MILLENNIUM
SECURE YOUR WORLD

MILLENNIUM
SECURE YOUR WORLD

Millennium Xtra
A&E Specifications

Millennium Xtra A&E Specifications

SECTION 28 13 50

ELECTRONIC ACCESS CONTROL SYSTEM

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

PART 1 - GENERAL

1.01 SECTION INCLUDES

A. Electronic access control system.

1.02 RELATED SECTIONS

Specifier Notes: Edit the following list as required for the project. List other sections with work directly related to the electronic access control system.

A. 08 71 00 - Door Hardware.

B. 08 74 00 - Door Schedule.

C. 28 13 40 - Basic Material And Methods

1.03 REFERENCES

Specifier Notes: List standards referenced in this section, complete with designations and titles. This article does not require compliance with standards, but is merely a listing of those used.

1.04 REFERENCES

A. Americans with Disabilities Act (ADA)

B. Crime Prevention Through Environmental Design (CPTED)

C. NFPA 70: National Electric Code (NEC)

D. NFPA 101: Life Safety Code

E. NFPA 730: Guide for Premises Security

F. NFPA 731: Standard for the Installation of Electronic Premises Security

G. BICSI's Electronic Safety and Security Design Reference Manual (ESSDRM)

H. Underwriter's Laboratories (UL) Applicable Standards

I. NECA 1: Standard Practice of Good Workmanship in Electrical Contracting

J. Electronic Industries Alliance (EIA) Applicable Standards

K. Telecommunications Industry Association (TIA) Applicable Standards

L. Institute of Electrical and Electronics Engineers (IEEE) Applicable Standards

Specifier Notes: The following list of definitions is to be used when specifying "Millennium Enterprise" On-Line Electronic Access Control System. Delete this list if "Millennium Enterprise" is not specified.

1.05 DEFINITIONS USED WITH ON-LINE ELECTRONIC ACCESS CONTROL SYSTEM

A. Access Level: A list of access points and the time zone that users will be allowed access.

B. Access Reader: Provides control of the access point by interfacing a card, electronic key, chip, or keypad with the system.

C. Alarm Monitoring: Provides the system a status of the alarm devices.

D. Distributed Architecture: Describes the operation of the system that allows the system to function with its normal routines without communications to the computers.

E. Door Controller: Provides the system the interface of the reader and alarm inputs along with the relay outputs and communicates the information to the computer.

F. Elevator Controller: Restricts user access to the floors by user access group.

G. Operator Log-On: Computer operator that has been granted access to the system software by a user ID and password.

H. Relay Control: Provides control of devices by time zones or linking events by the software.

I. Controller: Provides the interface of 100 DCD's (Door Control Device) and 10 RCD's (Relay Control Device) with the computer.

J. Site Ethernet Interface: Provides TCP/IP connectivity via an Ethernet network with any number of control units.

K. Time Period: Start and end period along with days of the week that can be used to control user access, automatic unlocking access points, alarms inputs, reports, and relay operations.

L. Cardholder: Holder of a card, biometric, or keypad ID.

1.06 SYSTEM DESCRIPTION

Specifier Notes: Prepare a system description for the specified electronic access control system components as required for the specific application.

A.

1.07 SUBMITTALS

A. Comply with Section 01 33 00 - Submittal Procedures.

B. Product Data: Submit manufacturer's product data, including installation instructions.

C. Operating and Maintenance Instructions: Submit manufacturer's operating and maintenance instructions.

D. Warranty: Submit manufacturer's standard warranty.

1.08 QUALITY ASSURANCE

A. Manufacturer Qualifications:

Specifier Notes: Edit or delete the following manufacturer qualifications as required for the project.

1. Responsible for all components.
2. Continuously engaged in electronic access control system construction with a minimum of 15 years successful experience.
3. Able to demonstrate successful performance on comparable projects.
4. Responsible for system design, including:
   a. Preparation of engineering and production documentation.
   b. Development of testing program and interpretation of test results.
5. Design and Manufacturing Process: ISO 9001 certified.

