

SECTION 16nnn

CIRCON ACCESS CONTROL SYSTEM

This document is a guide specification template for a Circon access control system specification. It is intended to be modified where necessary for a specific project. In the document, the italicized phrase *<insert here>* indicates where the substitution of applicable information specific to the project is needed.

This document is provided in Word format so that it can be edited. For best results, please use the Word styles Normal, Heading 1, Heading 2, List ABC and List 123 .

CONTENTS

1	PART 1 – GENERAL	3
1.1	General	3
1.2	System description.....	3
1.3	Definitions, acronyms and abbreviations	3
2	PART 2 – PRODUCTS.....	6
2.1	Host computer and operating system software	6
2.2	Relational database software.....	6
2.3	Access control application software	6
2.4	LNS network database software	8
2.5	LNS network management software	8
2.6	Access Point controllers.....	8
2.7	Card readers	11
2.8	Credentials – cards and fobs	13
2.9	Power Supplies	14
2.10	Request to exit devices.....	15
2.11	Electric locking devices.....	15
2.12	Electrical control, power and low voltage wiring.....	15
3	PART 3 – EXECUTION	17
3.1	Inspection.....	17
3.2	Preparation.....	17
3.3	Installation	17
3.4	System testing and certification	17
3.5	Training	18

1 PART 1 – GENERAL

1.1 GENERAL

The intent of this section is to specify the minimum criteria for the design, supply, installation and commissioning of a complete, LonWorks network-based, integrated access control system.

1.2 SYSTEM DESCRIPTION

A Overview

1. *<insert a description of the access control system you are specifying>*

B Products Supplied and installed

1. Access control system host computer and operating system software
2. Access control application software
3. Relational database software
4. LNS network database software
5. LNS network management software
6. LonWorks network interface
7. Access point controllers
8. Card readers
9. Cards
10. Power supplies
11. Alarm input devices including, but not limited to, door position switches
12. Request to exit devices
13. Electric locking devices

C Related Sections

1. Section 16050 – Basic Electric materials and Methods
2. Section 16100 – Wiring Methods
3. Section 16200 – Electrical Power
4. Section 16400 – Low Voltage Distribution

1.3 DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Access group – a collection of access users. The access permissions for the access group define the access permissions for all members of the access group. Access user members of an access group are granted access at same access points at the same scheduled times.

Access group schedule – An access group schedule defines the range of hours and days when members of the access group are granted and denied access at the access points associated with the access group. An access group schedule is in effect only when the access point's operating mode is Controlled Access

Access point – An access point represents either a physical door or gate, or a call button in an elevator cab, at which access users are granted or denied access. An access point is also a logical entity in the SQL database.

Access user - An access user is an individual, to whom a card (or multiple cards) is issued, allowing him or her to gain access at one or more access points, based on access permissions.

Action – An action specifies an output variable and how that output variable is manipulated when the action is triggered by its associated event. An action specifies the manipulation as an on value, duration and an off value. The action is triggered by an associated event generated by the APC-300. Typical events are: access granted, enclosure tamper, door held open, and so on. The output variable may be either an output point or a shared network variable on the APC-300.

Alarm – An alarm is an event of significant importance in the day-to-day operation of an access control system. Operators and facility managers of the access control system typically want to be notified immediately when alarm events occur. Alarms are generated by APC-300s and sent to Access Integrator for logging. Operators

APC-300 - APC-300 is an acronym for Circon's **Access Point Controller -300**, a LonMark-certified device that provides access control for one or two access points.

APC-300-EAC - APC-300-EAC is an acronym for Circon's **Access Point Controller -300 Elevator Access Control**, a LonMark-certified device that provides access control for one to thirty-two access points or call buttons in an elevator cab.

Antipassback – is the capability of an access control system to prevent access users that have entered a designated antipassback zone, via a valid credential presentation, from entering that zone again without first verifying that they have left the zone, by presenting their credentials to an exit reader.

