ACCESS CONTROL SYSTEM

DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

28 10 00  Electronic Access Control and Intrusion Detection
28 13 00  Access Control

Notes to Specifier:

1. Where several alternative parameters or specifications exist, or where, the specifier has the option of inserting text, such choices are presented in <bold text>.

2. Explanatory notes and comments are presented in colored text.
ACCESS CONTROL SYSTEM

PART 1  GENERAL

1.01  SUMMARY

A. This Section includes an IP based security access control system (ACS) consisting of an ACS Host Workstation, supporting networked workstation(s), operating system and application software, and field-installed IP based Reader-Controllers connected by a high-speed electronic data transmission network. This system’s features include regulating access through controlled openings, credential management, monitoring of field devices, and reporting.

B. Related Requirements

1. 14 28 16 Elevator Controls
2. 28 16 33.16 Intrusion Detection Interfaces to Access Control Hardware
3. 28 16 43 Perimeter Security Systems

1.02  REFERENCES

A. Abbreviations and Acronyms

1. ACS Access Control System
2. AES Advanced Encryption Standard
3. I/O Input/Output
4. LAN Local Area Network
5. LED Light-Emitting Diode
6. PC Personal Computer
7. RFID Radio Frequency Identification
8. TCP/IP Transport Control Protocol/Internet Protocol
9. UPS Uninterruptible Power Supply
10. WAN Wide Area Network

B. Definitions

1. ACS Host Workstation - A PC with software designated as the main controlling PC of the security access system.
2. IP Based Reader-Controller - An intelligent network-connected reader controller unit with inputs, outputs and data storage capability.
3. Credential - RFID based token assigned to an entity and used to identify that entity.
4. Identifier - A credential card, keypad personal identification number or code, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.
5. Modbus TCP/IP - Industrial automation networking communication protocol for communications between devices connected to the same network.
6. PC (Personal Computer) An ACS Host Workstation or Server and any supporting workstations.
7. **RFID** - An automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.

8. **RS-232** - A TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines certain signal characteristics for interfacing computer equipment.

9. **Workstation** - A PC with software that is configured for specific limited security system functions.

### C. Reference Standards

1. **SIA BIO-01-1993.02(R2000.06)** - Biometric Standard - Vocabulary for Testing
2. Institute of Electronic and Electrical Engineers (IEEE) 802.3 standards
3. Underwriters Laboratories
   - a. UL 294 - Access Control System Units
   - b. UL 294B - Power Over Ethernet
4. **FCC 47, CFR Part 15**
6. **National Institute of Standards and Technology (NIST)**
   - a. FIPS 197 - Advanced Encryption Standard (AES)
7. **ISO 14443A, 14443B** - Proximity Cards
8. **EIA/TIA-569** - Commercial Building Standard for Telecommunications Pathways and Spaces
9. **ETSI EN300, EN330-2, EN301 489-1**

### 1.03 ACTION SUBMITTALS

A. **Product Data**

1. Manufacturers’ printed and electronic data sheets, including operating characteristics, furnished specialties, and accessories.
2. References for each product to a location on Drawings.
3. Test and evaluation data presented in compliance with SIA BIO-01
4. Manufacturers’ installation and operation manuals

B. **Shop Drawings**

1. Diagrams for cable management system.
2. System labeling schedules, including electronic copy of labeling schedules that are part of the cable and asset identification system of the software specified in Part 2.
3. **Wiring Diagrams.** Show typical wiring schematics including the following:
   - a. Workstation outlets, jacks, and jack assemblies.
   - b. Patch cords.
   - c. Patch panels.
   - d. Active network components.

C. **System installation planning documents**

### 1.04 CLOSEOUT SUBMITTALS
A. Field quality-control test reports
B. End User Training Plan
C. Operation and Maintenance Data
   1. Microsoft Windows software documentation.
   2. For each PC, installation and operating documentation, manuals, and software for the PC and all
      installed peripherals.
      a. Include system restore, emergency boot diskettes, and drivers for all installed hardware.
      b. The software manual shall describe the functions of all software and shall include all other
         information necessary to enable proper programming and operation. The manual shall fully
         explain all procedures and instructions for the operation of the system
D. List of recommended spare parts

1.05 QUALIFICATIONS
A. Manufacturer shall have a minimum of ten years of experience in manufacturing access control
   equipment.
B. Installers shall have been trained, certified, and approved by the Manufacturer.

