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 either a ACS Host Server or Cloud Host Service, client workstations utilizing any supported web browser and field-installed IP based Reader-Controllers and/or IPBridges 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.	ISAM	Indexed Sequential Access Method
5.	LAN	Local area network.
6.	LED	Light-emitting diode
7.	PC	Personal Computer
8.	RFID	Radio Frequency Identification
9.	TCP/IP	Transport Control Protocol/Internet Protocol
10.	UPS	Uninterruptible power supply.
11.	WAN	Wide area network

B. Definitions

1. ACS Cloud Service – A cloud based service hosted and maintained by the Manufacturer for administrating and communicating to Reader Controllers and IPBridges.
2. ACS Host Server - A Windows Server with software designated for providing a web based interface to administrate and communicate to Reader Controllers and IPBridges.
3. ACS Host – Either the Cloud Service or Host Server listed above.
4. IP based Reader-Controller - An intelligent network-connected reader controller unit with inputs, outputs and data storage capability.
5. IPBridge – An intelligent interface to legacy based access control systems using traditional structured cabling and proximity readers.
6. Access Point – Any Reader Controller or port on an IPBridge connected to the ACS Host.
7. Credential - RFID based token assigned to an entity and used to identify that entity.
8. Mobile Credential – Token using Bluetooth® Low Energy on any Android or Apple device

9. 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.
10. RFID - An automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders.
11. Client - Any device with a supported web browser that can connect to either the Cloud Service or Host Server.

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
5. Industry Canada - Radio Standards Specification RSS-210 Licence-exempt Radio Apparatus
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

3. System installation and setup guides.

D. List of recommended spare parts

1.05 QUALIFICATIONS

A. Manufacturer shall have a minimum of ten year’s 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 cloud service as they are available and will be automatically granted. On premise software updates are available through a software upgrade program.

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 Either Pure Access™ Cloud or Pure Access™ Manager
2. Hardware Pure IP Reader Controller and/or Powernet IPBridge

C. Alternates: None

2.02 DESCRIPTION

A. The system shall consist of a ACS Host; either Cloud Service or a local Server Host, one or more client workstations, IP based Reader-Controllers and/or IPBridges connected by a high-speed electronic data transmission network.

1. The Cloud Service shall be host on Amazon Web Services and provide for a minimum of 99.95% uptime. The Manufacturer shall closely monitor all conditions related to the Cloud Service infrastructure.

B. The network connecting the ACS Host, 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. Credential cards and readers
3. Credential creation and credential holder database and management
4. Monitoring of field-installed devices
5. Reporting

D. Third Party Devices - In addition to supporting the Manufacturer's own multi-card readers, the system shall support the following types of readers:

1. Wiegand output devices including but not limited to:
   a. Biometric devices
   b. Long Range Readers such as Tagmaster
   c. Barcode scanners

2.03 SYSTEM SOFTWARE

A. The ACS Host application software shall provide the interface between the Client, IPBridges, IP based Reader-Controllers, report alarms, generate reports and provide all other system functions.

B. The system shall provide a web based User Interface using standard browsers such as Chrome, Firefox and Microsoft Edge. Mobile devices such as tablets and smart phones will be able to log in via the same such browsers and have a User Interface optimized for mobile experience.

C. The system software license shall be licensed as follows:

1. ACS Cloud Service

a. Shall provide for an unlimited number of Access Points depending on the license utilized

b. Shall provide for an unlimited number of concurrent users with no additional licensing.

c. Shall be licensed by the number of Access Points in common increments up to two hundred-fifty (250), two hundred and fifty-one (251+) and over shall be unlimited.

1) When using a license for over fifty-one (51) Access Points the system shall include Microsoft Active Directory integration at no cost.

d. Shall be an annual fee paid to maintain the Cloud Service and provide regular updates.

2. ACS Host Server

a. Shall provide the same User Interface as the Cloud for ease of use.

b. Shall provide for an unlimited number of Access Points with no additional licensing.

c. Shall provide for an unlimited number of concurrent Clients with no additional licensing.

d. Shall provide Microsoft Active Directory integration with no additional licensing.

e. Shall have a Software Upgrade Plan to cover updates the software platform.