Custom field – A custom field is an optional data entry field that extends access user properties with information unique to the partition of which the access user is a member. For example, the license number of their motor vehicle, their hire date or a brief description of a distinguishing personal characteristic.

Equipment schedule – An equipment schedule provides a "door schedule" that sets the level of access permitted (no access, controlled access, and public access) by an access point to an authorized access user at any particular day and time.

Event – An event is something important that happens and is detected and logged by an APC-300. The importance of an event is indicated during the configuration of the APC-300 by enabling the type of event to be logged. Some types of events are also considered to be alarms.

LNS – LonWorks Network Service, a product from Echelon Corporation, provide the network operating software for LonWorks networks.

Operating mode –The operating mode determines the level of security at an access point, on a time-of-day basis. There are three possible operating modes:

No Access – the access point is locked and cannot be unlocked by any access user. In elevator access control, the call button is disabled.

Controlled Access – the access point is locked but unlocks temporarily upon presentation of certain access user's credentials. In elevator access control, the call button is disabled but is enabled temporarily upon presentation of certain access user's credentials.

The credential must pass the test of who, where and when as determined by the properties of an access group of which the access user is a member.

Public Access - the access point is unlocked and anyone may gain access freely. In elevator access control, the call button is enabled and anyone may gain access freely to that floor.

The operating mode set by the equipment schedule state.

Operator - An operator is an individual who logs in to Access Integrator to administer the access control system. An operator has defined access capabilities and permissions to view and/or change parts of the access control system. An operator's capability can be very broad or it can be greatly restricted, or anywhere in between. Operator access is password protected.

Partition – A partition represents a virtual access control system - a segment of Access Integrator's SQL database that can be protected by unique permissions to limit access to authorized operators. A site can have multiple partitions to contain different access control system information, with each partition having different permissions and authorized operators. Partitions can be used in a commercial building with multiple tenants where each tenant has their own partition and all tenants share control of a partition for common areas of the facility. Partitions allow one site to appear as multiple "virtual" access control systems.

Plug-in - A plug-in is an add-on software interface launched from the network management tool environment that provides point-and-click access to the internal configuration properties of a LonWorks device.

Test - a powerful mechanism for influencing certain decisions or functions of the access control system. A test can be used to:

- determine whether or not an access user should be granted access,
- override an access point operating mode
- reset the location of access users in an antipassback zone

2 PART 2 – PRODUCTS

2.1 HOST COMPUTER AND OPERATING SYSTEM SOFTWARE

- A Host computer - the host computer shall be installed at the location indicated by the owner. The host computer shall be connected to the LonWorks network by a local network interface or a remote network interface, to gain access to the APC-300s. The host computer shall include, at a minimum, the following components:
1. Processor: Intel Pentium 4, 1 GHz or higher
 2. Memory: 256 Mbytes RAM, 512 Mbytes recommended
 3. Hard drive: 4 GB for application and databases
 4. Display: 1024 X 768 resolution
 5. Backup: writable DVD drive
 6. Ethernet: 10/100 Mbps port
 7. LonWorks network interface: internal card or Ethernet-connected remote interface
 8. CD ROM drive
 9. Keyboard and mouse
- B Operating System Software – the host computer’s operating system shall be Microsoft Windows XP Professional with Service Pack 2 and all other necessary patches.

2.2 RELATIONAL DATABASE SOFTWARE

- A Microsoft SQL Server 2005 Express Edition shall be used as the relational database software that resides on the host computer.
- B Optional: for SQL database with intended size greater than four Gbytes and for advanced features such as high availability, use the appropriate Microsoft SQL Server 2005 edition: Workgroup, Standard, or Enterprise.