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

6. Capability of providing manufacturer-employed field service personnel for installation assistance as required.
7. Capability of providing 24-hour, 7 days per week technical service assistance through a toll free telephone number after acceptance of work by the Owner.
8. Capability of providing manufacturer-employed field service personnel for technical service and maintenance after acceptance of work by the Owner.

B. Installer Qualifications:

1. Trained in installation by manufacturer.
2. Approved by manufacturer.

Specifier Notes: Describe requirements for a meeting to coordinate the installation of the electronic access control system and to sequence related work. Delete this paragraph if not required.

C. Pre-installation Meeting: Convene a pre-installation meeting [2] [_____] weeks before start of installation of electronic access control system. Require attendance of parties directly affecting work of this section, including Contractor, Architect, installer, and manufacturer's representative. Review installation, field quality control, adjusting, demonstration, and coordination with other work.

1.09 DELIVERY, STORAGE, AND HANDLING

A. Delivery: Deliver materials to site in manufacturer's original, unopened containers and packaging, with labels clearly identifying product name and manufacturer.

B. Storage: Store materials indoors, in a clean, dry area in accordance with manufacturer's instructions.

C. Handling: Protect materials and finishes during handling and installation to prevent damage.

PART 2 - PRODUCTS

2.01 MANUFACTURER

Specifier Notes: The following address is for technical and sales information - commercial on-line. Delete if not required.

Millennium Group, Inc.
16 Tech Circle
Natick, MA 01760
Phone: (866) 455-5222
Fax: (508) 651-2902
Web Site: www.millennium-groupinc.com.

Specifier Notes: Consult Millennium Group for assistance in specifying the required electronic access control system components for the specific application.

2.02 ON-LINE ELECTRONIC ACCESS CONTROL SYSTEM – MILLENNIUM XTRA

Specifier Notes: Consult Millennium Group for assistance in editing this article for the specific application.

A. On-Line Electronic Access Control System: Millennium Xtra.

1. System shall have capability to perform:
   a. Access control.
   b. Alarm monitoring.
   c. Programmable relay control.
   d. View events in real time.
   e. Print selected events in real time.
   f. Elevator control.
   g. Support Microsoft SQL Server

B. Computer System Characteristics:

1. An off-the-shelf stand-alone computer or readily available server.
2. Processor: 2.8 GHz or faster, 64 bit
3. RAM: 8 GB minimum.
4. Upgrades: System hardware shall allow computer upgrades without replacement of system hardware.
5. Communication: TCP/IP
6. Hard Drive: 120GB for storage of events that have occurred on system.
7. CD/DVD-ROM/RW.
8. Printer: Support any Windows installed printer for reports.
9. Operating System: Windows 7, 8, 8.1, Server , VMWare or MS Hyper-V

C. Software:

1. Server: 64 bit
2. Client: Web Browser based, have extensive context sensitive on-line help, and provide familiar icon-driven, tabbed dialog menu options. Supports all common browsers including Internet Explorer, Edge, Firefox, Chrome, and Safari.
3. Client require operator logon to function.

D. Database:

1. Supplied with full support of Microsoft SQL 2000 –2012 database server application to allow archiving of history, database repair functions, and import/export.
2. Support near-real-time import and export of data.
3. Support automatic update of user access rights as a result of the import process.
4. Allow for a unique industry standard ISO card number to be generated on demand as part of import process.
5. Provide a partition feature; allows specific system entities in the database to be seen and manipulated only by certain "Partition". Such entities can be cardholders, operators, sites and elevator floors. When the database is divided into spheres of control in this way, operators in a given partition will control data such as sites, doors, cardholders for their own partition(s) only. The database itself is complete, but views are generated such that what the operator can view, add, modify, delete or print reports, is limited by the Partition(s) to which they have rights to as well as by Operator level.

E. Operators:

1. Limits system operation by different operator levels.

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

2. Assign individual operator passwords for logging on.
3. Custom configured operator levels. Operators may have rights to view, add, change, delete, or execute program features
4. Provide an automatic operator logoff delay.