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

1. User/Credential Management

a. Shall provide for an unlimited number of Users and Credentials with no additional licensing.

b. Shall provide an unlimited number of User Groups.

c. Users configuration shall have the following attributes:

1) First name, middle initial and last name.

2) User Image

3) Alert email address for the User to receive Alert emails

4) Ten (10) customizable User Defined Fields

5) Web Access with customizable User Roles to define what the User can view and edit in the Client. Passwords for Web Access shall be forced to use strong passwords.

6) Unlimited number of credentials using either a Badge, PIN or Mobile credential

7) Can reside in an unlimited number of User Groups.

8) Can be associated with Custom Rules

d. When deactivating a User, the system shall deactivate all associated credentials with that User. Any credential can be deactivated without deactivating the associated User.

e. Microsoft Active Directory Integration

1) System shall allow for the integration to Microsoft Active Directory unless it is utilizing a Cloud Service license of under fifty (50) Access points. This Integration will synchronize Users from Active Directory to the ACS Host. The ACS Host will poll the Active Directory server regularly for changes and synchronize those changes to its database.

2. Access Point Programming and Management
   a. Provide an easy to use wizard to add Access points to the software. Shall include the ability for a technician to use an Android or Apple mobile device to enroll devices by scanning the MAC address of the Access Point.
   b. Wizard shall include a full test of all Access Point components
   c. Configurable door latch interval
   d. Input enable/disable and configuration
   e. Number of Access Point Groups - Unlimited
3. Weekly Schedules
   a. Number of Weekly Schedules - Unlimited
   b. Interval assignments - Any day of the week with optional Holiday Over Ride
4. Weekly Rules - Unlimited number
5. Holidays - Unlimited number
6. Alarm and Event Logging - provide for logging of all system alarms and events chronologically including time and date stamp. Specific alarm conditions monitored shall be included but not limited to:
   a. Door Unauthorized Open Alarm
   b. Door Extended Open Alarm
   c. Reader-Controller Tamper Alarm
   d. Device Offline Alert
7. System Scheduling - provide for scheduling of events including:
   a. Access Point or Access Point Group unlock for specified Schedule.
   b. Access Point or Access Point Group unlock with specified Badge(s), Access Point(s) shall remain locked until an authorized Credential is read.
8. System Dashboards – Monitoring Attributes
   a. Shall provide unlimited customizable Dashboards for Monitoring of the ACS. Each dashboard shall contain four (4) customizable widgets. These Dashboards shall be fully customizable, able to filter on all events, able to filter on all devices where applicable and include the following:
      1) Ability to display single Access Point status with the following:
         a) Live update of door status including physical door status and all event history
         b) Ability to Admit entry for the latch interval time
         c) Ability to Lock, Unlock and Lockdown the Access Point
         d) Display User images if available
      2) Ability to display multiple Access Points, up to twelve (12) in a single widget with the following:
         a) Live update of door status
         b) Ability to Admit entry for the latch interval time
         c) Ability to Lock, Unlock and Lockdown the Access Point
      3) Ability to display History in the system filtered to be filtered by Users, Groups and/or Access Points.
      4) Ability to add a single Admit widget for an Access Point to admit entry for the latch interval.

5) Ability to add a Lockdown widget to Lockdown a single Access Point, a Group of Access Points or All Access Points.
6) Ability to show User profiles for a single Access Point or multiple Access Points. The User Profile shall show the event and Users image if applicable.

b. Dashboards shall be able to be restricted by User Groups and/or Areas.

c. Dashboards shall also include an unlimited number of Floor Plans to be created and displayed in the system. Floor Plans shall show the status of all doors displayed on the Floor Plan at creation. Floor Plans shall allow for a User to Admit, Unlock or Lockdown a single Access Point or multiple Access Points shown on the Floor Plan.