2.3 ACCESS CONTROL APPLICATION SOFTWARE

- A Circon Access Integrator shall be used as the access control application and shall include, at a minimum, the following features:
1. Access Integrator shall provide a single application that allows authorized system administrators to manage the access control system and access users.
 2. Access Integrator shall provide scalable solutions to meet the needs of any size organization, from an entry-level two-reader system to a large corporation with several facilities and thousands of access points and access users located around the world.
 3. Access Integrator shall be fully integrated with the LNS network database
 4. Access Integrator shall support multiple operators that can be assigned various permission levels to restrict their access to certain Access integrator functions.
 5. Access Integrator shall keep a log of operator activities.

6. Access Integrator shall allow operators to partition the database into multiple segments, to limit the display and manipulation of tenant data. By partitioning the database, individual tenant administrators can view and manage only those access users, card formats and APC-300s within their authorized partition.
7. Access Integrator shall support unlimited access groups. All members of the access group are assigned the same permissions.
8. Access Integrator shall allow operators to assign up to four actions to access groups which are initiated by the APC-300 when any member of the group is granted access.
9. Access Integrator shall allow operators to maintain access users' records that include an individual's name, description, expiry dates for the cards (optional), a picture, and a signature and so on. There should also be a disable function, which allows a card to be temporarily disabled (i.e. access will be denied at all access points) if the card is lost or stolen.
10. Access Integrator shall allow operators to create custom fields that allow the access user information to be expanded with fields that are specific to the owner's requirements, such as license plate number, employee number and so on.
11. Access Integrator shall allow operators to configure access users' access permissions. Permissions are assigned to the access group and therefore apply to all access users in the group. The permissions define when the access users are granted access and the access points where they may gain access.
12. Access Integrator shall allow operators to maintain a separate equipment schedule for each access point. An equipment schedule uses facility automation system occupancy state terminology that is translated by the APC-300 into its access control operating mode: Controlled Access, No Access, and Public Access.
13. Access Integrator shall allow operators to maintain access group schedules. Each access group has an access group schedule defined for its access user members that the APC-300 uses to determine when they are to be granted or denied access. The access group schedule allows for simple control of personnel and other access users into and out of a facility or area within a facility based on days, dates and times.
14. Access Integrator shall allow operators to assign multiple unique cards to an access user. Each card shall be configured with enable/disable, expiry date and optional PIN code.
15. Access Integrator shall display alarms graphically and with audible annunciation the moment they are received from an APC-300. Using standard email systems, alarms can be transmitted automatically to administrators or guards in the field, in real-time without operator intervention. Alarm acknowledgement with an associated text comment is also supported.
16. Access Integrator shall periodically query each APC-300, uploads its event information, and save event information in the SQL database to

provide historical data for future investigation and analysis. This information can also be exported in a format suitable for use with standard analytical tools such as Microsoft Excel.

17. Access Integrator shall provide access to information in its SQL database through built-in formatted reports and through ad-hoc reports in tabular format. The built-in reports contain information about access users, access groups and access points and “who-where-when”. The reporting interface is designed for ease-of-use; end user training should not be required. The reports are formatted for printing on standard office printers on 8/12 by 11 size paper.
18. Access Integrator shall allow operators to create ad-hoc views of recorded events in tabular format and export events to another software tool. Log Viewer allows you to analyze the event data in many ways: to discover usage trends, to trace access user activity or to prepare who, where, when views, for example.
19. Access Integrator shall allow operators to override APC-300 decision and grant access to an access user at a particular door.
20. Access Integrator shall allow operators to launch the LNS configuration plug-in for an access point controller.

2.4 LNS NETWORK DATABASE SOFTWARE

- A Echelon Corporation’s LNS Turbo Edition software shall be used as the LonWorks network database software and shall include all necessary service packs.

2.5 LNS NETWORK MANAGEMENT SOFTWARE

- A Circon Network Integrator software shall be used as the LNS network management application.