F. Software Functions and Options:

1. Software to provide support for the following:
   a. Unlimited number of users.
   b. Each Site Control Unit: 100 access readers, 10 Relay Output boards
   c. Up to 1,000 site controllers.
   d. Number of Partitions: Unlimited.
   e. Number of Access Levels: Unlimited (30 per card).
2. Multiple door hardware support (Millennium DCD, Salto remote locks, Mercury Controllers)
3. Support multiple access reader technologies and protocol on same system simultaneously.
4. Support simultaneously 2 custom ABA formats and 2 Wiegand formats for access readers.
5. Support combination access readers with one Wiegand output. Support custom Wiegand outputs from 0 to 50bits, including 32 bits, 37 bits, HID Corporate 1000 program, and Motorola 27 bits.
6. Support Suprema fingerprint readers
7. Support user pin number along with a card that is enabled by a time period.
8. Support a door pin number that is enabled by a time period.
9. Able to accept any facility code of card provided. (0 to 31bit facility code)
10. Not allow duplication of Employment ID.
11. Option to rename fields on the cardholder page.
12. Allow up to three cards to be programmed per cardholder.
13. Support “disable card” function for each access card.
14. Support anti-passback modes
15. Support a door control device address and text description name in a field minimum of 19 characters..
16. Support 2 relays included with each door control device.
17. Support unlocking a strike/magnetic lock automatically in accordance with a programmable time period.
18. Support unlocking a strike/magnetic lock device at a defined time, but only after first valid user accesses access reader.
19. Notify when status of a door or relay controller changes because of a communication or device problem.
20. Support programmable reports viewed on monitor or printed.
21. Provide capability of sorting history events by time, dates, cardholders, access readers, and operators.
22. Ability to preprogram dates for Daylight Savings Time.
23. Support relays that can be programmed to operate by a time period, alarms, or by events linked to access points.
24. Have the Owner’s name encrypted and displayed on monitor.
25. Capability to automatically archive transaction data and be able to select dates of data being archived.
26. Provide communication to sites using TCP/IP.
27. Advise and display on computer monitor status of door and relay controller(s) if

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

communication or power is lost on system.

G. Software Optional Functions

1. Support system lockdown on programmable Threat Levels.
2. Support system lockdown by pre-programming access point (device) groups. Support linking any system alarm point or action with lockdown function.
3. Support system Toggle function allowing first valid card to unlock and hold unlock. The next valid card will lock the door. This function can be set to follow a schedule.
4. CCTV Integrated Software Module Option:
   a. The CCTV module supports an Exacq VMS.
   b. Allows display the appropriate CCTV camera in response to an alarm.
5. Suprema Fingerprint reader interface
6. Salto wireless reader integration
7. Support operation of Mercury Access Control panels
8. Suppport integration with DMP alarm panels

H. Alarm Monitoring Software:

1. Support a minimum of 7 supervised alarm inputs per door control unit with time period disable feature, and a programmable shunt delay timer from 0 to 255 seconds.
2. Supervision of alarm points can be either two (Alarm, Reset) or three state (Alarm, Trouble, Reset) determined at software configuration.
3. Provide a forced-door entry alarm and a door ajar alarm. Forced-door alarm shall have a shunt delay timer of 0 to 255 seconds. Ajar alarm shall have a programmable delay timer of 1 to 255 minutes.
4. Support adding comments to the alarm/events.
5. Support prioritizing of alarms to 100 levels.
6. Support linking specific alarms to relay control devices.
7. Require acknowledgment text so personnel monitoring alarms shall provide response information.
8. Include an alarm monitor application separate which shall display alarms graphically in the priority with which they were programmed. Application shall be able to be run from any Windows based computer. Allow Alarm acknowledgment from any computer with synchronization between operators.
9. Provide alarm monitor with capability to display a user portrait in response to valid or invalid access attempts.