1.06 WARRANTY
A. Manufacturer shall provide a limited one year hardware warranty for the product to be free of defects
   in material and workmanship.
B. Manufacturer shall provide software updates for a minimum of 365 days after commissioning.
C. Manufacturer shall make available an extended warranty and maintenance support option.

END OF SECTION
PART 2  PRODUCTS

2.01  EQUIPMENT

A. Manufacturer: ISONAS
   4750 Walnut Street
   Suite 110
   Boulder, Colorado 80301 USA
   Phone: +1 (303) 567-6516 | Fax: +1 (303) 567-6991
   Web: www.isonas.com
   E-mail: sales@isonas.com

B. Models:
   1. Software  DBCrystal, EasyWeb 2015
   2. Hardware  PowerNet Reader Controller; IPBridge

C. Alternates: None

2.02  DESCRIPTION

A. The system shall consist of system software, one networked Microsoft Windows based server and, optionally, one or more client workstations, true IP based Reader-Controllers and input/output modules connected by a high-speed electronic data transmission network. Systems utilizing door controllers that have been modified with an Ethernet connection are not acceptable.

B. The network connecting the ACS Host Workstation, Client Workstation(s), IP Bridge and IP based Reader-Controllers shall be a Local Area Network (LAN) or Wide Area Network (WAN) utilizing TCP/IP communications protocol and having the capacity of connecting an unlimited number of devices and workstations

C. Functions - The systems primary functions shall include:
   1. Regulating access through doors, gates, turnstiles, and other entrance portals
   2. Regulating access to medical cabinets, data cabinets, vehicles and other devices that is beneficial to control access and provide an electronic audit
   3. Tracking Zones and Mustering/Anti-Passback
   4. Credential cards and readers
   5. Credential creation and credential holder database and management
   6. Monitoring of field-installed devices
   7. Reporting

D. Third Party Devices - In addition to supporting the Manufacturer’s own proximity readers, the system shall support the following types of readers:
   1. Any device with a wiegand based output including, but not limited to, the following:
      a. Biometric readers from multiple manufacturers
b. Long range vehicle readers commonly used in parking garages, gated areas, etc.
c. Combination proximity reader and electric locking devices

2.03 SYSTEM SOFTWARE

A. The access control application software shall provide the interface between the ACS Host Workstation, IP Bridge, IP based Reader-Controllers, input/output modules in order to monitor sensors, report alarms, generate reports and provide all other system functions.

B. The system shall provide software modules for system administration, credentialing, ACS Host functions and creation of system reports.

C. The system software shall not be licensed by number of doors, card readers, card holder, client connections, etc. Licensed features such as web based administration, Microsoft Active Directory integration and Badge Printing are acceptable.

D. The system software shall have no recurring yearly software maintenance fees.

E. System Functions - The access control system software functions shall include the following:

1. Door Programming
   a. Extended open alarms
   b. Individual Extended open timers per door
   c. Personal Identification Number (PIN) Codes – Up to 9 digits
   e. Number of Door Groups - Unlimited

2. Shifts
   a. Number of shifts - Unlimited
   b. Interval assignments - Any day of the week

3. Permissions - Unlimited number

4. Holidays - Unlimited number

5. Door Control
   a. Door control based on dual-authentication rules.
      1) Support requiring credentials belonging to two people
      2) Support requiring two credentials belong to same person
   b. Cardholder use limits
      1) Elapsed Time based
      2) Number of usage based
   c. Configurable individual door strike times.
   d. Configurable extended individual door hold open times.

6. Elevator Control - provide elevator control for an unlimited number of floors.

7. System Graphical Tree - provide for graphical tree displays of the configured door hardware.

8. Alarm and Event Logging - provide for logging of all system alarms and events chronologically including time and date stamp. Specific alarm conditions monitored include:
   a. Door Unauthorized Open Alarm
   b. Door Extended Open Alarm
   c. Reader-Controller Tamper Alarm
d. Data link interruption Alarm

9. System Scheduling - provide for scheduling of events including:
   a. Open Door, Open Door Group
   b. Deactivate Badges

