operation and extend the contact life of mechanical relay 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.

![Diagram of Output Wiring](image)

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

IMPORTANT: 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.