I. Scheduler; integrated software:

1. Fully configurable integrated module allowing scheduled actions for any access points of the system, overriding the normal door unlock/lock set up
2. Unlimited number of schedules supported
3. Configurable actions;
   a. Unlock – Lock
   b. Shunt alarms

J. System Hardware:

1. System components to include Site Controllers, Door Controllers, Power Supplies, optional Relay controllers, optional Elevator Controllers,

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

2. System shall be able to be configured from 1 to 100 access readers for each site control unit.
3. Controllers shall store basic parameters, including real-time clock, for a minimum of 24 hours, in case of AC loss of power and battery backup is exhausted.
4. System shall use a fully-distributed architecture in which system alarms, access, relays, and elevator control shall continue to function in a normal mode without computer communications.
5. Site controller shall be able to communicate to computer via TCP/IP, either on-board or with an optional interface.
6. Site controller shall have a local relay to monitor status of communications with door control units. In case of device failure relay will open, providing a means of triggering an external monitoring device.
7. Site, door, relay, and elevator controller features shall have capability to be field upgraded by a firmware change. Such firmware upgrades shall be offered as needed to registered users on an exchange basis.
8. Door controller shall support any Wiegand standard based readers in any bit format up to 50 total; bit patterns fully programmable within software.
9. Supported reader types to include but are not limited to: Wiegand, Mag stripe, Bar Code, Proximity, Keypad, Biometrics, combination keypad with Wiegand/Proximity/Magnetic stripe.
10. Door control Unit shall be able to be programmed for custom ABA formats from the software, including ability to ignore user specified characters in format.
11. Door control Unit shall be programmable to accept either normal or inverted strobe signals from ABA format readers.
12. Door control Unit shall be programmed for appropriate access reader technologies.
13. Site controller shall buffer the last 2,000 events from door controllers when computer communications has been lost or terminated.
14. Each door control Unit shall buffer an additional 2,000 events when site controller buffer has filled.
15. All system control Units shall have a built-in tamper alarm to detect when a cover to the controller is removed.
16. Door Control Unit shall include:
    a. Request to Exit input.
    b. Single reader input .
    c. Function at full capacity without communications to computer, and buffer events up to a maximum of 2,000 during this period.
    d. Continue to function on battery backup at a minimum of 9 V DC.
17. Door and relay control Unit shall have Form C dry contact configuration.
18. Door and relay control Unit shall have relays with a minimum current rating of 24 V DC at 2 A with solid-state automatically resettable overcurrent protection for contacts.
19. Door control Unit shall have a relay that can be programmed by software for: Valid User, Auto Activate, First User Auto Activate, Any User, Rejected User, Dual Custody (2 valid token to be presented within 5 sec), or Alarm Options.
20. Relay control Unit shall have relays that can be configured by software for Time Zone Activation, Timed Activation, Timed Released, First Event Activation, and First Event Released and Last Person Out.
21. Relay on door controller shall have a programmable timer and settings in software for strike

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

and magnetic lock operation.

22. Site controller to door control Unit communication shall conform to EIA RS-485 with a recommended total cable length of 5,000 feet (1,524 m).
23. Power Supply:
    a. Battery backup capable of providing power for system during temporary AC power outage.
    b. Provide an output to notify system when there is a loss of AC power.

K. System Access Readers:

1. Wiegand Output Format Readers: Output of 26-bit Wiegand format or a custom bit configuration from 13 to 50 with configurable facility codes
2. Example supported reader types include but are not limited to: Proximity, Mag Stripe, Bar Code, Wiegand, Keypad, Biometrics, combination keypad with Wiegand/Proximity/Magnetic stripe.
3. ABA Format Readers: ABA, ABA inverted.