2.6 ACCESS POINT CONTROLLERS

- A The Circon Access Point Controller (APC-300) shall be used as the access point controller for doors and gates.
- B The Circon Access Point Controller (APC-300) shall include, at a minimum, the following hardware features:
 1. The APC-300 shall be an intelligent, distributed, single-circuit-board device with a 32-bit microprocessor to run the application and a Neuron processor to run the ANSI/EIA/CEA 709.1 (LonTalk) protocol communications. It is LonMark certified.
 2. The APC-300 shall support two independent access points with entry readers or one access point with both entry and exit readers. The APC-300 shall accept card data from both card readers simultaneously.
 3. The access user card and permissions database and the device configuration information shall be stored in non-volatile memory.
 4. The application program shall be stored in non-volatile memory.
 5. The APC-300 shall contain a real-time clock chip. The application shall use the clock to timestamp events, validate schedules and time the durations of I/O events. The clock shall automatically adjust for leap year

and daylight savings time adjustments. It shall include the capability to retain its date and time for 10 days in the event of a power outage.

6. The APC-300 shall provide six supervised, dry contact input points that are user-configurable for door position switches, request to exit devices, special needs request or other peripheral devices
7. The APC-300 shall provide four user-configurable form C relay output points with individual status LEDs. The outputs shall be user-configurable for electromagnetic or electric strike door lock devices, door opening devices or controlling other peripheral devices.
8. The APC-300 shall provide two Wiegand reader interfaces.
9. The APC-300 shall provide a dry contact input point for optional tamper detection. If tamper detection is not required, this input point can be used for other purposes.
10. The APC-300 shall provide auxiliary 12 VDC power terminals capable of sourcing 1.5 Amps.
11. The APC-300 power requirements shall not exceed 24VAC at 2 Amps.

C The Circon Access Point Controller (APC-300) shall include, at a minimum, the following application features:

1. The APC-300 shall come with a complete set of LonMark certified resource files and LNS plug-in software.
2. The APC-300 shall operate independently of the host computer. Once the access users, schedules and access groups are downloaded, it makes access control decisions, unlocks doors and records events without communicating to the host computer or other APC-300s (except when antipassback is implemented).
3. The APC-300 shall support cards with up to 128 bits of information.
4. The APC-300 shall hold up to 10,000 access user cards in its internal, non-volatile database.
5. The APC-300 shall hold up to 64 access groups and 64 access group schedules in its internal, non-volatile database.
6. The APC-300 shall include an event log that holds 1,500 events. The events shall be uploaded periodically to the host computer.
7. The APC-300 shall support hard and soft antipassback with several options for resetting the condition.
8. The APC-300 shall afford access users with special needs special consideration by the access point sequence of operation in the form of extended entry time and automatic door opening.
9. The APC-300 shall, upon presentation of a credential to a reader, respond with access granted or denied in less than 500 milliseconds.
10. The APC-300 shall support any reader that communicates with the standard Wiegand interface.
11. The APC-300 shall support the Indala reader/keypad that communicates with the standard Wiegand interface, when card and PIN access requests are required.

12. The APC-300 shall allow the electric locking mechanism to be user-configurable to be controlled as fail safe or fail secure.
 13. The APC-300 shall be capable of generating various alarm events that the user can choose to enable or disable, per access point. Alarm events shall be transmitted to the host computer in real-time for annunciation. The APC-300 shall detect the following alarm conditions:
 - access denied
 - door open warning and door open alarm
 - door forced open
 - tamper
 - duress
 - antipassback violation
 14. The APC-300 shall allow the timeout interval for the door held open warning, door held open alarm and the special needs extra delay for these timeouts to be user-configurable.
 15. The APC-300 shall allow the timeout interval for the momentary door unlock to be user-configurable.
 16. The APC-300 shall be capable of operating each access point independently in the following modes:
 - Controlled Access* – access through the door is controlled based on schedules and access group permissions
 - No Access* – door is locked and no entry or exit is allowed.
 - Public* – door is unlocked; anyone can enter and exit freely.
 17. The APC-300 shall support actions which allow the user to configure a simple sequence that is triggered when access is granted or when a specified event occurs. The sequence can activate an output point for local annunciation or update an output network variable to implement interoperability with other LonWorks devices on the network, such as HVAC or lighting.
 18. The APC-300 shall support tests which the user to configure simple conditions which result is a true or false evaluation, based on an input point or input network variable. The test results can be used to implement advanced access control functions.
 19. The APC-300 shall allow its configuration information to be modified and its application program to be downloaded over the LonWorks network without the need to physically gain access to the device.
- D The Circon Access Point Controller for Elevator Access Control (APC-300-EAC) shall be used as the access point controller for elevator floor access.
- E The Circon Access Point Controller for Elevator Access Control (APC-300-EAC) shall include, at a minimum, the following hardware features:
1. The APC-300-EAC shall consist of the same APC-300 hardware platform, described earlier, combined with an elevator access control application that is different from the door access control application and uses the hardware capabilities differently.
- F The Circon Access Point Controller for Elevator Access Control (APC-300-EAC) shall include, at a minimum, the following application features:

1. The APC-300-EAC shall come with a complete set of LonMark certified resource files and LNS plug-in software.
2. The APC-300-EAC shall operate independently of the host computer. Once the access users, schedules and access groups are downloaded, it makes access control decisions, enable floor buttons and records events without communicating to the host computer or other APC-300s.
3. The APC-300-EAC shall support cards with up to 128 bits of information.
4. The APC-300-EAC shall hold up to 10,000 access user cards in its internal, non-volatile database.
5. The APC-300-EAC shall hold up to 64 access groups and 64 access group schedules in its internal, non-volatile database.
6. The APC-300-EAC shall include an event log that holds 1,500 events. The events shall be uploaded periodically to the host computer.
7. The APC-300-EAC shall support any reader that communicates with the standard Wiegand interface.
8. The APC-300-EAC shall support the Indala reader/keypad that communicates with the standard Wiegand interface, when card and PIN access requests are required.
9. The APC-300-EAC shall support one elevator cab and up to 32 floors when external I/O devices are added. Without external I/O, it controls four floors.
10. The APC-300-EAC shall support call button feedback for up to 32 floors as provided by an external I/O device.
11. The APC-300-EAC shall be capable of generating various alarm events that the user can choose to enable or disable, per access point. Alarm events shall be transmitted to the host computer in real-time for annunciation. The APC-300 shall detect the following alarm conditions:
 - access denied
 - tamper
 - duress
12. The APC-300-EAC shall allow the timeout interval for the momentary floor button enable to be user-configurable.
13. The APC-300-EAC shall be capable of operating each access point (floor button) independently in the following modes:
 - Controlled Access* – access to the floor is controlled based on schedules and access group permissions
 - No Access* – no access to the floor is allowed.
 - Public* – floor button is enabled; anyone can enter and exit freely.

2.7 CARD READERS

A General

1. Reader shall function in access control system's normal or anti-passback mode without changes to the reader.
2. Reader shall be a sealed unit with no moving parts that connects to the APC-300 via a 5-conductor cable.

3. Standard Output Data Configuration: Wiegand protocol.
4. Status Indicator: Independently controlled tri-color LED and independently controlled audio tone.
5. Input Voltage: 4-16 VDC.
6. Operating Temperature Range: -30 to 150 degrees F (-35 to 65 degrees C).
7. Required Certifications: UL 294, FCC Part 15, I-ETS 300 330 and CE marked per directive 89/336/EEC.
8. Operating Requirements:
 - User status: LED flash and audio tone capability to advise user that a credential has been read and data transmitted to the controller.
9. Reader shall be capable of being wired up to 500 feet from the APC-300. Readers requiring special adapters to drive signal this distance are not acceptable.
10. Reader wiring cable shall be shielded and the shield shall be wired to ground at one end.