10. Help Documentation – provide access to documentation online

11. Alarm and Monitoring Attributes - provide for programming of the following:
   a. Display of alarm events at the ACS Host workstation, or support networked workstation
   b. Require the reader-controller, which generated the alarm to be restored to its normal state before the alarm is cleared
   c. Require acknowledgment of an alarm to clear the alarm
   d. Support auto-clearing of network related communication alarms
   e. Trigger a programmed system actions(s) when the alarm is initiated or cleared.
   f. Restriction of alarm acknowledgment to authorized personnel only

12. Programming Downloads - provide for downloading of programming from the ACS Host to the Reader-controller-controllers as follows:
   a. Credential holders and authorized time zones
   b. Time zones.
   c. Latch intervals.
   d. TTL output on REX, Tamper, Unauthorized.
   e. Beep on events (REX, Tamper, Reject)
   f. Complete database download of 10,000 cardholder records in less than 15 minutes with system continuing to operate normally during this time.

13. Reader-controller Programming Options
   a. Request to exit and door position switch - Provide programming for flexible processing of the request to exit and door position switch
   b. Manual activation of outputs - Provide for configurable activation of outputs from a credential presentation
   c. User definable door strike time - Provide user definable/programmable door strike functionality for each reader-controller
   d. In/ out Reader-controller configuration - Reader-controller programmed as either an in reader, an out reader, or a toggle reader for recording of time in and time out data
   e. Input/output linking - Provide programming for linking of reader outputs with inputs

F. ACS Host Software Functions - The system ACS Host software shall provide for the following features and functions:
   1. Multi-user multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations
   2. Device Status Monitoring
      a. Alarm Status Indication - Provide real time status display that indicates the current status of all devices in the device tree
      b. Reader-controller status - Provide display of Reader-controllers that are off line
   3. Device Group Programming
      a. Reader-controller Groups - Provide for programming of Reader-controller groups
b. Input Groups - Provide for programming of input groups

c. Output Groups - Provide for programming of output groups

4. Historical Trace - provide for historical trace on any reader-controller or cardholder

5. Test Utilities - Provide system test utilities to allow for testing of the following functions:
   a. Alarm inputs status.
   b. Output operations.
   c. Credential Presentations.
   d. LED and buzzer operations
   e. Content Verification of Reader-Control's internal database

6. The graphical user interface shall show pull-down menus and a menu tree format that complies with interface best-practices of Microsoft Windows operating system.
   a. Real-Time Graphical Maps - provide graphical maps that display reader-controller status and allow for manual operation of the reader-controller
   b. Map Device Icons - Icons shall dynamically change to reflect the current state of the devices
   c. Map Formats - Support import of maps to include the following file formats:
      1) JPEG (.jpg)
      2) Static Graphics Interchange Format (.gif)
      3) Windows Bitmap (.bmp)

7. Database Management
   a. The database shall be Microsoft SQL Server.

G. ACS Web Based Administration – The system shall provide a web based client utilizing Microsoft Internet Information Services (IIS).
   1. The web interface shall be one single license and provide unlimited concurrent users.
   2. The web based interface shall be browser agnostic and be useable by any Apple or Android based device.
   3. Must provide an easy to use interface for day-to-day end user administration of the ACS.
   4. Must provide simplified step based tasks for end user administrators.
   5. Shall provide at a minimum the following functionality –
      a. Add People, Credentials and provide them Rules to access doors during a defined schedule through a single window
      b. Provide the ability to Admit access, Unlock, Lock or Lockdown a single door, group of doors or all doors in the system via the system dashboard
      c. Provide the ability to run History reports
      d. Provide the ability to configure Badge Unlock and Auto Unlock rules for a single door or group of doors
      e. Provide the ability to configure user logins and restrict the roles that login can perform within the web interface
      f. Provide the ability to initiate any number of Scripts within the system

H. Credential Management Software Functions - The system credential management software shall provide for the following features and functions:
   1. Modification of cardholder records - Add, Modify and Delete records based upon user logon permissions.
   2. Access and Credential Management
a. Provide for the following credential management functions:
   1) Assignment of single or unlimited number of active badges to an individual.
   2) Programming personnel groups
   3) Programming of group access permissions
   4) Programming the scheduled activation and deactivation of group access permissions
   5) Programming of individual access permissions
b. Microsoft Active Directory Integration
   1) Optionally support receiving adds/changes/deletes of personnel information from Microsoft’s Active Directory, and update the associated entries in the system databases.
c. Program Use Limits - Limiting the number of times that cardholders may use their credential to gain access

3. Badge Design - Provide badge design software that is integrated to the access control database with the following badge layout tools:
   1) Complete Badge design and Layout
   2) Badge Generation

4. ID Printers - Provide support for industry standard printers and Microsoft Certified Windows 2008r2 and above, Windows 7 and above printer drivers and the following badge print formats:
   1) Double-sided full color printing
   2) Edge to edge printing

I. Operating System
   1. The system software shall be based on Microsoft Windows Server 2008r2 and above, Windows 7 32 or 64 bit and above.
   2. The system shall support virtualization through Microsoft Hyper-V or VMware.