9. System Alerts – Alarm Attributes

a. System shall provide a dedicated page for monitoring of Alerts in the system. These alerts shall notify the User of the number of Alerts in the system and can easily configure email and/or SMS alerts to notify Users.

b. Alerts shall queue in the system until they are Acknowledged and Cleared. Notes can be added to individual reports.

c. Alerts shall be able to be Disabled or set to Auto-Clear from the queue.

d. The types of Alerts available shall be:

1) Unauthorized Open
2) Extended Open
3) Tamper
4) AUX
5) REX
6) Credential Rejected
7) Credential Expired
8) Credential Over Limit

10. Reports

a. System shall provide both customizable ad hoc reporting and scheduled reports that can be emailed on a daily or weekly basis.

b. Reports shall be able to be saved as standard PDF or CSV files.

c. Reports shall be able to be filtered by all attributes within the report.

d. The following reports should be included at a minimum:

1) History
2) Users
3) Access Points
4) Schedules
5) Holidays
6) Attendance
7) Permissions

11. Custom Rules Engine

a. System shall provide a flexible Custom Rules Engine to trigger unique actions from various events in the system. The Engine shall allow for the use of multiple triggers in the system to configure these events. System triggers shall include but not be limited to:

1) A User’s Credential is Accepted or Rejected
2) An Access Point has a specific Alert or any Alert
3) The Access Point has disconnected
4) During or not during a configured Schedule
5) At an Access Point or Access Point Group

b. System Actions shall include but not be limited to:
   1) Email a User or User Group
   2) Lockdown an Access Point or Access Point Group
   3) Create an Alert in the system
   4) Unlock an Access Point or Access Point Group
   5) Disable a Credential

E. ACS Host Server - Operating System (If Applicable)

1. The system software shall be based on Microsoft Windows Server 2012r2 or 2016.

2. The system shall support running in a Virtual Environment.

2.04 HARDWARE COMPONENTS

A. ACS Local Host Server (If Applicable)

1. Minimum hardware requirements
   a. Processor type and speed – Intel i5 or greater
   b. System memory requirements – 8GB RAM minimum
   c. Minimum hard drive space – 500GB
   d. Network card - Ethernet 10/100 Base-T Minimum
   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 Client 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 and IPBridges.
   b. Data exchange between the ACS Host 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 shall include status data such as status reports, and entry-control records.

2. IP Bridge - The system shall have available an IPBridge 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 connection of up to thirty-two (32) IPBridges to a single network switch port.

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 with a capacity of:
      1) 64,000 cardholders
      2) 5000 access events
      3) 32 time zones per cardholder

   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 Stand-Alone mode to reduce network traffic and system load.

f. The IP Bridge shall support the following inputs (per access point):
1) Three (3) configurable sensor inputs for door sense, request to exit and auxiliary.
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 access point):
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) beeper control
3) Two (2) TTL outputs
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 upgradeable
3) Dual-mode reset button - Power-cycle IPBridge and Reset-to-Factory defaults

j. Physical and Environmental
1) Operating Temperature - -40º to +50º 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) Bluetooth Low Energy
c) Operating Frequency - 125 KHz (FSK modulation)
d) Proximity Read Time - <250msec
e) Read range - 2 - 5 inches

2) Multi-Technology Card Model
a) Card Formats Read - MiFare, PIV, iClass
b) Bluetooth Low Energy
c) Operating Frequency - 13.5 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 - Two configurable (Default usage - door sense, request for exit/auxiliary)
2) Outputs
a) One solid state relay controlling the electric lock rated at 12vdc 600ma.

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

e. Security
1) Tamper detection via accelerometer
2) Encrypted lock control with optional module

f. Electrical
1) Power – PoE and 12vdc
2) Operating Current - <150mA peak
3) Auxiliary Power Output – 12vdc @ 600ma

g. 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

h. Physical and Environmental
1) Operating Temperature - -40º to +50º C
2) Humidity - 0 - 100%
3) Weather Resistance – Conformal Coated components for weather resistance
4) Certifications
a) UL-294 Compliant
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 – Wall mount and mullion mount
c) Dimensions –
   i. Mullion (5.1" x 1.7" x 0.71")
   ii. Wall mount (5.1" x 3.25" x 0.17")

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.

C. System Capacity

1. Number of Locations - Unlimited (dependent on license)
2. Access Points - Unlimited (dependent on license)
3. Total access credentials - 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 with typical network latency.
2. Alarms shall be annunciated at the ACS Host 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 with typical network latency.
3. Alarm and status changes shall be displayed within 1 second after receipt of data by the ACS Host with typical network latency.
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 with typical network latency.

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 deg 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 deg F minus 40 to plus 50 deg 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.

END OF SECTION

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 deg F (10 and 30 deg 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 deg F (-40 and 50 deg 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 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.

END OF SECTION