B Reader Types:

1. Type A mullion:
 - maximum size (HxWxT): 4.5x1.70x0.85 inches (114x43x21.5 mm).
 - mounting: metal door frames/mullions.
 - color: [White] [Beige] [Gray] [Black] [As selected by architect from manufacturer's standard color range; minimum 4 colors].
 - read range: up to 5 inches.
2. Type B wallswitch:
 - maximum size (HxWxT): 4.5x3.0x0.85 inches (114x76x21.5 mm).
 - mounting: metal or plastic single gang outlet box
 - color: [White] [Beige] [Gray] [Black] [As selected by architect from manufacturer's standard color range; minimum 4 colors].
 - read range: Up to 5 inches.
3. Type C midrange:
 - maximum Size (HxWxT): 5.1x6.1x1.1 inches (130x155x28 mm).
 - mounting: metal or plastic single or double gang outlet box.
 - color: [White] [Beige] [Gray] [Black] [As selected by architect from manufacturer's standard color range; minimum 4 colors].
 - read range: up to 12 inches.
4. Type D long range:
 - maximum size (HxWxT): 5.1x6.1x1.1 inches (130x155x28 mm).
 - mounting: As specified by manufacturer.
 - color: black.
 - read range: up to 28 inches.
5. Type E heavy duty PIN pad and proximity:
 - maximum size (HxWxT): 4.7x2.9x1.1 inches (119x74x28 mm).
 - mounting: Metal or plastic single gang outlet box.
 - color: [Beige] [Black] [As selected by architect from manufacturer's standard color range; minimum 2 colors].

C Performance Requirements

1. Proximity readers shall read user credentials without physical contact, process credential encoded data and output data to access system controller resulting in instructions to allow/deny access.
2. Credential shall be readable when presented in any orientation or at any angle to reader surface.
3. Reader data output time to controller: 110 milliseconds or less.
4. Transmission of radio frequency signals into the reader shall not compromise the system.
5. Presence of small metal objects, such as keys or coins, near the credential shall not alter the code nor prevent the code from being read.
6. Different types of credentials may be used interchangeably and shall be compatible with all readers in the system.

D Fabrication

1. Electronics Module: single piece weatherproof construction enclosed in epoxy potting.
2. Bezel: snap-on plastic cover (to conceal electronics module mounting screws) with locking screw or snap to restrict removal.

E Manufacturer

1. Qualifications: minimum 10 years experience in producing proximity access control readers and credentials.
2. Manufacturers:
Indala Corporation; 6850B Santa Teresa Blvd; San Jose, CA 95119; tel. (408) 361-4700; fax. (408) 361-4701

HID Global; 9292 Jeronimo Road, Irvine, CA 92618, tel (800) 237-7769

F Products

1. Warranty - lifetime
2. Delivery Storage and Handling – follow manufacturers instructions
3. Installation - – follow manufacturers instructions

2.8 CREDENTIALS – CARDS AND FOBS

A General

1. Passive operation: must be readable without use of battery.
2. Operating temperature range: -22 to 150 degrees F (-30 to 65 degrees)

B Credential Types

1. Type 1
LifeTime proximity card; credit card size plastic card with beveled edges.
Size: 3.38x2.12x0.065 inches (86x54x1.7 mm) maximum thickness.
Read Range: up to 12 inches (305 mm) depending on reader.
ID Marking: [None] [Encoded, offset or random numbers].
Coding: [Wiegand] [_____].
Slot Punch: [Vertical].
Graphics: [None] [Custom color printing using owner supplied artwork].

2. Type 2
Proximity key tag; molded plastic with slot to fit key ring, chain or ID lanyard.
Maximum size: 1.725x1.197x0.215 inches (43.8x30.4x5.46 mm).
Read Range: up to 6 inches (152 mm) depending on reader.
ID Marking: [None] [Encoded, offset or random numbers].
Coding: [Wiegand] [_____].
3. Type 3
Image-able proximity card; credit card size plastic card conforming to ISO 7813. Front face suitable for edge to edge dye sublimation printing.
Size: 3.38x2.12x0.033 inches (86x54x0.84 mm) thick.
Read Range: up to 12 inches (305 mm) depending on reader.
ID Marking: [None] [Encoded, offset or random numbers].
Coding: [Wiegand] [_____].
Slot Punch: [None] [Vertical] [Horizontal].
Finish: Front: [Glossy White] Back: [Glossy White]
Graphics: [None] [Front] [and] [back] [full custom color graphics using owner supplied artwork].
[Magnetic Stripe: Embedded 3-track high coercivity.]