2.04 HARDWARE COMPONENTS
A. Server/Client Workstation
   1. Recommended hardware requirements
      a. Processor type and speed – Intel i5 or greater.
      b. System memory requirements – 8GB RAM
      c. Minimum hard drive space – 500GB Hard Drive 7200rpm
      d. Network card - Ethernet 10/100 Base-T
      e. Minimum monitor resolution - 1024 x 768 pixels
      f. Monitor card - SVGA video card with minimum 256Mb memory.
      g. Keyboard and mouse - USB keyboard and optical scroll mouse
   2. The ACS Host Workstation shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring.

B. Field Devices
   1. Functionality
      a. Field equipment shall include IP based Reader-Controllers, IP Bridges. Modbus/TCP I/O Modules.
b. Data exchange between the ACS Host Workstation and the IP based Reader-Controllers shall include down-line transmission of commands, software, and databases to IP based Reader-Controllers.

c. The up-line data exchange from the IP based Reader-Controller to the ACS Host Workstation shall include status data such as status reports, and entry-control records.

2. IP Bridge - The system shall have available an IP Bridge module to interface existing analog or IP access control equipment to the access control system specified herein over the IP network.

a. The IP Bridge shall have the capacity to interface to up to three (3) doors.

1) The IP Bridge shall have two (2) RJ-45 network connections, allowing daisy-chaining of multiple bridges.

---

**Note:** Consult factory for power considerations when interconnecting multiple IP Bridges. 12VDC is recommended for IP Bridges beyond the first.

---

b. The IP Bridge shall eliminate the need for a stand-alone door controller.

c. The IP Bridge shall have the ability to be configured and accessed by the ACS Host software.

1) Information shall be exchanged on an asynchronous interrupt basis without the need for polling by the ACS Host software.

2) IP Bridge microcode updates shall be provided over the network, when necessary.

d. The IP Bridge shall support AES encryption.

e. The IP Bridge shall have the ability to function autonomously in a Local mode to reduce network traffic and system load.

f. The IP Bridge shall support the following inputs (per door):

1) Three (3) configurable sensor inputs

2) Wiegand card reader connection up to 500 feet

---

**Note:** The three sensor inputs are typically used for door sense (normally closed), request for exit (REX, normally open) and an optional input for flexibility (AUX, normally open).

---

g. The IP Bridge shall support the following outputs (per door):

1) Door Control relay (for electric lock, rated 2.0 A @ 30 VDC, form C)

2) Wiegand interface

a) Power - 10 VDC regulated, regardless of input power to IP Bridge

b) LED control

c) buzzer control

3) Two (2) TTL outputs with (configurable default state)

4) Auxiliary 12 VDC power

---

**Note:** The POE+ version of its IPBridge product supports 19 watts (1.6 A @ 12 VDC) power output.
h. The IP Bridge shall have the capability to be powered by IEEE 802.3af POE, IEEE 802.3at POE+, or by 12 or 24 VDC

i. User
   1) Indicators
      a) Power
      b) Network Status
      c) Door Status (one indicator per door)
   2) Programming - Microcode flash upgradable
   3) Dual-mode reset button - Power-cycle IPBridge and Reset-to-Factory defaults

j. Physical and Environmental
   1) Operating Temperature - -40° to +50° C
   2) Humidity - 0 - 90%, non-condensing
   3) Enclosure
      a) PC/ABS Flame-retardant per UL94 V-0
      b) Form Factor - DIN Rail Mounting
      c) Dimensions – 6.3” x3.6” x 2.3”