L. Door Control Device (DCD):

1. Description:
    a. Designed to control a single access point.
    b. Contains a real-time clock and sufficient memory to provide access control independent of main PC.
    c. Transaction history shall be automatically buffered when not on line with PC.
    d. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full.
2. Power: 9 to 14 V DC, supplied by central power supply; 80 to 110 mA, depending upon reader technology. 225 mA additional required during unlock of Marlok rotating cylinder (7 seconds maximum). Accessory relays require additional 20 mA each.
3. Power Protection: Reverse polarity, over voltage, transient.
4. Reader Technologies Supported: Wiegand card (any bit format up to 50), ABA/ISO Track 2, proximity, keypad, combination reader/keypad, biometrics.
5. Reader Interfaces Supported: clock/data, clock/data inverted, Wiegand.
6. History Buffer: 2,000 transactions.
7. Priority Event Buffer: 100 transactions.
8. On-Board Memory and Clock Backup: 24 hours minimum.
9. Maximum Users Stored in Memory: either 10,000 or 60,000, depending on hardware.
10. Alarm Input Points: 7 total, 2-wire supervised, 2 or four state selectable (EOL resistor) including built-in door contact monitoring.
11. Alarm Input Monitoring Circuit: Analog to digital conversion.
12. Tamper Alarm: On-board switch.
13. Output Relays: 2 each with Form C contacts rated 2 A, 30 V.
14. Output Relay Contact Protection: Solid-state polymeric resettable.
15. Connectors: 5 mm plug-on screw terminal.
16. Address Switches: Rotary, direct-reading 00 to 99.
17. Communications: Multi-drop RS-485, proprietary protocol.
18. Operating Environment:
    a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
    b. Less than 90 percent noncondensing humidity.

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

19. Support T-TAP, Daisy Chained or in a Star Topology connectivity

M. Site Control Unit (SCU):

1. Description:
   a. Designed to control a maximum of 100 door controllers and a maximum of 10 relay controllers.
   b. Normally used for a single site or building, contains a real-time clock and sufficient memory to supervise site.
   c. Maximum of 1,000 site controllers can be addressed in a system.
   d. Transaction history is automatically buffered when not on line with PC.
   e. Priority event buffer assures alarms are annunciated in a timely manner even if history buffer is full.
   f. On-board switches select operational modes.
2. Power: 9 to 14 V DC, supplied by central power supply; 50 mA standby, 90 mA maximum.
3. Power Protection: Reverse polarity, over voltage, transient.
4. PC to SCU Communications Interface: RS-232, RS-485 4-wire, or TCP/IP.
5. SCU to DCD Communications Interface: RS-485 multi-drop 2-wire.
6. Supervisory Relay: Rated 2 A, 30 V Form C. Opens on-site fault.
7. History Buffer: 2,000 transactions.
8. Priority Event Buffer: 100 transactions.
9. On-Board Memory and Clock Backup: 24 hours minimum.
10. Alarms: Lost AC input.
11. Tamper Alarm: On-board switch.
12. Connectors: 5 mm screw terminal.
13. Address Switches: Rotary, direct-reading 000 to 999.
14. Operating Environment:
   a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
   b. Less than 90 percent noncondensing humidity.
15. Support T-TAP, Daisy Chained or in a Star Topology connectivity

N. Relay Control Device (RCD):

1. Power: 9 to 14 V DC, supplied by central power supply; 35 mA standby current, 20 mA additional for each relay activated.
2. Memory and Clock Backup: 24 hours minimum.
3. Relay Outputs: 7 Form C contacts, rated 30 V DC maximum at 2 A.
4. Supervisory Function: Relay 0 on first board installed. Opens on system fault.
5. Communications: Multi-drop RS-485, proprietary protocol.
6. Tamper Alarm: On-board switch.
7. Configuration Jumpers: J3, relay polarity select all 16 relays; J5, relay override select.
8. Address Switch: Rotary, direct-reading 0 to 9.
9. Operating Environment:
   a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
   b. Less than 90 percent noncondensing humidity.

O. Power Supply:

1. Power: [120 V AC, 60 Hz, 2 A, unswitched] [240 V AC, 50 Hz, 1 A, unswitched (export)].
2. Fuses: 2 A AC input slow-blow, 1 A AC input (export), 8 A (battery output protection).

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

3. Output: 13.8 V DC nominal, 5 A maximum.
4. Battery Backup: 2 gelled lead acid cell, 6 V DC, 8.0 Ah, supplied with power supply.
5. Alarm Outputs: Cover tamper switch and AC or power supply failure (dry contacts).