C Manufacturer

1. Qualifications: minimum 10 years experience in producing proximity access control readers and credentials.
2. Manufacturers:
Indala Corporation; 6850B Santa Teresa Blvd; San Jose, CA 95119; tel. (408) 361-4700; fax. (408) 361-4701

HID Global; 9292 Jeronimo Road, Irvine, CA 92618, tel (800) 237-7769

D Products

1. Warranty (all types) - lifetime
2. Delivery Storage and Handling – follow manufacturers instructions

2.9 POWER SUPPLIES

- A The host computer shall operate using standard 120-volt AC, 50/60-Hz power. The connection to the main building power supply shall be performed in accordance with the general terms and conditions of this contract. An Uninterruptible Power Supply (UPS) shall be provided. It shall be sized to support the host computer, display, and attached peripherals in the event of a building power supply failure of up to 10 minutes.
- B The access point controllers shall operate using standard, unswitched 120-volt AC, 50/60-Hz power. The connection to the main building power supply shall be performed in accordance with the general terms and conditions of this contract.
 1. An in-line or plug-in Class 2 transformer rated at 24VAC at 50VA shall provide power.

2.10 REQUEST TO EXIT DEVICES

- A Request to Exit buttons shall be supplied at all reader-controlled doors that incorporate electromagnetic locks. When a request to exit button is not suitable, touch sense bars shall be used to release the electromagnetic locks.

2.11 ELECTRIC LOCKING DEVICES

- A Electric strikes shall be grade one, fire rated, <insert name of loc manufacturer here> models. These units shall be <insert fail-secure or fail-safe here>, operate at 12VDC and shall be capable of 100% duty cycle operation.
- B Electromagnetic locks shall be <insert name of loc manufacturer here> models . These units shall operate at 12VDC and be capable of 100% duty cycle operation.
- C A MOV (Metal Oxide Varistor) shall be wired across the electric locking device, within 18 inches of the device.

2.12 ELECTRICAL CONTROL, POWER AND LOW VOLTAGE WIRING

- A General
 1. Provide power wiring, conduit and connections for access controllers locking hardware, door sensors, request-to-exit devices and other devices controlled by this Section.
 2. Provide all other wiring required for the complete operation of the access control system.
 3. Install all wiring raceway systems complying with the requirements of the National Electrical Code. All installations shall be installed in Electrical Metallic Tubing (EMT).
- B LonWorks Network Communication Requirements
 1. Echelon has qualified a variety of cables for use with twisted-pair networks. Based on the cost, performance and availability of these different cable types, use the most appropriate cable for application.
 2. The network topology shall be doubly terminated bus topology with bus topology terminators attached at each end of each channel.
 3. Wired network communication shall be via channels consisting of a non-shielded 22 AWG twisted pair installed in a 3/4" EMT.
 4. In all communication conduits, provide one spare twisted pair to be installed, tagged and labeled at each end.
 5. Communication conduits shall not be installed closer than six feet from high power transformers or run parallel within six feet of electrical high power cables. Care shall be taken to route the cable as far from interference generating devices as possible.
 6. All shields shall be grounded (earth ground) at one point only, to eliminate ground loops.
 7. There shall be no power wiring, in excess of 30 VAC rms, run in conduit with communications wiring. In cases where signal wiring is run in conduit with communication wiring, all communication wiring and signal wiring shall be run using separate twisted shielded pairs (24awg) with the shields grounded in accordance with the manufacturer's wiring practices.
- C Input/Output Control Wiring

1. Binary control function wiring shall be a minimum of number 18 gauge.
2. Binary input wiring shall be a minimum of number 22 gauge.