3. Reader-Controller - The reader-controller shall have the following properties:
   a. Credentials
      1) Proximity Model
         a) Card Formats Read - Proprietary RFID and HID Proximity
         b) Operating Frequency - 125 KHz (FSK modulation)
         c) Proximity Read Time - <250msec
         d) Read range - 2 - 5 inches
      2) Multi-Technology Card Model
         a) Card Formats Read - MiFare, PIV, iClass
         b) Operating Frequency - 13.56 MHz (ISO 14443A & 14443B)

Note: The features of the ISONAS multi-technology card model are In addition to the proximity model's capabilities.

b. Stand-alone Capability
   1) 64,000 cardholders
   2) 5000 access events
   3) 32 time zones per cardholder

c. Input/output
   1) Inputs - Three configurable (Default usage - door sense, request for exit, auxiliary)
   2) Outputs
      a) Two TTL outputs (configurable default state)
      b) One form-C relay output (2.0 A @ 30VDC)
      c) Control (4) four fail-secure cabinets with optional module.

d. Communications Interface
   1) Ethernet, TCP/IP via RJ-45 connector.
   2) Non-polled asynchronous messaging.
### Communication mode configurable between Network-Client and Network-Server.

### RS-232 interface for connection of serial devices such as key pads.

### Wiegand data via an external Wiegand adaptor

### Security

1. Optical tamper
2. Encrypted lock control with optional module

### Electrical

1. Power - POE, 12VDC, 24VDC
2. Operating Current - <125mA peak
3. Auxiliary Power Output - 0.6A @12VDC

### User

1. LED Indicators (2) - reader status, network connection
2. Programming - Microcode flash upgradeable
3. Dual-mode reset button - Power-cycle reader and Reset-to-Factory defaults

### Stand–Alone Capability

1. 20,000 cardholders
2. 5,000 access events
3. 32 time zones

### Physical and Environmental

1. Operating Temperature - -40º to +50º C
2. Humidity - 0 - 100%
3. Weather Resistance - Potted components for weather resistance

### Certifications

a) UL-294
b) FCC 47 CFR Part 15
c) RSS-210
d) ETSI EN 300, EN 330-2, EN 301 489-1

5. Enclosure

a) Durable U/V stabilized, flame-retardant ABS
b) Form Factor - Mullion mount
c) Dimensions - 1.625” x 6.750” x .940”

### 2.05 SYSTEM PERFORMANCE

**A.** The system shall use a single database for access-control and credential-creation functions.

**B.** Distributed Processing - The system shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to the IP based Reader/Controllers so that each IP based Reader-Controller can make access-control decisions for that location. If communications to ACS Host Workstation is lost, all IP based Reader-Controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall automatically be uploaded to the ACS Host Workstation

**C.** System Capacity
1. Number of Locations - Unlimited, using a single PC with LAN/WAN TCP/IP connections
2. Reader-controlled doors - Unlimited
3. Total access credentials - Unlimited
4. Alarm inputs - Unlimited
5. Programmable outputs - Unlimited

D. System Response to Alarms
1. Reader-Controllers network shall provide a system end-to-end response time of 3 second or less for every device connected to the system.
2. Alarms shall be annunciated at the ACS Host Workstation within 3 second of the alarm occurring at a IP based Reader-Controller or device controlled by a local IP based Reader-Controller, and within 1 second if the alarm occurs at the ACS Host Workstation.
3. Alarm and status changes shall be displayed within 1 second after receipt of data by the ACS Host Workstation.
4. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within 15 seconds of alarm receipt at the security console.

E. Network
1. The TCP/IP network interconnecting the system components shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
2. Network communication issues shall not require operator initiation or response, and the network shall return to normal after partial or total network interruption such as power loss or transient upset.
3. Data Line Supervision - The system shall monitor the status of the data transmission lines with the use of heartbeat messages. The loss of the heartbeat messages will cause an alarm condition within the ACS host, and the reader-controller to switch to standalone mode.