P. Elevator Control Unit (ECU):

1. Description:
   a. Designed to provide access control for a maximum of 16 floors.
   b. Each site controller can support a maximum of 4 Elevator Control Units, giving a maximum of 64 floors per Site Controller.
   c. Each group of elevator control units supports a maximum of 10 elevator readers.
2. Power: [120 V AC, 60 Hz, 1 A, unswitched] [220 V AC, 50 Hz, 1 A, unswitched (export)].
3. Power Supply Output: 5 V DC, 1 A, for local circuit board only.
4. Memory and Clock Backup: 24 hours minimum
5. Relay Outputs: 16 Form C.
6. Contact Ratings: 5 A, 30 V DC; 10 A, 125 V AC; 6 A, 277 V AC.
7. Normal Mode: Energized.
8. Override Input: Normally closed.
9. Unit Address: 4 position dip.
10. Alarm Inputs: 4 unsupervised.
11. Tamper: Built-in switch with activation spring.

Q. Elevator Control Device (ECD):

1. Description:
   a. Designed to mount inside an elevator car.
   b. Contains reader and communications circuitry to interface with elevator control unit.
   c. Maximum of 10 elevator control devices can be used for each site controller.
2. Power: 9 to 14 V DC, supplied by power cube (local) or central power supply; 80 to 110 mA depending upon reader technology.
3. Power Protection: Reverse polarity, over voltage, transient.
4. Reader Technologies Supported: Wiegand card (any bit format up to 50), ABA/ISO track 2, proximity, keypad, biometrics.
5. Reader Interfaces Supported: clock/data, clock/data inverted, Wiegand.
6. Connectors: 5 mm plug-on screw terminal.
7. Address Switches: Rotary, direct-reading 0 to 9.
8. Communications: Multi-drop RS-485, proprietary protocol.
9. Operating Environment:
   a. Between 14 degrees F and 104 degrees F (-10 degrees C and 40 degrees C).
   b. Less than 90 percent noncondensing humidity.

R. Site Ethernet Interface (SEI):

1. Description: Designed to provide communications between Millennium Windows PC and site control unit(s) by means of Ethernet networks utilizing TCP/IP protocol.
2. Power: 12 to 15 V DC, supplied by either central power supply or auxiliary power supply; 800 mA maximum.
3. IP Address Setting: Software through RS-232 port.
4. Data Backup: Nonvolatile memory.
5. Network Interface: 10 base T, AUI.

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

6. SCU Interface: RS-232-C, 9,600 baud.
7. Communications Protocol (Network): TCP/IP.
8. Communications Protocol (SCU Interface): Proprietary.
9. Operating Environment:
   a. Between 32 degrees F and 104 degrees F (0 degrees C and 40 degrees C).
   b. Less than 90 percent noncondensing humidity.

PART 3 EXECUTION

3.01 EXAMINATION

A. Examine areas to receive electronic access control system. Notify Architect if areas are not acceptable. Do not begin installation until unacceptable conditions have been corrected.

3.02 INSTALLATION

A. Install electronic access control system in accordance with manufacturer's instructions.

B. Install system at locations as indicated on the [drawings] [Electronic Access Control System Schedule].

C. Install door hardware as specified in Section 08710.

D. Install electrical wiring to on-line system components as specified in Section 16100.

E. Use manufacturer’s supplied hardware.

F. Replace defective or damaged components as directed by the Architect.

G. Furnish to the Owner all required keys and keycards.

3.03 FIELD QUALITY CONTROL

A. Test completed installation to verify each component of electronic access control system is properly installed and operating.

3.04 ADJUSTING

A. Adjust electronic access control system as required to perform properly.

B. Adjust locksets for smooth operation without binding.

3.05 CLEANING

A. Clean surfaces in accordance with manufacturer's instructions.

B. Use cleaners approved by manufacturer, as some cleaners may damage keylok/keyreaders.

C. Do not use abrasive cleaners.

Specifier Notes: The following is optional. Delete if not required.

3.06 DEMONSTRATION

A. Provide a maximum of 2 consecutive days of on-site service by manufacturer.
   1. Demonstrate system to Owner’s personnel.

16 Tech Circle | Natick, MA 01760 | www.millennium-groupinc.com | t 866.455.5222 | f 508.651.2902

2. Train Owner's personnel in proper operation and maintenance.

16 Tech Circle | Natick, MA 01760
P 866.455.5222 | F 508.651.2902
www.millennium-groupinc.com