D Splices

1. Splices in shielded cables shall consist of terminations and the use of shielded cable couplers, which maintain the integrity of the shielding. Terminations shall be in accessible locations. Cables shall be harnessed with cable ties as specified herein.

E Conduit and Fittings

1. Conduit for control wiring, control cable and transmission cable: EMT with compression fittings, cold rolled steel, zinc coated or zinc-coated rigid steel with threaded connections.
2. Outlet Boxes (dry location): Sheradized or galvanized drawn steel suited to each application, in general, four inches square or octagon with suitable raised cover.
3. Outlet Boxes (exposed to weather): Threaded hub cast aluminum or iron boxes with gasket device plate.
4. Pull and Junction Boxes: Size according to number, size, and position of entering raceway as required by National Electrical Codes. Enclosure type shall be suited to location.

3 PART 3 – EXECUTION

3.1 INSPECTION

- A Do not proceed with the work of this section until conditions detrimental to the proper and timely completion of the work have been corrected in an acceptable manner.
- B Card Readers
 - 1. Examine substrates upon which readers will be installed.
 - 2. Coordinate with responsible entity to perform corrective work on unsatisfactory substrates.
 - 3. Commencement of work by installer is acceptance of substrate.

3.2 PREPARATION

- A Coordinate and inform other trades of locations of all pieces of equipment to be installed under this section for proper functional interface with other equipment or hardware to avoid any interference or delay in the progress of the work.

3.3 INSTALLATION

- A System equipment and wiring installation shall be by the properly licensed company, either the original equipment manufacturer or the factory distributor for the brand of equipment used. Furnish wiring diagrams and wire runs for the raceway system installed by the licensed electrical contractor, under Division 16.
- B Card Readers
coordination is required between the different contractors working on a project to insure that the installation of the readers and associated wiring suit the building design as they are the most visible component. In all applications, follow the manufacturer's installation instructions. Install reader with centerline at 4'-0" above finished floor.
- C Electronic locking devices and request-to-exit devices
coordination is required between the different contractors working on a project to insure that the installation of the locking devices and request-to-exit devices suit the building. The associated wiring for these devices should be hidden and not visible to public view. In all applications, follow the manufacturer's installation instructions.
- D End-of-line resistors
if the request-to-exit and door sensor circuits are to be supervised by the access controller, resistors shall be installed as close to the end-of-line device as allowed by the installation. Refer to the installation guide of the access controller for resistor circuit specifications.
- E The APC-300s shall be enclosed in a metal cabinet with a door hinged on the side with key lock and installed on the secure side of the door.

3.4 SYSTEM TESTING AND CERTIFICATION

- A The access control system shall be tested in accordance with the following:
 - 1. The contractor shall conduct a complete inspection and test of all installed access control and security monitoring equipment. This includes testing

and verifying connection to equipment of other divisions, such as Life Safety and Elevators.

2. The Contractor shall provide staff to test all devices and all operational features of the system for witness by the owner's representative and the Authority Having Jurisdiction (AHJ). The contractor shall provide two way radio communications to assist in the testing. The owner's representative, prior to acceptance, must witness all testing.

B The testing and certification shall take place as follows:

1. System shall be tested in conjunction with the manufacturer's representative.
2. All deficiencies noted in the above test shall be corrected.
3. Test results shall be submitted to the consultant or owner's representative.
4. System test witnessed by owner's representative and correction of any deficiencies noted.
5. The owner's representative shall accept the system.
6. System test shall be witnessed by the AHJ. Any deficiencies noted shall be corrected.
7. A letter of certification shall be provided to indicate that the tests have been performed and all devices are operational.

3.5 TRAINING

- A A minimum one day course shall be conducted for system operators and owner.

END OF SECTION