F. Environmental - The system shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:
1. Interior, Controlled Environment - System components, except computer workstation units, installed in air-conditioned temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of 2 to 50 deg C dry bulb and 0 to 90 percent relative humidity, non-condensing.
2. Interior, Uncontrolled Environment - System components installed in non-air-conditioned non-temperature-controlled interior environments shall be rated for continuous operation in ambient conditions of minus 20 to plus 50 degrees C) dry bulb and 0 to 100 percent relative humidity, non-condensing.
3. Exterior Environment - System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of minus 40 to plus 120 degrees F minus 40 to plus 50 degrees C dry bulb and 0 to 100 percent relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 85 mph (137 km/h) and snow cover up to 24 inches (610 mm) thick.
PART 3 EXECUTION

3.01 DELIVERY, STORAGE, AND HANDLING

A. ACS Host Workstation and Supporting Workstations:
   1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 degrees F (10 and 30 degrees C), and not more than 80 percent relative humidity, non-condensing.
   2. Open each container; verify contents against packing list, and file copy of packing list, complete with container identification for inclusion in operation and maintenance data.
   3. Mark packing list with designations that have been assigned to materials and equipment.

B. IP Bridges and IP-based Reader-Controllers:
   1. Store in temperature and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between -40 and 120 degrees F (-40 and 50 degrees C).
   2. Open each container; verify contents against packing list, and file copy of packing list, complete with container identification for inclusion in operation and maintenance data.
   3. Mark packing list with designations that have been assigned to materials and equipment.

3.02 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, IP based Reader-Controllers, Reader-controllers, non-IP readers, doors, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.03 PREPARATION

A. Comply with recommendations in SIA CP-01.

B. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

C. Develop Project planning forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.
   1. Record setup data for control station and workstations.
   2. For each Location, record setup of IP based Reader-Controller features and access requirements.
   3. Propose start and stop times for shifts and holidays, and match up permissions for doors.
   4. Set up groups, and list inputs and outputs for each IP based Reader-Controller.
5. Prepare and install alarm graphic maps.
6. Discuss badge layout options; design badges.
7. Complete system diagnostics and operation verification.
8. Prepare a specific plan for system testing, startup, and demonstration.
9. Develop acceptance test concept and, on approval, develop specifics of the test.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

3.04 INSTALLATION
A. Install all equipment in accordance with the manufacturer’s installation manuals, wiring diagrams and recommendations.
B. Install, configure and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner

3.05 FIELD QUALITY CONTROL
A. Contractor shall engage a factory-authorized and trained service representative to inspect, test, and adjust components and equipment installation.
1. Results shall be reported in writing.
B. Contractor shall perform the following field tests and inspections and prepare test reports:
   1. LAN Cable Procedures - Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
   2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
   3. Operational Test - After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.
C. Contractor shall remove and replace malfunctioning devices and circuits and retest as specified above.

3.06 STARTUP SERVICE
A. Contractor shall engage a factory-authorized and trained service representative to supervise and assist with system startup service.
1. Representative shall complete installation and startup checks according to approved procedures that were developed in Section 3.03 and with manufacturer's written instructions.

B. Contractor shall engage a factory-authorized and trained service representative to train Owner's maintenance personnel to adjust, operate, and maintain security access system.

1. Representative shall develop separate training modules for the following:
   a. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software
   b. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel
   c. Security personnel
   d. Hardware maintenance personnel
   e. Corporate management

The Specifier may wish to use the following language here or elsewhere in the project specification:

CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Contracting."
B. Install cables and wiring according to requirements in Division 28 Section "Conductors and Cables for Electronic Safety and Security."
C. Wiring Method: Install wiring in raceway except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.
D. Wiring Method: Install LAN cables using techniques, practices, and methods that are consistent with Category 5 rating of components and that ensure Category 5 performance of completed and linked signal paths, end to end.
E. Install cables without damaging conductors, shield, or jacket.
F. Boxes and enclosures containing security system components or cabling, and which are easily accessible to employees or to the public, shall be provided with a lock. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

CABLE APPLICATION

A. Comply with EIA/TIA-569, "Commercial Building Standard for Telecommunications Pathways and Spaces."
B. Cable application and requirements shall be compliant with manufacturer's recommendations.

GROUNDING
A. Comply with Division 26 Section "Grounding and Bonding for Electrical Systems."
B. Comply with IEEE 1100, "Power and Grounding Sensitive Electronic Equipment."
C. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.
D. Bond shields and drain conductors to ground at only one point in each circuit.

IDENTIFICATION
A. In addition to requirements in this Article, comply with applicable requirements in Division 26 Section "Identification for Electrical Systems" and with TIA/EIA-606.
B. Label each terminal strip and screw terminal in each cabinet, rack, or panel.
   1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.
   2. Each wire connected to building-mounted devices shall be numbered at the device and shall be consistent with the associated wire connected and numbered within the panel or cabinet.